Autor:Jack Dylan

Apostila iniciantes hacker!

OBS:essa apostila foi criada para iniciantes no mundo hacking para os integrantes do grupo EVIL SOCIETY é proibido compartilhá-la com outros grupos sem a PERMISSÃO de Jack Dylan.

Índice

O'Que é um hacker?

Hacker é uma palavra em inglês do âmbito da informática que indica uma pessoa que possui interesse e um bom conhecimento nessa área, sendo capaz de fazer hack (uma modificação) em algum sistema informático.

Em inglês, a palavra hack é um verbo que significa cortar alguma coisa de forma irregular ou grosseira. Assim, a partir da década de 50 do século XX, a palavra hack começou a ser usada para designar uma alteração inteligente em alguma máquina. Mais tarde, este termo passou a ser usado exclusivamente no âmbito da programação informática.

Dicionário hacker

White hat hackers – esses são considerados os hackers do bem. São especialistas em segurança, agindo para expor e resolver possíveis brechas e falhas nos sistemas das empresas que os contratam;

Black hat hackers – esses são os "bandidos", que invadem redes e computadores, criam vírus e malwares sempre com intenções não lícitas, como roubar senhas de bancos, dados confidenciais e outros;

Hacktivists – agem por motivos ideológicos. O representante mais famoso da categoria é o ANONYMOUSE que age para proteger as liberdades individuais e civis dos internautas. Os hacktivists são os principais responsáveis por quedas em sites de governos, órgãos e empresas multinacionais

Engenharia social

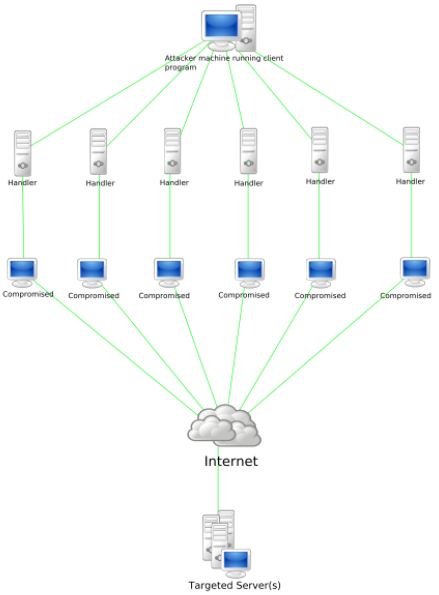
A engenharia social, no contexto de segurança da informação, refere-se à manipulação psicológica de pessoas para a execução de ações ou divulgar informações confidenciais. Este é um termo que descreve um tipo psicotécnico de intrusão que depende fortemente de interação humana e envolve enganar outras pessoas para quebrar procedimentos de segurança. Um ataque clássico na engenharia social é quando uma pessoa se passa por um alto nível profissional dentro das organizações e diz que o mesmo possui problemas urgentes de acesso ao sistema, conseguindo assim o acesso a locais restritos.

Exemplo 1 :você recebe uma mensagem e-mail, onde o remetente é o gerente ou alguém em nome do departamento de suporte do seu banco. Na mensagem ele diz que o serviço de internet Banking está apresentando algum problema e que tal problema pode ser corrigido se você executar o aplicativo que está anexado à mensagem. A execução deste aplicativo apresenta uma tela análoga àquela que você utiliza para ter acesso a conta bancária, aguardando que você digite sua senha. Na verdade, este aplicativo está preparado para furtar sua senha de acesso a conta bancária e enviá-la para o atacante.

EXEMPLO 2:
você recebe uma mensagem de e-mail, dizendo que seu computador está infectado por um vírus. A mensagem sugere que você instale uma ferramenta disponível em um site da internet, para eliminar o vírus de seu computador. A real função desta ferramenta não é eliminar um vírus, mas sim permitir que alguém tenha acesso ao seu computador e a todos os dados nele armazenados.

Ataques ddos

Um ataque de negar o serviço (também conhecido como DoS Attack, um acrônimo em inglês para Denial of Service), é uma tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores. Alvos típicos são servidores web, e o ataque procura tornar as páginas hospedadas indisponíveis na WWW. Não se trata de uma invasão do sistema, mas sim da sua invalidação por sobrecarga.



