Tipos de atacantes nas corporações: hackers, lammers, script kidies, crackers e insiders

Apresentar os principais conceitos existentes dentro do universo Hacker, bem como esclarecer e orientar o aluno sobre quem são os hackers, sua hierarquia e os principais tipos de ataques para cometer fraudes dentro do ambiente virtual.

Hacker

Geralmente, quando ouvimos falar no termo **hacker**, a figura de um garoto com óculos de grau forte na frente de uma máquina rapidamente é formada em nosso pensamento; também pensamos naquelas pessoas que não possuem convívio social, muito inteligentes e que só ficam na frente de computadores.

Porém, antes de afirmamos que só esse grupo de pessoas caracteriza os hackers, devemos entender o significado do que é ser hacker.

De maneira mais simples, podemos dizer que um hacker é um indivíduo que possui muito conhecimento sobre um assunto de tecnologia e está sempre em busca de maiores informações. Acaba por vezes se deparando com pontos fracos de alguma tecnologia. Eles podem utilizar suas técnicas para acessar sistemas alheios, porém nunca executam ações que possam prejudicar os sistemas da rede acessada.

Como existem o bem e o mal, também começaram a aparecer nesse cenário pessoas que viram que poderiam ter algum tipo de proveito acessando a máquina que se encontrava desprotegida.

Dessa maneira, surgiram os primeiros invasores, comumente conhecidos como **crackers**, que não resistiram às tentações que eram oferecidas e assim passaram a utilizar as informações obtidas para o seu próprio proveito ou passaram a alterar, roubar, vender, destruir informações que obtinham por meio das suas ações. Nesse caso, ao contrário dos hackers, além de acessar os computadores de outras pessoas praticam ações sem a autorização delas e comprometem logicamente as aplicações dos computadores.

Assim, existe uma deturpação da palavra **hacker** devido a uma série de informações que foram divulgadas na mídia e acabaram por transformar essa palavra em sinônimo de criminoso.

Na medida em que os computadores começaram a povoar as residências e empresas e passaram a ser uma ferramenta indispensável para a realização das atividades dos colaboradores da organização, os noticiários começaram, quando ocorria algum incidente de segurança em que houvesse roubo de informações, a atribuir a palavra hacker àquele especialista de computador que consegue vencer todas as barreiras e roubar a informação, e é por isso que a maioria da população acabou associando essa palavra ao contexto de criminoso.

Nesse cenário, vários filmes que também contribuíram para que essa fama se popularizasse foram lançados no mercado cinematográfico, como, por exemplo, o filme *Hackers – piratas de computador,* feito pela Angelina Julie, bem como os filmes *Superman* e *WarGames*, em que o primeiro mostra a cena de um técnico que conseguiu desviar dinheiro do banco, passando centavos da conta das pessoas para a sua conta pessoal e ficou com muito dinheiro, e o segundo mostra garotos que conseguiram, devido a uma vulnerabilidade nos computadores da área de segurança dos Estados Unidos, manipular um computador de grande porte responsável pelo controle de defesa americano.

Um hacker, dependendo de diversos fatores – sociais, psicológicos ou financeiros –, pode vir a se transformar num cracker (invasor). Uma grande ofensa a um hacker do bem é confundi-lo com um cracker (invasor).

A palavra **hacker,** antigamente, era usada para designar alguém que conhecia muito sobre o assunto de computadores, geralmente muito curioso e que adorava mexer em sistemas em busca de falhas de segurança.

A idéia original era identificar alguma falha dentro do sistema e buscar uma solução para ela; caso conseguisse, o responsável pelo sistema deveria ser informado das ações a ser desenvolvidas para que a falha não voltasse a ocorrer, e assim manter o ambiente mais seguro.

Normalmente, quando um hacker conseguia ter acesso ao Servidor vulnerável, não fazia nada: apenas olhava, identificando as possíveis falhas e soluções.

