# Introdução

13.0.1

## Por que devo cursar este módulo?

Quem está atacando nossa rede e por quê? Neste módulo, você aprenderá sobre white hats, grey hats, e black hats. Você também aprenderá sobre as técnicas e ferramentas usadas por esses “hackers”. Continue lendo para saber mais!

13.0.2

## O que vou aprender neste módulo?

**Título do módulo:** Atacantes e suas ferramentas

**Objetivo do módulo:** Explicar como as redes são atacadas.

| **Título do Tópico** | **Objetivo do Tópico** |
| --- | --- |
| Quem está atacando nossa rede | Explicar como as ameaças à rede evoluíram. |
| Ferramentas do agente da ameaça | Descrever os vários tipos de ferramentas de ataque usadas pelos agentes de ameaças. |

# Quem está atacando nossa rede?

13.1.1

## Ameaça, vulnerabilidade e risco

Estamos sob ataque e os atacantes querem acesso aos nossos bens. Os ativos são tudo de valor para uma organização, como dados e outras propriedades intelectuais, servidores, computadores, smartphones, tablets e muito mais.



Para entender melhor qualquer discussão sobre segurança de rede, é importante conhecer os seguintes termos:

| **Termo** | **Explicação** |
| --- | --- |
| **Ameaça** | Um perigo potencial para um ativo, como dados ou a própria rede. |
| **Vulnerabilidade** | Uma fraqueza em um sistema ou em seu design que pode ser explorada por uma ameaça. |
| **Superfície de ataque** | Uma superfície de ataque é a soma total das vulnerabilidades em um determinado sistema que são acessíveis a um invasor. A superfície de ataque descreve diferentes pontos em que um invasor pode entrar em um sistema e onde ele pode obter dados do sistema. Por exemplo, o sistema operacional e o navegador da Web podem precisar de patches de segurança. Cada um deles é vulnerável a ataques e está exposto na rede ou na internet. Juntos, eles criam uma superfície de ataque que o ator ameaça pode explorar. |
| **Exploit** | O mecanismo que é usado para alavancar uma vulnerabilidade para comprometer um ativo. As explorações podem ser remotas ou locais. Uma exploração remota é aquela que funciona através da rede sem qualquer acesso prévio ao sistema de destino. O invasor não precisa de uma conta no sistema final para explorar a vulnerabilidade. Em uma exploração local, o ator de ameaça tem algum tipo de acesso administrativo ou de usuário ao sistema final. Uma exploração local não significa necessariamente que o invasor tenha acesso físico ao sistema final. |
| **Risco** | A probabilidade de uma determinada ameaça explorar uma vulnerabilidade específica de um ativo e resultar em uma consequência indesejável. |

A gestão de riscos é o processo que equilibra os custos operacionais de provisão de medidas de proteção com os ganhos obtidos através da proteção do ativo. Existem quatro maneiras comuns de gerenciar o risco, como mostrado na tabela:

| **Estratégia de gestão de riscos** | **Explicação** |
| --- | --- |
| **Aceitação de riscos** | Isso ocorre quando o custo das opções de gerenciamento de risco supera o custo do próprio risco. O risco é aceito, e nenhuma ação é tomada. |
| **Prevenção de riscos** | Isto significa evitar qualquer exposição ao risco eliminando a atividade ou dispositivo que apresenta o risco. Ao eliminar uma atividade para evitar riscos, todos os benefícios possíveis da atividade também são perdidos. |
| **Redução de risco** | Isto reduz a exposição ao risco ou reduz o impacto do risco, tomando medidas para diminuir o risco. É a estratégia de mitigação de riscos mais utilizada. Essa estratégia requer uma avaliação cuidadosa dos custos de perda, da estratégia de mitigação e dos benefícios obtidos com a operação ou atividade que está em risco. |
| **transferência de risco** | Parte ou todo o risco é transferido para um terceiro disposto, como uma companhia de seguros. |

Outros termos de segurança de rede comumente usados incluem:

* **Contramedida** — As ações que são tomadas para proteger ativos, atenuando uma ameaça ou reduzindo o risco.
* **Impacto** - O dano potencial à organização causado pela ameaça.

**Observação:** uma exploração local requer acesso interno à rede, como um usuário com uma conta na rede. Uma exploração remota não requer uma conta na rede para explorar a vulnerabilidade dessa rede.

[Ir para o conteúdo](https://contenthub.netacad.com/cyberops/13.0.1?lng=pt-br#chunks-container)

*                                        
*                             

1. Invasores e suas ferramentas
2. Quem está atacando nossa rede?

# Quem está atacando nossa rede?

13.1.1

## Ameaça, vulnerabilidade e risco

Estamos sob ataque e os atacantes querem acesso aos nossos bens. Os ativos são tudo de valor para uma organização, como dados e outras propriedades intelectuais, servidores, computadores, smartphones, tablets e muito mais.



Para entender melhor qualquer discussão sobre segurança de rede, é importante conhecer os seguintes termos:

| **Termo** | **Explicação** |
| --- | --- |
| **Ameaça** | Um perigo potencial para um ativo, como dados ou a própria rede. |
| **Vulnerabilidade** | Uma fraqueza em um sistema ou em seu design que pode ser explorada por uma ameaça. |
| **Superfície de ataque** | Uma superfície de ataque é a soma total das vulnerabilidades em um determinado sistema que são acessíveis a um invasor. A superfície de ataque descreve diferentes pontos em que um invasor pode entrar em um sistema e onde ele pode obter dados do sistema. Por exemplo, o sistema operacional e o navegador da Web podem precisar de patches de segurança. Cada um deles é vulnerável a ataques e está exposto na rede ou na internet. Juntos, eles criam uma superfície de ataque que o ator ameaça pode explorar. |
| **Exploit** | O mecanismo que é usado para alavancar uma vulnerabilidade para comprometer um ativo. As explorações podem ser remotas ou locais. Uma exploração remota é aquela que funciona através da rede sem qualquer acesso prévio ao sistema de destino. O invasor não precisa de uma conta no sistema final para explorar a vulnerabilidade. Em uma exploração local, o ator de ameaça tem algum tipo de acesso administrativo ou de usuário ao sistema final. Uma exploração local não significa necessariamente que o invasor tenha acesso físico ao sistema final. |
| **Risco** | A probabilidade de uma determinada ameaça explorar uma vulnerabilidade específica de um ativo e resultar em uma consequência indesejável. |

A gestão de riscos é o processo que equilibra os custos operacionais de provisão de medidas de proteção com os ganhos obtidos através da proteção do ativo. Existem quatro maneiras comuns de gerenciar o risco, como mostrado na tabela:

| **Estratégia de gestão de riscos** | **Explicação** |
| --- | --- |
| **Aceitação de riscos** | Isso ocorre quando o custo das opções de gerenciamento de risco supera o custo do próprio risco. O risco é aceito, e nenhuma ação é tomada. |
| **Prevenção de riscos** | Isto significa evitar qualquer exposição ao risco eliminando a atividade ou dispositivo que apresenta o risco. Ao eliminar uma atividade para evitar riscos, todos os benefícios possíveis da atividade também são perdidos. |
| **Redução de risco** | Isto reduz a exposição ao risco ou reduz o impacto do risco, tomando medidas para diminuir o risco. É a estratégia de mitigação de riscos mais utilizada. Essa estratégia requer uma avaliação cuidadosa dos custos de perda, da estratégia de mitigação e dos benefícios obtidos com a operação ou atividade que está em risco. |
| **transferência de risco** | Parte ou todo o risco é transferido para um terceiro disposto, como uma companhia de seguros. |

Outros termos de segurança de rede comumente usados incluem:

* **Contramedida** — As ações que são tomadas para proteger ativos, atenuando uma ameaça ou reduzindo o risco.
* **Impacto** - O dano potencial à organização causado pela ameaça.

**Observação:** uma exploração local requer acesso interno à rede, como um usuário com uma conta na rede. Uma exploração remota não requer uma conta na rede para explorar a vulnerabilidade dessa rede.

13.1.2

## Hacker vs. Ameaças

Como sabemos, “hacker” é um termo comum usado para descrever um ator de ameaça. No entanto, o termo “hacker” tem uma variedade de significados, como se segue:

* Um programador inteligente capaz de desenvolver novos programas e codificar alterações em programas existentes para torná-los mais eficientes.
* Um profissional de rede que usa habilidades sofisticadas de programação para garantir que as redes não sejam vulneráveis a ataques.
* Uma pessoa que tenta obter acesso não autorizado a dispositivos na internet.
* Um indivíduo que executa programas para impedir ou retardar o acesso à rede a um grande número de usuários, ou corromper ou eliminar dados em servidores.

A figura mostra que existem hackers White, Gray e Black Hat. O hacker de chapéu branco é identificado como 1, chapéu cinza 2 e chapéu preto 3.

Hackers de Chapéu Cinza

Hackers de Chapéu Preto

Hackers de Chapéu Branco

Conforme mostrado na figura, os termos White hat, Gray hat e Black hat são freqüentemente usados para descrever hackers.

1. Os hackers White Hat são hackers éticos que usam suas habilidades de programação para propósitos bons, éticos e legais. Eles podem realizar testes de penetração de rede na tentativa de comprometer redes e sistemas, usando seu conhecimento de sistemas de segurança de computador para descobrir vulnerabilidades de rede. As vulnerabilidades de segurança são relatadas aos desenvolvedores e equipes de segurança que tentam consertar a vulnerabilidade antes que ela possa ser explorada. Algumas organizações concedem prêmios ou recompensas a hackers White hat quando fornecem informações que ajudam a identificar vulnerabilidades.
2. Hackers Gray Hat são indivíduos que cometem crimes e fazem coisas possivelmente antiéticas, mas não para ganho pessoal ou para causar danos. Um exemplo seria alguém que compromete uma rede sem permissão e, em seguida, divulga a vulnerabilidade publicamente. Hackers Gray hat podem revelar uma vulnerabilidade para a organização afetada após terem comprometido sua rede. Isso permite que a organização resolva o problema.
3. Os hackers Black hat são criminosos antiéticos que violam a segurança do computador e da rede para ganho pessoal ou por motivos maliciosos, como ataques a redes. Os hackers de Black hat exploram vulnerabilidades para comprometer os sistemas de computador e rede.

Bom ou ruim, hacking é um aspecto importante da segurança da rede. Neste curso, o termo ator de ameaça é usado quando se refere a indivíduos ou grupos que podem ser classificados como hackers grey ou black hat.

13.1.3

**Evolução dos atores de ameaças**

A atividade de hacker começou nos anos 1960 com o freaking (ou phreaking) telefônico, que se refere ao uso de várias frequências de áudio para manipular sistemas telefônicos. Naquela época, as centrais telefônicas usavam vários tons, ou discagem por tom, para indicar funções diferentes. Os primeiros agentes de ameaça perceberam que, imitando um tom usando um apito, eles poderiam explorar os comutadores telefônicos para fazer chamadas gratuitas de longa distância.

Em meados da década de 1980, conexões discadas e modems foram usados para conectar computadores a redes. Atores de ameaças escreveram programas de “discagem de guerra” que discavam cada número de telefone em uma determinada área em busca de computadores, sistemas de boletins e aparelhos de fax. Quando um número de telefone era encontrado, programas de quebra de senha eram usados para obter acesso. Desde então, os perfis e motivos gerais dos agentes de ameaças mudaram um pouco.

Existem muitos tipos diferentes de agentes de ameaça.

Script Kiddies

Script kiddies surgiram na década de 1990 e se refere a adolescentes ou atores de ameaças inexperientes executando scripts, ferramentas e explorações existentes para causar danos, mas normalmente sem fins lucrativos.

Corretores de Vulnerabilidades

Os corretores de vulnerabilidade normalmente se referem a hackers Grey Hat que tentam descobrir exploits e relatá-los aos fornecedores, às vezes por prêmios ou recompensas.

Hackvistas

Hacktivistas é um termo que se refere a hackers Grey Hat que se manifestam e protestam contra diferentes ideias políticas e sociais. Os hacktivistas protestam publicamente contra organizações ou governos, publicando artigos, vídeos, vazando informações confidenciais e realizando ataques DDoS (Denial of Service, Negação de serviço).

Cybercriminals

Criminoso cibernético é um termo para hackers black hat que são autônomos ou trabalham para grandes organizações do crime cibernético. A cada ano, os criminosos virtuais são responsáveis por roubar bilhões de dólares de consumidores e empresas.

Patrocinados pelo estado

Os hackers patrocinados pelo Estado são atores de ameaças que roubam segredos do governo, coletam informações e sabotam redes de governos estrangeiros, grupos terroristas e corporações. A maioria dos países do mundo participam, em algum grau, em ataques de hackers patrocinados pelo estado. Dependendo da perspectiva de uma pessoa, estes são hackers de white hat ou black hat.

13.1.4

**Cybercriminals**

Os cibercriminosos são atores de ameaça que estão motivados a ganhar dinheiro usando todos os meios necessários. Embora às vezes os cibercriminosos trabalhem de forma independente, eles são mais frequentemente financiados e patrocinados por organizações criminosas. Estima-se que, globalmente, os cibercriminosos roubam bilhões de dólares de consumidores e empresas todos os anos.

Os cibercriminosos operam em uma economia subterrânea onde compram, vendem e comercializam explorações e ferramentas. Eles também compram e vendem as informações pessoais e propriedade intelectual que roubam das vítimas. Os cibercriminosos visam pequenas empresas e consumidores, bem como grandes empresas e setores.

13.1.5

**Tarefas de cibersegurança**

Atores de ameaça não discriminam. Eles têm como alvo os dispositivos finais vulneráveis de usuários domésticos e empresas de pequeno a médio porte, bem como grandes organizações públicas e privadas.

Para tornar a Internet e as redes mais seguras e seguras, todos temos de desenvolver uma boa consciência da segurança cibernética. A segurança cibernética é uma responsabilidade compartilhada que todos os usuários devem praticar. Por exemplo, devemos denunciar crimes cibernéticos às autoridades apropriadas, estar ciente de possíveis ameaças no e-mail e na Web e proteger informações importantes contra roubo.

As organizações devem agir e proteger seus ativos, usuários e clientes. Eles devem desenvolver e praticar tarefas de segurança cibernética, como as listadas na figura.



13.1.6

**Indicadores de ameaças cibernéticas**

Muitos ataques de rede podem ser evitados compartilhando informações sobre **indicadores de comprometimento** (COI). Cada ataque tem atributos identificáveis únicos. Indicadores de compromisso são a evidência de que um ataque ocorreu. Os IOCs podem ser recursos que identificam arquivos de malware, endereços IP de servidores que são usados em ataques, nomes de arquivos e alterações características feitas no software final do sistema, entre outros. Os IOCs ajudam o pessoal de segurança cibernética a identificar o que aconteceu em um ataque e desenvolver defesas contra o ataque. Um resumo do COI para um pedaço de malware é mostrado na figura.

Malware File - &quot;studiox-link-standalone-v20.03.8-stable.exe&quot;

sha256 6a6c28f5666b12beecd56a3d1d517e409b5d6866c03f9be44ddd9efffa90f1e0

sha1 eb019ad1c73ee69195c3fc84ebf44e95c147bef8

md5 3a104b73bb96dfed288097e9dc0a11a8

DNS requests

domain log.studiox.link

domain my.studiox.link

domain \_sips.\_tcp.studiox.link

domain sip.studiox.link

Connections

ip 198.51.100.248

ip 203.0.113.82

Por exemplo, um usuário recebe um e-mail afirmando que ganhou um grande prêmio. Clicar no link no e-mail resulta em um ataque. O COI poderia incluir o fato de o usuário não ter entrado no concurso, o endereço IP do remetente, a linha de assunto do e-mail, o URL a ser clicado, ou um anexo para baixar, entre outros.

**Indicadores de ataque** (IOA) se concentram mais na motivação por trás de um ataque e nos potenciais meios pelos quais os atores da ameaça têm, ou irão, comprometer vulnerabilidades para obter acesso a ativos. As IOAs estão preocupadas com as estratégias usadas pelos atacantes. Por esse motivo, em vez de informar a resposta a uma única ameaça, o IOAS pode ajudar a gerar uma abordagem de segurança proativa. Isso ocorre porque as estratégias podem ser reutilizadas em vários contextos e ataques múltiplos. Defender contra uma estratégia pode, portanto, impedir ataques futuros que utilizem a mesma estratégia, ou similar.

13.1.7

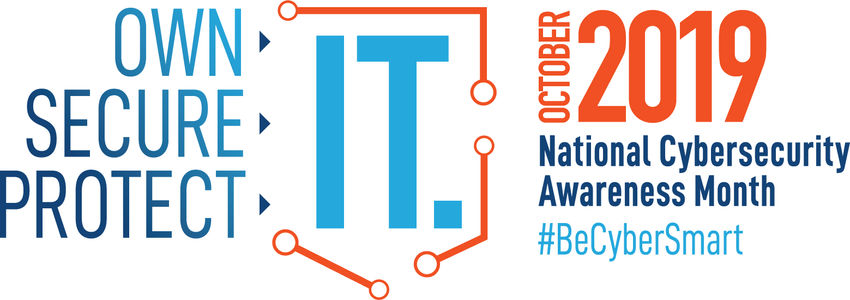
## Compartilhamento de ameaças e criação de conscientização

Os governos estão agora promovendo ativamente a segurança cibernética. Por exemplo, a Agência de Infraestrutura e Segurança Cibernética dos EUA (CISA) está liderando esforços para automatizar o compartilhamento de informações de segurança cibernética com organizações públicas e privadas sem nenhum custo. A CISA usa um sistema chamado Automated Indicator Sharing (AIS). O AIS permite o compartilhamento de indicadores de ataque entre o governo dos EUA e o setor privado assim que as ameaças são verificadas. A CISA oferece muitos recursos que ajudam a limitar o tamanho da superfície de ataque dos Estados Unidos.

