ETHICAL HACKER E CYBERWAR (COMUNICAÇÃO DE DADOS)

SAGAH
SOLUÇÕES EDUCACIONAIS INTEGRADAS

Hacking

Diego Vrague Noble

OBJETIVOS DE APRENDIZAGEM

- Definir *hacking*.
- Identificar os tipos de *hackers*.
- Explicar as ferramentas e tecnologias utilizadas pelos *hackers*.

Introdução

É cada vez mais comum lermos notícias de que uma determinada empresa sofreu um ataque por *hacker*. Ataques desse tipo tendem a se tornar cada vez mais comuns, e os alvos podem não ser necessariamente empresas ou grandes instituições. Em um relatório da NTT (2021), empresa ligada ao setor de serviços de tecnologia, foi observado um aumento de 300% no número de ataques ao setor de manufatura e de 200% ao setor de saúde.

O uso de tecnologias remotas para o trabalho tem feito cada vez mais pessoas exporem tanto os dados pessoais quanto os dados e informações das empresas na internet. Entretanto, a atenção à segurança de informação não tem acompanhado esse crescimento. É necessário, portanto, maior divulgação de questões relacionadas à segurança de informação. Não é surpresa que a demanda por profissionais desse tipo esteja em alta, visto que há escassez de longa data no mercado.

Neste capítulo, você vai estudar o conceito de *hacker*, a pessoa especialista em sistemas de computadores, e verá que existem vários tipos — inclusive, nem todos são mal-intencionados. Além disso, serão apresentadas as principais ferramentas empregadas por *hackers*.

O que é *hacking*?

No contexto de TI, *hacking* é uma palavra que significa "[...] ganhar acesso ilegal a um computador, a uma rede, a um sistema, etc." (HACK, 2021, documento *on-line*). Aquele que usa métodos e ferramentas para obter esse acesso é chamado de *hacker*. O acesso ilegal a sistemas computacionais pode ser motivado por diversos fatores: um ex-empregado descontente com uma demissão ou um profissional contratado por alguma agência governamental para espionar alguma nação, como exemplos (MCCARTHY, 2014). Definiremos a parte violada como o "alvo" do *hacker* e o processo de adquirir o acesso como um "ataque".

Conseguir o acesso a um sistema por si só não é o objetivo principal de um *hacker*, pois, a partir desse acesso ilegal, ele pode roubar informações sigilosas para vendê-las em mercados ilegais, apagar registros e documentos importantes, desativar ou adulterar o funcionamento de subsistemas, cobrar resgates ou então chantagear as vítimas.

A motivação do *hacker*, assim como seu grau de domínio, serão temas abordados em mais detalhes na próxima seção.

Conceitos básicos

A internet foi criada a partir da suposição de confiança mútua entre todas as partes envolvidas (GOODRICH; TAMASSIA, 2013). Afinal, eram pesquisadores acadêmicos que se conheciam mesmo trabalhando em diferentes universidades. No desenvolvimento da rede que veio a ser a internet, não se pensou em participantes perversos conectados a ela. O que era justificável no início dos anos 1980 está, ainda, presente na forma com que a internet opera atualmente, já que o sistema não pode ser simplesmente abandonado e substituído por um sistema mais seguro.

Definimos uma vulnerabilidade como um potencial meio de acesso indesejável. Uma porta de comunicação aberta é uma vulnerabilidade, mesmo que nunca venha a ser violada. É fundamental que vulnerabilidades sejam identificadas para evitar ataques — e estamos falando aqui de vulnerabilidades de forma geral. Uma porta USB no servidor é uma vulnerabilidade nesse sentido, assim como um programa com erros que faz um mau gerenciamento da memória ou de algum recurso computacional. Um sinônimo de vulnerabilidade é brecha.

O papel do profissional de segurança de TI é reduzir ao máximo o número de vulnerabilidades de um sistema de TI. Estar seguro contra ameaças e ataques é estar protegido de invasões indesejáveis. O tipo de dano causado pela exploração de vulnerabilidade pode ser dependente do tipo de serviço que a empresa ou instituição presta. No pior caso, o dano causado por um ataque não mitigado pode levar ao fim das operações da empresa. Quando um ataque tem por intenção revelar as vulnerabilidades de um sistema e é feito com o consentimento do responsável pelo sistema-alvo, o ataque é chamando de *pentest*, uma abreviação de *penetration test*, ou teste de penetração, em português.

