



Módulo 14: Ameaças e ataques comuns



CyberOps Associate v1.0

Prof. Clemilson Oliveira

clemilson.oliveira@edu.sc.senai.br



Objetivos do módulo

Título do módulo: Ameaças e ataques comuns

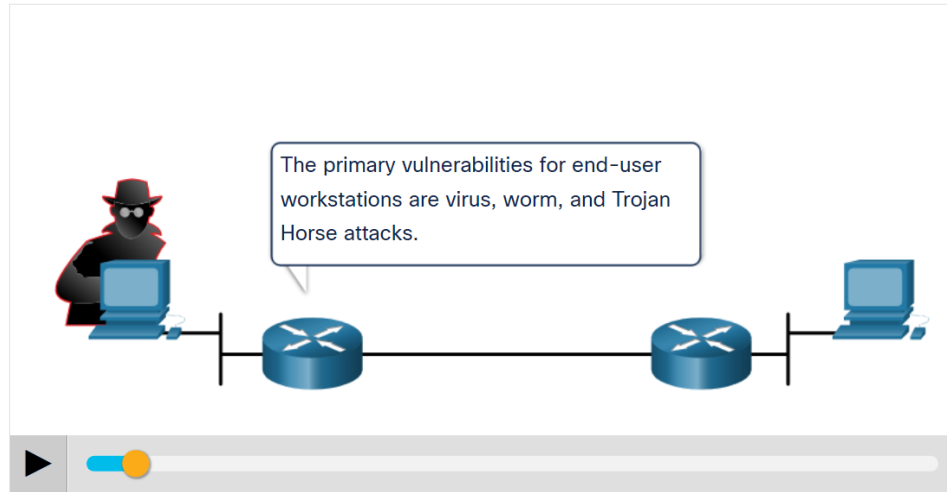
Objetivo do módulo: explicar os vários tipos de ameaças e ataques.

Título do Tópico	Objetivo do Tópico
Malware	Descrever os tipos de malware.
Ataques de rede comuns - reconhecimento, acesso e engenharia social	Explicar ataques de rede de reconhecimento, acesso e engenharia social.
Ataques de rede - negação de serviço, estouro de buffer e evasão	Explique os ataques de negação de serviço, estouro de buffer e evasão.

14.1 Malware

Ameaças e tipos de malware comuns

- Malware é um código ou software projetado para danificar, interromper, roubar ou infligir alguma outra ação "ruim" ou ilegítima em dados, hosts ou redes.
- Os três tipos mais comuns de malware são vírus, worm e cavalo de Tróia.
- Reproduza a animação para ver exemplos dos diferentes tipos de malware.



Vírus de ameaças e ataques comuns

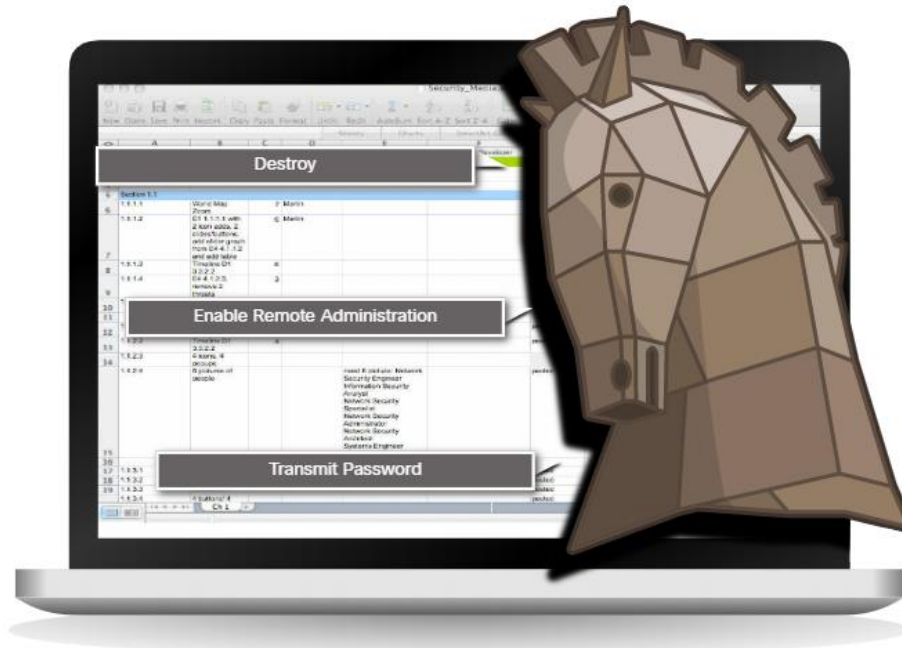
- Um vírus é um tipo de malware que se espalha inserindo uma cópia de si mesmo em outro programa.
- Depois que o programa é executado, os vírus se espalham de um computador para outro, infectando assim os computadores.
- Um vírus simples pode instalar-se na primeira linha de código em um arquivo executável.
- Os vírus podem ser inofensivos, para aqueles que exibem uma imagem na tela, ou podem ser destrutivos. Eles também podem modificar ou excluir arquivos no disco rígido.
- A maioria dos vírus espalhados por unidades de memória USB, CDs, DVDs, compartilhamentos de rede e e-mail. Os vírus de e-mail são um tipo comum de vírus.

Cavalos

- O malware Cavalo de Tróia é um software que parece ser legítimo, mas contém código malicioso que explora os privilégios do usuário que o executa.
- Os cavalos de Tróia são encontrados anexados a jogos online.
- Os usuários são comumente induzidos a carregar e executar o cavalo de Tróia em seus sistemas
- O conceito do cavalo de Tróia é flexível.
- Pode causar danos imediatos, fornecer acesso remoto ao sistema ou acesso através de uma porta traseira.
- Cavalos de Tróia escritos sob medida com um alvo específico são difíceis de detectar.

Classificação de Cavalos de Tróia e Ataques comuns

- Os cavalos de Tróia são geralmente classificados de acordo com os danos que causam, ou a maneira pela qual violam um sistema.