A CISA e a National Cyber Security Alliance (NCSA) promovem a segurança cibernética a todos os usuários. Por exemplo, eles têm uma campanha anual em outubro chamada “National Cybersecurity Awareness Mês” (NCASM). Esta campanha foi desenvolvida para promover e aumentar a conscientização sobre segurança cibernética.

O tema para o NCASM para 2019 foi “**TI Própria. Proteja a TI. Proteja a TI.**” Esta campanha incentivou todos os cidadãos a serem mais seguros e mais pessoalmente responsáveis pela utilização das melhores práticas de segurança online. A campanha fornece material sobre uma grande variedade de tópicos de segurança, incluindo:

* Segurança das redes sociais
* Atualizando configurações de privacidade
* Reconhecimento da segurança de aplicativos de dispositivos
* Manter o software atualizado
* Compras online seguras
* Segurança Wi-Fi
* Protegendo os dados do cliente



A Agência da União Europeia para a Cibersegurança (ENISA) presta aconselhamento e soluções para os desafios da cibersegurança dos Estados-Membros da UE. A ENISA desempenha um papel na Europa semelhante ao papel da CISA nos EUA.

# Ferramentas do agente da ameaça

13.2.1

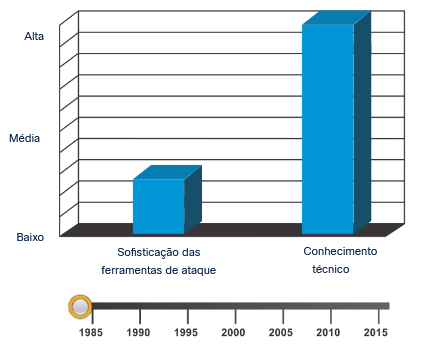
## Introdução de ferramentas de ataque

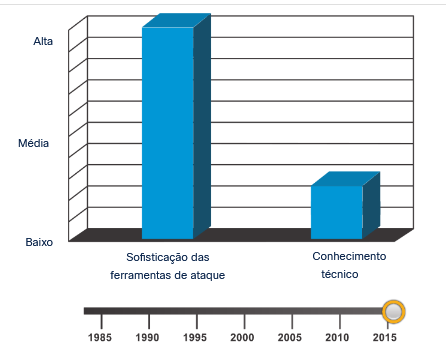
Para explorar uma vulnerabilidade, um agente de ameaça deve ter uma técnica ou ferramenta. Ao longo dos anos, as ferramentas de ataque tornaram-se mais sofisticadas e altamente automatizadas. Essas novas ferramentas requerem menos conhecimento técnico para serem implementadas.

Na figura, arraste o círculo branco pela linha do tempo para visualizar o relacionamento entre a sofisticação das ferramentas de ataque e o conhecimento técnico necessário para usá-las.

mostra uma barra com sofisticação de ataque à esquerda e uma barra com conhecimento técnico à direita. Em 1985, os ataques não eram muito sofisticados e exigiram muito conhecimento técnico. Com o passar do tempo, a sofisticação do ataque aumentou e o conhecimento técnico necessário diminuiu.

### Sofisticação das ferramentas de ataque x conhecimento técnico





13.2.2

**Evolução das ferramentas de segurança**

O hacking ético envolve o uso de muitos tipos diferentes de ferramentas para testar a rede e os dispositivos finais. Para validar a segurança de uma rede e seus sistemas, muitas ferramentas de teste de penetração de rede foram desenvolvidas. No entanto, muitas dessas ferramentas também podem ser usadas por atores ameaçadores para exploração.

Atores de ameaças também criaram várias ferramentas de hacking. Essas ferramentas são escritas explicitamente por motivos nefastos. O pessoal de segurança cibernética também deve saber como usar essas ferramentas ao realizar testes de penetração na rede.

Explore as categorias de ferramentas comuns de teste de penetração de rede. Observe como algumas ferramentas são usadas pelos white hats e black hats. Lembre-se de que a lista não é exaustiva, pois novas ferramentas são continuamente desenvolvidas.

**Nota**: Muitas dessas ferramentas são baseadas em UNIX ou Linux; portanto, um profissional de segurança deve ter uma sólida experiência em UNIX e Linux.

| **Categorias de Ferramentas** | **Descrição** |
| --- | --- |
| crackers da senha | As senhas são a ameaça de segurança mais vulnerável. As ferramentas de quebra de senha são freqüentemente chamadas de ferramentas de recuperação de senha e podem ser usadas para quebrar ou recuperar a senha. Isso é feito removendo a senha original, depois de ignorar a criptografia de dados, ou pela descoberta direta da senha. Os crackers de senhas repetidamente fazem suposições para decifrar a senha e acessar o sistema. Exemplos de ferramentas de quebra de senha incluem John the Ripper, Ophcrack, L0phtCrack, THC Hydra, RainbowCrack e Medusa. |
| ferramentas de hacking sem fio | As redes sem fio são mais suscetíveis a ameaças à segurança da rede. As ferramentas de hackers sem fio são usadas para invadir intencionalmente uma rede sem fio para detectar vulnerabilidades de segurança. Exemplos de ferramentas de hacking sem fio incluem Aircrack-ng, Kismet, InSSIDer, KisMAC, Firesheep e NetStumbler. |
| digitalização de rede e ferramentas de hacking | As ferramentas de verificação de rede são usadas para investigar dispositivos, servidores e hosts de rede em busca de portas TCP ou UDP abertas. Exemplos de ferramentas de digitalização incluem Nmap, SuperScan, Angry IP Scanner e NetScanTools. |
| ferramentas de elaboração de pacotes | Ferramentas de criação de pacotes são usadas para sondar e testar a robustez de um firewall usando pacotes forjados especialmente criados. Exemplos de tais ferramentas incluem Hping, Scapy, Socat, Yersinia, Netcat, Nping e Nemesis. |
| sniffer de pacotes | As ferramentas de farejadores de pacotes são usadas para capturar e analisar pacotes em LANs Ethernet ou WLANs tradicionais. As ferramentas incluem Wireshark, Tcpdump, Ettercap, Dsniff, EtherApe, Paros, Fiddler, Ratproxy e SSLstrip. |
| detectores de rootkit | Um detector de rootkit é um verificador de integridade de diretório e arquivo usado por white hats para detectar root kits instalados. Exemplos de ferramentas incluem AIDE, Netfilter e PF: OpenBSD Packet Filter. |
| fuzzers para pesquisar vulnerabilidades | Fuzzers são ferramentas usadas por agentes de ameaças ao tentar descobrir vulnerabilidades de segurança de um sistema de computador. Exemplos de difusores incluem Skipfish, Wapiti e W3af. |
| ferramentas forenses | Hackers White hat usam ferramentas forenses para farejar qualquer vestígio de evidência existente em um sistema de computador específico. Exemplos de ferramentas incluem Sleuth Kit, Helix, Maltego e Encase. |
| Depuradores | Ferramentas de depuração são usadas por Black Hats para fazer engenharia reversa de arquivos binários ao escrever exploits. Eles também são usados por white hats ao analisar malware. As ferramentas de depuração incluem GDB, WinDbg, IDA Pro, and Immunity Debugger. |
| hackeando sistemas operacionais | Os sistemas operacionais de hacking são sistemas operacionais especialmente projetados, pré-carregados com ferramentas e tecnologias otimizadas para hackers. Exemplos de sistemas operacionais de hacking especialmente projetados incluem Kali Linux, SELinux, Knoppix, Parrot OS e BackBox Linux. |
| ferramentas de criptografia | Essas ferramentas salvaguardam o conteúdo dos dados de uma organização quando são armazenados ou transmitidos. As ferramentas de criptografia usam esquemas de algoritmo para codificar os dados e evitar o acesso não autorizado aos dados. Exemplos dessas ferramentas incluem VeraCrypt, CipherShed, Open SSH, OpenSSL, OpenVPN e Stunnel. |
| ferramentas de exploração de vulnerabilidade | Essas ferramentas identificam se um host remoto é vulnerável a um ataque de segurança. Exemplos de ferramentas de exploração de vulnerabilidade incluem Metasploit, Core Impact, Sqlmap, Social Engineer Tool Kit e Netsparker. |
| scanner de vulnerabilidades | Essas ferramentas examinam uma rede ou sistema para identificar portas abertas. Eles também podem ser usados para verificar vulnerabilidades conhecidas e verificar VMs, dispositivos BYOD e bancos de dados do cliente Exemplos dessas ferramentas incluem Nipper, Securia PSI, Core Impact, Nessus, SAINT e Open VAS. |

13.2.3

**Categorias de ataques**

Os atores da ameaça podem usar as ferramentas mencionadas anteriormente ou uma combinação de ferramentas para criar vários ataques. A tabela exibe tipos comuns de ataques. No entanto, a lista de ataques não é exaustiva, pois novas maneiras de atacar redes são continuamente descobertas.

É importante entender que os atores de ameaças usam uma variedade de ferramentas de segurança para realizar esses ataques.

| **Categoria de Ataque** | **Descrição** |
| --- | --- |
| Ataque de escuta | Um ataque de espionagem ocorre quando um agente de ameaça captura e escuta o tráfego da rede. Esse ataque também é chamado de sniffing ou snooping. |
| Ataque de modificação de dados | Ataques de modificação de dados ocorrem quando um agente de ameaça capturou o tráfego da empresa e alterou os dados nos pacotes sem o conhecimento do remetente ou receptor. |
| Ataque de Falsificação de Endereços IP | Um ataque de falsificação de endereço IP ocorre quando um ator de ameaça constrói um pacote IP que parece se originar de um endereço válido dentro da intranet corporativa. |
| Ataques baseados em senha | Ataques baseados em senha ocorrem quando um ator de ameaça obtém as credenciais de uma conta de usuário válida. Em seguida, os atores de ameaças usam essa conta para obter listas de outros usuários e informações de rede. Eles também podem alterar as configurações de servidor e rede e modificar, redirecionar ou excluir dados. |
| Ataque de negação de serviço (DoS) | Um ataque de DoS impede o uso normal de um computador ou rede por usuários válidos. Depois de obter acesso a uma rede, um ataque DoS pode travar aplicativos ou serviços de rede. Um ataque de DoS pode inundar um computador ou toda a rede com tráfego até que um desligamento ocorra devido à sobrecarga. Um ataque de DoS também pode bloquear o tráfego, o que resulta na perda de acesso aos recursos da rede por usuários autorizados. |
| Ataque man-in-the-middle (MiTM) | Um ataque MiTM ocorre quando os agentes da ameaça se posicionam entre a origem e o destino. Agora eles podem monitorar, capturar e controlar ativamente a comunicação de forma transparente. |
| Ataque de chave comprometida | Um ataque de chave comprometida ocorre quando um ator de ameaça obtém uma chave secreta. Isto é referido como uma chave comprometida. Uma chave comprometida pode ser usada para obter acesso a uma comunicação segura sem que o remetente ou o destinatário esteja ciente do ataque. |
| Ataque Sniffer | Um sniffer é um aplicativo ou dispositivo que pode ler, monitorar e capturar trocas de dados de rede e ler pacotes de rede. Se os pacotes não estiverem criptografados, um sniffer fornece uma visão completa dos dados dentro do pacote. Até mesmo pacotes encapsulados (encapsulados) podem ser quebrados abertos e lidos, a menos que sejam criptografados e que o ator de ameaça não tenha acesso à chave. |

# Resumo de invasores e suas ferramentas

13.3.1

## O que aprendi neste módulo?

**Quem está atacando nossa rede?**

Compreender a segurança da rede requer que você entenda os seguintes termos: ameaça, vulnerabilidade, superfície de ataque, exploração e risco. A gestão de riscos é o processo que equilibra os custos operacionais de provisão de medidas de proteção com os ganhos obtidos através da proteção do ativo. Quatro formas comuns de gerenciar riscos são a aceitação de riscos, a prevenção de riscos, a redução de riscos e a transferência de riscos. Hacker é um termo usado para descrever um ator de ameaça. Os hackers White hat são hackers éticos que usam suas habilidades para propósitos bons, éticos e legais. Hackers Grey hat são indivíduos que cometem crimes e fazem coisas antiéticas, mas não para ganho pessoal ou para causar danos. Os hackers Black hat são criminosos que violam a segurança do computador e da rede para ganho pessoal ou por motivos maliciosos, como ataques a redes. Os atores de ameaças incluem crianças de script, corretores de vulnerabilidade, hacktivistas, criminosos cibernéticos e hackers patrocinados pelo Estado. Muitos ataques de rede podem ser evitados compartilhando informações sobre indicadores de comprometimento (COI). Muitos governos estão promovendo a segurança cibernética. CISA e NCSA são exemplos de tais organizações.

**Introdução de ferramentas de ataque**

Atores de ameaça usam uma técnica ou ferramenta. As ferramentas de ataque se tornaram mais sofisticadas e altamente automatizadas. Muitas das ferramentas são baseadas em Linux ou UNIX e um conhecimento delas é útil para um profissional de segurança cibernética. As ferramentas incluem crackers de senhas, ferramentas de hacking sem fio, ferramentas de varredura e hacking de segurança de rede, ferramentas de criação de pacotes, ferramentas de criação de pacotes, sniffers de pacotes, detectores de rootkit, fuzzers para pesquisar vulnerabilidades, ferramentas forenses, depuradores, sistemas operacionais de hacking, ferramentas de criptografia, vulnerabilidade ferramentas de exploração e scanners de vulnerabilidade. As categorias de ataques incluem ataques de espionagem, ataques de modificação de dados, ataques de falsificação de endereços IP, ataques baseados em senha, ataques de negação de serviço, ataques de man-in the-middle, ataques de chave comprometidos e ataques de farejador.

13.3.2

# Introdução

14.0.1

## Por que devo cursar este módulo?

Agora você sabe por que nossas redes são atacadas. Neste módulo, você aprenderá sobre ameaças e ataques comuns.

14.0.2

## O que vou aprender neste 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, estouros de buffer e evasão | Explicar os ataques de negação de serviço, estouro de buffer e evasão. |

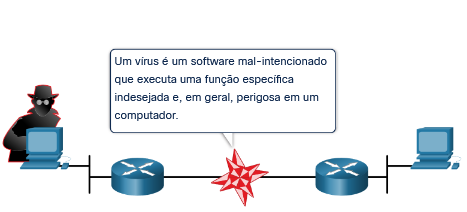
# Malware

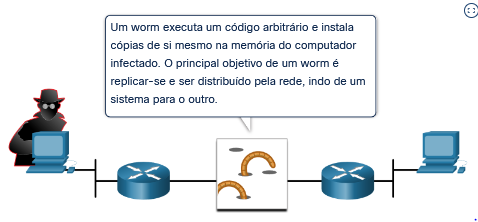
14.1.1

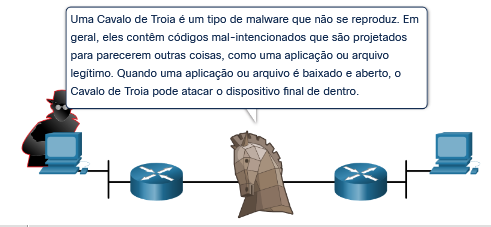
## Tipos de Malware

Os dispositivos finais são especialmente propensos a ataques de malware. Portanto, o foco deste tópico é sobre ameaças a dispositivos finais. Malware é a abreviatura de software malicioso ou código malicioso. É um código ou software projetado especificamente para danificar, interromper, roubar ou geralmente infligir alguma outra ação “ruim” ou ilegítima em dados, hosts ou redes. É importante saber sobre malware porque os agentes de ameaças e criminosos online freqüentemente tentam induzir os usuários a instalar malware para ajudar a explorar as lacunas de segurança. Além disso, o malware se transforma tão rapidamente que os incidentes de segurança relacionados ao malware são extremamente comuns porque o software antimalware não pode ser atualizado com rapidez suficiente para impedir as novas ameaças.

Reproduza a animação para ver exemplos dos três tipos mais comuns de malware: vírus, worm e cavalo de Tróia.







14.1.2

## Vírus

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 os computadores. A maioria dos vírus requer ajuda humana para se espalhar. Por exemplo, quando alguém conecta uma unidade USB infectada ao PC, o vírus entrará no PC. O vírus pode então infectar uma nova unidade USB e se espalhar para novos PCs. Os vírus podem ficar inativos por um período prolongado e, em seguida, ativá-los em uma hora e data específicas.

Um vírus simples pode instalar-se na primeira linha de código em um arquivo executável. Quando ativado, o vírus pode verificar o disco em busca de outros executáveis para que ele possa infectar todos os arquivos que ainda não infectou. Os vírus podem ser inofensivos, como os que exibem uma imagem na tela, ou podem ser destrutivos, como os que modificam ou excluem arquivos do disco rígido. Os vírus também podem ser programados para se modificar e evitar a detecção.

A maioria dos vírus agora se espalha por unidades de memória USB, CDs, DVDs, compartilhamentos de rede e e-mail. Os vírus de e-mail são um tipo comum de vírus.

14.1.3

**Cavalos de Troia**

O termo cavalo de Tróia originou-se da mitologia grega. Guerreiros gregos ofereceram ao povo de Tróia (os troianos) um cavalo oco gigante como um presente. Os troianos trouxeram o cavalo gigante para sua cidade murada, sem saber que continha muitos guerreiros gregos. À noite, depois que a maioria dos troianos dormia, os guerreiros saíram do cavalo, abriram os portões da cidade e permitiram que uma força considerável entrasse e tomasse a cidade.

O malware de cavalo de Tróia é um software que parece ser legítimo, mas contém código malicioso que explora os privilégios do usuário que o executa. Muitas vezes, 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. Ao jogar o jogo, o usuário não notará um problema. Em segundo plano, o cavalo de Tróia foi instalado no sistema do usuário. O código malicioso do cavalo de Tróia continua a funcionar mesmo depois que o jogo foi fechado.