Saiba mais

Em um artigo clássico, mas ainda atual, publicado em 1975, Saltzer e Schroeder definiram os dez princípios para a segurança de sistemas computacionais. Alguns não se aplicam no contexto atual; outros são tidos como padrões da área. Veja a seguir.

- **1. Economia de mecanismo:** sistemas simples tendem a ser mais seguros do que sistemas complexos.
- **2. *Defaults* seguros contra falhas:** a configuração inicial de um sistema deve dar direitos mínimos de acesso a arquivos e recursos para usuários recém-criados.
- **4. Projeto aberto:** o projeto e a arquitetura do sistema devem ser abertos ao público.
- **6. Menor privilégio:** o usuário deve operar apenas com os direitos essenciais para realizar a sua tarefa, nada de direitos desnecessários.
- **8. Aceitação psicológica:** interfaces de usuário devem incentivar o uso de mecanismos de segurança.

Mais detalhes, assim como a lista completa de princípios, podem ser encontrados no capítulo 1.1.4 do livro *Introdução à segurança de computadores*, de Goodrich e Tamassia (2013). Além disso, Smith (2012) revisita esses princípios em um artigo mais recente.

Assim que as vulnerabilidades são identificadas por um *hacker*, o ataque se torna uma certeza. O *hacker*, ou grupo de *hackers*, usualmente segue passos listados a seguir (PATIL *et al.*, 2017):

1. **Reconhecimento:** é quando o *hacker* coleta em segredo a maior quantidade de informações sobre um sistema-alvo. Aqui são identificadas as máquinas com a interface pública do sistema, quais portas de comunicação estão abertas, qual sistema operacional é usado, quais serviços estão associados às portas de comunicação e é feito o mapeamento da rede do sistema.

2. **Varredura e enumeração:** varredura é o processo de procura por portas abertas no sistema e por vulnerabilidades nos serviços associados a essas portas. É aqui que se determina se um provedor está ativo, se os *firewalls* estão ligados e configurados corretamente, se existem sistemas de detecção de intrusos, quais são os dispositivos de roteamento e servidores na rede. Enumeração é o ataque inicial em que é estabelecida ativamente a conexão com o alvo. Na enumeração, o *hacker* precisa manter a sua identidade em segredo.
3. **Ganho de acesso:** nesse momento, com a ajuda de ferramentas, o *hacker* consegue burlar o sistema de autenticação de usuário (*login*) na máquina-alvo. Burlar o sistema de autenticação pode ser por meio da descoberta da senha de usuário ou então por meio de ferramentas como o konboot, que permitem fazer o *by-pass* (pular/evitar) dessa etapa.
4. **Manutenção de acesso:** uma vez logado, o *hacker* pode explorar novas vulnerabilidades do sistema e usufruir de novos recursos. Nesse ponto, ele está dentro do sistema. Ferramentas como *rootkits* permitem a exploração de ações de controle do sistema operacional, e aqui o *hacker* obtém acesso de administrador. O *hacker* pode baixar dados ou documentos, ir embora sem causar nenhum dano ou então instalar programas como cavalos de Tróia, que facilitarão novos ataques no futuro. Até então, os usuários do sistema sequer suspeitam que o sistema tenha sido comprometido.
5. **Remoção de vestígios:** feito o ataque, o *hacker* precisa eliminar qualquer vestígio, já é de seu interesse que a sua identidade se mantenha anônima. A remoção de vestígios pode incluir a alteração de arquivos de registro (*logs*), ou, então, a remoção de usuários temporários usados para facilitar o ataque. O objetivo nessa etapa é garantir que o sistema não tenha sinais de violação e que pessoas responsáveis pelo sistema não desconfiem do que ocorreu no sistema.

Os principais tipos de *hackers*

Apesar de o termo *hacker* estar associado a um indivíduo oculto e mal-intencionado, nem sempre isso é verdade. Existem *hackers* de todos os tipos, inclusive aqueles que colaboram com entidades governamentais para encontrar e indiciar criminosos (PAYÃO, 2016).

Podemos classificar *hackers* quanto à motivação e quanto ao nível de conhecimento. Veja os principais tipos quanto à motivação.

