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

Alan T. Norman

Guia Para Iniciantes Em Hacking De Computadores

«Tektime S.r.l.s.»

Norman A.

Guia Para Iniciantes Em Hacking De Computadores / A. Norman — «Tektime S.r.l.s.»,

Este livro ensinará como você pode se proteger dos ataques mais comuns de hackers, sabendo como os hackings realmente funcionam! Afinal, para evitar que seu sistema seja comprometido, você precisa ficar um passo à frente de qualquer hacker criminoso. Você pode fazer isso aprendendo como hackear e como fazer um contra-hack. Este livro ensinará como você pode se proteger dos ataques mais comuns de hackers, sabendo como os hackings realmente funcionam! Afinal, para evitar que seu sistema seja comprometido, você precisa ficar um passo à frente de qualquer hacker criminoso. Você pode fazer isso aprendendo como hackear e como fazer um contra-hack. Neste livro, existem técnicas e ferramentas usadas por hackers tanto criminais quanto éticos - tudo o que você encontrará aqui mostrará como a segurança das informações pode ser comprometida, e como você pode identificar um ataque em um sistema que você está tentando proteger . Ao mesmo tempo, você também aprenderá como minimizar qualquer dano em seu sistema ou interromper um ataque em andamento. Com o Hacking: Guia para Iniciantes em Hacking de computadores ..., você aprenderá tudo o que precisa saber para entrar no mundo secreto dos hackers de computadores. Ele fornece uma visão geral completa de hackers, crackers e seus efeitos no mundo. Você aprenderá sobre os pré-requisitos para hackers, os vários tipos de hackers e os vários tipos de ataques de hacking: - Ataques Ativos - Ataques Mascarados - Ataques De Repetição Modificação De Mensagens Técnicas De Falsificação - Hacking Wifi - Ferramentas De Hacking - Hacking Seu Primeiro Hacker Ataques Passivos Download Hacking: Guia Para Iniciantes Em Hacking De Computadores Como Hackear Redes Sem Fio, Segurança Básica E Testes De Penetração, Kali Linux, Seu Primeiro Hack Imediatamente - Esta Incrível Nova Edição Coloca Uma Vasta Riqueza De Conhecimentos À Sua Disposição. Você aprenderá como hackear uma senha de e-mail, técnicas de spoofing, hacking WiFi e dicas para hackers éticos. Você até aprenderá como fazer seu primeiro hack. Role Para Cima E Comece A Desfrutar Deste Negócio Incrível Instantaneamente

Содержание

Alan T. Norman
Guia Para Iniciantes Em Hacking de Computadores

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

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 ameaçarão controlar o sistema – ou impedir o acesso de outros – e chantagearão o proprietário a pagar um resgate antes de renunciar ao controle. Um hacker é considerado um chapéu preto, mesmo que tenha o que eles mesmos descreveriam como intenções nobres. Em outras palavras, mesmo os hackers que estão hackeando para fins sociais ou políticos são chapéus pretos, porque pretendem explorar as vulnerabilidades que descobrem. Da mesma forma, entidades de estados-nação adversários que estão hackeando para fins de guerra podem ser consideradas black hats, independentemente de suas justificativas ou do status internacional de sua nação.

Chapéu Branco (White Hat)

Como existem muitas maneiras criativas e imprevistas de acessar computadores e redes, geralmente, a única maneira de descobrir fraquezas exploráveis é tentar invadir o próprio sistema antes que alguém com intenções maliciosas o faça primeiro, causando danos irreparáveis. Um hacker ***white hat*** foi especificamente autorizado, pelo proprietário ou responsável por um sistema de destino, a descobrir e testar suas vulnerabilidades. Isto é conhecido como ***teste de penetração*** . O hacker de chapéu branco usa as mesmas ferramentas e procedimentos que um hacker de chapéu preto e, geralmente, possui conhecimentos e habilidades iguais. De fato, não é incomum que um ex-chapéu preto encontre emprego legítimo como um chapéu branco, porque os black hats, geralmente, têm uma grande experiência prática com penetração do sistema. Sabe-se que agências e corporações governamentais empregam criminosos de computador, anteriormente processados, para testar sistemas vitais.