O conceito do cavalo de Tróia é flexível. Pode causar danos imediatos, fornecer acesso remoto ao sistema ou acesso através de uma porta traseira. Ele também pode executar ações conforme instruído remotamente, como “me envie o arquivo de senha uma vez por semana.“ Esta tendência de malware para enviar dados de volta para o cibercriminoso destaca a necessidade de monitorar o tráfego de saída em busca de indicadores de ataque.

Cavalos de Tróia escritos sob medida, como aqueles com um alvo específico, são difíceis de detectar.

## Cavalo de Tróia Classificação

Os cavalos de Tróia são geralmente classificados de acordo com o dano que eles causam, ou a maneira pela qual eles violam um sistema, como mostrado na figura.

| **Tipo do Cavalo de Troia** | **Descrição** |
| --- | --- |
| Acesso remoto | Permite acesso remoto não autorizado. |
| Envio de dados | Fornece ao agente de ameaça dados confidenciais, como senhas. |
| Destrutivo | Corrompe 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. |

14.1.5

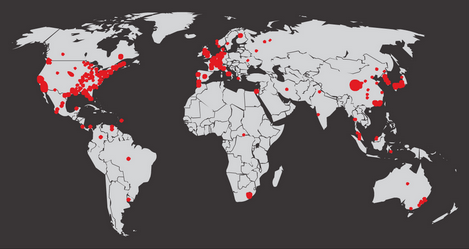
**Worms**

Os worms de computador são semelhantes aos vírus porque se replicam e podem causar o mesmo tipo de dano. Especificamente, os worms se replicam explorando vulnerabilidades nas redes de forma independente. Os worms podem retardar as redes à medida que se espalham de sistema para sistema.

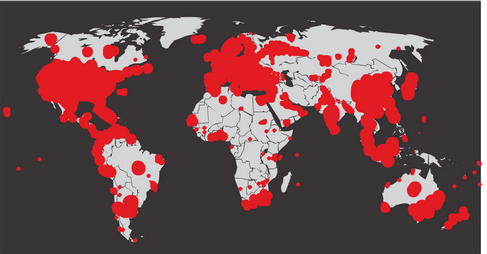
Enquanto um vírus requer um programa host para execução, os worms podem ser executados de modo autônomo. Exceto pela infecção inicial, eles não necessitam mais da participação do usuário. Após infectar um host, um worm pode ser transmitido muito rapidamente pela rede.

Os worms são responsáveis por alguns dos ataques mais devastadores da Internet. 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

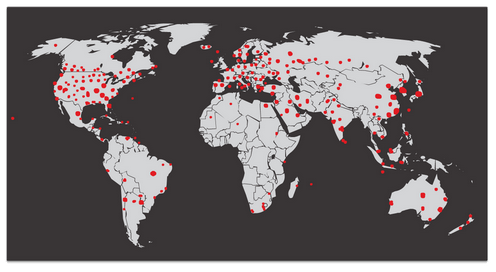


Infeccção por cóigo vermelho 19 horas depois

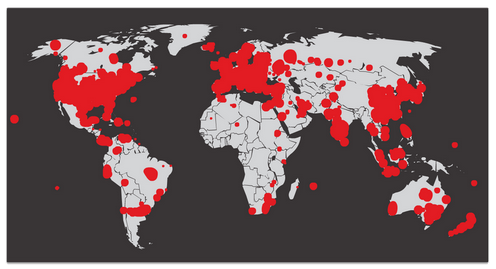


A infecção inicial do worm SQL Slammer é conhecida como o worm que comeu a internet. O SQL Slammer foi um ataque de negação de serviço (DoS) que explorava um bug de estouro de buffer no SQL Server da Microsoft. No seu pico, o número de servidores infectados dobrou de tamanho a cada 8,5 segundos. É por isso que ele foi capaz de infectar mais de 250 mil hosts em 30 minutos. Quando foi lançado no fim de semana de 25 de janeiro de 2003, interrompeu a internet, instituições financeiras, caixas eletrônicos e muito mais. Ironicamente, um patch para esta vulnerabilidade tinha sido lançado 6 meses antes. Os servidores infectados não tinham o patch atualizado aplicado. Essa foi uma chamada de ativação para muitas organizações implementarem uma política de segurança exigindo que atualizações e patches fossem aplicados em tempo hábil.

Infecção inicial do SQL Slammer



Infecção SQL Slammer 30 minutos depois



Worms compartilham características semelhantes. Todos eles exploram uma vulnerabilidade habilitadora, têm uma maneira de se propagar e todos contêm uma carga útil.

14.1.6

## Componentes do Worm

Apesar das técnicas de mitigação que surgiram ao longo dos anos, os vermes continuaram a evoluir e representam uma ameaça persistente. Worms tornaram-se mais sofisticados ao longo do tempo, mas eles ainda tendem a ser baseados na exploração de fraquezas em aplicativos de software.

A animação mostra os 3 componentes de um ataque de worm; permitindo vulnerabilidade, mecanismo de propagação e carga útil.

### Padrão comum de worm

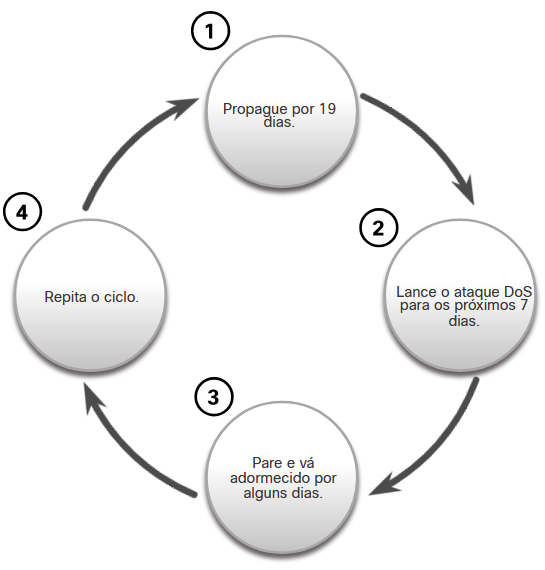
* Habilitar vulnerabilidade
* Mecanismo de propagação
* Carga útil

A maioria dos ataques de worm consiste em três componentes, conforme listado na animação acima.

* **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.
* **Carga útil** - 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 a um ator de ameaça acessar o host infectado ou criar um ataque DoS.

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. Seus mecanismos de propagação são comumente implantados de uma forma difícil de detectar.

A técnica de propagação usada pelo worm Code Red é mostrada na figura.



**Nota**: 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.

14.1.7

**Ransomware**

Os atores de ameaças usaram vírus, worms e cavalos de Tróia para transportar suas cargas úteis e por outros motivos maliciosos. No entanto, o malware continua a evoluir.

Atualmente, o malware mais dominante é o ransomware. Ransomware é um malware que nega acesso ao sistema de computador infectado ou aos seus dados. Os criminosos cibernéticos, em seguida, exigem pagamento para liberar o sistema de computador.

O ransomware evoluiu para se tornar o tipo de malware mais lucrativo da história. Na primeira metade de 2016, as campanhas de ransomware concentradas em usuários corporativos e individuais se tornaram mais amplas e eficientes.

Existem dezenas de variantes de ransomware. Ransomware usa frequentemente um algoritmo de criptografia para criptografar arquivos e dados do sistema. A maioria dos algoritmos de criptografia de ransomware conhecidos não pode ser descriptografada facilmente, deixando as vítimas com poucas opções a não ser pagar o preço pedido. Os pagamentos são normalmente pagos em Bitcoin porque os usuários de bitcoin podem permanecer anônimos. Bitcoin é uma moeda digital de código aberto que ninguém possui ou controla.

Email e publicidade maliciosa, também conhecidos como malvertising, são vetores para campanhas de ransomware. A engenharia social também é usada, como quando os cibercriminosos que se identificam como técnicos de segurança chamam de residências e persuadem os usuários a se conectar a um site que baixa o ransomware para o computador do usuário.

14.1.8

**Outro Malware**

Estes são alguns exemplos das variedades de malware moderno:

| **Tipo de Malware** | **Descrição** |
| --- | --- |
| 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. |
| 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. |

Esta lista continuará a crescer à medida que a Internet evolui. Novos malwares serão sempre desenvolvidos. Um dos principais objetivos das operações de segurança cibernética é aprender sobre novos malwares e como mitigá-lo prontamente.

14.1.9

## Comportamentos comuns de malware

Os cibercriminosos modificam continuamente o código de malware para alterar a forma como ele se espalha e infecta computadores. No entanto, a maioria produz sintomas semelhantes que podem ser detectados através do monitoramento de log de rede e dispositivo.

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.

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

14.2.1

## Tipos de ataques de rede

Malware é um meio de obter uma carga útil entregue. Quando é entregue e instalada, a carga útil pode ser usada para causar uma variedade de ataques internos à rede. Os atores de ameaças também podem atacar a rede de fora.

Por que os atores ameaçadores atacam redes? Há muitos motivos, incluindo dinheiro, ganância, vingança ou crenças políticas, religiosas ou sociológicas. Os profissionais de segurança de rede devem compreender os tipos de ataques usados para combater essas ameaças para garantir a segurança da LAN.

Para atenuar os ataques, é útil primeiro categorizar os vários tipos de ataques. Ao categorizar ataques de rede, é possível abordar tipos de ataques em vez de ataques individuais.

Embora não haja uma maneira padronizada de categorizar os ataques de rede, o método utilizado neste curso classifica os ataques em três categorias principais.

* Ataques de Reconhecimento
* Ataques de Acesso
* Ataques de DoS
* 14.2.2

**Ataques de Reconhecimento**

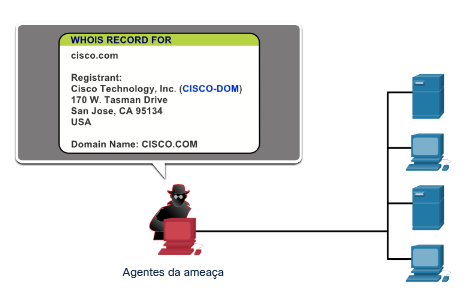
Reconhecimento é coleta de informações. É análogo a um ladrão que inspeciona um bairro indo de porta em porta fingindo vender alguma coisa. O que o ladrão está realmente fazendo é procurando casas vulneráveis, como residências desocupadas, residências com portas ou janelas fáceis de abrir e residências sem sistemas de segurança ou câmeras de segurança.

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.

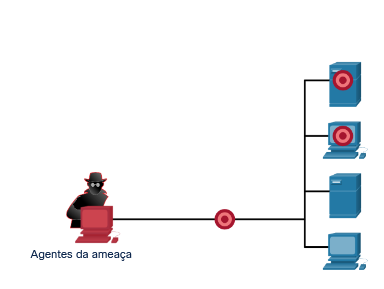
Algumas das técnicas usadas pelos atores de ameaças mal-intencionadas para realizar ataques de reconhecimento estão descritas na tabela.

| **Técnicas** | **Descrição** |
| --- | --- |
| **Executar uma consulta de informações de um alvo** | O agente de 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 de destino. 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. |
| **Executar 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. |
| **Executar 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. |

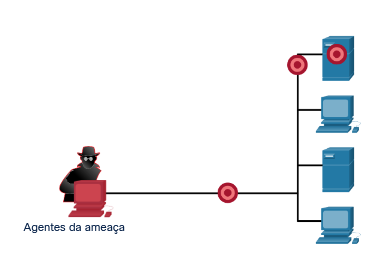
Consultas de informações da internet



Executando varreduras de ping



Executando verificações de porta



14.2.4

## Ataques de Acesso

Os ataques de acesso exploram vulnerabilidades conhecidas em serviços de autenticação, serviços de FTP e serviços da Web. O objetivo desse tipo de ataque é obter acesso a contas da web, bancos de dados confidenciais e outras informações confidenciais.

Os atores de ameaças usam ataques de acesso a dispositivos de rede e computadores para recuperar dados, obter acesso ou escalar privilégios de acesso ao status de administrador.

**Ataques de senha**

Em um ataque de senha, o agente de ameaça tenta descobrir senhas críticas do sistema usando vários métodos. Os ataques de senha são muito comuns e podem ser iniciados usando uma variedade de ferramentas de quebra de senha.

**Ataques de falsificação (spoofing)**

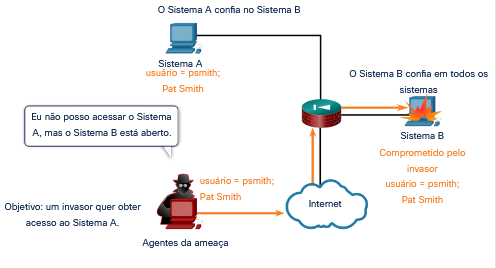
Nos ataques de falsificação, o dispositivo do agente de ameaças tenta se passar por outro dispositivo falsificando os dados. Ataques comuns incluem falsificação IP (IP spoofing), falsificação MAC (MAC spoofing), e falsificação DHCP (DHCP spoofing). Esses ataques de falsificação serão discutidos em mais detalhes posteriormente neste módulo

Outros ataques de acesso incluem:

* Exploração de confiança
* Redirecionamento de porta
* ataque man in the middle
* ⁪ataque de saturação do buffer

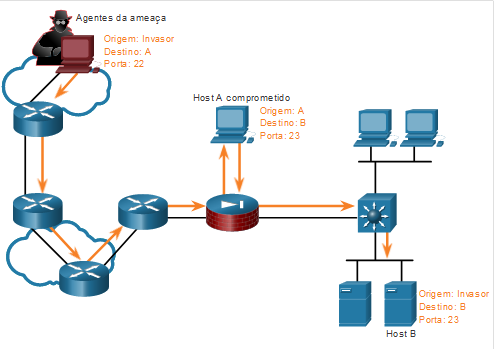
Exemplo de exploração de confiança

Em um ataque de exploração de confiança, um agente de ameaça usa privilégios não autorizados para obter acesso a um sistema, possivelmente comprometendo o alvo. Clique em Reproduzir na figura para visualizar um exemplo de exploração de confiança.



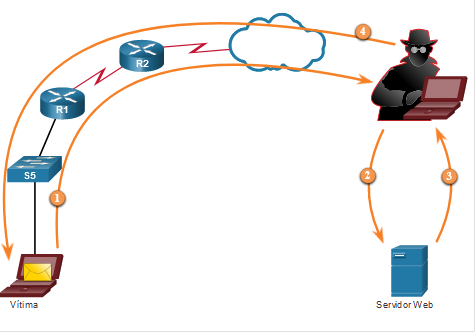
Exemplo de redirecionamento de porta

Em um ataque de redirecionamento de porta, um agente de ameaça usa um sistema comprometido como base para ataques contra outros alvos. O exemplo na figura mostra um agente de ameaça usando SSH (porta 22) para conectar-se a um host A. comprometido. O host A é confiável pelo host B e, portanto, o agente de ameaça pode usar o Telnet (porta 23) para acessá-lo.



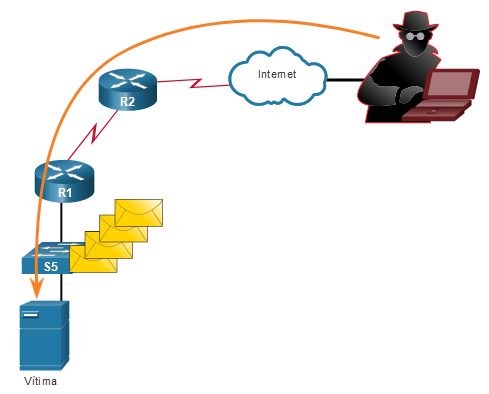
Exemplo de Ataque a Man in the middle

Em um ataque man-in-the-middle, o agente de ameaça é posicionado entre duas entidades legítimas para ler ou modificar os dados que passam entre as duas partes. A figura mostra um exemplo de ataque do tipo man-in-the-middle.



Ataques de Buffer overflow

Em um ataque de estouro de buffer, o agente de ameaça explora a memória do buffer e a sobrecarrega com valores inesperados. Isso geralmente torna o sistema inoperante, criando um ataque de DoS. A figura mostra que o agente de ameaça está enviando muitos pacotes para a vítima na tentativa de sobrecarregar o buffer da vítima.



14.2.6

## Ataques de engenharia social

Engenharia social é um ataque de acesso que tenta manipular indivíduos para realizar ações ou divulgar informações confidenciais. Algumas técnicas de engenharia social são realizadas pessoalmente, enquanto outras podem usar o telefone ou a Internet.

Os engenheiros sociais frequentemente dependem da boa vontade das pessoas para ajuda. Eles também atacam as fraquezas das pessoas. Por exemplo, um agente de ameaças pode chamar um funcionário autorizado com um problema urgente, que requer acesso imediato à rede. O agente de ameaças pode recorrer à vaidade do funcionário, valer-se de autoridade usando técnicas que citam nomes ou apelar para a ganância do funcionário.

Informações sobre técnicas de engenharia social são mostradas na tabela.

| **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. |
| Algo por Algo | Às vezes chamado de Quid pro quo, é quando um ator da 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 o agente 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. |

O Social Engineer Toolkit (SET) foi projetado para ajudar hackers whitehat e outros profissionais de segurança de rede a criar ataques de engenharia social para testar suas próprias redes. É um conjunto de ferramentas baseadas em menu que ajudam a lançar ataques de engenharia social. O SET é apenas para fins educacionais. Está disponível gratuitamente na Internet.

As empresas devem educar seus usuários sobre os riscos da engenharia social e desenvolver estratégias para validar identidades por telefone, via email ou pessoalmente.

A figura mostra práticas recomendadas que devem ser seguidas por todos os usuários.

A figura mostra as 8 práticas a seguir para proteção contra ataques de engenharia social: Nunca forneça suas credenciais de nome de usuário / senha a ninguém ; Sempre destrua as informações confidenciais de acordo com a política da organização ; Sempre denuncie indivíduos suspeitos; ; Nunca reutilize senhas relacionadas ao trabalho ; Nunca divulgue informações relacionadas ao trabalho em sites de mídia social ; Nunca abra e-mails de fontes não confiáveis ; Nunca deixe suas credenciais de nome de usuário / senha onde possam ser facilmente encontradas.