- *Whitehat hacker* — O *hacker whitehat*, chapéu branco, em tradução literal, é também conhecido como *ethical hacker*. Seu objetivo é encontrar vulnerabilidades em sistemas computacionais com o consentimento de quem administra o sistema; portanto, é um ataque legal. Sua motivação é, portanto, estabelecer um relatório de todos os pontos a serem reforçados e melhorados no sistema a fim de evitar futuros ataques.
- *Blackhat hacker* — Diferentemente do *hacker whitehat*, o *hacker blackhat* (chapéu preto) age de forma ilegal, sem o consentimento do administrador do sistema. Sua motivação é sempre de causar algum dano ao sistema ou, então, de se beneficiar com o roubo e a posterior venda de informações sigilosas. Alguns autores usam o termo *cracker* para definir esse *hacker*, por considerarem que o termo *hacker* deva ser neutro quanto à motivação do invasor.
- *Grayhat hacker* — Esse tipo de *hacker* está entre o *hacker whitehat* e o *hacker blackhat*, razão do nome *grayhat* (chapéu cinza). Quando um *hacker* acidentalmente ou sem má intenção realiza um acesso desautorizado e, portanto, ilegal, a um sistema ou à parte dele, ele é considerado um *grayhat*. O acesso desautorizado, mesmo que inofensivo, pode ser, um dia, publicado em alguma plataforma de internet ou então revelado a pessoas mal-intencionadas. Atualmente, algumas empresas até oferecem prêmios e recompensas para quem descobrir vulnerabilidades nos sistemas. O Microsoft Bug Bounty Program é um exemplo. Um *hacker* que em alguns momentos se comporta como um *whitehat*; e em outros, como um *blackhat*, também é chamado de *greyhat*.
- *Hacktivist* — A motivação desse tipo de *hacker* é causar algum impacto negativo na sociedade para chamar atenção a causas políticas, sociais ou religiosas. Ele opera não necessariamente em benefício próprio ou da instituição atacada.
- *Hackers* patrocinados pelo Estado — Existem *hackers* cuja motivação é definida por algum órgão governamental. Geralmente, esses *hackers* operam de forma secreta, e o objetivo é o ataque de sistemas que fazem o controle de infraestrutura de outros países potencialmente inimigos. O foco dos ataques podem ser, por exemplo, usinas hidrelétricas ou sistemas de transporte. Também são chamados de *ciberterroristas*.

- *Hacker* suicida — O *hacker* suicida é um tipo de *hacker* que não faz questão de esconder os vestígios ou de ocultar a identidade. A sua motivação em causar algum dano é do tipo "tudo ou nada". Esse tipo de *hacker* não é comum.
- *Spy hacker* — Esse é o *hacker* espião cuja motivação é roubar informações sigilosas de alguma empresa ou instituição e repassá-las à empresa concorrente, que, por sua vez, financia toda a operação.

Existem, ainda, alguns tipos alternativos de *hacker* que não têm uma definição precisa e unânime. Esses conceitos variam de contexto para contexto. Entre eles estão o *greenhat*, o *bluehat* e o *redhat*.

Quanto ao nível de conhecimento e domínio das tecnologias, os *hackers* são classificados nos seguintes tipos.

- *Script kiddie* — Esse é o *hacker* iniciante, também chamado de *noob*. Ele usa ferramentas desenvolvidas por terceiros e não tem um entendimento profundo das tecnologias usadas. A chance de ter a sua identidade revelada — e de consequentemente ser pego — é alta.
- *Admins* — Ess é o *hacker* intermediário, que tem conhecimento prático sobre a administração de sistemas. É um *hacker* capaz de criar ferramentas de ataque.
- Elite — É o *hacker* mais avançado, capaz de criar as próprias ferramentas para a invasão de sistemas. O *hacker* de elite é capaz de descobrir novas vulnerabilidades em códigos de aplicativos de sistemas e vender essa informação. Ele pode ser chamado de *coder*, quando se beneficia da criação das ferramentas de ataque em vez do ataque em si. Entretanto, o termo *coder* não se refere necessariamente a um *hacker* de elite.

Fique atento

Nem todo *hacker* é mal-intencionado. Alguns autores usam o termo *hacker* de forma neutra; para separar o *hacker* mal-intencionado do hacker bem-intencionado, são usados termos como *cracker* e *hacker* ético, respectivamente.