Chapéu Cinza (Gray Hat)

Como o nome indica, o termo ***gray hat*** (geralmente escrito como "grey") é um pouco menos concreto na sua caracterização na ética hacker. Um hacker de chapéu cinza não tem, necessariamente, a permissão de um proprietário ou responsável pelo sistema e, portanto, pode ser considerado um comportamento anti-ético a sua tentativa de detectar vulnerabilidades de segurança. No entanto, um chapéu cinza não está executando estas ações com a intenção de explorar as vulnerabilidades ou ajudar outras pessoas a fazê-lo. Em vez disso, eles estão, essencialmente, conduzindo testes de penetração não autorizados, com o objetivo de alertar o proprietário sobre possíveis falhas. Freqüentemente, chapéus cinzas vão hackear com o propósito expresso de fortalecer um sistema que eles usam ou desfrutam, para impedir qualquer subversão futura por parte de atores com intenções mais maliciosas.

Consequências do Hacking

As consequências do acesso não autorizado a computadores variam dos menores custos e inconvenientes da segurança das informações cotidianas, a situações severamente perigosas e até mortais. Embora possa haver sérias penalidades criminais contra hackers, quando capturados e processados, a sociedade em geral arca com o peso dos custos financeiros e humanos dos hackings maliciosos. Devido à natureza interconectada do mundo moderno, um único indivíduo inteligente, sentado em um café com um laptop, pode causar enormes danos à vida e à propriedade. É importante entender as ramificações do hacking, de forma a saber onde concentrar os esforços para a prevenção de certos crimes relacionados ao computador.

Criminalidade

É claro que há consequências legais para hackers flagrados invadindo um sistema ou rede de computadores. Leis e penalidades específicas variam entre nações e entre estados e municípios. A aplicação das leis também varia entre as nações. Alguns governos simplesmente não priorizam a ação penal, especialmente quando as vítimas estão fora de seu próprio país. Isto permite que muitos hackers operem impunemente em certas partes do mundo. De fato, algumas nações avançadas têm elementos em seus governos nos quais o hacking é uma função prevista. Algumas agências militares e civis de segurança e aplicação da lei apresentam divisões cujo mandato é invadir os sistemas sensíveis de adversários estrangeiros. É um ponto de discórdia quando algumas destas agências invadem arquivos e comunicações particulares de seus próprios cidadãos, muitas vezes levando a consequências políticas.

As multas por invasão ilegal dependem amplamente da natureza da própria transgressão. Acessar as informações privadas de alguém sem a sua autorização provavelmente acarretaria uma penalidade menor do que usar o acesso para roubar dinheiro, sabotar equipamentos ou cometer traição. Processos de alto nível resultaram de hackers roubando e procedendo ou à venda ou à disseminação de informações pessoais, confidenciais ou classificadas.

Vítimas

As vítimas de hacking variam de ser destinatários de piadas e trotes relativamente inofensivos nas mídias sociais, a serem publicamente envergonhadas pelo lançamento de fotos ou e-mails pessoais, ou ainda, a vítimas de roubo, vírus destrutivos e chantagem. Nos casos mais graves de hacking, em que a segurança nacional é ameaçada pela liberação de informações confidenciais ou pela destruição de infraestrutura crítica, a sociedade como um todo é a vítima.