### Práticas recomendadas de proteção de engenharia social



14.2.7

**Fortalecimento do elo mais fraco**

A cibersegurança é tão forte quanto seu elo mais fraco. Como computadores e outros dispositivos conectados à Internet se tornaram uma parte essencial de nossas vidas, eles não parecem mais novos ou diferentes. As pessoas se tornaram muito casuais em seu uso desses dispositivos e raramente pensam em segurança de rede. 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. Por isso, 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 - negação de serviço, estouros de buffer e evasão

14.3.1

## Vídeo - Ataques de Negação de Serviços

14.3.2

## Ataques de DoS

Um ataque de negação de serviço (DoS) cria algum tipo de interrupção dos serviços de rede para usuários, dispositivos ou aplicativos. Existem dois tipos principais de ataque de negação de serviço (DoS):

* **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. Isso faz com que os tempos de transmissão e resposta diminuam. Também pode travar um dispositivo ou serviço.
* **Pacotes maliciosamente formatados** – O invasor envia um pacote formatado maliciosamente para um host ou aplicativo e o receptor não consegue manipulá-lo. Isso causa lentidão ou falha na execução do dispositivo receptor.

Ataque Dos

Os ataques de DoS são um grande risco, porque interrompem a comunicação e causam perda significativa de tempo e dinheiro. Esses ataques são relativamente simples de conduzir, mesmo por um invasor não capacitado.

Ataque DDos

Um ataque de negação de serviço distribuída (DDoS) é semelhante a um ataque de negação de serviço (DoS), porém é originado por várias fontes coordenadas. Por exemplo, um agente de ameaça cria uma rede de hosts infectados, conhecidos como zumbis. O agente de ameaças usa um sistema de comando e controle (CnC) para enviar mensagens de controle aos zumbis. Os zumbis constantemente examinam e infectam mais hosts com malware bot. O malware bot é projetado para infectar um host, tornando-o um zumbi que pode se comunicar com o sistema CnC. Um grupo de zumbis é chamada de botnet. Quando pronto, o agente de ameaça instrui o sistema CnC a fazer com que o botnet de zumbis execute um ataque DDoS.

Um ataque de negação de serviço distribuída (DDoS) é semelhante a um ataque de negação de serviço (DoS), porém é originado por várias fontes coordenadas. Por exemplo, um agente de ameaça cria uma rede de hosts infectados, conhecidos como zumbis. O agente de ameaças usa um sistema de comando e controle (CnC) para enviar mensagens de controle aos zumbis. Os zumbis constantemente examinam e infectam mais hosts com malware bot. O malware bot é projetado para infectar um host, tornando-o um zumbi que pode se comunicar com o sistema CnC. Um grupo de zumbis é chamada de botnet. Quando pronto, o agente de ameaça instrui o sistema CnC a fazer com que o botnet de zumbis execute um ataque DDoS.

14.3.4

## Vídeo — Mirai Botnet

Mirai é malware que direcionou dispositivos IoT configurados com informações de login padrão. Câmeras de televisão de circuito fechado (CCTV) constituíam a maioria dos alvos de Mirai. Usando um ataque de dicionário de força bruta, Mirai correu através de uma lista de nomes de usuário padrão e senhas que eram amplamente conhecidos na internet.

* root/default
* root/1111
* root/54321
* admin/admin1234
* admin1/password
* guest/12345
* tech/tech
* support/support

Depois de obter acesso bem-sucedido, Mirai direcionou os utilitários BusyBox baseados em Linux que são executados nesses dispositivos. Esses utilitários foram usados para transformar os dispositivos em bots que poderiam ser controlados remotamente como parte de uma botnet. O botnet foi então usado como parte de um ataque distribuído de negação de serviço (DDoS). Em setembro de 2016, uma botnet Mirai com mais de 152.000 CCTVs e gravadores de vídeo digitais (DVRs) foi responsável pelo maior ataque DDoS conhecido até então. Com o pico de tráfego de mais de 1 TB/s, ele derrubou os serviços de hospedagem de uma empresa de hospedagem na web com sede na França.

Em outubro de 2016, os serviços da Dyn, um provedor de serviços de nomes de domínio (DNS), foram atacados, causando interrupções na internet para milhões de usuários nos Estados Unidos e na Europa.

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

Nota: Em dezembro de 2017, três atores americanos de ameaças declararam-se culpados por conspirar para “conduzir ataques DDoS contra sites e empresas de hospedagem na web localizadas nos Estados Unidos e no exterior”. Os três criminosos enfrentam até 10 anos de prisão e 250 mil dólares em multas.

14.3.5

## Ataques de Buffer Overflow

A figura mostra um ator ameaçador com um laptop. uma flecha vai do ator da ameaça pela Internet, dois roteadores, um switch e chega a um servidor rotulado como vítima. há quatro envelopes empilhados próximos ao switch.

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. Explorar a memória do buffer sobrecarregando-a com valores inesperados geralmente torna o sistema inoperável, criando um ataque DoS.

Por exemplo, um ator de ameaça insere entrada maior do que o esperado pelo aplicativo em execução em um servidor. O aplicativo aceita a grande quantidade de entrada e armazena na memória. O resultado é que ele pode consumir o buffer de memória associado e potencialmente substituir a memória adjacente, eventualmente corrompendo o sistema e fazendo com que ele falhe.

Um exemplo inicial do uso de pacotes mal formados foi o **Ping of Death**. Nesse ataque herdado, o ator de ameaça enviou um ping de morte, que era uma solicitação de eco em um pacote IP maior que o tamanho máximo de pacote de 65.535 bytes. O host receptor não seria capaz de lidar com um pacote desse tamanho e ele iria falhar.

Os ataques de estouro de buffer estão evoluindo continuamente. Por exemplo, uma vulnerabilidade de ataque remoto de negação de serviço foi descoberta recentemente no Microsoft Windows 10. Especificamente, um ator de ameaça criou código malicioso para acessar memória fora do escopo. Quando esse código é acessado pelo processo AHCACHE.SYS do Windows, ele tenta acionar uma falha do sistema, negando serviço ao usuário. Pesquise na Internet no “blog TALOS-2016-0191” para acessar o site de inteligência de ameaças Cisco Talos e ler uma descrição de tal ataque.

**Observação**: Estima-se que um terço dos ataques mal-intencionados sejam o resultado de estouros de buffer.

14.3.6

**Métodos de Evasão**

Atores de ameaça aprenderam há muito tempo que “esconder é prosperar”. Isso significa que seus métodos de malware e ataque são mais eficazes quando não são detectados. Por esta razão, muitos ataques usam técnicas de evasão furtiva para disfarçar uma carga útil de ataque. Seu objetivo é evitar a detecção, evitando defesas de rede e host.

Alguns dos métodos de evasão usados por atores ameaçadores 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. |
| 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. |
| 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. |

Novos métodos de ataque estão constantemente sendo desenvolvidos. O pessoal de segurança da rede deve estar ciente dos métodos de ataque mais recentes para detectá-los.

# Resumo de ameaças e ataques comuns

14.4.1

## O que aprendi neste módulo?

**Malware**

Malware é a abreviatura de software malicioso ou código malicioso. Os atores de ameaças freqüentemente tentam enganar os usuários para instalar malware para ajudar a explorar vulnerabilidades do dispositivo final. Muitas vezes, o software antimalware não pode ser atualizado com rapidez suficiente para impedir novas ameaças. Três tipos comuns são vírus, worm e cavalo de Tróia. Um vírus é um tipo de malware que se espalha inserindo uma cópia de si mesmo em outro programa. A maioria dos vírus são espalhados por unidades de memória USB, CDs, DVDs, compartilhamentos de rede e e-mail. O malware de cavalo de Tróia é um software que parece ser legítimo, mas contém código malicioso que explora os privilégios do usuário que o executa. Muitas vezes, os cavalos de Tróia são encontrados em jogos online. Os cavalos de Tróia são geralmente classificados de acordo com os danos que causam. Os tipos de cavalos de Tróia incluem acesso remoto, envio de dados, destrutivo, proxy, FTP, desabler de software de segurança, DoS e keylogger. Os worms são semelhantes aos vírus porque se replicam e podem causar o mesmo tipo de dano. Os vírus exigem que um programa host seja executado. Os vermes podem correr sozinhos. A maioria dos ataques de worm consiste em três componentes: habilitação de vulnerabilidade, mecanismo de propagação e carga útil. Atualmente, o ransomware é o malware mais dominante. Ele nega o acesso ao sistema infectado ou aos seus dados. Os criminosos cibernéticos, em seguida, exigem pagamento para liberar o sistema de computador. Outros exemplos de malware incluem spyware, adware, scareware, phishing e rootkits.

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

Os atores de ameaças também podem atacar a rede de fora. Para atenuar os ataques, é útil categorizar os vários tipos de ataques. As três categorias principais são ataques de reconhecimento, acesso e DoS. Reconhecimento é coleta de informações. Os atores da ameaça fazem a descoberta e mapeamento não autorizado de sistemas, serviços ou vulnerabilidades. Os ataques Recon precedem os ataques de acesso ou DoS. Algumas das técnicas utilizadas incluem o seguinte: executar uma consulta de informações de um destino, iniciar uma varredura de ping da rede de destino, iniciar uma varredura de portas de endereços IP ativos, executar varreduras de vulnerabilidades e executar ferramentas de exploração. Os ataques de acesso exploram vulnerabilidades conhecidas em serviços de autenticação, serviços de FTP e serviços da Web. Esses ataques incluem ataques de senha, ataques de spoofing, ataques de exploração de confiança, redirecionamentos de porta, ataques man-in-the-middle e ataques de estouro de buffer. Engenharia social é um ataque de acesso que tenta manipular indivíduos para que executem ações inseguras ou divulguem informações confidenciais. Esses ataques incluem uso de pretextos, phishing, spear phishing, spam, algo por algo, isca, falsificação de identidade, uso não autorizado, surfe nos ombros e lixeira.

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

Os ataques DoS criam algum tipo de interrupção dos serviços de rede para usuários, dispositivos ou aplicativos. Existem dois tipos principais: quantidade esmagadora de tráfego e pacotes formatados com códigos maliciosos. 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. Os termos a seguir são usados para descrever ataques DDoS: zumbis, bots, botnet, manipuladores e botmaster. Mirai é malware que visa dispositivos IoT configurados com informações de login padrão. Mirai usa um ataque de dicionário de força bruta. Após o acesso bem-sucedido, Mirai visa os utilitários BusyBox baseados em Linux que são projetados para esses dispositivos. 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. Explorar a memória do buffer sobrecarregando-a com valores inesperados geralmente torna o sistema inoperável, criando um ataque DoS. Muitos ataques usam técnicas de evasão furtiva para disfarçar uma carga útil de ataque. Os métodos de evasão incluem criptografia e encapsulamento, exaustão de recursos, fragmentação de tráfego, interpretação errada em nível de protocolo, substituição de tráfego, inserção de tráfego, rotação, rootkits e proxies.

**Introdução**

15.0.1

**Por que devo cursar este módulo?**

Como todas as redes estão sob ataque, é importante que você entenda as ferramentas de monitoramento de rede e monitoramento de rede para ajudá-lo a defender e proteger a rede. Leia mais para saber mais sobre esses métodos e ferramentas!

15.0.2

**O que vou aprender neste módulo?**

**Título do módulo**: Monitoramento de rede e ferramentas

**Objetivo do módulo**: Explicar o monitoramento do tráfego de rede.

| **Título do Tópico** | **Objetivo do Tópico** |
| --- | --- |
| Introdução ao monitoramento de rede | Explique a importância do monitoramento da rede. |
| Introdução às ferramentas de monitoramento de rede | Explicar como o monitoramento de rede é realizado. |

15.0.3

**Atividade de Classe — O que está acontecendo?**

Nesta atividade, você identificará os processos em execução em um computador, o protocolo que eles estão usando e seus endereços de porta local e remota.

# Introdução ao monitoramento de rede

15.1.1

## Topologia de segurança de rede

“Todas as redes são alvos” é um ditado comum usado para descrever o cenário atual da segurança de rede. Portanto, para mitigar ameaças, todas as redes devem estar protegidas e protegidas.

Isso requer uma abordagem de defesa em profundidade. Ele requer o uso de métodos comprovados e uma infraestrutura de segurança que consiste em firewalls, sistemas de detecção de intrusões (IDS), sistemas de prevenção de intrusões (IPS) e software de segurança de terminais. Esses métodos e tecnologias são usados para introduzir monitoramento automatizado na rede, criar alertas de segurança ou bloquear automaticamente dispositivos ofensivos quando algo der errado.

No entanto, para grandes redes, uma camada extra de proteção deve ser adicionada. Dispositivos como firewalls e IPS operam com base em regras pré-configuradas. Eles monitoram o tráfego e o comparam com as regras configuradas. Se houver uma correspondência, o tráfego é tratado de acordo com a regra. Isso funciona de forma relativamente perfeita. No entanto, às vezes o tráfego legítimo é confundido com tráfego não autorizado. Chamadas de falsos positivos, essas situações exigem que os olhos humanos os vejam e avaliem antes que possam ser validados.

Uma parte importante do trabalho do analista de segurança cibernética é analisar todos os alertas gerados pelos dispositivos de rede e determinar a validade dos alertas. Esse arquivo que foi baixado pelo usuário X era realmente malware? Esse site que foi visitado pelo usuário Y é realmente malicioso? A impressora no terceiro andar está realmente comprometida porque está tentando se conectar a um servidor que está fora da internet? Estas são perguntas que são normalmente feitas por analistas de segurança diariamente. É seu trabalho determinar as respostas corretas.

15.1.2

## Métodos de monitoramento de rede

A operação diária de uma rede consiste em padrões comuns de fluxo de tráfego, uso de largura de banda e acesso a recursos. Juntos, esses padrões identificam o comportamento normal da rede. Os analistas de segurança devem estar intimamente familiarizados com o comportamento normal da rede porque o comportamento anormal da rede normalmente indica um problema.

Para determinar o comportamento normal da rede, o monitoramento da rede deve ser implementado. Várias ferramentas são usadas para ajudar a descobrir o comportamento normal da rede, incluindo IDS, analisadores de pacotes, SNMP, NetFlow e outros.

Algumas dessas ferramentas exigem dados de rede capturados. Existem dois métodos comuns usados para capturar o tráfego e enviá-lo para dispositivos de monitoramento de rede:

* Torneiras de rede, algumas vezes conhecidas como pontos de acesso de teste (TAPs, test access points)
* Espelhamento de tráfego usando o SPAN (Switch Port Analyzer) ou outro espelhamento de porta.

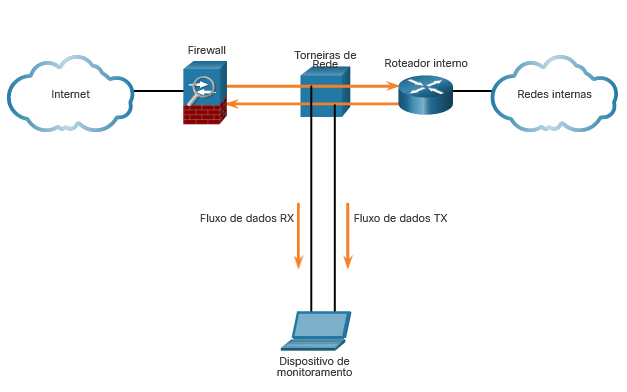
15.1.3

## Taps de rede

Uma torneira de rede é normalmente um dispositivo de divisão passiva implementado em linha entre um dispositivo de interesse e a rede. Uma torneira encaminha todo o tráfego, incluindo erros de camada física, para um dispositivo de análise, permitindo que o tráfego chegue ao destino pretendido.

A figura exibe uma topologia de amostra exibindo uma torneira instalada entre um firewall de rede e o roteador interno.

A imagem é um diagrama de rede que mostra uma torneira de rede posicionada em linha entre um firewall e um roteador. A torneira também está conectada a um dispositivo de monitoramento conectado em uma terceira porta.



Observe como a torneira envia simultaneamente o fluxo de dados de transmissão (TX) do roteador interno e o fluxo de dados de recebimento (RX) para o roteador interno em canais separados e dedicados. Isso garante que todos os dados cheguem ao dispositivo de monitoramento em tempo real. Portanto, o desempenho da rede não é afetado ou degradado pelo monitoramento da conexão.

As torneiras também são normalmente à prova de falhas, o que significa que se uma torneira falhar ou perder energia, o tráfego entre o firewall e o roteador interno não é afetado.

Pesquise na Internet para obter informações sobre NetScout Taps para Ethernet UTP de cobre, Ethernet de fibra e links seriais.

15.1.4

## Espelhamento de tráfego e SPAN

Os switches de rede segmentam a rede por projeto. Isso limita a quantidade de tráfego visível para dispositivos de monitoramento de rede. Como a captura de dados para monitoramento de rede requer que todo o tráfego seja capturado, técnicas especiais devem ser empregadas para contornar a segmentação de rede imposta pelos switches de rede. O espelhamento de portas é uma dessas técnicas. Suportado por muitos switches corporativos, o espelhamento de portas permite que o switch copie quadros recebidos em uma ou mais portas para uma porta SPAN (Switch Port Analyzer) conectada a um dispositivo de análise.