Classificação de Cavalos de Tróia de Ameaças e Ataques Comuns

Os tipos de cavalos de Tróia são os seguintes:

Tipo do Cavalo de Troia	Descrição
Acesso remoto	Permite acesso remoto não autorizado.
Envio de dados	Fornece ao agente da ameaça dados confidenciais, como senhas.
Destrutivo	Corrupta ou exclui arquivos.
Proxy	Usa o computador da vítima como dispositivo de origem para lançar ataques e realizar outras atividades ilegais.
FTP	Habilita serviços de transferência de arquivos não autorizados em dispositivos finais.
Desativador do software de segurança	Impede o funcionamento de programas antivírus ou firewalls.
Negação de Serviço (DoS)	Retarda ou interrompe a atividade da rede.
Agentes de log de digitação	Tenta ativamente roubar informações confidenciais, como números de cartão de crédito, gravando as teclas digitadas em um formulário da web.

vermes comuns

- Os worms de computador são semelhantes aos vírus porque se replicam explorando vulnerabilidades nas redes de forma independente.
- Os worms podem retardar as redes à medida que se espalham de sistema para sistema.
- Os vermes podem ser colocados sem um host do programa.
- No entanto, uma vez que o host é infectado, o worm se espalha rapidamente pela rede.
- Em 2001, o worm Code Red infectou inicialmente 658 servidores. Em 19 horas, o worm infectou mais de 300.000 servidores.



Infecção de worm de código vermelho inicial



Infecção por código vermelho 19 horas depois

Worms (cont.)

- A infecção inicial do worm SQL Slammer é conhecida como o worm que comeu a internet.
- O SQL Slammer foi um ataque de Negação de Serviço (DoS) que explorava um bug de estouro de buffer no SQL Server da Microsoft.
- O número de servidores infectados dobrou de tamanho a cada 8,5 segundos.
- Os servidores infectados não tinham o patch atualizado lançado 6 meses antes.
- Por isso, é essencial que as organizações implementem uma política de segurança que exija que atualizações e patches sejam aplicados em tempo hábil.



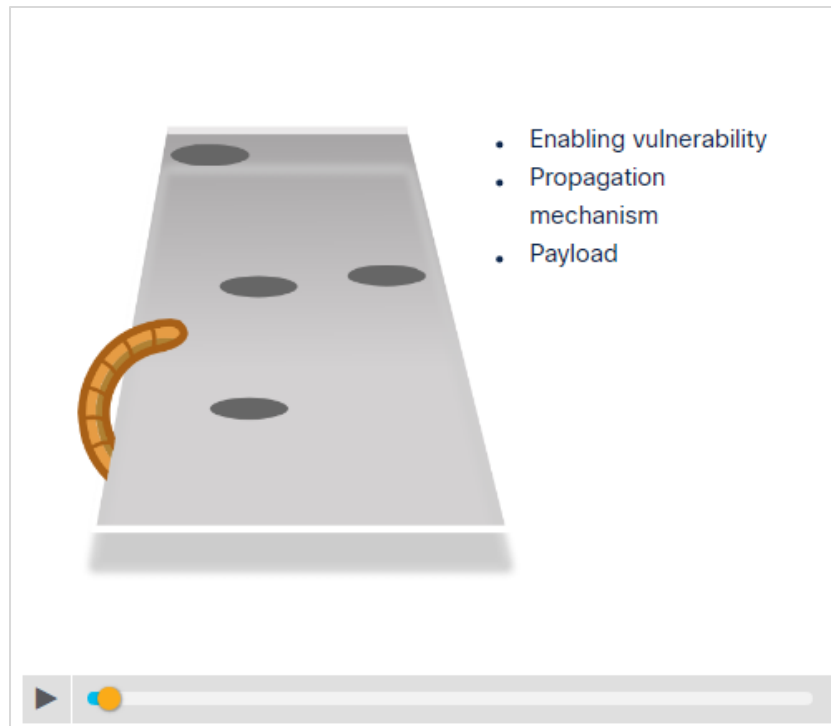
Infecção inicial do SQL Slammer



Infecção SQL Slammer 30 minutos depois

Ameaças comuns e componentes de worms de ataque

Clique em Reproduzir na figura para visualizar os três componentes dos ataques de worm.



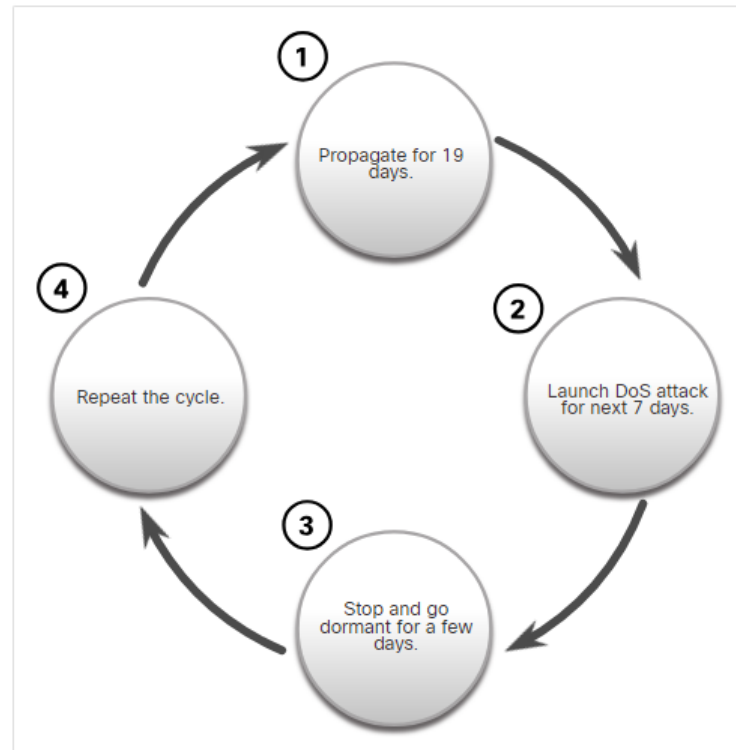
Componentes comuns do worm de ameaças e ataques (Cont.)

Os três componentes do worm são os seguintes:

- **Habilitando vulnerabilidade**- Um worm se instala usando um mecanismo de exploração, como um anexo de e-mail, um arquivo executável ou um cavalo de Tróia, em um sistema vulnerável.
- **Mecanismo de propagação**- Depois de obter acesso a um dispositivo, o worm se replica e localiza novos alvos.
- **Payload**- Qualquer código malicioso que resulte em alguma ação é uma carga útil. Na maioria das vezes, isso é usado para criar um backdoor que permite que um ator de ameaça acesse o host infectado ou crie um ataque DoS.

Componentes comuns do worm de ameaças e ataques (Cont.)

- Worms são programas autônomos que atacam um sistema para explorar uma vulnerabilidade conhecida.
- Após a exploração bem-sucedida, o worm se copia do host atacante para o sistema recém-explorado e o ciclo começa novamente.
- Esse mecanismo de propagação é comumente implantado de uma forma difícil de detectar.
- **Observação:** Worms nunca param de se espalhar na internet. Depois de serem liberados, os vermes continuam a se propagar até que todas as fontes possíveis de infecção sejam devidamente corrigidos.