Para se cometer um crime, basta ter um motivo e, a partir daí, utilizar a arma que achar mais interessante.

Dessa maneira, qualquer pessoa pode ser hacker, bastando apenas ter uma motivação, que pode ser a necessidade de ganhos financeiros, ação de vingança, necessidade de aceitação ou respeito, curiosidade ou busca de emoção.

Um adolescente pode ser um hacker quando tem por motivação ser aceito num grupo ou mesmo ganhar a atenção pelos seus conhecimentos, e, dessa forma, demonstrar poder para os seus colegas fazendo as grandes corporações ficarem paralisadas pelas suas ações.

Classificação

Da mesma forma que as organizações apresentam uma série de profissões em que cada profissional tem uma determinada característica, no mundo dos hackers o mesmo acontece, sendo que essa classificação vai desde os hackers iniciantes até aqueles com grande inteligência e capacidade de destruição.

Lammer – algumas literaturas consideram esse indivíduo o iniciante na hierarquia dos hackers. Não conhece nada, mas pelo fato de ter um computador e escutar algumas histórias de invasão e roubo, acredita que já pode invadir tudo. Estão dentro dessa categoria os usuários que têm conhecimentos muito básicos de informática.

Wannabe – é o principiante que já teve o seu *update* de conhecimento e começou a utilizar alguns programas que possibilitavam acessar informações protegidas nos computadores, como senhas, portas de comunicações e outras vulnerabilidades básicas. Não tem nenhum conhecimento real do que os programas que estão utilizando fazem. Apenas instalam o aplicativo e colocam e execução para ver o que acontece e o que eles conseguem ver.

Larva – na hierarquia, esse indivíduo já pode ser considerado um perigo potencial, pois, além de saber utilizar ferramentas específicas, ou seja, ferramentas que já se encontram à disposição no meio da internet, também tem conhecimento do que essas ferramentas são capazes de fazer e como elas agem. Além disso, devido ao seu conhecimento adquirido durante o tempo, já é capaz de desenvolver suas próprias ferramentas de ataques que muitas vezes são invisíveis às ferramentas de segurança de computadores que ainda não estão preparadas para elas.

Carders – dentro da hierarquia, esse tipo de indivíduo já pode ser considerado como criminoso, pois suas ações estão relacionadas a invasores que criam/utilizam cartões de crédito falsos para fazer transações pela internet. Para fazer esses cartões, a maioria deles se utiliza de programas que fazem tentativas para descobrir o número das chaves de combinação dos cartões de crédito.

Phreaker – os Phreakers são crackers que utilizam os seus altos conhecimentos em telefonia para fazer chamadas telefônicas sem pagar. Esse termo é muito utilizado fora do Brasil e em inglês pode ser encontrado como *freak, phone, free* (torne livre o uso do telefone). Além de usar o acesso à telefonia sem pagar, tem como intenção secundária se ocultar no mundo digital para não ser rastreado quando estiver cometendo o seu ato ilegal.

Defacer – são atribuídos a esse grupo os indivíduos que invadem sites e alteram a página principal do site web, colocando outras informações que acabam descaracterizando o site da empresa. Algumas vezes são colocadas fotos com imagens pornográficas ou apenas fazem a alteração de conteúdos com frases engraçadas e de mau gosto.

Write hat hacker e black hat hacker – o hacker também recebe dois tipos de títulos, dependendo da sua forma de atuar. Na realidade esses títulos eram utilizados para separar o Hacker do Bem (Ético) e o Hacker do Mau (Cracker). Costuma-se atribuir o título Black Hat Hacker (Hacker chapéu preto) ao indivíduo que usa os seus conhecimentos para o mal, ou seja, invadir e fazer ações danosas em outros computadores, e o Write Hat Hacker (Hacker chapéu Branco) é atribuído ao hacker que utiliza seus conhecimentos apenas para identificar falhas e avisar as pessoas dessas vulnerabilidades.