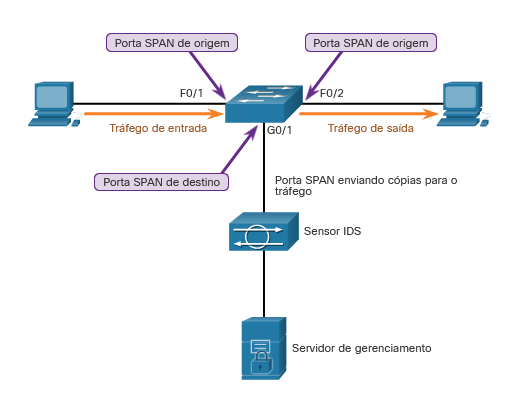
A tabela identifica e descreve os termos usados pelo recurso SPAN.

| **Termo do SPAN** | **Descrição** |
| --- | --- |
| **Tráfego de entrada** | Tráfego que entra no switch. |
| **Tráfego de saída** | Tráfego que sai do switch. |
| **Porta de origem (SPAN)** | As portas de origem são monitoradas à medida que o tráfego que as insere é replicado (espelhado) para as portas de destino. |
| **Porta de destino (SPAN)** | Uma porta que espelha portas de origem. As portas SPAN de destino geralmente se conectam a dispositivos de análise, como um analisador de pacotes ou um IDS. |

A figura mostra um switch que interconecta dois hosts e espelha o tráfego a um IDS (dispositivo de detecção de intrusão) e servidor de gerenciamento de rede.

O diagrama de rede mostra um switch posicionado na rede com duas portas SPAN de origem e uma única porta SPAN de destino.

### SPAN



O switch encaminhará o tráfego de entrada em F0/1 e o tráfego de saída em F0/2 para a porta SPAN G0/1 de destino que se conecta a um IDS.

A associação entre as portas de origem e uma porta de destino é chamada de sessão SPAN. Em uma única sessão, uma ou várias portas podem ser monitoradas. Em alguns switches Cisco, o tráfego de sessão pode ser copiado para mais de uma porta de destino. Como alternativa, uma VLAN de origem pode ser especificada na qual todas as portas na VLAN de origem se tornam fontes de tráfego SPAN. Cada sessão SPAN pode ter portas ou VLANs como origens, mas não ambas.

**Observação**: uma variação de SPAN chamada SPAN Remote SPAN (RSPAN) permite que um administrador de rede use a flexibilidade de VLANs para monitorar o tráfego em switches remotos.

# Introdução às ferramentas de monitoramento de rede

15.2.1

## Ferramentas de monitoramento de segurança de rede

As ferramentas comuns que são usadas para monitoramento de segurança de rede incluem:

* Analisadores de protocolo de rede como Wireshark e Tcpdump
* NetFlow
* Sistemas de gerenciamento de eventos e informações de segurança (SIEM)

Também é comum que analistas de segurança confiem em arquivos de log e SNMP (Simple Network Management Protocol) para detecção de comportamento de rede.

Praticamente todos os sistemas geram arquivos de log para gravar e comunicar suas operações. Ao monitorar de perto os arquivos de log, um analista de segurança pode coletar informações extremamente valiosas.

O SNMP permite que os analistas solicitem e recebam informações sobre a operação de dispositivos de rede. É outra boa ferramenta para monitorar o comportamento de uma rede.

Os analistas de segurança devem estar familiarizados com todas essas ferramentas.

O diagrama lista três ferramentas diferentes de monitoramento de rede: analisadores de protocolo, SIEM e NetFlow.

### Ferramentas comuns de monitoramento de segurança de rede



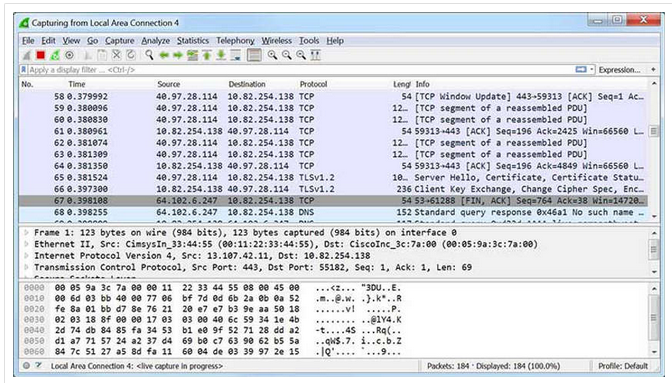
15.2.2

## Analisadores de protocolo

Analisadores de protocolo de rede (ou aplicativos de “sniffer de pacotes”) são programas usados para capturar tráfego. Os analisadores de protocolo mostram o que está acontecendo na rede, muitas vezes através de uma interface gráfica do usuário. Os analistas podem usar esses aplicativos para ver as trocas de rede até o nível do pacote. Se um computador foi infectado com malware e atualmente está atacando outros computadores na rede, o analista pode ver isso claramente capturando tráfego de rede em tempo real e analisando os pacotes.

Os analisadores de protocolo de rede não são usados apenas para análise de segurança. Eles também são muito úteis para solução de problemas de rede, desenvolvimento de software, desenvolvimento de protocolo e educação. Por exemplo, na perícia de segurança, um analista de segurança pode tentar reconstruir um incidente a partir de capturas de pacotes relevantes.

Wireshark, mostrado na figura, é uma ferramenta analisadora de protocolo de rede muito popular que é usada em ambientes Windows, Linux e Mac OS. Wireshark é um software livre que pode ser baixado e usado por qualquer pessoa. É uma ferramenta muito útil para aprender sobre comunicações de protocolo de rede. As habilidades do analisador de protocolo de rede são essenciais para analistas de segurança cibernética.



Os quadros capturados pelo Wireshark são salvos em um arquivo PCAP. Os arquivos PCAP contêm as informações de quadro, informações de interface, comprimento do pacote, carimbos de data/hora e até mesmo arquivos binários inteiros que são enviados pela rede.

A execução de uma captura de pacotes de longo prazo produz arquivos PCAP grandes.

O Wireshark também pode abrir arquivos que contêm tráfego capturado de outros softwares, como o utilitário **tcpdump**. Popular entre os sistemas Unix como Linux, **tcpdump** é um utilitário poderoso com inúmeras opções de linha de comando. O exemplo na saída do comando exibe uma **tcpdump** captura de exemplo de **ping** pacotes.

[root@secOps analyst]# **tcpdump -i hl-eth0 -n**

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on hl-eth0, link-type EN10MB (Ethernet), capture size 262144 bytes

10:42:19.841549 IP 10.0.0.12 > 10.0.0.11: ICMP echo request, id 2279, seq 5, length 64

10:42:19.841570 IP 10.0.0.11 > 10.0.0.12: ICMP echo reply, id 2279, seq 5, length 64

10:42:19.854287 IP 10.0.0.12 > 10.0.0.11: ICMP echo request, id 2279, seq 6, length 64

10:42:19.854304 IP 10.0.0.11 > 10.0.0.12: ICMP echo reply, id 2279, seq 6, length 64

10:42:19.867446 IP 10.0.0.12 > 10.0.0.11: ICMP echo request, id 2279, seq 7, length 64

10:42:19.867468 IP 10.0.0.11 > 10.0.0.12: ICMP echo reply, id 2279, seq 7, length 64

^C

6 packets captured

6 packets received by filter

0 packets dropped by kernel

[root@secOps analyst]#

**Observação**: \*\*windump\*\* é uma variante do Microsoft Windows do \*\*tcpdump\*\*. \*\*tshark\*\* é uma ferramenta de linha de comando Wireshark semelhante a \*\*tcpdump\*\*.

15.2.3

## NetFlow

NetFlow é uma tecnologia Cisco IOS que fornece estatísticas 24 horas por dia, 7 dias por semana em pacotes que fluem através de um roteador Cisco ou switch multicamada. NetFlow é o padrão para coletar dados operacionais IP em redes IP. O NetFlow agora é compatível com plataformas não Cisco. IP Flow Information Export (IPFIX) é uma versão do NetFlow que é um protocolo padrão IETF.

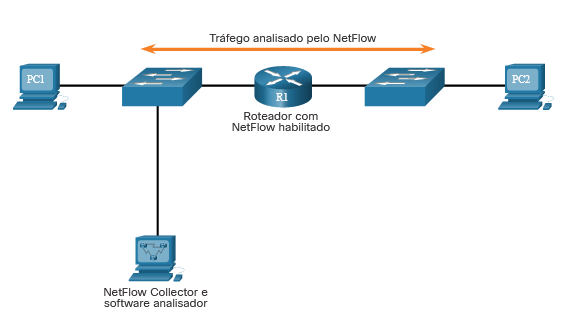
O NetFlow pode ser usado para monitoramento de rede e segurança, planejamento de rede e análise de tráfego. Ele fornece uma trilha de auditoria completa de informações básicas sobre cada fluxo de IP encaminhado em um dispositivo. Essas informações incluem as informações de IP do dispositivo de origem e destino, a hora da comunicação e a quantidade de dados transferidos. O NetFlow não captura o conteúdo real no fluxo. A funcionalidade NetFlow é frequentemente comparada a uma conta telefônica. A conta identifica o número de destino, a hora e a duração da chamada. No entanto, ele não exibe o conteúdo da conversa telefônica.

Embora o NetFlow armazene informações de fluxo em um cache local no dispositivo, ele deve sempre ser configurado para encaminhar dados para um coletor NetFlow que armazene os dados NetFlow. Há várias ferramentas de terceiros para análise de dados NetFlow.

Por exemplo, na figura, PC1 se conecta ao PC2 usando um aplicativo como HTTPS.

A imagem é um diagrama de rede. Da esquerda para a direita, há dois PCs conectados a um switch, conectados a um roteador rotulado R1, que está conectado a outro switch e a outro PC. R1 é um roteador habilitado para NetFlow. No diagrama, um dos PCs à esquerda é rotulado como NetFlow Collector and Analyzer Software. O diagrama tem uma seta bidirecional acima de R1 mostrando que o tráfego que flui através de R1 está sendo analisado pelo NetFlow.

### NetFlow na rede



O NetFlow pode monitorar essa conexão de aplicativo rastreando contagens de bytes e pacotes para esse fluxo de aplicativo individual. Em seguida, envia as estatísticas para um servidor externo chamado coletor NetFlow.

Por exemplo, o Cisco Stealthwatch coleta estatísticas do NetFlow para executar funções avançadas, incluindo:

* **Costura de fluxo -** Ele agrupa entradas individuais em fluxos.
* **Desduplicação de fluxo** - Filtra entradas duplicadas de vários clientes NetFlow.
* **Costura NAT** - Simplifica os fluxos com entradas NAT.

Há um canal Cisco Stealthwatch no YouTube que fornece muitos detalhes sobre o Stealthwatch e seus usos.

15.2.4

**SIEM e SOAR**

Os analistas de segurança de rede devem avaliar com rapidez e precisão o significado de qualquer evento de segurança e responder às seguintes perguntas críticas:

* Quem está associado a este evento?
* O usuário tem acesso a outros recursos confidenciais?
* Esse evento representa um problema de conformidade em potencial?
* O usuário tem acesso a propriedade intelectual ou informações confidenciais?
* O usuário está autorizado a acessar esse recurso?

Para ajudar a responder a essas perguntas, os analistas de segurança usam:

* Gerenciamento de eventos de informações de segurança (SIEM, Security Information Event Management)
* Orquestração, automação e resposta de segurança (SOAR, Security orchestration, automation and response,)

SIEM

O SIEM (Security Information Event Management) é uma tecnologia usada em organizações empresariais para fornecer relatórios em tempo real e análise de longo prazo de eventos de segurança.

Dispositivos de rede, incluindo firewall, IPSs, ESAs, WSAs, roteadores, switches, servidores e hosts, são configurados para enviar eventos de log para o software SIEM. O software SIEM correlaciona milhões de eventos usando aprendizado de máquina e software de análise especial para identificar o tráfego que deve ser investigado.

Os sistemas SIEM incluem as seguintes funções essenciais:

* **Análise forense** — A capacidade de pesquisar logs e registros de eventos de fontes em toda a organização. Ele fornece informações mais completas para análise forense.
* **Correlação** — examina logs e eventos de diferentes sistemas ou aplicativos, acelerando a detecção e reação a ameaças de segurança.
* **Agregação** - A agregação reduz o volume de dados de eventos consolidando registros de eventos duplicados.
* **Reporting** - Reporting apresenta os dados de eventos correlacionados e agregados em monitoramento em tempo real e resumos de longo prazo.

O SIEM fornece detalhes sobre a origem da atividade suspeita:

* Informações do usuário, como nome de usuário, status de autenticação, localização.
* Informações do dispositivo, como fabricante, modelo, versão do sistema operacional, endereço MAC, método de conexão de rede e localização.
* Informações de postura, como se o dispositivo é compatível com a política de segurança, tem arquivos antivírus atualizados e é atualizado com os patches de SO mais recentes.

SOAR

A orquestração, automação e resposta de segurança (SOAR) aprimora o SIEM. Ele ajuda as equipes de segurança a investigar incidentes de segurança e adiciona coleta de dados aprimorada e várias funcionalidades que ajudam na resposta a incidentes de segurança.

Soluções SOAR:

* Fornece ferramentas de gerenciamento de casos que permitem que o pessoal de segurança cibernética pesquise e investigue incidentes, frequentemente integrando inteligência contra ameaças à plataforma de segurança de rede.
* Use inteligência artificial para detectar incidentes e auxiliar na análise e resposta a incidentes.
* Automatize procedimentos complexos de resposta a incidentes e investigações, que são tarefas potencialmente intensas de mão-de-obra executadas pela equipe do centro de operações de segurança (SOC) executando livros de execução. Esses são playbooks que executam ações como acessar e analisar dados relevantes, tomar medidas para isolar sistemas comprometidos e pesquisar ameaças para validar alertas e executar uma resposta a incidentes.
* Oferece painéis e relatórios para documentar a resposta a incidentes para melhorar os principais indicadores de desempenho do SOC e pode melhorar consideravelmente a segurança da rede para as organizações.

O SIEM ajuda a soar o alarme para atividades mal-intencionadas. Os analistas terão que agir sobre a ameaça. A SOAR ajuda os analistas a responder à ameaça.

15.2.5

**Sistemas SIEM**

Existem vários sistemas SIEM. O SolarWinds Security Event Manager e o Splunk Enterprise Security são dois dos sistemas SIEM proprietários mais populares usados pelos SoCs. Pesquise na internet para saber mais sobre esses produtos.

Neste curso, usaremos um produto de código aberto chamado Security Onion que inclui o pacote ELK para a funcionalidade SIEM. ELK é um acrônimo para três produtos da Elastic:

* **Elasticsearch** - Mecanismo de pesquisa de texto completo orientado para documentos
* **Logstash** - Sistema de processamento de pipeline que conecta “entradas” a “saídas” com “filtros” opcionais entre
* **Kibana** - Análise baseada em navegador e painel de pesquisa para Elasticsearch

Pesquise na internet para saber mais sobre Elastic.co e seu conjunto de produtos.

# Resumo de monitoramento e ferramentas de rede

15.3.1

## O que aprendi neste módulo?

**Topologia de segurança de rede**

Para mitigar ameaças, todas as redes devem ser protegidas usando uma abordagem de defesa profunda. Isso requer o uso de métodos comprovados e uma infraestrutura de segurança que consiste em firewalls, sistemas de detecção de intrusões (IDS), sistemas de prevenção de intrusões (IPS) e software de segurança de terminais. Para redes grandes, uma camada extra de proteção deve ser adicionada. Um analista de segurança cibernética precisa revisar todos os alertas gerados por dispositivos de rede e validá-los. Para determinar o comportamento normal da rede, o monitoramento da rede deve ser implementado. As ferramentas incluem IDS, analisadores de pacotes, SNMP, NetFlow e outros. Dois métodos comuns usados para capturar tráfego e enviá-lo para dispositivos de monitoramento de rede são torneiras de rede (TAPs) e espelhamento de tráfego usando o SPAN (Switch Port Analyzer) ou outro espelhamento de porta. Um Tap de rede é normalmente um dispositivo de divisão passiva implementado em linha entre um dispositivo de interesse e a rede. Um Tap encaminha todo o tráfego, incluindo erros de camada física, para um dispositivo de análise, permitindo que o tráfego chegue ao destino pretendido. Os switches de rede segmentam o design da rede Isso limita a quantidade de tráfego visível para dispositivos de monitoramento de rede. Devido a isso, a captura de dados para monitoramento de rede requer que todo o tráfego ignore a segmentação de rede imposta pelos switches de rede. O espelhamento de portas é uma técnica que permite isso. Os termos a seguir são usados pelo recurso SPAN: tráfego de entrada, tráfego de saída, porta (SPAN) de origem e porta (SPAN) de destino.

**Introdução às ferramentas de monitoramento de rede**

Ferramentas comuns que são usadas para monitoramento de segurança de rede incluem analisadores de protocolo de rede (Wireshark e Tcpdump), NetFlow e Sistemas de Gerenciamento de Eventos e Informações de Segurança (SIEM). Também é comum que analistas de segurança confiem em arquivos de log e SNMP (Simple Network Management Protocol) para detecção de comportamento de rede. Os analisadores de protocolo de rede (“sniffers de pacotes”) são programas usados para capturar tráfego. Eles mostram o que está acontecendo na rede, muitas vezes através de uma interface gráfica do usuário. Os analistas podem usar esses aplicativos para ver as trocas de rede até o nível do pacote. Netflow é um recurso Cisco IOS que fornece estatísticas 24 horas por dia, 7 dias por semana em pacotes que fluem por meio de um roteador Cisco ou switch multicamada. Ele pode ser usado para monitoramento de rede e segurança, planejamento de rede e análise de tráfego. O SIEM é uma tecnologia que é usada para fornecer relatórios em tempo real e análise de longo prazo de eventos de segurança. O SIEM inclui análise forense e funções de correlação, agregação e geração de relatórios. Existem vários sistemas SEIM, incluindo SolarWinds Security Manager e Splunk Enterprise Security. Os sistemas de orquestração de seguranças, automação e resposta (SOAR) fornecem aprimoramentos ao SIEM.