Propagação de Worm Vermelho

© 2016 Cisco e/ou suas afiliadas. Todos os direitos reservados.
Confidencial da Cisco

Ransomware de ameaças e ataques comuns

- Ransomware é um malware que nega acesso ao sistema de computador infectado ou aos seus dados.
- Ransomware usa frequentemente um algoritmo de criptografia para criptografar arquivos e dados do sistema.
- Email e publicidade maliciosa, também conhecidos como malvertising, são vetores para campanhas de ransomware.
- A engenharia social também é usada, quando criminosos cibernéticos fingindo ser técnicos de segurança fazem chamadas aleatórias em casas e persuadem os usuários a se conectar a um site que baixa ransomware para o computador do usuário.

Ameaças e ataques comuns a outros malwares

Os exemplos de malware moderno são os seguintes:

Tipo de Malware	Descrição
Scareware	Inclui software fraudulento que usa engenharia social para chocar ou induzir ansiedade criando a percepção de uma ameaça. Ele geralmente é direcionado a um usuário desavisado e tenta persuadir o usuário a infectar um computador, tomando medidas para resolver a ameaça falsa.
Phishing	Tenta convencer as pessoas a divulgar informações confidenciais. Exemplos incluem o recebimento de um e-mail do banco solicitando que os usuários divulguem suas contas e números PIN.
Rootkits	Instalado em um sistema comprometido. Depois de ser instalado, ele continua a ocultar sua intrusão e fornecer acesso privilegiado ao ator da ameaça.
Spyware	Usado para coletar informações sobre um usuário e enviar as informações para outra entidade sem o consentimento do usuário. Spyware pode ser um monitor de sistema, cavalo de Tróia, Adware, cookies de rastreamento e keyloggers.
Adware	Exibe pop-ups irritantes para gerar receita para seu autor. O malware pode analisar os interesses do usuário rastreando os sites visitados. Em seguida, ele pode enviar anúncios pop-ups relacionados a esses sites.

comuns Comportamentos de malware

- Os computadores infectados com malware geralmente apresentam um ou mais dos seguintes sintomas:
 - Aparência de arquivos, programas ou ícones da área de trabalho estranhos
 - Programas antivírus e de firewall estão desativando ou reconfigurando configurações
 - A tela do computador está congelando ou o sistema está travando
 - E-mails são enviados espontaneamente sem o seu conhecimento para a sua lista de contatos
 - Os arquivos foram modificados ou excluídos
 - Maior uso da CPU e/ou da memória
 - Problemas de conexão a redes
 - Velocidade lenta do computador ou do navegador da Web
 - Processos ou serviços desconhecidos em execução
 - Portas TCP ou UDP desconhecidas abertas
 - Conexões são feitas para hosts na Internet sem ação do usuário
 - Comportamento estranho do
- **Observação:** o comportamento de malware não se limita à lista acima.

Laboratório de ameaças e ataques comuns — Anatomia do malware

Neste laboratório, você pesquisará e analisará alguns malwares recentes.

14.2 Ataques de rede comuns - reconhecimento, acesso e engenharia social

Ataques de rede comuns - tipos de ataques de rede de reconhecimento, acesso e engenharia social

- Malware é um meio de obter uma carga útil entregue.
- Quando uma carga útil é entregue e instalada, ela pode ser usada para causar uma variedade de ataques relacionados à rede, tanto internos quanto externos.
- Os ataques de rede são classificados em três categorias:
 - Ataques de Reconhecimento
 - Ataques de Acesso
 - Ataques de DoS

Ataques de rede comuns - ataques de reconhecimento, acesso e engenharia social

- Reconhecimento é coleta de informações.
- Os atores de ameaças usam ataques de reconhecimento (ou recon) para fazer descobertas e mapeamentos não autorizados de sistemas, serviços ou vulnerabilidades.
- Os ataques Recon precedem ataques de acesso ou ataques DoS.

reconhecimento, acesso e engenharia social (cont.)

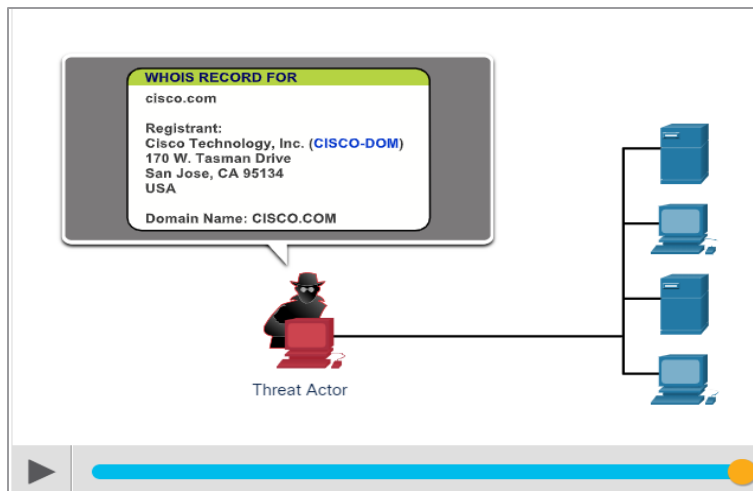
As técnicas usadas por agentes de ameaças maliciosas para realizar ataques de reconhecimento são as seguintes:

Técnicas	Descrição
Executar uma consulta de informações de um alvo	O agente da ameaça está procurando informações iniciais sobre um alvo. Várias ferramentas podem ser usadas, incluindo a pesquisa no Google, o site das organizações, whois e muito mais.
Iniciar uma varredura de ping da rede de destino	A consulta de informações geralmente revela o endereço de rede do alvo. O agente de ameaça agora pode iniciar uma varredura de ping para determinar quais endereços IP estão ativos.
Iniciar uma verificação de porta nos endereços IP ativos	Isso é usado para determinar quais portas ou serviços estão disponíveis. Exemplos de scanners de portas incluem Nmap, SuperScan, Angry IP Scanner e NetScanTools.
Execute o scanner de vulnerabilidades	Isso é para consultar as portas identificadas para determinar o tipo e a versão do aplicativo e do sistema operacional que está sendo executado no host. Exemplos de ferramentas incluem Nipper, Secuna PSI, Core Impact, Nessus v6, SAINT e Open VAS.
Execute ferramentas de exploração	O agente de ameaças agora tenta descobrir serviços vulneráveis que podem ser explorados. Existe uma variedade de ferramentas de exploração de vulnerabilidades, incluindo Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit e Netsparker.