O roubo de identidade é um dos crimes de computador mais comuns. Os hackers direcionam as informações pessoais de indivíduos inocentes, usando os dados para ganho pessoal ou vendendo-os para outras pessoas. As vítimas geralmente não sabem que suas informações foram comprometidas, até verem atividades não autorizadas no cartão de crédito ou nas contas bancárias. Embora os dados pessoais sejam frequentemente obtidos por hackers visando vítimas individuais, alguns criminosos sofisticados conseguiram, nos últimos anos, acessar grandes bancos de dados de informações pessoais e financeiras, invadindo servidores de varejistas e provedores de serviços on-line com milhões de contas de clientes. Estas violações de dados de alta visibilidade têm um custo enorme em termos monetários, mas também prejudicam a reputação das empresas-alvo, e abalam a confiança do público na segurança da informação. Violações de dados semelhantes resultaram na distribuição pública de e-mails e fotografias pessoais, muitas vezes causando vergonha, prejudicando relacionamentos e resultando na perda de emprego das vítimas.

Custos de Prevenção

Existe um clássico "Ardil-22" quando se trata da prevenção de hackers. Para a maioria das pessoas, é preciso pouco mais que senso comum, vigilância, boas práticas de segurança e alguns softwares disponíveis gratuitamente para se manter protegido da maioria dos ataques. No entanto, com o aumento da popularidade da computação em nuvem, onde os arquivos são armazenados em um

servidor externo, além de ou em vez de em dispositivos pessoais, os indivíduos têm menos controle sobre a segurança de seus próprios dados. Isto impõe um grande ônus financeiro aos guardiões dos servidores em nuvem, de forma a proteger um volume cada vez mais alto de informações pessoais centralizadas.

Assim, grandes empresas e entidades governamentais costumam gastar, anualmente, em segurança de computadores, dinheiro igual ou a mais do que poderiam perder nos ataques mais comuns. No entanto, estas medidas são necessárias porque um ataque sofisticado e bem-sucedido, em larga escala – embora improvável – , pode ter consequências catastróficas. Da mesma forma, indivíduos que desejam se proteger de criminosos cibernéticos adquirem software de segurança ou serviços de proteção contra roubo de identidade. Estes custos, juntamente com o tempo e o esforço despendidos praticando boa segurança das informações, podem ser um fardo indesejável.

Segurança Nacional e Global

A crescente dependência dos sistemas de controle industrial em computadores e dispositivos em rede, juntamente com a natureza rapidamente interconectada da infraestrutura crítica, deixaram os serviços vitais das nações industriais altamente vulneráveis a ataques cibernéticos. Os serviços municipais de energia, água, esgoto, internet e televisão podem ser interrompidos por sabotadores, seja para fins de ativismo político, chantagem ou terrorismo. Mesmo a interrupção a curto prazo de alguns destes serviços pode resultar em perda de vidas ou bens. A segurança das usinas nucleares é particularmente preocupante, como vimos nos últimos anos, pois hackers podem implantar vírus em componentes eletrônicos comumente usados para interromper máquinas industriais.

Os sistemas bancários e as redes de negociação financeira são alvos de alto valor para os hackers, estejam eles buscando ganhos financeiros ou causando turbulência econômica em um país rival. Alguns governos já estão implantando abertamente seus próprios hackers para guerra eletrônica. Os alvos para ataques governamentais e militares também incluem os veículos e instrumentos de guerra, cada vez mais em rede. Os componentes eletrônicos podem ser comprometidos pelos hackers na linha de produção antes mesmo de chegarem a um tanque, navio de guerra, jato de combate, aeronave aérea ou outro veículo militar – fazendo com que os governos tenham cuidado com quem contratam na linha de suprimento. As comunicações confidenciais por email, telefone ou satélite também devem ser protegidas contra adversários. Não são apenas os estados-nação que ameaçam os sistemas militares avançados. As organizações terroristas estão se tornando cada vez mais sofisticadas, e estão mudando para métodos mais tecnológicos.