# Introdução

16.0.1

## Por que devo cursar este módulo?

Protocolos são a base das comunicações de dados. Por esta razão, eles têm sido alvo de agentes ameaçadores há muito tempo. Os analistas de segurança cibernética devem entender como os atores de ameaças usam recursos de protocolos comuns em ataques cibernéticos.

Este módulo fornece uma visão geral dos campos de pacotes IP da Camada 3 e dos campos de segmento TCP e UDP da Camada 4, e discute as vulnerabilidades de cada um.

16.0.2

## O que vou aprender neste módulo?

**Título do módulo:** Atacando a Fundação

**Objetivo do módulo:** Explicar como as vulnerabilidades de TCP / IP permitem ataques à rede.

| **Título do Tópico** | **Objetivo do Tópico** |
| --- | --- |
| Detalhes de PDU IP | Explicar a estrutura de cabeçalho IPv4 e IPv6. |
| Vulnerabilidades de IP | Explicar como as vulnerabilidades de IP possibilitam ataques de rede. |
| Vulnerabilidades TCP e UDP | Explicar como as vulnerabilidades de TCP e UDP possibilitam ataques de rede. |

# Detalhes de PDU IP

16.1.1

## IPv4 e IPv6

O IP foi projetado como um protocolo sem conexão de Camada 3. Ele fornece as funções necessárias para entregar um pacote de um host de origem a um host de destino por meio de um sistema interconectado de redes. O protocolo não foi projetado para rastrear e gerenciar o fluxo de pacotes. Essas funções, se necessárias, são executadas principalmente pelo TCP na camada 4.

O IP não faz nenhum esforço para validar se o endereço IP de origem contido em um pacote realmente veio dessa origem. Por esse motivo, os agentes de ameaças podem enviar pacotes usando um endereço IP de origem falsificado. Além disso, os agentes da ameaça podem adulterar os outros campos do cabeçalho IP para realizar seus ataques. Portanto, é importante que os analistas de segurança entendam os diferentes campos dos cabeçalhos IPv4 e IPv6.

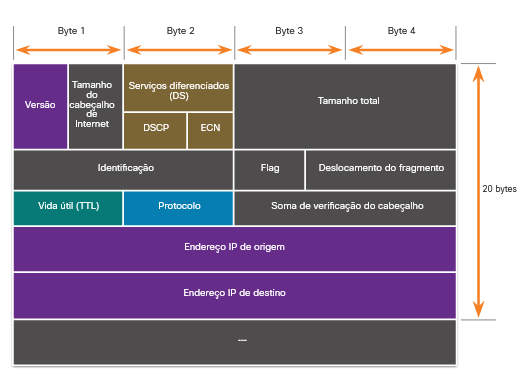
16.1.2

## O cabeçalho do pacote IPv4

Os campos no cabeçalho do pacote IPv4 são mostrados na figura.

A figura mostra cinco linhas de palavras. Acima das linhas estão quatro seções uniformes rotuladas byte 1 byte 2 byte 3 byte 4. Abaixo do lado das linhas, há uma linha com setas em ambas as extremidades correndo de cima para baixo rotuladas 20 bytes. A linha superior tem 4 blocos principais. O primeiro bloco é rotulado versão e seu tamanho é metade do byte 1. O próximo bloco é o comprimento do cabeçalho da internet que leva o resto do byte 1. Byte 2 é tomado por serviços diferenciados (DS) que é subdividido em DSCP e ECN. Bytes 3 e 4 têm um bloco rotulado comprimento total. A segunda linha tem três seções: identificação que é executada em bytes 1 e 2, sinalizador que usa até três quartos do byte 3 e deslocamento de fragmento que leva o resto. A linha 3 tem 3 seções principais rotuladas tempo para viver que ocupa byte 1, protocolo que ocupa byte 2 e soma de verificação de cabeçalho que leva bytes 3 e 4. A linha 4 é rotulada de origem i p endereço e é executada através dos 4 bytes. A linha 5 é rotulada destino i p endereço e é executada através dos 4 bytes.

### Cabeçalho do Pacote IPv4



A tabela descreve os campos de cabeçalho IPv4.

| **Campo de cabeçalho IPv4** | **Descrição** |
| --- | --- |
| **Versão** | * Contém um valor binário de 4 bits definido como 0100 que identifica isso como um pacote IPv4. |
| **Comprimento do cabeçalho da Internet** | * Um campo de 4 bits contendo o comprimento do cabeçalho IP. * O comprimento mínimo de um cabeçalho IP é de 20 bytes. |
| **Serviços diferenciados ou DiffServ (DS)** | * Anteriormente chamado de campo Tipo de serviço (ToS), o campo DS é um campo de 8 bits usado para determinar a prioridade de cada pacote. * Os seis bits mais significativos do campo DiffServ são o Ponto de código de serviços diferenciados (DSCP). * Os dois últimos bits são os bits de notificação de congestionamento explícito (ECN). |
| **Comprimento total** | * Especifica o comprimento do pacote IP, incluindo o cabeçalho IP e os dados do usuário. * O campo de comprimento total é de 2 bytes, portanto, o tamanho máximo de um pacote IP é de 65.535 bytes, no entanto, os pacotes são muito menores na prática. |
| **Deslocamento de identificação, bandeira e fragmento** | * À medida que um pacote IP se move pela Internet, talvez seja necessário cruzar uma rota que não possa lidar com o tamanho do pacote. * O pacote será dividido, ou fragmentado, em pacotes menores e remontado posteriormente. * Esses campos são usados para fragmentar e remontar pacotes. |
| **Tempo de Vida (TTL)** | * Contém um valor binário de 8 bits que é usado para limitar a vida útil de um pacote. * O remetente do pacote define o valor inicial do TTL e este é subtraído de um toda vez que o pacote é processado por um roteador. * Se o campo TTL for decrementado até zero, o roteador descartará o pacote e enviará uma mensagem ICMP de tempo excedido para o endereço IP de origem. |
| **Protocolo** | * O campo é usado para identificar o protocolo de próximo nível. * O valor binário de 8 bits indica o tipo de carga de dados que o pacote está carregando, o que permite que a camada de rede transfira os dados para o protocolo apropriado das camadas superiores. * Valores comuns incluem ICMP (1), TCP (6) e UDP (17). |
| **Cabeçalho checksum** | * Um valor calculado com base no conteúdo do cabeçalho IP. * Usado para determinar se algum erro foi introduzido durante a transmissão. |
| **Endereço IPv4 Origem** | * Contém um valor binário de 32 bits que representa o endereço IPv4 de origem do pacote. * O endereço de origem IPv 4 é sempre um endereço unicast. |
| **Endereço IPv4 de destino** | * Contém um valor binário de 32 bits que representa o endereço IPv4 de destino do pacote. |
| **Opções e Preenchimento** | * Este é um campo que varia em comprimento de 0 a um múltiplo de 32 bits. * Se os valores de opção não forem um múltiplo de 32 bits, 0s serão adicionados ou preenchidos para garantir que este campo contenha um múltiplo de 32 bits. |

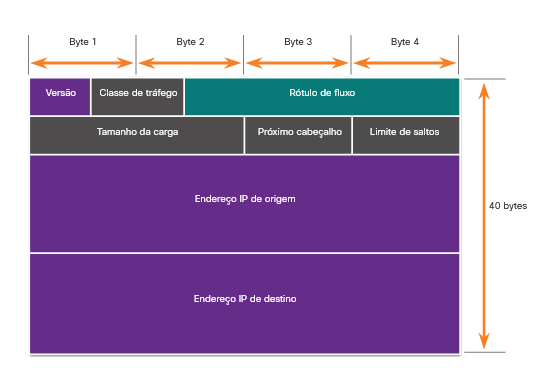
16.1.4

## O cabeçalho do pacote IPv6

Há oito campos no cabeçalho do pacote IPv6, como mostrado na figura.

A figura mostra quatro linhas de palavras. Acima das linhas estão quatro seções uniformes rotuladas byte 1 byte 2 byte 3 byte 4. Abaixo do lado das linhas, há uma linha com setas em ambas as extremidades correndo de cima para baixo rotuladas 40 bytes. A linha superior tem 4 blocos principais. O primeiro bloco é rotulado versão e seu tamanho é metade do byte 1. O próximo bloco é a classe de tráfego que leva o resto do byte 1 e metade do byte 2. O último bloco é rotulado rótulo de fluxo que leva metade do byte 2 e todos os bytes 3 e 4. Byte 2 é tomado por serviços diferenciados (DS) que é subdividido em DSCP e ECN. Bytes 3 e 4 têm um bloco rotulado comprimento total. A segunda linha tem três seções: comprimento de carga que é executado em bytes 1 e 2, próximo cabeçalho que usa byte 3 e limite de salto que usa byte 4. A terceira linha é rotulada de origem i p endereço e é executado através dos 4 bytes. A quarta linha é rotulada destino i p endereço e é executado através dos 4 bytes.

### Cabeçalho do Pacote IPv6



A tabela descreve os campos de cabeçalho IPv6.

| **Campo de cabeçalho IPv6** | **Descrição** |
| --- | --- |
| **Versão** | * Este campo contém um valor binário de 4 bits definido como 0110 que o identifica como um pacote IPv6. |
| **Classe de tráfego** | * Este campo de 8 bits é equivalente ao campo IPv4 Differentiated Services (DS). |
| **Rótulo de fluxo** | * Este campo de 20 bits sugere que todos os pacotes com o mesmo rótulo de fluxo recebem o mesmo tipo de tratamento pelos roteadores. |
| **Tamanho da carga** | * Este campo de 16 bits indica o comprimento da porção de dados ou carga útil do pacote IPv6. |
| **Próximo cabeçalho** | * Este campo de 8 bits é equivalente ao campo do protocolo IPv4. * Ele exibe o tipo de carga de dados que o pacote está carregando, permitindo que a camada de rede transfira os dados para o protocolo apropriado das camadas superiores. |
| **Limite de saltos** | * Este campo de 8 bits substitui o campo TTL IPv4. * Esse valor é subtraído de um por cada roteador que encaminha o pacote. * Quando o contador chega a 0, o pacote é descartado e uma mensagem ICMPv6 de Tempo Excedido é encaminhada ao host emissor, indicando que o pacote não atingiu seu destino por causa do limite de saltos. |
| **Endereço IPv6 Origem** | * Este campo de 128 bits identifica o endereço IPv6 do host de envio. |
| **Endereço IPv6 Destino** | * Este campo de 128 bits identifica o endereço IPv6 do host receptor. |

Um pacote IPv6 também pode conter cabeçalhos de extensão (EH) que fornecem informações opcionais da camada de rede. Opcionais, os cabeçalhos de extensão ficam posicionados entre o cabeçalho IPv6 e a carga. EHs são usados para fragmentação, segurança, suporte à mobilidade e muito mais.

Ao contrário de IPv4, os roteadores não fragmentam os pacotes IPv6 roteados.

# Vulnerabilidades de IP

16.2.1

## Vulnerabilidades de IP

Existem diferentes tipos de ataques que visam IP. A tabela lista alguns dos ataques mais comuns relacionados a IP.

| **Ataques IP** | **Descrição** |
| --- | --- |
| **Ataques ICMP** | Os atores de ameaças usam pacotes de eco (pings) do ICMP (Internet Control Message Protocol) para descobrir sub-redes e hosts em uma rede protegida, gerar ataques de inundação de DoS e alterar as tabelas de roteamento de hosts. |
| **Ataques de negação de serviço (DoS)** | Os atores da ameaça tentam impedir que usuários legítimos acessem informações ou serviços. |
| **Ataques de negação de serviço distribuída (DDoS)** | Semelhante a um ataque DoS, mas apresenta um ataque simultâneo e coordenado de várias máquinas de origem. |
| **Ataque de Falsificação de Endereços** | Os atores da ameaça falsificam o endereço IP de origem na tentativa de executar falsificação cega ou não cega. |
| **Ataque man-in-the-middle (MiTM)** | Os agentes de ameaças se posicionam entre uma fonte e um destino para monitorar, capturar e controlar de forma transparente a comunicação. Eles poderiam simplesmente espiar inspecionando os pacotes capturados ou alterando os pacotes e encaminhando-os ao seu destino original. |
| **sequestro de sessão** | Os atores da ameaça obtêm acesso à rede física e, em seguida, usam um ataque MiTM para sequestrar uma sessão. |

16.2.2

## Ataques ICMP

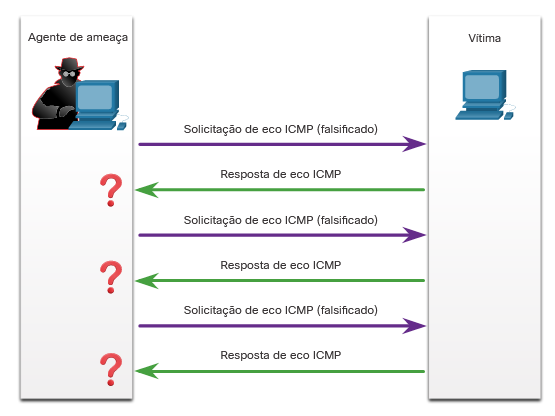
O ICMP foi desenvolvido para transportar mensagens de diagnóstico e relatar condições de erro quando rotas, hosts e portas não estão disponíveis. Mensagens ICMP são geradas por dispositivos quando ocorre um erro de rede ou uma interrupção. O comando ping é uma mensagem ICMP gerada pelo usuário, chamada de solicitação de eco, usada para verificar a conectividade com um destino.

Os agentes de ameaças usam o ICMP para ataques de reconhecimento e varredura. Isso permite que eles lancem ataques de coleta de informações para mapear uma topologia de rede, descobrir quais hosts estão ativos (acessíveis), identificar o sistema operacional do host (impressão digital do sistema operacional) e determinar o estado de um firewall.

Os atores de ameaças também usam ICMP para ataques DoS e DDoS, conforme mostrado no ataque de inundação ICMP na figura.

A figura mostra um atacante e p c à esquerda e um p c rotulado vítima à direita. O invasor envia uma solicitação de eco i c m p (falsificada). O computador da vítima responde com uma resposta de eco i c m p. Um ponto de interrogação é mostrado sob o atacante. O invasor envia uma solicitação de eco i c m p (falsificada) novamente. O computador da vítima envia outra resposta i c m p eco com um ponto de interrogação sob o atacante. Os atacantes enviam outro pedido de eco i c m p (falsificado) para o computador da vítima e o computador da vítima responde com uma resposta de eco icmp. Há o mesmo ponto de interrogação sob o ícone do atacante.

### Inundação ICMP



Agente de ameaçaVítimaSolicitação de eco ICMP (falsificado)Solicitação de eco ICMP (falsificado)Solicitação de eco ICMP (falsificado)Resposta de eco ICMPResposta de eco ICMPResposta de eco ICMP

**Nota**: O ICMP para IPv4 (ICMPv4) e o ICMP para IPv6 (ICMPv6) são suscetíveis a tipos semelhantes de ataques.

A tabela lista mensagens ICMP comuns de interesse para os atores da ameaça.

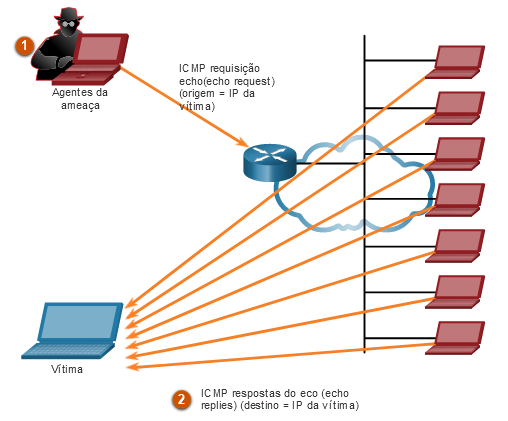
| **Mensagem ICMP** | **Descrição** |
| --- | --- |
| **ICMP solicitação de eco (echo request) e resposta do eco (echo reply)** | Isso é usado para executar verificação de host e ataques de DoS. |
| **ICMP inacessível** | Isso é usado para executar ataques de reconhecimento e varredura de rede. |
| **Resposta da máscara ICMP** | Isso é usado para mapear uma rede IP interna. |
| **redirecionamentos ICMP** | Isso é usado para atrair um host alvo para enviar todo o tráfego através de um dispositivo comprometido e criar um ataque MiTM. |
| **Descoberta de rotas ICMP** | Isso é usado para injetar entradas de rota falsas na tabela de roteamento de um host de destino. |

As redes devem ter uma filtragem rigorosa da lista de controle de acesso ICMP (ACL) na borda da rede para evitar a sondagem ICMP vindo da Internet. Os analistas de segurança devem ser capazes de detectar ataques relacionados ao ICMP, observando o tráfego capturado e os arquivos de log. No caso de grandes redes, os dispositivos de segurança, como firewalls e sistemas de detecção de intrusão (IDS), devem detectar tais ataques e gerar alertas para os analistas de segurança.

16.2.4

## Ataques de amplificação e reflexão

Os agentes de ameaças geralmente usam técnicas de amplificação e reflexão para criar ataques de negação de serviço (DoS). O exemplo na figura ilustra como uma técnica de amplificação e reflexão chamada ataque Smurf é usada para sobrecarregar um host alvo.



Agentes da ameaçaICMP requisição echo(echo request) (origem = IP da vítima)VítimaICMP respostas do eco (echo replies) (destino = IP da vítima)

1. **Amplification** - The threat actor forwards ICMP echo request messages to many hosts. Essas mensagens contêm o endereço IP de origem da vítima.
2. **Reflection** - These hosts all reply to the spoofed IP address of the victim to overwhelm it.

**Nota**:Novas formas de ataques de amplificação e reflexão, como ataques de reflexão e amplificação com base no DNS e ataques de amplificação do Network Time Protocol (NTP), agora estão sendo usados.

Os agentes de ameaças também usam ataques de exaustão de recursos. Esses ataques consomem os recursos de um host de destino para travá-lo ou consumir os recursos de uma rede.