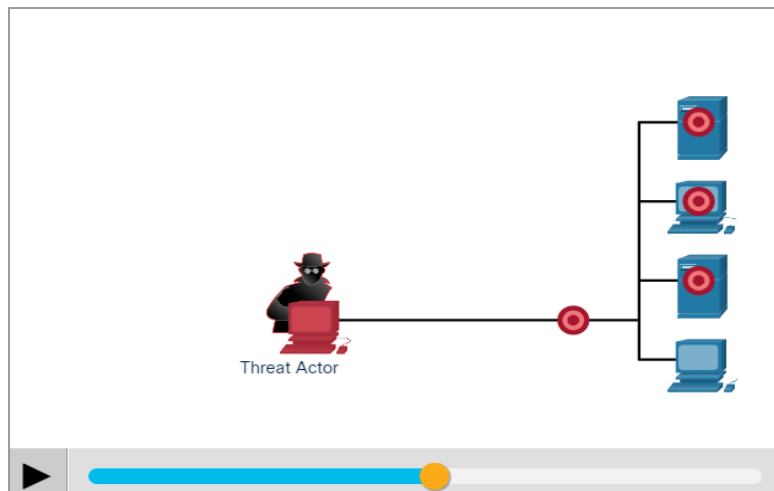
Ataques de rede comuns - Ataques de reconhecimento, acesso e engenharia social (cont.)

Consultas de informações da Internet:

Clique em Reproduzir na figura para ver uma animação de um ator de ameaça usando o comando who is para encontrar informações sobre um alvo.

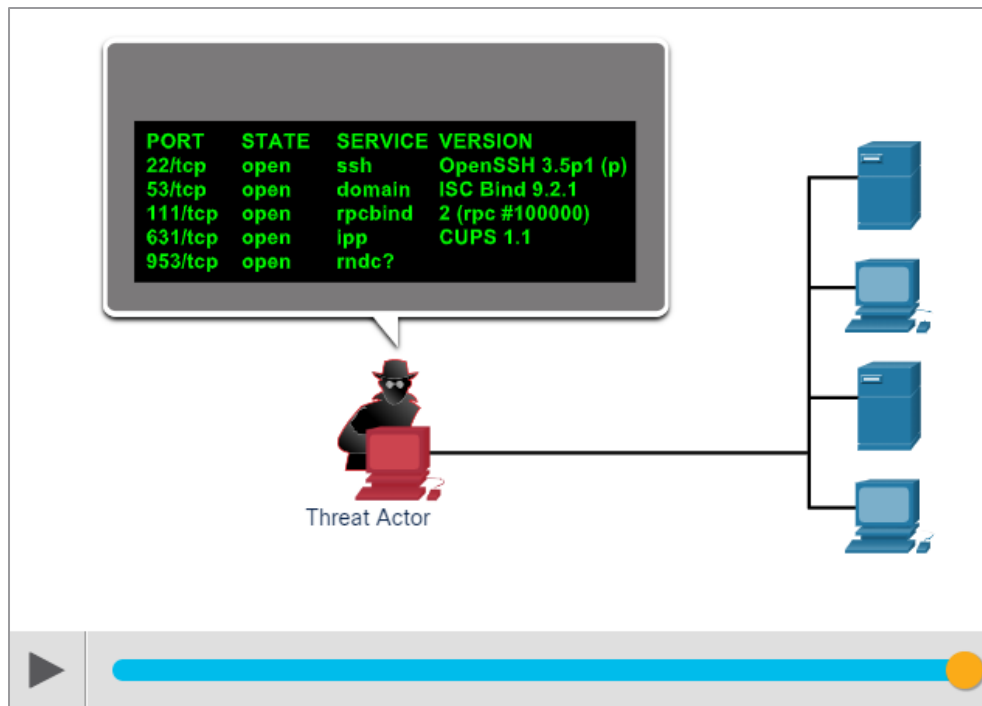


Execução da varredura de ping: Clique em Reproduzir na figura para visualizar uma animação de um ator de ameaça fazendo uma varredura de ping do endereço de rede do alvo para descobrir endereços IP ativos e ativos.



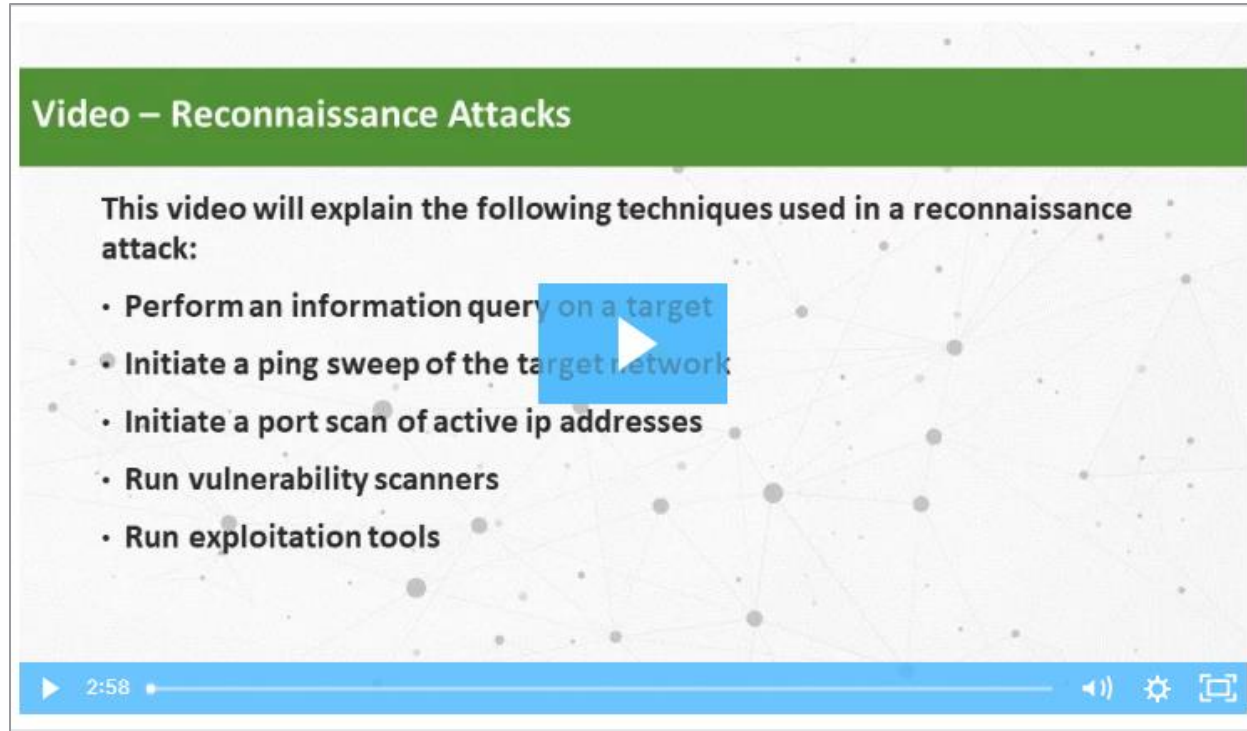
Ataques de rede comuns - Ataques de reconhecimento, acesso e engenharia social (cont.)

