Hacking Para Leigos, Tradução da 3ª Edição

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 3ª 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)

Hacking PARA LEIGOS®

Tradução da 3ª Edição

por Kevin Beaver

Prefácio de Stuart McClure

ALTA BOOKS
EDITORA
Rio de Janeiro, 2014

Sumário Resumido

Prefácio xxi

Introdução 1

Parte I: Construindo a Base para o Hackeamento Ético 7

Capítulo 1: Introdução ao Hackeamento Ético 9
Capítulo 2: Decifrando o Pensamento Hacker 25
Capítulo 3: Desenvolvendo o Seu Projeto para um Hackeamento Ético 35
Capítulo 4: Metodologia do Hackeamento 45

Parte II: Colocando o Hackeamento Ético em Movimento 59

Capítulo 5: Engenharia Social 61
Capítulo 6: Segurança Física 77
Capítulo 7: Senhas 87

Parte III: Hackeando a Rede 117

Capítulo 8: Infraestrutura de Rede 119
Capítulo 9: Redes Locais sem Fios (Wireless LANs) 153

Parte IV: Hackeando Sistemas Operacionais 181

Capítulo 10: Windows 183
Capítulo 11: Linux 209
Capítulo 12: Novell NetWare 231

Parte V: Hackeando Aplicaticos 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 Hackeamento 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

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 3ª 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 defenda-se, 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 3ª 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 3ª Edição, é um guia de referência sobre hackear seus sistemas para melhorar a segurança. Técnicas de hackeamento 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 hackeamento para testar seus sistemas até como corrigir as falhas e gerir um avançado programa de hackeamento 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 3ª 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 "hackearem" 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.