Gray hat hackers (hackers chapéu cinza) – existe ainda outra classificação, não muito utilizada, que procura definir um cracker que já foi do lado negro da força (alusão a *Guerra nas Estrelas*) e que agora utiliza o seu poder de conhecimento para ajudar as empresa a se defenderem de invasores perigosos. Dessa forma, o Gray Hat Hacker (Hacker chapéu cinza) tem as habilidades e intenções de um hacker de chapéu branco, mas também tem o conhecimento para propósitos menos nobres dos Hackers chapéu preto. Alguns deles são contratados como especialistas de segurança para proteção de sistemas de grandes corporações.

Script kiddies – pessoas com pouco conhecimento técnico de informática e que simplesmente fazem o download de scripts já prontos da internet. Esses scripts são capazes de ajudar o atacante inexperiente a ter acesso a funções do computador que podem deixá-lo vulnerável para uma ação danosa qualquer.

Insider – na realidade, um insider é uma denominação para um atacante que se encontra dentro da própria organização que será alvo do ataque. Muitas vezes são funcionários insatisfeitos que querem agir de forma maldosa para provocar algum tipo de inconveniente para a organização. Esse tipo de atacante pode ser desde um Lammer até mesmo um Black Hat Hacker.

É fácil aprender a "hackear"

Existem, no universo da Internet, dezenas de milhares de sites que disponibilizam ferramentas específicas de ataque para que o aspirante a invasor tente em alguma vítima. É claro que a primeira vítima já é o próprio iniciante, pois quando ele entra nesses tipos de sites e baixa algumas das ferramentas e as executa no seu computador, quem disse que essa ferramenta também não instalou algum agente nocivo no computador do aspirante?
Nos últimos anos, várias revistas especializadas foram lançadas e estão à disposição do hacker para no seu momento de lazer experimentar uma nova técnica.

Outra fonte de informação vem por meio dos colegas e amigos da escola, faculdade, rede social que fornecem receitas de bolo "Explicação passo a passo de como fazer o ataque" ou até mesmo links para onde se encontram manuais disponibilizados na rede mundial.

Antigamente era necessário ler para entender como manipular alguma ferramenta de ataque, hoje com o advento dos vídeos, basta entrar em um site específico que a "receita de bolo" é demonstrada online em um vídeo.

Como é o alvo típico?

Não é fácil determinar qual é o alvo típico de um ataque, porque os crackers atacam tipos de redes diferentes por motivações diferentes. Às vezes o ataque pode ser motivado por protesto ou manipulação política, ou até mesmo para ter destaque na mídia, e nesses casos os alvos são os sites dos governos, pois quando um ataque desse tipo é bem-sucedido pode trazer ao cracker grande prestígio dentro da sua comunidade de invasores, e a noticia se espalha rapidamente pela internet.

Procurando um alvo

Antes de sairmos para ir ao clube, ou à escola, ou ao cinema, costumamos fazer um desenho mental de tudo que teremos de realizar até atingir o nosso objetivo final. É claro que nem todos agem dessa maneira, porém aqueles que planejam suas ações têm maiores possibilidades de atingir o seu objetivo com maior facilidade do que aqueles que não planejam.

Voltando ao exemplo anterior, para ir de sua casa ao cinema, uma série de decisões deverá ser tomada, desde a escolha do filme, da roupa, do cinema, da condução etc. Geralmente essas escolhas acontecem de forma que possamos satisfazer alguma necessidade e de preferência que nos dê prazer.

O mesmo ocorre quando um hacker vai fazer um ataque. Ele terá que tomar uma série de decisões que vão desde o local a ser atacado até a ferramenta a ser utilizada.