Capítulo 2: Vulnerabilidades e Explorações

A essência do hacking é a exploração de falhas na segurança de um computador, dispositivo, componente de software ou rede. Estas falhas são conhecidas como ***vulnerabilidades***. O objetivo do hacker é descobrir as vulnerabilidades em um sistema que lhes darão o acesso ou controle mais fácil que atenda a seus propósitos. Uma vez que as vulnerabilidades são entendidas, a ***exploração*** dessas vulnerabilidades pode começar, por meio da qual o hacker tira proveito das falhas do sistema para obter acesso. Geralmente, os hackers de chapéu preto e chapéu branco pretendem explorar as vulnerabilidades, embora para propósitos diferentes, enquanto que chapéus cinza tentam notificar o proprietário a fim de que sejam tomadas medidas para proteger o sistema.

Vulnerabilidades

Vulnerabilidades nos sistemas de computação e rede sempre existiram e sempre existirão. Nenhum sistema pode ser 100% hermético porque alguém sempre precisará acessar as informações ou serviços que estão sendo protegidos. Além disso, a presença de usuários humanos representa uma vulnerabilidade por si só, porque as pessoas são notoriamente ruins em praticar boa segurança. À medida que as vulnerabilidades são descobertas e corrigidas, outras novas as substituem, quase instantaneamente. A alternância entre a exploração de hackers e a implementação de medidas de segurança representa uma verdadeira corrida armamentista, com cada lado se tornando mais sofisticado em paralelo.

Vulnerabilidades Humanas

Uma vulnerabilidade raramente discutida é a do usuário humano. A maioria dos usuários de computadores e sistemas de informação não são especialistas em informática ou profissionais de segurança cibernética. A maioria dos usuários sabe muito pouco sobre o que acontece entre seus pontos de interface e os dados ou serviços que estão acessando. É difícil fazer com que as pessoas, em larga escala, mudem seus hábitos e usem as práticas recomendadas para definir senhas, verificar cuidadosamente os emails, evitar sites maliciosos e manter o software atualizado. Empresas e agências governamentais gastam muito tempo e recursos treinando funcionários para seguir os procedimentos adequados de segurança da informação, mas é necessário apenas um elo fraco da cadeia para dar aos hackers a janela que eles procuram para acessar um sistema ou rede inteira.

Os firewalls mais sofisticados e caros e a prevenção de intrusões de rede dos sistemas são inúteis quando um único usuário interno clica em um link malicioso, abre um vírus em um anexo de email, conecta-se a uma unidade flash comprometida ou simplesmente fornece sua senha de acesso pela Internet, telefone ou email. Mesmo quando lembrado repetidamente das melhores práticas de segurança, os usuários comuns são a vulnerabilidade mais fácil e mais consistente a descobrir e explorar. Às vezes, as vulnerabilidades humanas são tão simples quanto praticar a segurança de senhas ruins, deixando as senhas escritas à vista de todos, às vezes até anexadas ao hardware em uso. O uso de senhas fáceis de adivinhar é outro erro comum do usuário. Um sistema corporativo específico foi comprometido quando um hacker inteligente deixou intencionalmente um pen drive USB no estacionamento de uma empresa. Quando um funcionário desavisado o encontrou, colocou a unidade no seu computador do trabalho e, em consequência, liberou um vírus. A maioria das pessoas não leva a sério a segurança de computador até que ocorra um incidente e, mesmo assim, costuma voltar aos mesmos hábitos. Os hackers sabem disso e aproveitam-se sempre que possível.

Vulnerabilidades de Software

Todos os computadores confiam no software (ou "firmware", em alguns dispositivos) para converter comandos de entrada ou usuário em ação. O software gerencia logins de usuários, realiza consultas a bancos de dados, executa envios de formulários de sites, controla hardware e periféricos e gerencia outros aspectos da funcionalidade do computador e da rede que podem ser explorados por um hacker. Além do fato de que os programadores cometem erros e omissões, é impossível para os desenvolvedores de software antecipar todas as vulnerabilidades possíveis em seu código. O máximo que os desenvolvedores podem esperar é corrigir e alterar seus softwares quando vulnerabilidades são descobertas. É por isso que é tão importante manter o software atualizado.