Executando a varredura da porta: Clique em Reproduzir na figura para ver uma animação de um ator de ameaça executando uma varredura de porta nos endereços IP ativos descobertos usando Nmap.



Vídeo - Ataques de reconhecimento

Assista ao vídeo para saber mais sobre as diferentes técnicas em um ataque de reconhecimento.



Video – Reconnaissance Attacks

This video will explain the following techniques used in a reconnaissance attack:

- Perform an information query on a target
- Initiate a ping sweep of the target network
- Initiate a port scan of active ip addresses
- Run vulnerability scanners
- Run exploitation tools

2:58

servados.

Ataques de reconhecimento, acesso e engenharia social

- Os ataques de acesso exploram vulnerabilidades conhecidas em serviços de autenticação, serviços de FTP e serviços da web para obter acesso a contas da web, bancos de dados confidenciais e outras informações confidenciais.

Ataques de senha

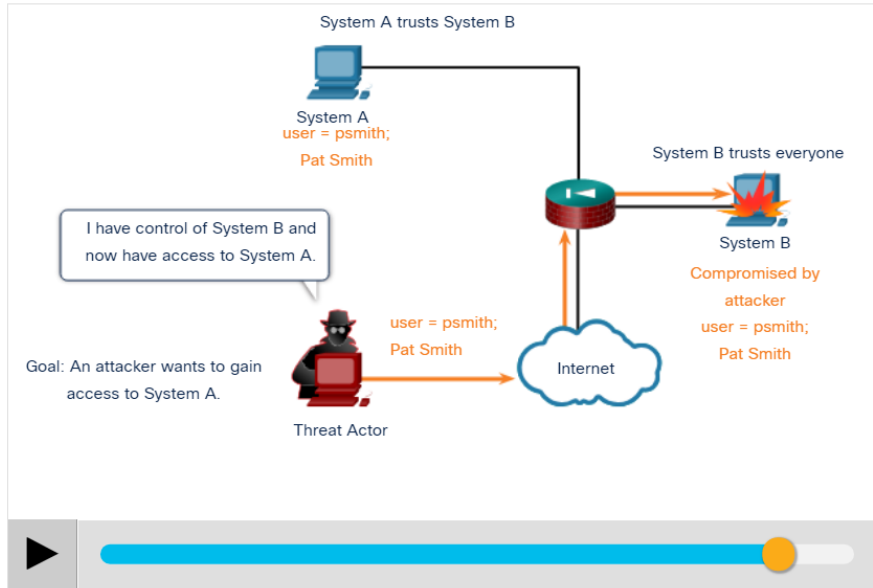
- O ator da ameaça tenta descobrir senhas críticas do sistema usando uma variedade de ferramentas de quebra de senha.

Ataques de falsificação (spoofing)

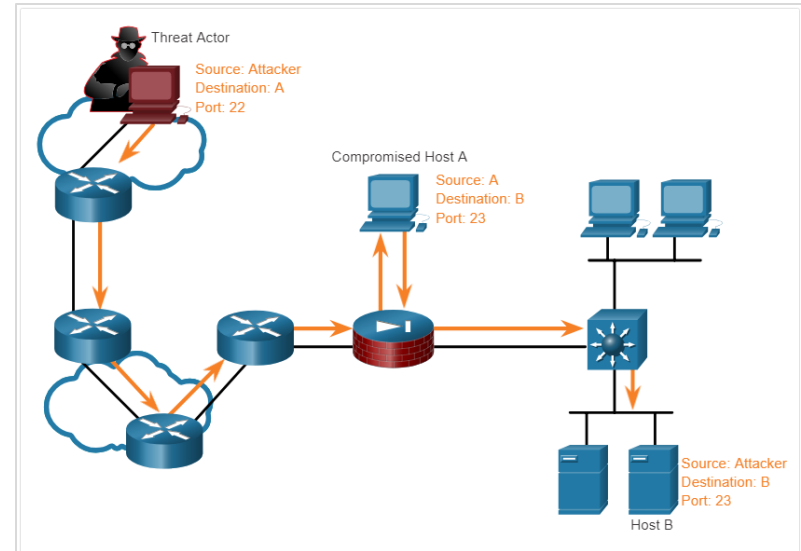
- O dispositivo do ator da ameaça tenta se passar por outro dispositivo falsificando dados.
- Ataques comuns incluem falsificação IP (IP spoofing), falsificação MAC (MAC spoofing), e falsificação DHCP (DHCP spoofing).
 - Exploração de confiança
 - Redirecionamento de porta
 - ataque man in the middle
 - ataque de saturação do buffer

Ataque de acesso (Cont.)

Exemplo de exploração de confiança: Clique em Executar na figura para ver um exemplo de exploração de confiança.

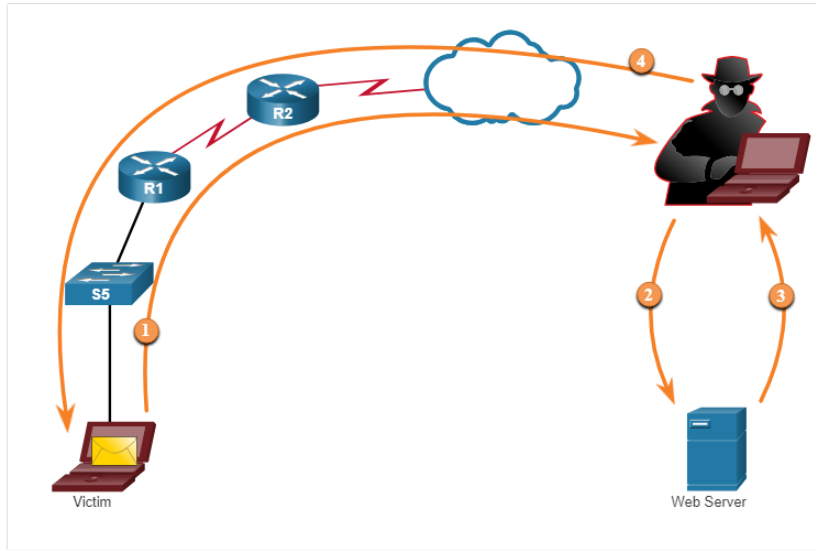


Redirecionamento de porta Exemplo: O exemplo mostra um agente de ameaça usando SSH (porta 22) para se conectar a um Host A comprometido confiável pelo Host B. Portanto, o agente de ameaça pode usar Telnet (porta 23) para acessá-lo.