Dentre os passos utilizados para a escolha do alvo podemos citar:

- Varrer a rede da internet em busca de potenciais alvos com um número muito elevado de vulnerabilidades **(varredura de endereço de rede)**.
- Obter informações que são disponibilizadas pelo próprio alvo dentro do ambiente da internet, como por exemplo, utilizar os serviços de WHOIS em busca de Nome de proprietário de domínios, contato técnico, endereço do Servidor que está registrado na Internet, informações estas muito úteis para um ataque no futuro **(levantamento de informações)**.
- O cracker, muitas vezes, precisa ter conhecimento do que está instalado ou está rodando como

serviço na máquina que deverá ser comprometida e então utiliza-se de ferramentas que têm a função de procurar por portas de comunicação TCP/UDP e também determinar o tipo de sistema operacional que está sendo executado no computador alvo **(varredura de portas)**.

- O próximo passo é a "identificação da topologia da rede", e não é preciso para isso utilizar ferramentas avançadas para fazer o processo de mapeamento. Estando conectado fisicamente ou logicamente à rede alvo, por meio de comandos internos da rede podem-se conseguir várias informações que poderão servir de munição para a batalha futura **(mapeamento da topologia de rede)**.

- Depois disso o próximo passo é tentar identificar o sistema operacional que está rodando na máquina alvo, sendo que essa atividade pode ser simples ou complexa, dependendo da segurança aplicada no alvo que será invadido **(identificação do sistema operacional da máquina- alvo)**.
- De posse do nome do sistema operacional, bastará agora identificar quais vulnerabilidades podem existir sobre esse sistema e verificar se a máquina-alvo as possuía. Muitas vezes são utilizadas ferramentas que inicialmente nasceram para aplicar a defesa do ambiente. Como assim? Para que os sistemas pudessem ser defendidos, foram criadas ferramentas que localizavam e apontavam as falhas para que os administradores de rede pudessem resolvê-las **(buscar as vulnerabilidades)**.

Selecionar o método de ataque

A partir de agora o craker irá selecionar um ou mais métodos de ataque específicos, que deverão ser usados com base nas informações obtidas nos estágios anteriores.

Efetuar o ataque

Nessa fase, o cracker executa os ataques no alvo que havia sido selecionado.

Técnicas de hacking

Existem diversas técnicas de ataque das quais um cracker poderá se valer para realizar a sua tarefa de invasão de acordo com os objetivos previamente estabelecido pelo seu mapeamento de ataque.

A seguir serão citadas as principais técnicas.

Denial of Service (DoS)

Técnica que consiste em sobrecarregar o sistema-alvo forçando para que ele fique sobrecarregado ou completamente fora de serviço.

O DoS é um ataque em que não se pretende roubar informações ou invadir sistemas; seu objetivo maior é tentar paralisar serviços da máquina invadida de forma que esta não consiga realizar nenhum serviço dentro da rede e impedir que usuários legítimos façam uso dos seus recursos.

Nesse tipo de ataque são usadas técnicas que visam sobrecarregar uma rede de tal modo, ao ponto que os verdadeiros usuários não consigam usá-la. A ideia fundamental é derrubar uma conexão entre dois ou mais computadores, fazendo tantas requisições a um site até que este não consiga mais ser acessado.

DDOS: Distributed DoS

Trata-se de uma variação do ataque DoS, em que são utilizadas várias máquinas para acometerem de forma simultânea a outra máquina específica. Para que esse tipo de ação dê resultados, é necessário que as outras máquinas que participaram do ataque já tenham sido comprometidas pelos atacantes com a instalação de um programa que transforma essa máquina em um zumbi.

Esses computadores ditos zumbis entram em contato com máquinas chamadas mestres, que são máquinas também comprometidas pelo atacante, tendo como única diferença o programa responsável para comandar o ataque. O atacante precisa desses computadores que serviram como "laranjas" no ataque para poder ficar oculto em uma possível investigação por parte das autoridades.

Port scanner

Técnica utilizada pelo cracker para fazer um levantamento dentro da rede em busca de

máquinas que possuem portas ou serviços ativos e que podem estar com algum problema de segurança. Após descobertas sobre as vulnerabilidades, o atacante verificará qual deverá ser a melhor ferramenta para poder iniciar o seu ataque.