Algumas vulnerabilidades de software são devido a erros na programação, mas a maioria é simplesmente devido a falhas imprevistas no design. O software geralmente é seguro quando usado como projetado, mas combinações imprevistas e não intencionais de entradas, comandos e condições geralmente resultam em consequências imprevisíveis. Sem controles rígidos sobre como os usuários interagem com o software, muitas vulnerabilidades são descobertas por engano ou aleatoriamente. Os hackers procuram descobrir essas anomalias o mais rápido possível.

Explorações

Encontrar e explorar vulnerabilidades para obter acesso aos sistemas é uma arte e uma ciência. Devido à natureza dinâmica da segurança da informação, existe um jogo constante de "gato e rato" entre hackers e profissionais de segurança, e até mesmo entre adversários de nações. Para permanecer à frente (ou pelo menos não ficar muito para trás), é preciso não apenas ficar a par das últimas tecnologias e vulnerabilidades, mas também ser capaz de prever como os hackers e o pessoal de segurança reagirão às mudanças no sistema. paisagem geral.

Acesso

O objetivo mais comum da exploração é obter acesso e algum nível de controle de um sistema de destino. Como muitos sistemas têm vários níveis de acesso para fins de segurança, geralmente ocorre que cada nível de acesso tem sua própria camada de vulnerabilidades sendo, geralmente, mais difícil de invadir conforme existam funcionalidades mais vitais. O golpe final de acesso para um hacker é atingir o nível de super usuário ou ***raiz*** – um termo UNIX – conhecido como "obtendo raiz" na linguagem dos hackers. Este nível mais alto permite o controle do usuário de todos os sistemas, arquivos, bancos de dados e configurações em um determinado sistema independente.

Pode ser bastante difícil violar o nível raiz de um sistema de computador seguro em uma única exploração. Mais frequentemente, os hackers exploram vulnerabilidades mais fáceis ou aproveitam os usuários menos experientes para obter primeiro acesso de baixo nível. A partir desse ponto, outros métodos podem ser empregados para atingir níveis mais altos dos administradores até a raiz. Com o acesso root, um hacker pode visualizar, baixar e substituir informações à vontade e, em alguns casos, remover quaisquer vestígios de que estiveram no sistema. Por esse motivo, obter a raiz em um sistema de destino é um ponto de orgulho como a maior conquista entre hackers de chapéu preto e chapéu branco.

Negando Acesso

Em muitos casos, obter acesso a um determinado sistema de destino é impossível, extremamente difícil, ou nem mesmo desejado por um hacker. Às vezes, o objetivo de um hacker é simplesmente impedir que usuários legítimos acessem um site ou rede. Este tipo de atividade é conhecida como ***negação de serviço*** (DoS). O propósito de conduzir um ataque DoS pode variar. Uma vez que é relativamente simples de executar, muitas vezes é um exercício iniciante para um hacker inexperiente ("novato", "n00b" ou "neófito") na linguagem) para ganhar direito de se gabar. Hackers mais experientes podem executar ataques DoS sustentados, que interrompem servidores comerciais ou governamentais por um longo período de tempo. Assim, grupos organizados de hackers muitas vezes mantêm um site "refém" e exigem um resgate dos proprietários em troca de parar o ataque, tudo sem nunca ter que ter acesso.

Capítulo 3. Primeiros Passos

Os hackers têm a reputação de serem indivíduos altamente inteligentes e prodigiosos em muitos aspectos. Pode, portanto, parecer ser uma tarefa trabalhosa e difícil começar do zero e alcançar qualquer nível prático de proficiência . Deve-se lembrar que todos devem começar em algum lugar quando aprendem uma matéria ou habilidade. Com dedicação e perseverança, é possível ir tão longe no mundo do hacking quanto sua vontade puder levá-lo. Uma coisa que vai ajudar no processo de se tornar um hacker é definir algumas metas. Pergunte a si mesmo por que você quer aprender hacking e o que você pretende realizar. Alguns só querem aprender o básico para que possam entender como proteger a si mesmos, sua família ou seus negócios contra ataques maliciosos. Outros estão procurando se preparar para uma carreira em hacking de chapéu branco ou segurança da informação. Quaisquer que sejam suas razões, você deve se preparar para aprender um pouco de novos conhecimentos e habilidades.