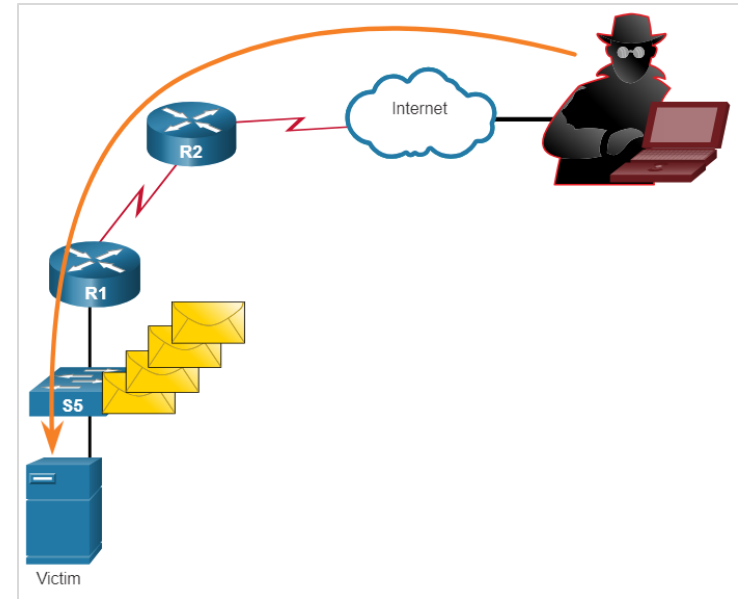


Ataque de acesso (Cont.)

Man-in-the-Middle Exemplo de ataque A figura mostra um exemplo de ataque man-in-the-middle.



Ataque de Buffer Overflow A figura mostra que o agente da ameaça está enviando muitos pacotes para a vítima em uma tentativa de estourar o buffer da vítima.



Vídeo - Ataques de acesso e engenharia social

Assista ao vídeo para ver a demonstração dos tipos de acesso e ataques de engenharia social.



Ataques de engenharia social

- Engenharia Social é um ataque de acesso que tenta manipular os indivíduos para que realizem ações ou divulguem informações confidenciais.
- Algumas técnicas de engenharia social são realizadas pessoalmente ou por telefone ou internet.
- Técnicas de engenharia social são explicadas na tabela abaixo.

Ataques de engenharia social	Descrição
Pretexting	Um ator de ameaça finge precisar de dados pessoais ou financeiros para confirmar a identidade do destinatário.
Phishing	Um agente de ameaças envia e-mails fraudulentos, disfarçados de fontes legítimas e confiáveis, para induzir o destinatário a instalar malware em seu dispositivo ou compartilhar informações pessoais ou financeiras.
Spear phishing	Um agente de ameaça cria um ataque de phishing direcionado, personalizado para um indivíduo ou organização específico.
Spam	Também conhecido como lixo eletrônico, este é um e-mail não solicitado que geralmente contém links prejudiciais, malware ou conteúdo enganoso.

Ataques de engenharia social (cont.)

Ataques de engenharia social	Descrição
Algo por Algo	Às vezes chamado de “quid pro quo”, é quando um ator de ameaça solicita informações pessoais de uma parte em troca de algo como um presente.
Iscas	Um agente de ameaça deixa uma unidade flash infectada por malware em um local público. Uma vítima encontra a unidade e a insere inconscientemente em seu laptop, instalando involuntariamente malware.
Representação	Nesse tipo de ataque, um ator de ameaça finge ser outra pessoa para ganhar a confiança da vítima.
Tailgating	É aqui que um agente de ameaças segue rapidamente uma pessoa autorizada para um local seguro para obter acesso a uma área segura.
Navegação bisbilhoteira	É aqui que um ator de ameaça olha discretamente por cima do ombro de alguém para roubar suas senhas ou outras informações.
Busca de informações na lixeira	É aqui que um ator de ameaças vasculha latas de lixo para descobrir documentos confidenciais.

Ataques de engenharia social (cont.)

- O Social Engineer Toolkit (SET) foi projetado para ajudar hackers de chapéu branco e outros profissionais de segurança de rede a criar ataques de engenharia social para testar suas próprias redes.
- As empresas devem educar seus usuários sobre os riscos da engenharia social e desenvolver estratégias para validar identidades por telefone, via email ou pessoalmente.



Práticas de proteção de engenharia social

Fortalecendo o elo mais fraco

- A segurança cibernética é tão forte quanto o seu elo mais fraco.
- O elo mais fraco na segurança cibernética pode ser o pessoal dentro de uma organização, e a engenharia social é uma grande ameaça à segurança.
- Uma das medidas de segurança mais eficazes que uma organização pode tomar é treinar seu pessoal e criar uma “cultura consciente da segurança”.

Ataques de rede comuns - reconhecimento, acesso e engenharia social

Laboratório - Engenharia Social

Neste laboratório, você pesquisará exemplos de engenharia social e identificará maneiras de reconhecê-lo e evitá-lo.

