Guia Para Iniciantes Em Hacking de Computadores

Como Hackear Redes Sem Fio, Segurança Básica e Testes De Penetração, Kali Linux, Seu Primeiro Hack

ALAN T. NORMAN

Tradutor: Duda Junqueira Machado

Aviso de Isenção de Responsabilidade:

Por favor, observe que as informações contidas neste documento são apenas para fins educacionais e de entretenimento. Foram feitas todas as tentativas para fornecer informações completas, precisas, atualizadas e confiáveis. Nenhuma garantia de qualquer tipo é expressa ou implícita.

Ao ler este documento, o leitor concorda que, sob nenhuma circunstância, o autor é responsável por quaisquer perdas, diretas ou indiretas, incorridas como resultado da emissão de informações contidas neste documento, incluindo, mas não se limitando a erros, omissões , ou imprecisões.

Isenção de Responsabilidade
Requisitos para Criar seu próprio Keylogger
Capítulo 11. Configurando o Ambiente
Capítulo 12. Configurando o ambiente Eclipse
Etapas Para Configurar o Ambiente para Codificação:
Capítulo 13. Noções Básicas de Programação (Curso Relâmpago em C ++)
Termos
Noções Básicas Sobre Instruções de Código
Capítulo 14. Um Programa Típico
Loops:
Capítulo 15. Ponteiros e Arquivos
Pointers:
Arquivos:
Capítulo 16. Keylogger Básico
Capítulo 17. Letras Maiúsculas e Minúsculas
Capítulo 18. Abrangendo outros caracteres
Capítulo 19. Ocultar a janela do console do Keylogger
Conclusão
Livro de bônus: Baleias Bitcoin
Outros Livros de Alan T. Norman

Por Que Você Deve Ler Este Livro?

Como qualquer outro avanço tecnológico na história humana, os benefícios obtidos pela humanidade através da informatização e digitalização do nosso mundo têm um preço. Quanto mais informações podemos armazenar e transmitir, mais elas se tornam vulneráveis a roubo ou destruição. Quanto mais dependentes nossas vidas se tornam da tecnologia e da comunicação rápida e instantânea, maiores são as consequências de perder o acesso a esses recursos. Não é apenas possível, mas, na verdade, uma rotina, a transferência de bilhões de dólares para o exterior em um piscar de olhos. Bibliotecas inteiras podem ser armazenadas em dispositivos não maiores que um polegar humano. É comum ver crianças jogando jogos bastante comuns em smartphones ou tablets que têm mais poder de computação do que máquinas que, há apenas 50 anos, teriam preenchido salas inteiras.

Esta concentração sem precedentes de dados e riqueza digital, aliada à crescente dependência da sociedade dos meios digitais de armazenamento e comunicação, tem sido uma vantagem para oportunistas inteligentes e mal-intencionados, ansiosos por aproveitar todas as vulnerabilidades. De indivíduos que cometem pequenos furtos e fraudes, a ativistas políticos, grandes quadrilhas criminais, altamente organizadas, grupos terroristas e membros de estados-nações, o hacking de computadores se tornou uma indústria global multi-bilionária - não apenas na prática dos próprios crimes, mas devido ao tempo, esforço e capital dedicados à proteção de informações e recursos. É impossível exagerar as implicações da segurança digital em nossos dias atuais. A infraestrutura crítica de cidades e nações inteiras está inextricavelmente ligada às redes de computadores. Registros de transações financeiras diárias são armazenados digitalmente, cujo roubo ou exclusão poderia causar estragos em economias inteiras. Comunicações sensíveis por e-mail podem influenciar eleições

políticas ou processos judiciais quando divulgadas ao público. Talvez a mais preocupante de todas as vulnerabilidades em potencial esteja na esfera militar, onde instrumentos de guerra se encontram cada vez mais mantidos em rede e informatizados, e devem ser mantidos fora das mãos erradas a todo custo. Estas ameaças de alto nível são acompanhadas por efeitos menores, porém cumulativos, de transgressões em menor escala, como roubo de identidade e vazamento de informações pessoais, com consequências devastadoras para a vida das pessoas comuns.