Aprendizagem

A arma mais importante no arsenal de um hacker é o conhecimento. Não só é importante que um hacker aprenda o máximo possível sobre computadores, redes e softwares – mas, para se manter competitivo e eficaz, eles devem manter-se atualizados sobre as constantes e rápidas mudanças nos computadores e na segurança dos computadores. Não é necessário que um hacker seja um engenheiro, cientista da computação ou tenha conhecimento íntimo de microprocessador ou design de hardware de computador, mas eles devem entender como um computador funciona, os componentes principais e como eles interagem, como os computadores são em rede local e através da internet, como os usuários normalmente interagem com suas máquinas, e – o mais importante – como o software dita a função do computador. Um excelente hacker é fluente e experimentado em várias linguagens de computador e entende os principais sistemas operacionais. E também é muito útil para um hacker estar familiarizado com a história, matemática e prática de criptografia.

É possível, e cada vez mais comum, para um leigo, com pouca experiência de hacking e apenas conhecimento leve ou intermediário sobre programação, realizar um ataque contra um sistema. Muitas vezes as pessoas fazem isso usando scripts e seguindo procedimentos que foram desenvolvidos por operadores mais experientes. Isto acontece mais comumente com tipos mais simples de ataques, como negação de serviço. Esses hackers inexperientes são conhecidos na comunidade de hackers como ***script kiddies (garotos dos scripts)*** . O problema com este tipo de atividade é que os criminosos têm pouca apreciação pelo que está acontecendo no código que estão executando, e podem não ser capazes de antecipar efeitos colaterais ou outras consequências não intencionais. É melhor entender completamente o que você está fazendo antes de tentar um ataque.

Computadores e Processadores

Os computadores variam em tamanho, forma e propósito, mas a maioria deles tem, essencialmente, o mesmo design. Um bom hacker deve estudar como os computadores evoluíram desde as primeiras máquinas no século 20 até as máquinas muito mais sofisticadas que usamos hoje. No processo, torna-se evidente que os computadores têm os mesmos componentes básicos. Para ser um hacker eficaz, você deve conhecer os diferentes tipos de processadores que existem na maioria dos computadores modernos. Por exemplo, os três maiores fabricantes de microprocessadores são intel, American Micro Devices (AMD) e Motorola. Estes processadores compreendem a maioria dos computadores pessoais que um hacker encontrará, mas cada um tem seu próprio conjunto de instruções único. Embora a maioria dos hackers raramente tenha que lidar com linguagens de programação no nível da máquina, ataques mais sofisticados podem exigir uma compreensão das diferenças entre os conjuntos de instruções do processador.

Alguns processadores são programáveis pelo usuário final. Estes são conhecidos como Field-Programmable Gate Arrays (FPGA) e estão sendo usados cada vez mais para sistemas embarcados, particularmente em controles industriais. Os hackers são conhecidos por obter acesso a esses chips enquanto estão em produção, a fim de implantar software malicioso no destino final. Uma compreensão da arquitetura e programação FPGA é necessária para estes tipos de ataques sofisticados. Estes ataques incorporados são particularmente preocupantes a clientes militares e industriais que compram chips em larga escala para sistemas críticos.