SQL Injection

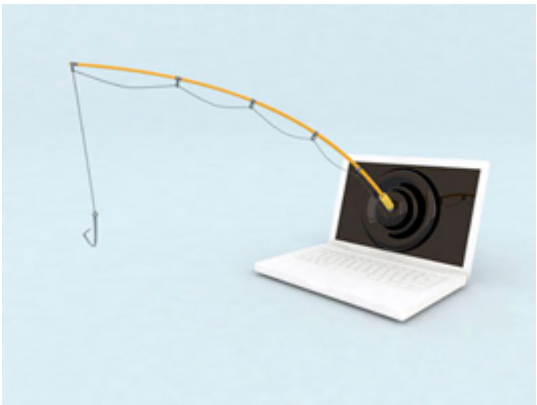
De maneira geral, o ataque de SQL Injection ocorre toda vez que um código sql é colocado dentro de uma *query* em um site, permitindo ao atacante obter dados importantes ou acesso a áreas restritas desses sites.

IP spoofing

O IP spoofing consiste na troca do IP original por outro, podendo assim se passar por outro equipamento e cometer seus ataques sem que possa ser identificado logo de início.

Phishing ou fishing scan

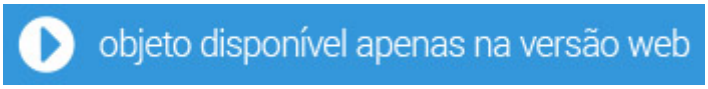
Nesse tipo de ataque, o cracker aplica a técnica de enviar e-mails fraudulentos para as caixas postais dos usuários da internet, com o intuito de induzi-los a efetuarem um cadastro colocando suas contas bancárias e seus números de cartão de crédito verdadeiros. Depois de o cadastro ser feito nessa página falsa, o cracker utiliza as informações obtidas para cometer os seus crimes. Normalmente esses e-mails vêm com alguns arquivos anexados com extensões perigosas, como "ponto" exe; "ponto" bat;, "ponto" com entre outras.

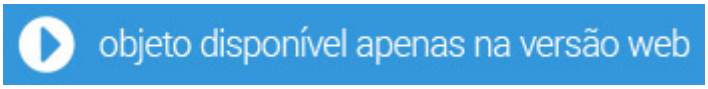


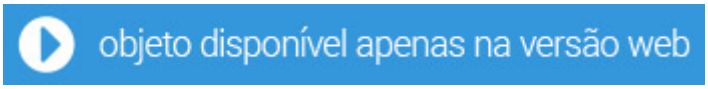
Man-in-the-middle

Tipo de ataque em que o cracker fica no meio da comunicação entre duas máquinas e todo o tráfego da conversação entre essas duas máquinas tem de passar antes pela máquina do cracker. Alguns crackers utilizam servidores "Proxy" como meio de enganar o usuário desavisado e conseguem ficar no meio da comunicação, coletando as informações que posteriormente serão analisadas pelo invasor.

Agora que você já estudou esta aula, resolva os exercícios e verifique seu conhecimento. Caso fique alguma dúvida, leve a questão ao Fórum e divida com seus colegas e professor.







Referências

GOMES, José Anchieschi. *Segurança total: protegendo-se contra hackers.* São Paulo: Makron Books, 2000.

MITNICK, Kevin D.; SIMON, William L. *A arte de invadir: as verdadeiras histórias por trás das ações de hackers, intrusos e criminosos eletrônicos.* São Paulo: Person Prentice Hall, 2005.

NAKAMURA, Emílio Tissato; GEUS, Paulo Lício de. *Segurança de redes em ambientes cooperativos*. São Paulo: Berkeley, 2002.

NORTHCUTT, Stephen; NOVAK, Judy; MCLACHLAN, Donald. *Segurança e prevenção em redes.* São Paulo: Berkeley, 2001.

STREBE, Matthew ; PERKINS, Charles. *Firewalls*. São Paulo: Makron Books, 2002.