As ferramentas e tecnologias usadas pelos *hackers*

A atividade de *hacking* exige um ferramental específico. Como vimos, o ataque em si tem diferentes momentos que requerem diferentes ferramentas (PATIL *et al.*, 2017). Nesta seção, vamos estudar as principais ferramentas. Esta não é uma explicação aprofundada de todas as ferramentas, mas uma apresentação inicial das principais.

Cada subseção está estruturada com o momento do ataque: reconhecimento, varredura e enumeração, ganho de acesso, manutenção de acesso e remoção de vestígios. O leitor é convidado a buscar por cada ferramenta na internet para conhecer melhor cada uma delas. Recomenda-se, ainda, que ele esteja familiarizado com os riscos associados ao uso dessas ferramentas antes de experimentá-las.

Reconhecimento

A etapa de reconhecimento não necessariamente requer uma troca de mensagens com o sistema-alvo. Portanto, uma busca no Google a respeito do sistema em questão já pode ser considerada uma ação de reconhecimento.

Uma das ferramentas mais usadas nessa etapa é o whois, um serviço que pode ser invocado da linha de comando de sistemas operacionais como o Linux, por exemplo, ou então por meio de serviços *on-line*. O whois faz uma busca para identificar o domínio e o endereço www do *site* em questão. Dentre as informações estão qual é organização por trás do endereço e a localização de sua sede. Informações sobre o endereço dos principais servidores também estão disponíveis.

Varredura e enumeração

Na etapa de varredura e enumeração, são trocadas mensagens com o sistema-alvo. As três ferramentas mais usadas na etapa de varredura e enumeração são:

- ping — Envia pacotes para determinar se o servidor está ativo e registra o tempo de resposta entre o disparo da mensagem e a resposta.
- traceroute — Determina o caminho entre a origem e o destino do pacote disparado na rede. No sistema Windows, esse comando se chama tracert e faz parte do sistema operacional.
- nmap — Envia pacotes para diferentes portas de comunicação de um servidor e devolve um relatório com a relação de portas abertas e quais serviços estão mapeados em cada porta.

Existem outras ferramentas disponíveis, como zenmap, que provê uma interface gráfica para o nmap, ou então o netcraft e o nikto WVS, que dispõem de tecnologias de análise mais avançadas.

Ganho de acesso

Com as portas abertas mapeadas e as vulnerabilidades determinadas, é preciso estabelecer o acesso não autorizado ao sistema. Para tal, as principais ferramentas usadas são as seguintes.

- John the ripper — Ferramenta usada para fazer um ataque de quebra de senha baseada em dicionários. Usa uma abordagem de força bruta e é bastante conhecida.
- Wireshark — Captura pacotes trafegando na rede e permite e inspeção visual desses pacotes.
- Konboot — É capaz de liberar o *login* em máquinas com sistema operacional Windows.
- Pwdump7 — É capaz de acessar informações de *hash* associadas às senhas de uma máquina.
- Aircrack — Captura pacotes de uma rede wi-fi e é capaz de quebrar protocolos de segurança WEP e WPA.
- Fluxion — Se passa por uma rede wi-fi fictícia com o intuito de enganar o usuário de rede wi-fi e fazer com que ele digite a senha da rede.
- Cain & Abel — Tenta quebrar a senha de usuário a partir da análise de pacotes de rede.

Manutenção de acesso

A manutenção do ataque é o momento em que o *hacker*, já com acesso ao sistema, precisa garantir eventuais próximos acessos. Aqui é o momento em que ele instala programas que auxiliarão no próximo acesso não autorizado.

- Metasploit Penetration Testing Software — É um *framework* com uma coleção de vulnerabilidades conhecidas que permite o planejamento e a execução de um ataque.
- Beast — Instala cavalos de Tróia (programas maliciosos) que abrem as portas da máquina a partir de comandos remotos feitos pelo *hacker*.