AtAques de sql

O SQL Injection é o nome dado a uma falha na codificação de uma aplicação qualquer (seja web ou local) que possibilita, por meio de um input qualquer, a manipulação de uma consulta SQL. Essa manipulação é chamada Injeção, então, o termo Injeção SQL. Resumindo: o SQL Injection é uma técnica de ataque baseada na manipulação do código SQL, que é a linguagem utilizada para troca de informações entre aplicativos e bancos de dados relacionais.

Pense em SQL Injection como uma simples falha lógica

É a linguagem de padrão universal para manipulação de dados em bancos de dados relacionais através dos SGBDs (Sistema de Gerenciamento de Banco de Dados Relacionais). É um tipo de ataque onde o "Hacker" consegue inserir comandos maliciosos (sql querys) no banco de dados através dos campos de formulários ou de URLs de uma aplicação vulnerável, ambicionando extrair informações guardadas no banco de dados".

Ataque de força bruta!

Em criptografia, um ataque de força bruta, ou busca exaustiva de chave, é um ataque criptoanalítico que pode, em teoria, ser usado contra quaisquer dados criptografados (exceto para dados criptografados de uma maneira segura na teoria da informação). Tal tipo de ataque pode ser usado quando não é possível tomar vantagem de outras fraquezas em um sistema de criptografia (se existir) que tornaram a tarefa mais fácil. Ele consiste de verificação sistemática de todas as possíveis chaves e senhas até que as corretas sejam encontradas. No pior dos casos, isto envolveria percorrer todo o espaço de busca.

A seleção de um tamanho de chave apropriado depende de possibilidade prática de fazer um ataque de força bruta. Ao ofuscar o dado a ser codificado, ataques de força bruta se tornam menos efetivos, sendo mais difícil determinar o sucesso da busca utilizado por analistas de vulnerabilidade.

Ataque de dicionário

Um ataque de dicionário é um método de cracking que consiste em tentar adivinhar uma senha provando todas as palavras do dicionário ou combinações de palavras. Este tipo de ataque costuma ser mais eficiente que um ataque de força bruta, já que muitos usuários costumam utilizar uma palavra existente em sua língua ou combinação de palavras como senha. Muitos usuário fazem isso para que a senha seja fácil de lembrar, o que não é uma prática recomendável.

Cavalo de troia

Malware cavalo de Tróia recebe esse nome devido a clássica história do cavalo de Tróia, pois ele imita a técnica de infectar computadores. Um cavalo de Tróia se ocultará em programas que parecem inofensivos, ou tentará enganá-lo para que você o instale.

Os cavalo de Tróia não se replicam ao infectar outros arquivos ou computadores. Em vez disso, eles sobrevivem ficando ocultos. Eles podem ficar silenciosos em seu computador, coletando informações ou configurando brechas em sua segurança, ou podem simplesmente controlar seu computador e bloquear seu acesso a ele

O que os cavalos de Tróia fazem?

Como os cavalos de Tróia são muito versáteis e passar desapercebidos, sua popularidade explodiu até eles se tornarem o malware favorito de muitos criminosos online.

Algumas das ações mais comuns que os cavalos de Tróia efetuam são:

Criar portas dos fundos: Os cavalos de Tróia normalmente alteram seu sistema de segurança de forma que outros malwares, ou mesmo um hacker, consigam invadir.

Espionar: alguns cavalos de Troia são essencialmente spyware projetado para aguardar até que você acesse suas contas online ou insira dados do seu cartão de crédito e depois enviar suas senhas e outros dados de volta ao seu mestre.

Transformar seu computador em um zumbi! às vezes, uma hacker não está interessado em você, mas quer usar seu computador como um escravo em uma rede sob seu controle.

Enviar mensagens caras de SMS: até mesmo smartphones pegam cavalos de Tróia e a maneira mais comum de criminosos ganharem dinheiro é usá-los para fazer seu telefone mandar mensagens caras de SMS para números especiais

Como me protejo dos cavalos de Tróia?
Ficar longe de sites questionáveis, materiais pirateados e links dúbios pode ajudar, mas, a longo prazo, algo escapará do seu controle.