Nem todos os hackers têm necessariamente intenção maliciosa. Em nações com liberdade de expressão prejudicada ou leis opressivas, os hackers servem para espalhar informações vitais entre a população, que normalmente poderia ser suprimida ou higienizada por um regime autoritário. Embora sua atividade ainda seja ilegal pelas leis de seu próprio país, muitos são considerados como servindo a um propósito moral. As linhas éticas são, portanto, frequentemente confusas, quando se trata de hackear com o objetivo de ativismo político ou de disseminar informações que possam ser de valor para o público ou para populações oprimidas. Para limitar os danos que podem ser causados por indivíduos e grupos com intenções menos que honrosas, é necessário acompanhar as ferramentas, procedimentos e mentalidades dos hackers. Os hackers de computador são altamente inteligentes, engenhosos, adaptáveis e extremamente persistentes. Os melhores entre eles sempre estiveram e, provavelmente, continuarão estando um passo à frente dos esforços para frustrá-los. Assim, os especialistas em segurança de computadores se esforçam para tornarem-se tão hábeis e experimentados na arte de invadir quanto seus adversários criminais. No processo de obtenção deste conhecimento, espera-se que o "hacker ético" se comprometa a não usar suas habilidades adquiridas para fins ilegais ou imorais.

Este livro pretende servir como uma introdução à linguagem, ambiente, ferramentas e procedimentos do hacking de

computador. Como guia para iniciantes, ele pressupõe que o leitor tenha pouco conhecimento prévio sobre hackers em computadores, além do que foi exposto na mídia ou em conversas casuais. Ele assume a familiaridade de um leigo geral com a terminologia moderna do computador e a Internet. Instruções detalhadas e procedimentos específicos de hacking estão fora do escopo deste livro, e são deixados para o leitor prosseguir, quanto mais ele ficar confortável com o material.

O livro começa em *Capítulo 1: O que é hacking?* com algumas definições básicas para que o leitor possa se familiarizar com parte da linguagem e jargão usados nos domínios de hackers e segurança de computadores, além de esclarecer quaisquer ambiguidades na terminologia. O capítulo 1 também distingue os diferentes tipos de hackers em relação às suas intenções éticas e legais, e às ramificações de suas atividades.

Em *Capítulo 2: Vulnerabilidades e Explorações,* é introduzido o conceito central de vulnerabilidade de destino, descrevendo as principais categorias de vulnerabilidade e alguns exemplos específicos. Isto leva a uma discussão sobre como os hackers tiram proveito das vulnerabilidades através da prática da exploração.

Capítulo 3: Introdução percorre as muitas disciplinas e habilidades com as quais um hacker iniciante precisa se familiarizar. Do hardware do computador e da rede, aos protocolos de comunicação e às linguagens de programação de computadores, são descritas as principais áreas tópicas da base de conhecimento de um hacker.

Capítulo 4: O Kit de Ferramentas do Hacker investiga as linguagens de programação, sistemas operacionais, hardwares e softwares mais comumente preferidos pelos hackers em geral para exercer suas atividades.

Os procedimentos gerais para alguns ataques comuns a

computadores são pesquisados em *Capítulo 5: Ganhando Acesso,* fornecendo alguns exemplos selecionados de ataques que, geralmente, são de interesse de hackers e profissionais de segurança de computadores.

Capítulo 6: Atividade e Código Maliciosos revela alguns dos ataques e construções mais nefastos de hackers que pretendem causar danos. As diferenças entre as variadas categorias de código malicioso são explicadas.

Capítulo 7: Hacking sem Fio concentra-se, especificamente, na exploração de vulnerabilidades nos protocolos de criptografia de rede Wi-Fi. As ferramentas específicas de hardware e software necessárias para executar ataques simples a Wi-Fi estão listadas.

O leitor recebe algumas orientações práticas sobre como configurar e praticar alguns hackings no nível iniciante em *Capítulo 8: Seu Primeiro Hack.* Dois exercícios são selecionados para ajudar o aspirante a hacker a dar os primeiros passos com algumas ferramentas simples e equipamentos baratos.

Capítulo9: Segurança Defensiva e Ética dos Hackers encerra esta introdução ao hacking com algumas notas sobre como se proteger dos hackers, e discute alguns dos problemas filosóficos associados à ética dos hackers.

Capítulo 1. O Que é Hacking?

É importante estabelecer as bases para uma introdução adequada ao hacking de computador, discutindo primeiro alguns termos comumente usados e esclarecendo quaisquer ambiguidades com relação a seus significados. Profissionais de informática e entusiastas sérios tendem a usar muito jargão, que evoluiu ao longo dos anos no que, tradicionalmente, era uma camarilha muito fechada e exclusiva. Nem sempre é claro o que certos termos significam, sem uma compreensão do contexto em que eles se desenvolveram. Embora, de modo algum, seja um léxico completo, este capítulo apresenta parte da linguagem básica usada entre hackers e profissionais de segurança de computadores. Outros termos aparecerão em capítulos posteriores, nos tópicos apropriados. Nenhuma destas definições é, de forma alguma, "oficial", mas representa um entendimento de seu uso comum.