14.3 Ataques de rede - negação de serviço, estouros de buffer e evasão

Vídeo - Ataques de negação de serviço

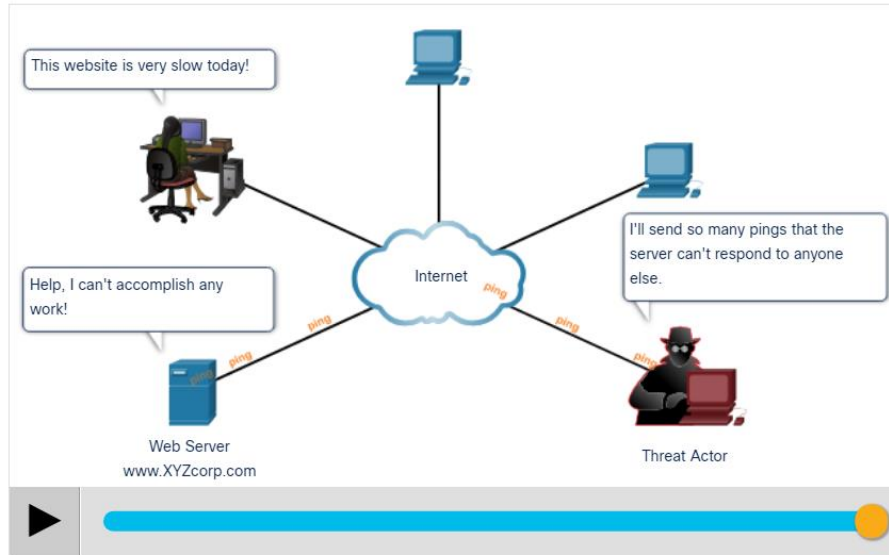
Assista ao vídeo para saber mais sobre ataques de negação de serviço.



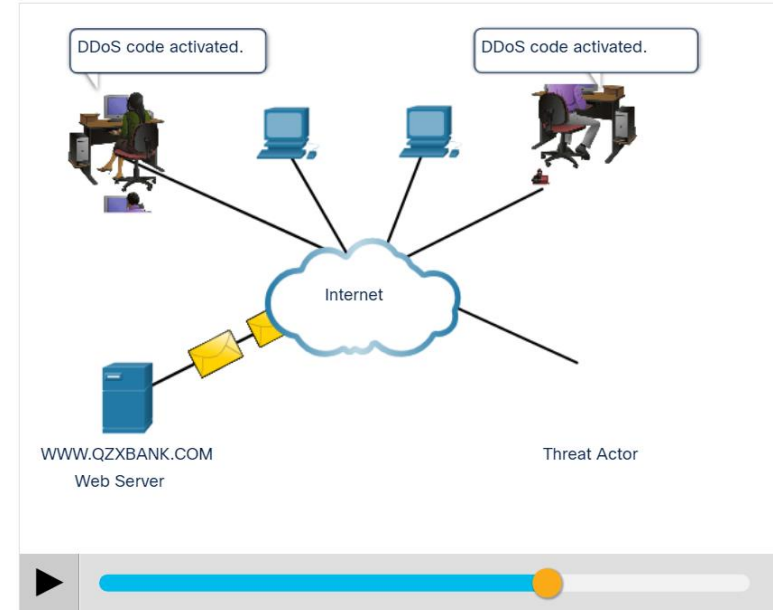
Ataques de rede - negação de serviço, estouros de buffer e evasão

Ataques DoS e DDoS (continuação)

Ataque DoS: Clique em Reproduzir na figura para ver a animação de um ataque DoS.



Ataque DDoS: Clique em Reproduzir na figura para ver as animações de um ataque DDoS.



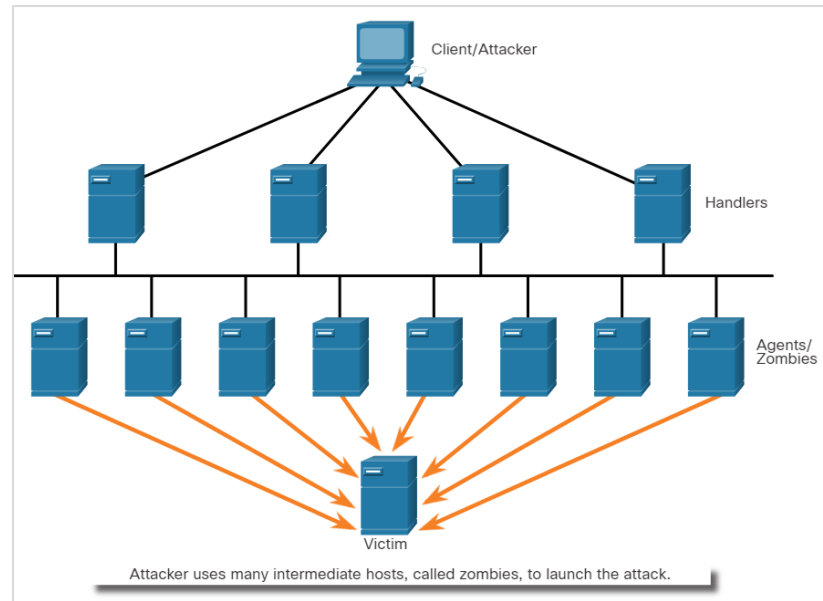
Ataques DoS e DDoS

- Um ataque de negação de serviço (DoS) cria algum tipo de interrupção nos serviços de rede para usuários, dispositivos ou aplicativos. Os dois tipos de ataques DoS são os seguintes:
- **Grande quantidade de tráfego** - O agente de ameaças envia uma enorme quantidade de dados a uma taxa que a rede, host ou aplicativo não pode manipular.
- **Pacotes formatados de forma maliciosa** - o agente de ameaça envia um pacote formatado de forma maliciosa a um host ou aplicativo e o receptor não consegue lidar com ele.

Componentes de ataques DDoS

Os termos a seguir são usados para descrever os componentes de um DDoS:

Componente	Descrição
zumbis	Um grupo de anfitriões comprometidos. Esses hosts executam código malicioso.
bots	Os bots são malware projetado para infectar um host e se comunicar com um sistema manipulador.
botnet	Um grupo de zumbis que foram infectados usando malware auto-propagado e são controlados por manipuladores.
handlers	Um servidor mestre de comando e controle (CNC ou C2) que controla grupos de zumbis.
Botmaster	Habilita serviços de transferência de arquivos não autorizados em dispositivos finais.



Demonstração de vídeo - Mirai Botnet

- Mirai é um malware que direcionou dispositivos IoT configurados com informações de login padrão.
- O botnet foi usado como parte de um ataque de negação de serviço distribuído (DDoS).