Rede e Protocolos

Um dos assuntos mais importantes para o aspirante a hacker estudar é o da arquitetura de rede e protocolos. Os computadores podem estar em rede em muitas configurações e tamanhos diferentes, e com diferentes tecnologias que regem sua interconexão. Desde fio de cobre, até fibra óptica, até conexões sem fio e satélite, bem como combinações de todas estas mídias, construímos uma vasta rede de computadores em todo o mundo. Esta rede pode ser entendida em sua totalidade, em grande escala, bem como vista como uma conexão de redes menores e independentes.

Em termos de tamanho, as redes de computadores têm sido tradicionalmente categorizadas como Redes de Área Local (LAN) e Redes de Área Ampla (WAN). Os WANs normalmente conectam vários LANs. Existem várias outras designações para diferentes tamanhos de redes, e a terminologia está sempre mudando à medida que novas tecnologias e condutividades se desenvolvem. Acompanhar estas mudanças é uma das tarefas constantes de um hacker.

As redes também possuem arquiteturas diferentes. A arquitetura é determinada não apenas pela configuração dos diferentes nódulos, mas também pelo meio que os conecta. Originalmente, computadores em rede eram sempre conectados por fios de cobre. Os cabos de rede de cobre comumente utilizados, muitas vezes conhecidos como cabos ***ethernet*** , consistem em pares torcidos de fio de cobre. Embora o mais comum destes cabos seja o cabo categoria cinco, ou CAT-5, está começando a dar lugar a um novo padrão, o CAT-6, que tem maior capacidade de transmissão de sinais. Para aplicações de alta velocidade e distâncias mais longas, os cabos de fibra óptica são geralmente escolhidos. A fibra óptica usa luz em vez de eletricidade e tem uma capacidade muito alta para transportar informações. Eles são usados para transmitir a televisão a cabo mais moderna e serviços de internet de alta velocidade. A fibra óptica serve como espinha dorsal para a internet. Em áreas menores, redes sem fio são muito comuns. Usando um protocolo Wireless Fidelity (Wi-Fi), existem redes sem fio em um grande número de LANs pessoais, privadas e comerciais. Os hackers estão frequentemente e particularmente interessados em invadir redes Wi-Fi, o que resulta na evolução dos padrões de segurança Wi-Fi.

Independentemente da arquitetura ou meio de transmissão, quando dois terminais estão se comunicando em uma rede, eles devem fazê-lo usando um conjunto comum de regras conhecido como ***protocolo*** . Os protocolos de rede evoluíram desde que as primeiras redes de computadores foram criadas, mas mantiveram a mesma abordagem básica em camadas. Em geral, uma rede é conceituada em termos de diferentes camadas que executam diferentes funções. Isto também é conhecido como uma pilha ***(stack)*** . Os protocolos de comunicação mais comuns utilizados hoje são o Protocolo de Internet (IP) e o Protocolo de Controle de Transmissão (TCP). Juntos, são comumente conhecidos como ***TCP/IP*** . Estes protocolos mudam e são padronizados de vez em quando. É fundamental que o hacker aprenda estes protocolos e como eles se relacionam com a comunicação entre as diferentes camadas da pilha. É assim que os hackers podem obter níveis cada vez maiores de acesso a um sistema.

Linguagens de Programação

Para quem nunca o fez antes, pode parecer assustador aprender uma linguagem de programação do zero, mas muitas pessoas acham que, uma vez que se tornam proficientes em uma linguagem de programação, é muito mais fácil e rápido aprender outras. Os hackers não só precisam entender linguagens de programação para serem capazes de explorar vulnerabilidades de software, mas muitos hackers precisam escrever seu próprio código, para serem capazes de executar um ataque específico. Ler, entender e escrever códigos é fundamental para hackear.

As linguagens de programação variam de código de máquina muito obscuro, que está em formato binário e hexadecimal e é usado para se comunicar diretamente com um processador, até linguagens orientadas a objetos de alto nível, que são usadas para o desenvolvimento de software. As linguagens comuns orientadas a objetos de alto nível são ***C++*** e ***Java*** . O código escrito em idiomas de alto nível é compilado no código de máquina apropriado para um determinado processador, o que torna as linguagens de alto nível muito portáteis entre diferentes tipos de máquinas. Outra categoria é uma linguagem roteirizada, onde os comandos são executados linha por linha em vez de serem compilados em código de máquina.