Este capítulo também tenta esclarecer o que é hackear como atividade, o que não é e quem são hackers. Representações e discussões sobre hackers na cultura popular podem tender a pintar uma imagem excessivamente simplista dos hackers e da atividade de hacking como um todo. De fato, um entendimento preciso é perdido na tradução de chavões e conceitos populares .

Hackers e Hacking

A palavra ***hacking*** , normalmente, evoca imagens de um ciber-criminoso solitário, curvado sobre um computador e transferindo dinheiro à vontade de um banco desavisado, ou baixando, com facilidade, documentos confidenciais de um banco de dados do governo. No inglês moderno, o termo hacking pode assumir vários significados diferentes, dependendo do contexto. Como uma questão de uso geral, a palavra normalmente se refere ao ato de explorar

vulnerabilidades de segurança de computadores para obter acesso

não autorizado a um sistema. No entanto, com o surgimento da ciber-segurança como uma grande indústria, o hacking por computador não é mais uma atividade exclusivamente criminosa e, geralmente, é realizado por profissionais certificados que foram especificamente solicitados a avaliar as vulnerabilidades de um sistema de computador (consulte a próxima seção sobre "white hat", "black hat" e "gray hat" hacking) testando vários métodos de penetração. Além disso, o hacking para fins de segurança nacional também se tornou uma atividade sancionada (reconhecida ou não) por muitos estados-nação. Portanto, um entendimento mais amplo do termo deve reconhecer que o hacking, geralmente, é autorizado, mesmo que o invasor em questão esteja subvertendo o processo normal de acesso ao sistema.

Um uso ainda mais amplo da palavra hacking envolve a modificação, o uso não convencional ou o acesso subversivo a qualquer objeto, processo ou parte da tecnologia - não apenas computadores ou redes. Por exemplo, nos primeiros dias da subcultura de hackers, era uma atividade popular "hackear" telefones públicos ou máquinas de venda automática, para ter acesso a eles sem o uso de dinheiro - e compartilhar as instruções de como fazê-lo com a comunidade de hackers em geral. O simples ato de colocar objetos domésticos normalmente descartados para usos novos e inovadores (usar latas de refrigerante vazias como porta-lápis etc.) é frequentemente chamado de hacking. Mesmo certos processos e atalhos úteis para a vida cotidiana, como usar listas de tarefas ou encontrar maneiras criativas de economizar dinheiro em produtos e serviços, são frequentemente chamados de hackings (geralmente chamados de "hackings de vida"). Também é comum encontrar o termo "hacker" em referência a qualquer pessoa que seja especialmente talentosa ou experiente no uso de computadores.

Este livro se concentrará no conceito de hacking que se preocupa, especificamente, com a atividade de obter acesso a software,

sistemas de computadores ou redes por meios não intencionais. Isso inclui desde as formas mais simples de engenharia social usadas para determinar senhas até o uso de hardware e software sofisticados para penetração avançada. O termo ***hacker*** será usado para se referir a qualquer indivíduo, autorizado ou não, que esteja tentando acessar clandestinamente um sistema ou rede de computadores, sem levar em consideração suas intenções éticas. O termo ***cracker*** também é comumente usado no lugar de hacker - especificamente em referência àqueles que estão tentando quebrar senhas, ignorar restrições de software ou burlar a segurança do computador.

Os "Chapéus (Hats)" do Hacking

As cenas clássicas do velho oeste americano de Hollywood mostravam, geralmente, pistoleiros adversários de uma forma quase cartunesca - geralmente, um xerife ou federal contra um bandido covarde ou um bando de malfeitores. Era comum distinguir os "mocinhos" dos "bandidos" pela cor de seus chapéus de cowboy. O protagonista corajoso e puro usava, geralmente, um chapéu branco, enquanto o vilão usava um chapéu de cor escura ou preta. Estas imagens foram transferidas para outros aspectos da cultura ao longo dos anos e, eventualmente, chegaram ao jargão da segurança de computadores.

Chapéu Preto (Black Hat)

Um hacker (ou cracker) do tipo ***chapéu preto/black hat*** é aquele que tenta, sem ambiguidade, subverter a segurança de um sistema de computador (ou código de software de código fechado) ou rede de informações

conscientemente, contra a vontade de seu dono. O objetivo do hacker black hat é obter acesso não autorizado ao sistema, para obter ou destruir informações, causar uma interrupção na operação, negar acesso a usuários legítimos ou assumir o controle do sistema para seus próprios fins. Alguns hackers tomarão ou


image
not
available


image
not
available


image
not
available


image
not
available


image
not
available


image
not
available


image
not
available