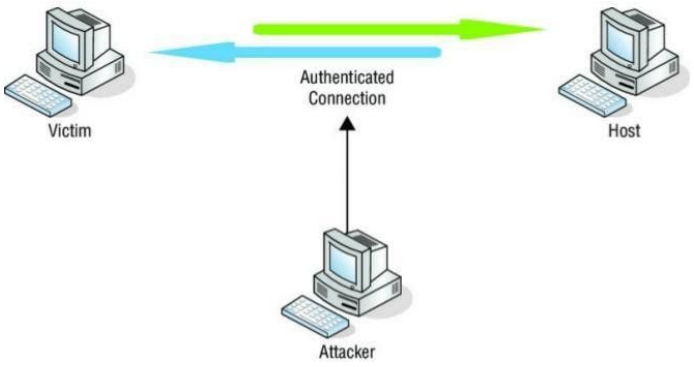
Se quiser realmente ficar protegido, será necessário um software anti malware (AntiVirus) para permanecer protegido.

Até mesmo especialistas em segurança contam com alguma forma de proteção para mantê-los em segurança. Você também deveria

Hijackers

Hijackers também chamados de spyware, os hijackers ("seqüestradores") são Cavalos de Tróia que modificam a página inicial do navegador e, muitas vezes, também direcionam toda página visitada para uma outra página escolhida pelo programador da praga. A ideia é vender os cliques que o usuário faz nessas páginas, o que gera lucro para o criador do hijacker.

O seqüestro de sessão é sinônimo de uma sessão roubada, na qual um invasor intercepta e assume uma sessão legitimamente estabelecida entre um usuário e um host. A relação usuário-host pode se aplicar ao acesso de qualquer recurso autenticado, como um servidor da Web, uma sessão Telnet ou outra conexão baseada em TCP. Os atacantes se colocam entre o usuário e o host, permitindo que eles monitorem o tráfego do usuário e lancem ataques específicos. Uma vez que aconteça um sequestro de sessão bem-sucedido, o invasor pode assumir o papel do usuário legítimo ou simplesmente monitorar o tráfego para injetar ou coletar pacotes específicos a fim de criar o efeito desejado.



Em seu sentido mais básico, uma sessão é um período de tempo acordado em que o estado conectado do cliente e do servidor é vetado e autenticado. Isso simplesmente significa que tanto o servidor quanto o cliente sabem (ou pensam que sabem) quem são, e com base nesse conhecimento, eles podem confiar que os dados enviados de qualquer forma acabarão nas mãos da parte apropriada.

- Hole: Um bug ou uma vulnerabilidade.
  Intrusion Detection System -IDS
  É um Sistema de Detecção de Intrusão, um software responsável por monitorar uma
  rede ou sistema e alertar sobre possíveis

- LAMMER:

É uma palavra que os hackers utilizam para identificar os indivíduos que se acham
hackers, mas estão ainda no estágio inicial de aprendizado.