Aprender linguagens de programação leva tempo e prática – não há outra maneira de se tornar proficiente. Longas noites e maratonas noturnas de escrita, depuração e recompilação de códigos são um rito comum de passagem entre hackers iniciantes.

Capítulo 4. Kit de Ferramentas do Hacker

Mesmo armado com conhecimento, desenvoltura e a quantidade certa de perseverança teimosa, o hacker ainda precisa de um certo conjunto de ferramentas físicas para realizar um ataque. No entanto, hacking não precisa ser uma profissão ou hobby caro. A maioria das ferramentas de software de que um hacker precisa pode ser obtida livremente porque são produtos de código aberto. Nem um hacker precisa de milhares de dólares em equipamentos de computação de alta potência – para a maioria dos ataques, um simples laptop ou computador desktop com uma quantidade razoável de memória, armazenamento e velocidade do processador será suficiente. Ao longo das décadas, os hackers tornaram-se notórios por realizar grandes feitos com orçamentos relativamente baixos. Embora cada indivíduo precise decidir por si mesmo qual combinação de hardware e software ele precisa para seus objetivos particulares, este capítulo servirá como um guia para ajudar a entender quais diferentes opções estão disponíveis e são preferidas na comunidade hacking .

Sistemas Operacionais & Distribuições

Um sistema operacional (OS) é o intermediário entre o hardware e o software de um computador. Um sistema operacional normalmente gerencia o sistema de arquivos, a comunicação periférica e as contas de usuário de um sistema de computador, entre outras responsabilidades. Existem várias marcas de sistemas operacionais, tanto comerciais quanto de código aberto, que podem ser instalados em qualquer plataforma de computador. O Microsoft Windows é o sistema operacional comercial mais conhecido e instalado para sistemas de estilo "PC". A Apple tem seu próprio SO que vem instalado em seu computador e sistemas móveis. O sistema operacional do Google, Android, de código aberto, está rapidamente ganhando popularidade.

O sistema operacional Linux, nomeado e desenvolvido por Linus Torvalds – uma figura lendária na cultura hacker – é um desdobramento de código aberto do sistema operacional UNIX (o Sistema Operacional da Apple também é baseado no sistema UNIX). O Linux ganhou popularidade ao longo dos anos entre hackers e entusiastas hardcore de computadores por sua flexibilidade e portabilidade. Várias distribuições do Linux evoluíram para diferentes propósitos através de ajustes constantes por parte de seus usuários. As distribuições são tipicamente distinguíveis umas das outras pelo seu tamanho, interface de usuário, drivers de hardware e as ferramentas de software que vêm pré-instaladas. Algumas distribuições populares do Linux, como Red Hat e Ubuntu, são para uso geral. Outros foram desenvolvidos para tarefas e plataformas específicas. O sistema operacional na plataforma de "ataque" de um hacker é o coração de seu kit de ferramentas.

Kali Linux

Anteriormente conhecido como Backtrack, Kali é um popular sistema operacional Linux de código aberto para hackers. Kali (as distribuições mais recentes do Kali Linux podem ser encontradas em www.kali.org/downloads) pode ser instalado em uma máquina dedicada, ou executado a partir de uma máquina virtual dentro de outro sistema operacional. Ao longo dos anos, Kali evoluiu para conter uma grande variedade dos programas de avaliação e exploração de vulnerabilidades mais úteis. É uma das primeiras ferramentas que um hacker iniciante deve obter. Kali não só fornece prática usando uma plataforma Linux, mas também contém tudo o que um hacker precisa para realizar alguns dos ataques mais básicos de nível inferior, a fim de obter uma experiência valiosa.

Конец ознакомительного фрагмента.