16.2.5

## Ataque de Falsificação de Endereços

Os ataques de falsificação de endereço IP ocorrem quando um agente de ameaça cria pacotes com informações falsas de endereço IP de origem para ocultar a identidade do remetente ou para se passar por outro usuário legítimo. O agente de ameaças pode obter acesso a dados inacessíveis ou burlar as configurações de segurança. A falsificação é geralmente incorporada a outro ataque, como um ataque Smurf.

Os ataques de falsificação podem ser cegos ou não cegos:

* **Falsificação não cega** - O agente da ameaça pode ver o tráfego que está sendo enviado entre o host e o destino. O agente de ameaça usa a falsificação não cega para inspecionar o pacote de resposta da vítima alvo. A falsificação não cega determina o estado de um firewall e prever número de sequência. Também pode seqüestrar uma sessão autorizada.
* **Falsificação cega** - O agente da ameaça não pode ver o tráfego que está sendo enviado entre o host e o destino. A falsificação cega é usada em ataques de negação de serviço.

Os ataques de falsificação de endereço MAC são usados quando os atores de ameaças têm acesso à rede interna. Os agentes de ameaças alteram o endereço MAC de seu host para corresponder a outro endereço MAC conhecido de um host de destino, conforme mostrado na figura. O host atacante envia um quadro pela rede com o endereço MAC recém-configurado. Quando o switch recebe o quadro, ele examina o endereço MAC de origem.

Um servidor e um agente de ameaças estão conectados ao mesmo switch. O serviidor com endereço MAC de AABBCC e está conectado na porta 1. O agente de ameaças está conectado na porta 2 e falsificou o endereço MAC para AABBCC. Um anúncio do agente de ameaça diz: Alterei o endereço MAC no meu computador para corresponder ao servidor. Um diagrama acima do switch indica que ele mapeou o AABBCC para a porta 1. A porta 2 não possui um mapeamento.

### Ator de ameaça falsifica o endereço MAC de um servidor

## 

O switch substitui a entrada atual da tabela CAM e atribui o endereço MAC à nova porta, como mostrado na figura. Em seguida, encaminha os quadros destinados ao host de destino para o host atacante.

Um servidor e um agente de ameaças estão conectados ao mesmo switch. O serviidor com endereço MAC de AABBCC e está conectado na porta 1. O agente de ameaças está conectado na porta 2 e falsificou o endereço MAC para AABBCC. o anúncio abaixo do switch diz: O dispositivo com endereço MAC AABBCC foi movido para a porta 2. Preciso ajustar minha tabela de endereços MAC apropriadamente. Um diagrama acima do switch indica que ele mapeou o AABBCC para a porta 2. A porta 1 não possui um mapeamento.

### O Switch atualiza a tabela CAM com endereço falsificadoSwitch atualiza a tabela CAM com endereço falsificado

## 

A falsificação de aplicativos ou serviços é outro exemplo de falsificação. Um agente de ameaça pode conectar um servidor DHCP não autorizado para criar uma condição MiTM.

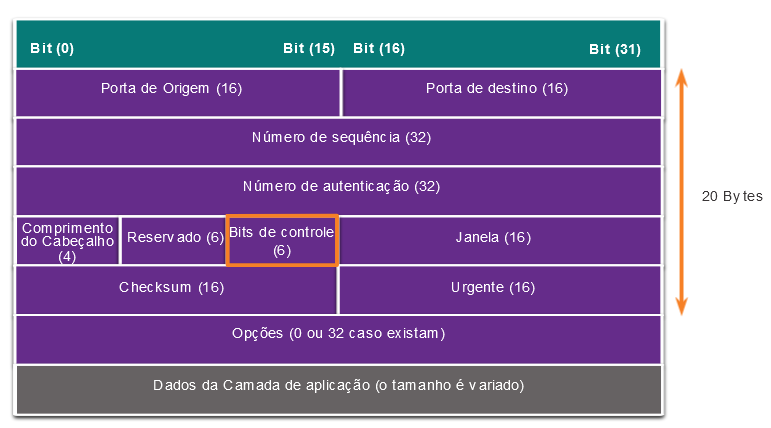
# Vulnerabilidades TCP e UDP

16.3.1

## Cabeçalho do segmento TCP

Enquanto alguns ataques têm como alvo o IP, este tópico discute ataques que têm como alvo o TCP e o UDP.

As informações do segmento TCP aparecem imediatamente após o cabeçalho IP. Os campos do segmento TCP e os sinalizadores para o campo bits de controle são exibidos na figura.



O diagrama mostra os campos de um cabeçalho de segmento TCP. Os campos e seus bits em tamanho são: Porta origem (16), porta destino (16), número de sequência (32), número de confirmação (32), tamanho do cabeçalho (4), reservado (6) bits de controle (6), janela (16), número de checagem (16), urgente (16), opções (0 ou 32, se houver). Os campos do cabeçalho são seguidos pelos dados da camada de aplicativo (o tamanho varia).

20 Bytes**Bit (0)Bit (15)Bit (16)Bit (31)**Porta de Origem (16)Porta de destino (16)Número de sequência (32)Número de autenticação (32)Comprimento do Cabeçalho (4)Janela (16)Checksum (16)Urgente (16)Opções (0 ou 32 caso existam)Dados da Camada de aplicação (o tamanho é variado)Reservado (6)Bits de controle (6)

A seguir, os seis bits de controle do segmento TCP:

* **URG** - Campo de ponteiro urgente significativo.
* **ACK** - Campo de confirmação significativo
* **PSH** - Função Push.
* **RST** - Redefina a conexão
* **SYN** - Sincronizar números de sequência
* **FIN** - Não há mais dados do remetente

16.3.2

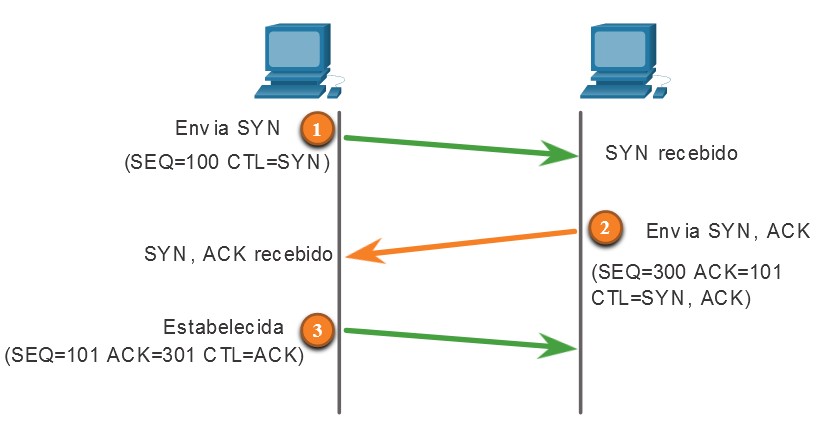
## Serviços TCP

O TCP fornece estes serviços:

* **Entrega confiável** - O TCP incorpora reconhecimentos para garantir a entrega, em vez de confiar nos protocolos da camada superior para detectar e resolver erros. Se uma confirmação não for recebida à tempo, o remetente retransmitirá os dados. Exigir reconhecimentos dos dados recebidos pode causar atrasos substanciais. Exemplos de protocolos da camada de aplicação que usam a confiabilidade do TCP incluem HTTP, SSL / TLS, FTP, transferências de zona DNS e outros.
* **Controle de fluxo** - O TCP implementa o controle de fluxo para solucionar esse problema. Em vez de reconhecer um segmento de cada vez, vários segmentos podem ser reconhecidos com um único segmento de reconhecimento.
* **Comunicação com estado** - A comunicação com estado TCP entre duas partes ocorre durante o aperto de mãos triplo TCP. Antes que os dados possam ser transferidos usando o TCP, um aperto de mãos triplo abre a conexão TCP, conforme mostrado na figura. Se ambos os lados concordarem com a conexão TCP, os dados poderão ser enviados e recebidos por ambas as partes usando o TCP.

O gráfico é uma ilustração da troca de mensagens entre dois hosts durante o aperto de mãos triplo do TCP. Começa quando o cliente envia uma mensagem com o bit de controle SYN definido (SEQ=100 CTL=SYN). Isso é recebido pelo servidor que responde enviando uma mensagem com os bits de controle SYN e ACK definidos (SEQ=300 ACK=101 CTL=SYN, ACK). O cliente recebe o SYN, ACK e responde enviando uma mensagem com o bit de controle ACK definido(SEQ=101 ACK=301 CTL=ACK) e a sessão é estabelecida.

### Aperto de mão de três vias TCP

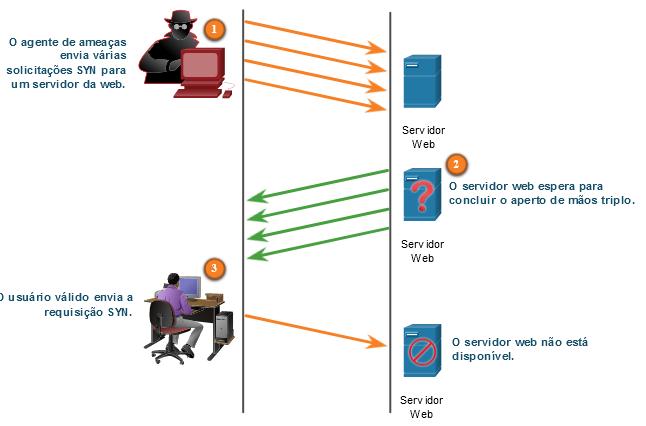


Envia SYN(SEQ=100 CTL=SYN)SYN, ACK recebidoEstabelecida(SEQ=101 ACK=301 CTL=ACK)SYN recebidoEnvia SYN, ACK(SEQ=300 ACK=101 CTL=SYN, ACK)

Uma conexão TCP é estabelecida em três etapas:

1. O cliente iniciador requisita uma sessão de comunicação cliente-servidor com o servidor.
2. O servidor confirma a sessão de comunicação cliente-servidor e requisita uma sessão de comunicação de servidor-cliente.
3. O cliente iniciador confirma a sessão de comunicação de servidor-cliente.

### Ataque de Inundação de SYN TCP



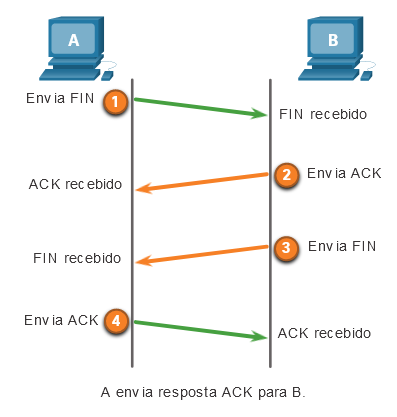
**O agente de ameaças envia várias solicitações SYN para um servidor da web.O usuário válido envia a requisição SYN.**  
Servidor Web**O servidor web espera para concluir o aperto de mãos triplo.O servidor web não está disponível.**  
Servidor Web  
Servidor Web

1. O ator da ameaça envia várias solicitações SYN a um servidor da web.
2. O servidor da web responde com SYN-ACKs para cada solicitação SYN e aguarda a conclusão do aperto de mãos triplo. O agente da ameaça não responde aos SYN-ACKs.
3. Um usuário válido não pode acessar o servidor da Web porque o servidor da Web possui muitas conexões TCP abertas pela metade.

**Ataque de redefinição de TCP**

Um ataque de redefinição de TCP pode ser usado para encerrar as comunicações TCP entre dois hosts. A figura mostra como o TCP usa uma troca de quatro direções para fechar a conexão TCP usando um par de segmentos FIN e ACK de cada extremidade da conexão TCP. Uma conexão TCP termina quando recebe um bit RST. Essa é uma maneira abrupta de interromper a conexão TCP e informar o host de recebimento para parar imediatamente de usar a conexão TCP. Um agente de ameaça pode fazer um ataque de redefinição de TCP e enviar um pacote falsificado contendo um TCP RST para um ou ambos os pontos de extremidade.

### Terminando uma conexão TCP



Envia FINACK recebido A envia resposta ACK para B.FIN recebidoEnvia ACKFIN recebidoEnvia ACKEnvia FINACK recebido

O encerramento de uma sessão TCP usa o seguinte processo de troca de quatro vias:

1. Quando o cliente não tem mais dados para enviar no fluxo, ele envia um segmento com um flag FIN ligado.
2. O servidor envia ACK para confirmar o recebimento de FIN para encerrar a sessão do cliente com o servidor.
3. O servidor envia um FIN ao cliente para encerrar a sessão do servidor-para-cliente.
4. O cliente responde com um ACK para reconhecer o FIN do servidor.

**Sequestro de sessão TCP**

Sequestro de sessão TCP é outra vulnerabilidade do TCP. Embora seja difícil de conduzir, um agente de ameaça assume um host já autenticado quando ele se comunica com o alvo. O agente de ameaça deve falsificar o endereço IP de um dos hosts, prever o próximo número de sequência e enviar um ACK para o outro host. Se for bem-sucedido, o agente da ameaça poderá enviar, mas não receber, dados do dispositivo de destino.

0

[Ir para o conteúdo](https://contenthub.netacad.com/cyberops/11.0.1?lng=pt-br#chunks-container)

*                            
*                                             
*                       

1. Ataque à base
2. Vulnerabilidades TCP e UDP

# Vulnerabilidades TCP e UDP

16.3.1

## Cabeçalho do segmento TCP

Enquanto alguns ataques têm como alvo o IP, este tópico discute ataques que têm como alvo o TCP e o UDP.

As informações do segmento TCP aparecem imediatamente após o cabeçalho IP. Os campos do segmento TCP e os sinalizadores para o campo bits de controle são exibidos na figura.

O diagrama mostra os campos de um cabeçalho de segmento TCP. Os campos e seus bits em tamanho são: Porta origem (16), porta destino (16), número de sequência (32), número de confirmação (32), tamanho do cabeçalho (4), reservado (6) bits de controle (6), janela (16), número de checagem (16), urgente (16), opções (0 ou 32, se houver). Os campos do cabeçalho são seguidos pelos dados da camada de aplicativo (o tamanho varia).

20 Bytes**Bit (0)Bit (15)Bit (16)Bit (31)**Porta de Origem (16)Porta de destino (16)Número de sequência (32)Número de autenticação (32)Comprimento do Cabeçalho (4)Janela (16)Checksum (16)Urgente (16)Opções (0 ou 32 caso existam)Dados da Camada de aplicação (o tamanho é variado)Reservado (6)Bits de controle (6)

A seguir, os seis bits de controle do segmento TCP:

* **URG** - Campo de ponteiro urgente significativo.
* **ACK** - Campo de confirmação significativo
* **PSH** - Função Push.
* **RST** - Redefina a conexão
* **SYN** - Sincronizar números de sequência
* **FIN** - Não há mais dados do remetente

16.3.2

## Serviços TCP

O TCP fornece estes serviços:

* **Entrega confiável** - O TCP incorpora reconhecimentos para garantir a entrega, em vez de confiar nos protocolos da camada superior para detectar e resolver erros. Se uma confirmação não for recebida à tempo, o remetente retransmitirá os dados. Exigir reconhecimentos dos dados recebidos pode causar atrasos substanciais. Exemplos de protocolos da camada de aplicação que usam a confiabilidade do TCP incluem HTTP, SSL / TLS, FTP, transferências de zona DNS e outros.
* **Controle de fluxo** - O TCP implementa o controle de fluxo para solucionar esse problema. Em vez de reconhecer um segmento de cada vez, vários segmentos podem ser reconhecidos com um único segmento de reconhecimento.
* **Comunicação com estado** - A comunicação com estado TCP entre duas partes ocorre durante o aperto de mãos triplo TCP. Antes que os dados possam ser transferidos usando o TCP, um aperto de mãos triplo abre a conexão TCP, conforme mostrado na figura. Se ambos os lados concordarem com a conexão TCP, os dados poderão ser enviados e recebidos por ambas as partes usando o TCP.

O gráfico é uma ilustração da troca de mensagens entre dois hosts durante o aperto de mãos triplo do TCP. Começa quando o cliente envia uma mensagem com o bit de controle SYN definido (SEQ=100 CTL=SYN). Isso é recebido pelo servidor que responde enviando uma mensagem com os bits de controle SYN e ACK definidos (SEQ=300 ACK=101 CTL=SYN, ACK). O cliente recebe o SYN, ACK e responde enviando uma mensagem com o bit de controle ACK definido(SEQ=101 ACK=301 CTL=ACK) e a sessão é estabelecida.

### Aperto de mão de três vias TCP

1 3

2

Envia SYN(SEQ=100 CTL=SYN)SYN, ACK recebidoEstabelecida(SEQ=101 ACK=301 CTL=ACK)SYN recebidoEnvia SYN, ACK(SEQ=300 ACK=101 CTL=SYN, ACK)

Uma conexão TCP é estabelecida em três etapas:

1. O cliente iniciador requisita uma sessão de comunicação cliente-servidor com o servidor.
2. O servidor confirma a sessão de comunicação cliente-servidor e requisita uma sessão de comunicação de servidor-cliente.
3. O cliente iniciador confirma a sessão de comunicação de servidor-cliente.

16.3.3

## Ataques TCP

Aplicações em Rede usam portas TCP ou UDP. Os atores de ameaças realizam varreduras de portas dos dispositivos de destino para descobrir quais serviços eles oferecem.

**Ataque de Inundação de SYN TCP**

O ataque de inundação SYN TCP explora o aperto de mãos triplo do TCP. A figura mostra um agente de ameaça enviando continuamente pacotes de solicitação de sessão TCP SYN com um endereço IP de origem falsificado aleatoriamente para um destino. O dispositivo de destino responde com um pacote TCP SYN-ACK ao endereço IP falsificado e aguarda um pacote TCP ACK. Essas respostas nunca chegam. Eventualmente, o host de destino é sobrecarregado com conexões TCP semi-abertas e os serviços TCP são negados a usuários legítimos.