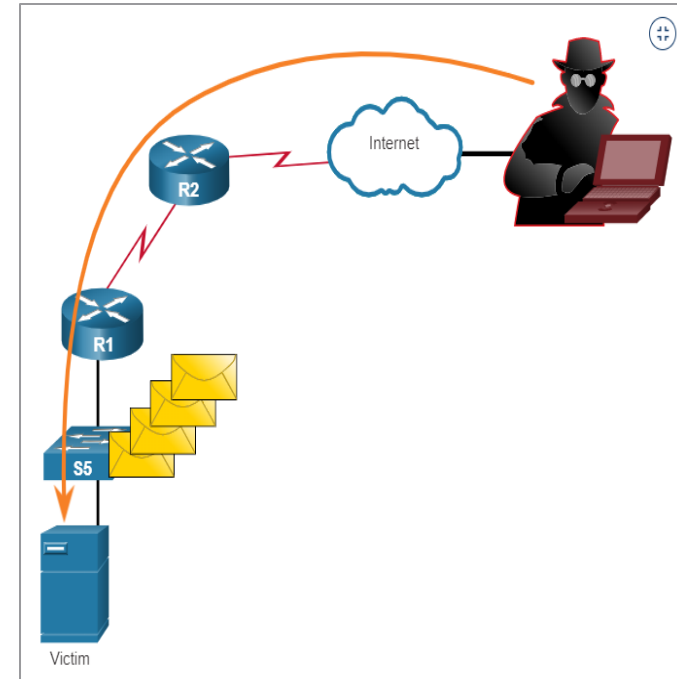
Ataques de rede - Demonstração de vídeo de negação de serviço, estouros de buffer e evasão — Mirai Botnet (Cont.)

Reproduza o vídeo para ver uma demonstração de como um ataque DDoS baseado em botnet torna os serviços indisponíveis.



Ataque de estouro de buffer

- O ator de ameaça usa o ataque DoS de estouro de buffer para localizar uma falha relacionada à memória do sistema em um servidor e explorá-la.
- Por exemplo, uma vulnerabilidade de ataque remoto de negação de serviço foi descoberta no Microsoft Windows 10, onde o ator de ameaça criou código mal-intencionado para acessar memória fora do escopo.
- Outro exemplo é **ping of death**, em que um ator ameaça envia um ping de morte, que é uma solicitação de eco em um pacote IP que é maior que o tamanho máximo do pacote.
- O host receptor não pode lidar com um tamanho de pacote e ele iria falhar.
- **Observação:** Estima-se que um terço dos ataques mal-intencionados sejam o resultado de estouros de buffer.



Métodos de Evasão

Os métodos de evasão usados pelos atores da ameaça incluem:

Método de Evasão	Descrição
Criptografia e encapsulamento	Essa técnica de evasão usa tunelamento para ocultar, ou criptografia para embaralhar, arquivos de malware. Isso torna difícil para muitas técnicas de detecção de segurança detectar e identificar o malware. Tunelamento pode significar ocultar dados roubados dentro de pacotes legítimos.
Esgotamento de recursos	Essa técnica de evasão torna o host de destino muito ocupado para usar corretamente técnicas de detecção de segurança.
Fragmentação do tráfego	Essa técnica de evasão divide uma carga maliciosa em pacotes menores para ignorar a detecção de segurança de rede. Depois que os pacotes fragmentados ignoram o sistema de detecção de segurança, o malware é remontado e pode começar a enviar dados confidenciais para fora da rede.

Métodos de evasão (cont.)

Método de Evasão	Descrição
Interpretação errada no nível do protocolo	Essa técnica de evasão ocorre quando as defesas de rede não manipulam corretamente recursos de uma PDU como um valor de soma de verificação ou TTL. Isso pode enganar um firewall para ignorar pacotes que ele deve verificar.
Substituição de tráfego	Nesta técnica de evasão, o ator ameaça tenta enganar um IPS ofuscando os dados na carga útil. Isso é feito codificando-o em um formato diferente. Por exemplo, o ator de ameaça poderia usar tráfego codificado em Unicode em vez de ASCII. O IPS não reconhece o verdadeiro significado dos dados, mas o sistema final de destino pode ler os dados.
Inserção de tráfego	Semelhante à substituição de tráfego, mas o agente de ameaça insere bytes extras de dados em uma sequência maliciosa de dados. As regras do IPS perdem os dados maliciosos, aceitando a sequência completa de dados.

Ameaças comuns e ataques de rede - Negação de serviço, estouros de buffer e métodos de evasão (Cont.)

Método de Evasão	Descrição
Pivotando	Essa técnica pressupõe que o ator da ameaça comprometeu um host interno e deseja expandir seu acesso ainda mais para a rede comprometida. Um exemplo é um ator de ameaça que obteve acesso à senha de administrador em um host comprometido e está tentando fazer login em outro host usando as mesmas credenciais.
Rootkits	Um rootkit é uma ferramenta agressora complexa usada por atores experientes em ameaças. Ele se integra com os níveis mais baixos do sistema operacional. Quando um programa tenta listar arquivos, processos ou conexões de rede, o rootkit apresenta uma versão higienizada da saída, eliminando qualquer saída incriminadora. O objetivo do rootkit é ocultar completamente as atividades do atacante no sistema local.
Proxies	O tráfego de rede pode ser redirecionado através de sistemas intermediários para ocultar o destino final para dados roubados. Desta forma, comando-e-controle conhecido não ser bloqueado por uma empresa porque o destino proxy parece benigno. Além disso, se os dados estiverem sendo roubados, o destino dos dados roubados pode ser distribuído entre muitos proxies, não chamando a atenção para o fato de que um único destino desconhecido está servindo como destino para grandes quantidades de tráfego de rede.

14.4 Resumo de ameaças e ataques comuns

Resumo de Ameaças e Ataques Comuns

O que Aprendi neste Módulo?

- Malware é a abreviatura de software malicioso ou código malicioso.
- A maioria dos vírus são espalhados por unidades de memória USB, CDs, DVDs, compartilhamentos de rede e e-mail.
- Os cavalos de Tróia são encontrados em jogos online.
- Três tipos comuns de malware são vírus, worm e cavalo de Tróia.
- Os atores de ameaças também podem atacar a rede de fora.
- As três categorias principais são ataques de reconhecimento, acesso e DoS.
- Os ataques Recon precedem os ataques de acesso ou DoS.
- Os ataques de acesso exploram vulnerabilidades conhecidas em serviços de autenticação, serviços de FTP e serviços da Web.
- Os ataques DoS criam algum tipo de interrupção dos serviços de rede para usuários, dispositivos ou aplicativos.

O que Aprendi neste Módulo? (Continuação)

- Os ataques DDoS são semelhantes em intenção aos ataques DoS, exceto que o ataque DDoS aumenta em magnitude porque ele se origina de várias fontes coordenadas.
- Mirai é um malware que visa dispositivos IoT configurados com informações de login padrão.
- O objetivo de um ator de ameaça ao usar um ataque DoS de estouro de buffer é encontrar uma falha relacionada à memória do sistema em um servidor e explorá-la.