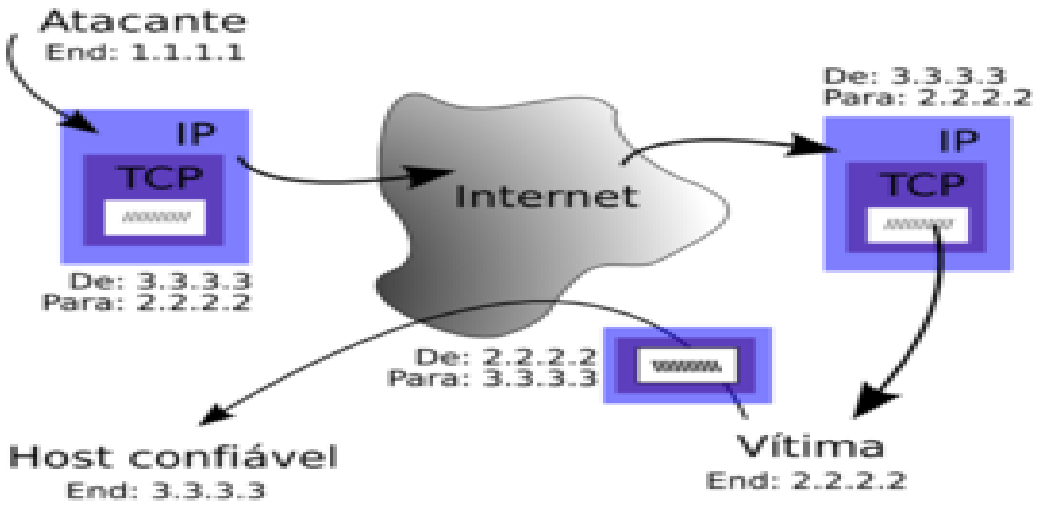
- Script Kiddie
  É o indivíduo que saiu do estágio de lammer mas que só sabe usar as "receitas de
  bolo", programas prontos e ainda não entende muito bem o que está fazendo.
- Trojan, Trojan Horse
  São os cavalos de tróia, programas que são entregues para o usuário de forma
  legítima (muitas vezes podem ser coisas interessantes como joguinhos, cartões
  virtuais, etc.), mas que internamente realizam ações maliciosas, tais como: gravar
  senhas, gravar toques de tecla, e posteriormente armazenar estas informações ou
  enviar para outra pessoa.

SNIFFERS

Os sniffers são ferramentas que interceptam e analisam o tráfego de uma rede, com ele você pode descobrir quais sites estão sendo acessados na rede, quais tipos de protocolos estão sendo usados (http, FTP, POP3, SMTP, etc) e até mesmo capturar senhas de sites com autenticação, como redes sociais, painéis administrativos, e mails, etc.

Hoje em dia existem vários e vários sniffers, alguns são simples e com poucos recursos, já outros são avançados e conseguem até mesmo importar arquivos e relatórios de outras ferramentas de análise de rede, dentre esses sniffers o que é mais usado e recomendável, sem dúvida alguma é o WireShark.

O site PenTestIT compilou um TOP 5 dos melhores sniffers gratuitos, veja abaixo a lista com o link para cada ferramenta:



Falsificação de um pacote: A cada pacote enviado estará geralmente associada uma resposta (do protocolo da camada superior) e essa será enviada para a vítima, pelo o atacante não pode ter conhecimento do resultado exato das suas ações — apenas uma previsão.

- Exploit
  Programas utilizados por hackers e crackers para explorar vulnerabilidades em determinados sistemas, conseguindo assim, acessos com maior privilégio.

- Back door:
  É um programa escondido, deixado por um intruso, o qual permite futuro acesso à máquina alvo. Este termo é um sinônimo para um termo mais antigo: trap door.

- Firewall
  Equipamento e/ou software utilizado para controlar as conexões (que entram ou saem) de uma rede. Eles podem simplesmente filtrar os pacotes baseados em regras simples, como também fornecer outras funções tais como: NAT, proxy, etc.

- Flood
  Sobrecarga (em geral, de pacotes) causada por eventos não esperados que causam lentidão da rede.
- Scanner
  Ferramenta utilizada por hackers ou especialistas em segurança que serve para "varrer" uma máquina ou uma rede, em busca de

portas abertas, informações ou
serviços vulneráveis

- Spoofing
  É uma forma de manter uma conexão com uma máquina se fazendo passar por outra na qual ela confie. Um termo muito utilizado é o IP Spoofing, que significa o uso de vulnerabilidades do Protocolo TCP/IP que permitem a ação descrita acima.
- Vulnerabilidade
  Estado de um componente de um sistema que compromete a segurança de todo o sistema, uma vulnerabilidade existe sempre, até que seja corrigida, existem vulnerabilidades que são intrínsecas ao sistema. Um ataque explora uma vulnerabilidade.
- Worm
  Um worm é semelhante a um vírus, mas difere pelo fato de não necessitar de um programa específico para se infectar e reproduzir. Muitos vírus hoje, possuem a característica de worms e vice e versa.

- Warez
  Nome utilizado por hackers para se referir a pirataria de software.
- Crack
  Programa utilizado para quebrar licenças de

outros programas. Também pode se referir a programas utilizados para quebrar senhas.

…….