Exemplo

A ferramenta nmap pode ser facilmente instalada e usada a partir de uma máquina com sistema operacional Linux. A seguir, é apresentado um exemplo de execução do comando `nmap 192.168.1.1`, executado a partir da linha de comando:

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-17 23:04
-03 Nmap scan report for 192.168.1.1
Host is up (0.0093s latency).
Not shown: 996 filtered ports
PORT          STATE SERVICE
22/tcp        open   ssh
53/tcp        open   domain
80/tcp        open   http
443/tcp       open   https
Nmap done: 1 IP address (1 host up) scanned in 5.07
seconds
```

Nesse resultado, é possível observar as seguintes informações: o estado do destino e o tempo de resposta, o número de portas filtradas, a relação de portas abertas, o protocolo da porta e o serviço associado a cada porta. Por exemplo, a linha `80/tcp  open  http` indica que a porta 80 está aberta usando o protocolo tcp e disponibilizando o serviço de http. O mesmo serviço de nmap pode ser feito por meio de servidores *on-line* ou, então, na própria máquina.

Remoção de vestígios

Essa é a etapa final do ataque. É quando o *hacker* remove qualquer sinal do ataque, com o objetivo de deixar o sistema no seu estado original, se for o caso de um ataque não destrutivo, ou, então, remover qualquer informação que leve à identificação do *hacker*.

A principal ferramenta usada nessa etapa é a OSForensics, que permite apagar e alterar os arquivos de *log* do sistema atacado de forma que o ataque não deixe vestígios. Arquivos de *log* fornecem um histórico de acesso ao sistema e, portanto, podem levantar suspeitas ao administrador do sistema.

Vimos que, no contexto de segurança de informação, *hacking* é a ação de ganhar acesso não autorizado a um sistema computacional. O *hacker* é o especialista nessa atividade. Vimos, também, que esse ato de inva-

são é dividido em cinco partes e que o *hacker* pode ter as mais variadas motivações. As principais ferramentas usadas por *hackers* podem ser catalogadas de acordo com algum momento da invasão. Por exemplo, na etapa inicial são usadas ferramentas para varrer as portas de um servidor na internet e, em outra etapa, são usadas outras ferramentas para remover os vestígios da invasão.

Referências

GOODRICH, M. T.; TAMASSIA, R. *Introdução à segurança de computadores*. Porto Alegre: Bookman, 2013.

HACK. *In*: MERRIAM-WEBSTER. [*Dictionary*]. [*S. l.*]: Merriam-Webster, 2021. Disponível em: https://www.merriam-webster.com/dictionary/hack. Acesso em: 13 ago. 2021.

MCCARTHY, N. K. *Resposta a incidentes de segurança em computadores*: planos para a proteção de informação em risco. Porto Alegre: Bookman, 2014.

NTT. *NTT global threat intelligence report*: up to 300% increase in attacks from opportunistic targeting. [*S. l.*]: NTT, 2021. Disponível em: https://hello.global.ntt/en-us/newsroom/ntt-global-threat-intelligence-report-2021. Acesso em: 13 ago. 2021.

PATIL, S. *et al*. Ethical hacking: the need for cyber security. *IEEE International Conference on Power, Control, Signals and Instrumentation Engineering*, [*s. l.*], p. 1602–1606, 2017.

PAYÃO, F. *Hacker ajuda polícia civil a encontrar pedófilos em São Paulo*. [*S. l.*]: Tecmundo, 2016. Disponível em: https://www.tecmundo.com.br/ataque-hacker/106502-hacker-ajuda-policia-civil-encontrar-pedofilos-paulo.htm. Acesso em: 13 ago. 2021.

SALTZER, J. H.; SCHOEDER, M. D. The protection of in formation in computer systems. *Proceedings of the IEEE*, [*s. l.*], v. 63, n. 9, p. 1278–1308, 1975.

SMITH, R. E. A contemporary look at Saltzer and Schroeder's 1975 design principles. *IEEE Security & Privacy*, [*s. l.*], v. 10, n. 6, p. 20–25, 2012.

Fique atento

Os *links* para *sites* da *web* fornecidos neste capítulo foram todos testados, e seu funcionamento foi comprovado no momento da publicação do material. No entanto, a rede é extremamente dinâmica; suas páginas estão constantemente mudando de local e conteúdo. Assim, os editores declaram não ter qualquer responsabilidade sobre qualidade, precisão ou integralidade das informações referidas em tais *links*.

Conteúdo:

SOLUÇÕES EDUCACIONAIS INTEGRADAS