### Ataque de Inundação de SYN TCP

1 1 2

3

**O agente de ameaças envia várias solicitações SYN para um servidor da web.O usuário válido envia a requisição SYN.**  
Servidor Web**O servidor web espera para concluir o aperto de mãos triplo.O servidor web não está disponível.**  
Servidor Web  
Servidor Web

1. O ator da ameaça envia várias solicitações SYN a um servidor da web.
2. O servidor da web responde com SYN-ACKs para cada solicitação SYN e aguarda a conclusão do aperto de mãos triplo. O agente da ameaça não responde aos SYN-ACKs.
3. Um usuário válido não pode acessar o servidor da Web porque o servidor da Web possui muitas conexões TCP abertas pela metade.

**Ataque de redefinição de TCP**

Um ataque de redefinição de TCP pode ser usado para encerrar as comunicações TCP entre dois hosts. A figura mostra como o TCP usa uma troca de quatro direções para fechar a conexão TCP usando um par de segmentos FIN e ACK de cada extremidade da conexão TCP. Uma conexão TCP termina quando recebe um bit RST. Essa é uma maneira abrupta de interromper a conexão TCP e informar o host de recebimento para parar imediatamente de usar a conexão TCP. Um agente de ameaça pode fazer um ataque de redefinição de TCP e enviar um pacote falsificado contendo um TCP RST para um ou ambos os pontos de extremidade.

### Terminando uma conexão TCP

1 2 3 4 A

B

Envia FINACK recebido A envia resposta ACK para B.FIN recebidoEnvia ACKFIN recebidoEnvia ACKEnvia FINACK recebido

O encerramento de uma sessão TCP usa o seguinte processo de troca de quatro vias:

1. Quando o cliente não tem mais dados para enviar no fluxo, ele envia um segmento com um flag FIN ligado.
2. O servidor envia ACK para confirmar o recebimento de FIN para encerrar a sessão do cliente com o servidor.
3. O servidor envia um FIN ao cliente para encerrar a sessão do servidor-para-cliente.
4. O cliente responde com um ACK para reconhecer o FIN do servidor.

**Sequestro de sessão TCP**

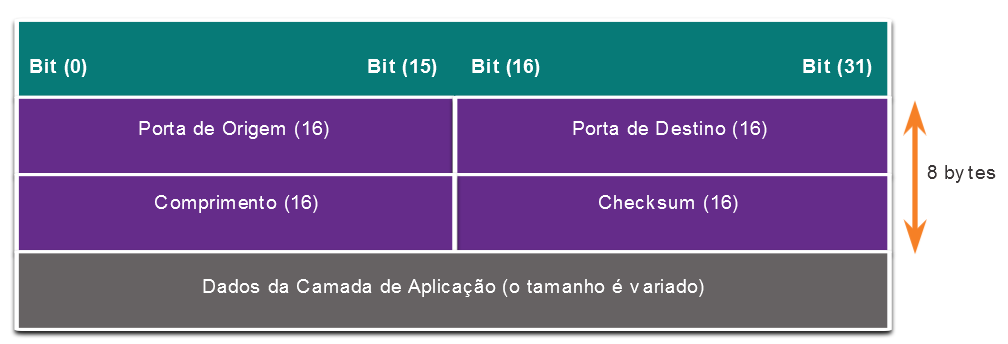
Sequestro de sessão TCP é outra vulnerabilidade do TCP. Embora seja difícil de conduzir, um agente de ameaça assume um host já autenticado quando ele se comunica com o alvo. O agente de ameaça deve falsificar o endereço IP de um dos hosts, prever o próximo número de sequência e enviar um ACK para o outro host. Se for bem-sucedido, o agente da ameaça poderá enviar, mas não receber, dados do dispositivo de destino.

16.3.4

## Operação e Cabeçalho do segmento UDP

UDP é comumente usado por DNS, DHCP, TFTP, NFS e SNMP. Também é usado com aplicações em tempo real, como streaming de mídia ou VoIP. UDP é um protocolo de camada de transporte não orientado à conexão. Ele tem uma sobrecarga muito mais baixa que o TCP, porque não é orientado a conexão e não oferece retransmissão, sequenciamento e mecanismos de controle de fluxo sofisticados que fornecem confiabilidade. A estrutura de segmentos UDP, mostrada na figura, é muito menor que a estrutura de segmentos da TCP.

**Nota**: o UDP realmente divide dados em datagramas. No entanto, o termo genérico “segmento” é comumente usado



Embora UDP seja normalmente chamado de não confiável, em contraste com a confiabilidade do TCP, isso não significa que os aplicativos que usam UDP são sempre não confiáveis, nem significa que o UDP é um protocolo inferior. Isso simplesmente significa que essas funções não são fornecidas pelo protocolo da camada de transporte e devem ser implementadas em outros locais, se houver necessidade.

A baixa sobrecarga do UDP o torna muito interessante para protocolos que efetuam transações simples de requisição e resposta. Por exemplo, usar TCP para o DHCP geraria tráfego de rede desnecessário. Se nenhuma resposta for recebida, o dispositivo reenvia a solicitação.

16.3.5

**Ataques UDP**

O UDP não está protegido por nenhuma criptografia. Você pode adicionar criptografia ao UDP, mas não está disponível por padrão. A falta de criptografia significa que qualquer pessoa pode ver o tráfego, alterá-lo e enviá-lo ao seu destino. Alterar os dados no tráfego alterará o número de checagem de 16 bits, mas o número de checagem é opcional e nem sempre é usado. Quando o número de checagem é usado, o agente de ameaça pode criar um novoo número de checagem com base na nova carga de dados e registrá-lo no cabeçalho como um novo o número de checagem. O dispositivo de destino descobrirá que o número de checagem corresponde aos dados sem saber que os dados foram alterados. Esse tipo de ataque não é amplamente utilizado.

**Ataques de inundação UDP**

É mais provável que você veja um ataque de inundação UDP. Em um ataque de inundação UDP, todos os recursos em uma rede são consumidos. O agente de ameaça deve usar uma ferramenta como UDP Unicorn ou Low Orbit Ion Cannon. Essas ferramentas enviam uma inundação de pacotes UDP, geralmente de um host falsificado, para um servidor na sub-rede. O programa varrerá todas as portas conhecidas tentando encontrar portas fechadas. Isso fará com que o servidor responda com uma mensagem inacessível da porta ICMP. Como existem muitas portas fechadas no servidor, isso cria muito tráfego no segmento, que consome a maior parte da largura de banda. O resultado é muito semelhante a um ataque de negação de serviço (DoS).

# Resumo de Atacando a Fundação

16.4.1

## O que aprendi neste módulo?

**Detalhes de PDU IP**

O IP foi projetado como um protocolo sem conexão de Camada 3. O cabeçalho IPv4 consiste em vários campos, enquanto o cabeçalho IPv6 contém menos campos. É importante que os analistas de segurança entendam os diferentes campos dos cabeçalhos IPv4 e IPv6.

**Vulnerabilidades de IP**

Existem diferentes tipos de ataques que visam IP. Os ataques comuns relacionados a IP incluem:

* Ataques ICMP
* Ataques de negação de serviço (DoS)
* Ataques Distribuídos de Negação de Serviço (DoS)
* Ataque de Falsificação de Endereços
* Ataque man-in-the-middle (MiTM)
* sequestro de sessão

O ICMP foi desenvolvido para transportar mensagens de diagnóstico e relatar condições de erro quando rotas, hosts e portas não estão disponíveis. Os agentes de ameaças usam o ICMP para ataques de reconhecimento e varredura. Os agentes de ameaças também usam ICMP para ataques DoS e DDoS. Os agentes de ameaças geralmente usam técnicas de amplificação e reflexão para criar ataques de negação de serviço (DoS). Os atores da ameaça também usam ataques de exaustão de recursos para consumir os recursos de um host de destino para travá-lo ou para consumir os recursos de uma rede. Os ataques de falsificação de endereço IP ocorrem quando um agente de ameaça cria pacotes com informações falsas de endereço IP de origem para ocultar a identidade do remetente ou para se passar por outro usuário legítimo. Os ataques de falsificação de endereços podem ser falsificação não cega para sequestrar uma sessão ou falsificação cega para criar um ataque DoS. Os ataques de falsificação de endereço MAC são usados quando os atores de ameaças têm acesso à rede interna.

**Vulnerabilidades TCP e UDP**

As informações do segmento TCP e do datagrama UDP aparecem imediatamente após o cabeçalho IP. É importante entender cabeçalhos da Camada 4 e suas funções na comunicação de dados. O TCP fornece entrega confiável, controle de fluxo e comunicação com estado. A comunicação com monitoração de estado TCP entre duas partes ocorre durante o handshake TCP de três vias. Os atores de ameaças podem realizar uma variedade de ataques relacionados ao TCP:

* Varreduras de porta TCP
* Ataque de Inundação de SYN TCP
* Ataque de redefinição de TCP
* Ataque de sequestro de sessão TCP

O segmento UDP (ou seja, datagrama) é muito menor do que o segmento TCP, o que o torna muito desejável para uso por protocolos que fazem transações simples de solicitação e resposta, como DNS, DHCP, SNMP e outros. Os atores de ameaças podem conduzir ataques de inundação UDP que varrem todas as portas UDP conhecidas em um servidor tentando encontrar portas fechadas. Isso pode criar uma situação DoS.

16.4.2

# Introdução

17.0.1

## Por que devo cursar este módulo?

As bases da rede devem ser protegidas, mas isso não é suficiente para proteger completamente a sua rede. Os protocolos que são usados para conduzir os negócios do dia-a-dia da organização também devem ser protegidos. Além disso, protocolos e software que fornecem serviços através da rede também podem ser alvo de agentes de ameaças. Um analista de segurança cibernética deve estar familiarizado com as vulnerabilidades e ameaças aos fundamentos da comunicação em rede.

Neste módulo, você aprenderá como os protocolos comuns usados na empresa funcionam e como eles são vulneráveis a ataques e exploração.

17.0.2

## O que vou aprender neste módulo?

**Título do módulo**: Atacando o que Fazemos

**Objetivo do módulo**: explicar como aplicativos e serviços de rede comuns são vulneráveis a ataques.

| **Título do Tópico** | **Objetivo do Tópico** |
| --- | --- |
| Serviços IP | Explicar vulnerabilidades de serviço IP |
| Serviços Corporativos | Explique como as vulnerabilidades de aplicativos de rede permitem ataques de rede |

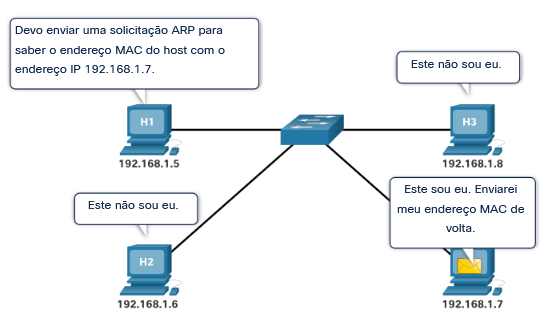
# Serviços IP

17.1.1

## Vulnerabilidades ARP

Os hosts transmitem uma solicitação ARP para outros hosts no segmento de rede para determinar o endereço MAC de um host com um endereço IP específico. Todos os hosts na sub-rede recebem e processam a solicitação ARP. O host com o endereço IP correspondente na solicitação ARP envia uma resposta ARP.

Jogue na animação para ver o processo ARP em funcionamento.



Qualquer cliente pode enviar uma resposta ARP não solicitada denominada "ARP gratuito". Isso geralmente é feito quando um dispositivo é inicializado para informar todos os outros dispositivos na rede local o endereço MAC do novo dispositivo. Quando um host envia um ARP gratuito, outros hosts na sub-rede armazenam o endereço MAC e o endereço IP contidos no ARP gratuito em suas tabelas ARP.

No entanto, esse recurso do ARP também significa que qualquer host pode reivindicar ser o proprietário de qualquer IP / MAC que escolher. Um ator de ameaça pode envenenar o cache ARP de dispositivos na rede local, criando um ataque MiTM para redirecionar o tráfego. O objetivo é associar o endereço MAC do ator de ameaça ao endereço IP do gateway padrão nos caches ARP dos hosts no segmento LAN. Isso posiciona o agente de ameaça entre a vítima e todos os outros sistemas fora da sub-rede local.

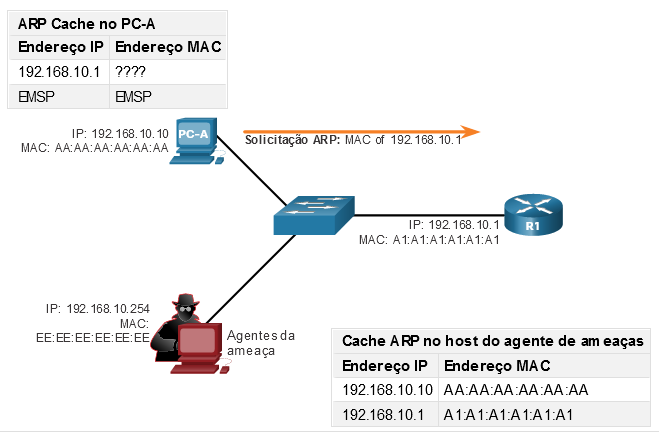
17.1.2

**Envenenamento de cache ARP**

O envenenamento do cache ARP pode ser usado para iniciar vários ataques do tipo man-in-the-middle.

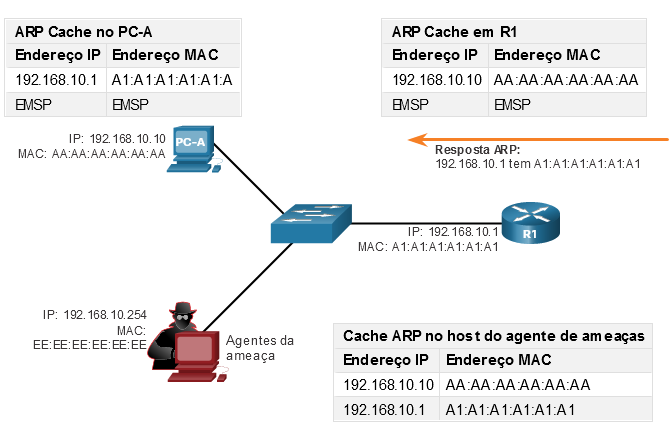
Requisição arp

A figura mostra como o envenenamento de cache do ARP funciona. PC-A requer o endereço MAC do seu gateway padrão (R1); então, ele envia uma solicitação ARP para o endereço MAC 192.168.10.1.



Resposta ARP

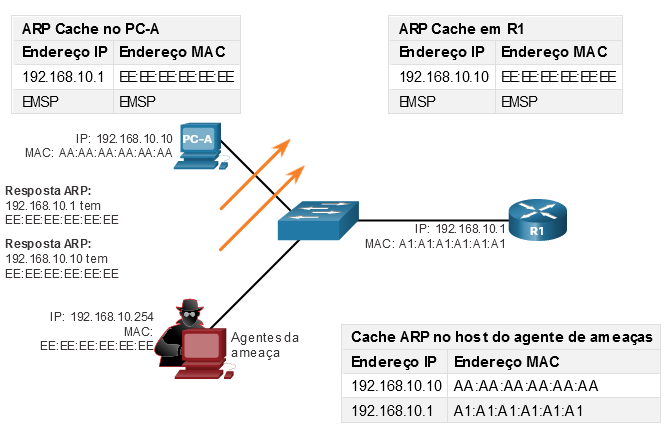
Nesta figura, o R1 atualiza seu cache ARP com os endereços IP e MAC do PC-A. R1 envia uma resposta ARP ao PC-A, que atualiza seu cache ARP com os endereços IP e MAC de R1.



Respostas falsas gratuitas de ARP

Na figura, o agente da ameaça envia duas respostas ARP gratuitas falsificadas usando seu próprio endereço MAC para os endereços IP de destino indicados. O PC-A atualiza seu cache ARP com seu gateway padrão, que agora está apontando para o endereço MAC do host do agente da ameaça. O R1 também atualiza seu cache ARP com o endereço IP do PC-A apontando para o endereço MAC do agente da ameaça.

O host do ator de ameaça está executando um ataque de envenenamento ARP. O ataque de envenenamento ARP pode ser passivo ou ativo. O envenenamento ARP passivo é onde os atores de ameaças roubam informações confidenciais. O envenenamento ARP ativo é onde os agentes de ameaças modificam dados em trânsito ou injetam dados maliciosos.



**Nota**: Existem muitas ferramentas disponíveis na Internet para criar ataques ARP MiTM, incluindo dsniff, Cain & Abel, ettercap, Yersinia e outros.

17.1.3

## Ataques de DNS

O protocolo DNS (Domain Name System) define um serviço automatizado que corresponde a nomes de recursos, como [www.cisco.com](http://www.cisco.com), com o endereço de rede numérico necessário, como o endereço IPv4 ou IPv6. Ele inclui o formato para consultas, respostas e dados e usa os registros de recursos (RR) para identificar o tipo de resposta DNS.

A proteção do DNS geralmente é ignorada. No entanto, é crucial para a operação de uma rede e deve ser protegido adequadamente.

Os ataques de DNS incluem os seguintes:

* Ataques de resolvedor aberto de DNS
* Ataques furtivos de DNS
* Ataques de sombreamento de domínio DNS
* Ataques de tunelamento de DNS

**Ataques de resolvedor aberto de DNS**

Muitas organizações usam os serviços de servidores DNS abertos ao público, como o GoogleDNS (8.8.8.8), para fornecer respostas às consultas. Esse tipo de servidor DNS é chamado de resolvedor aberto. Um resolvedor aberto de DNS responde a consultas de clientes fora de seu domínio administrativo. Os resolvedores abertos de DNS são vulneráveis a várias atividades maliciosas descritas na tabela.

| Legenda da tabela | |
| --- | --- |
| **Vulnerabilidades de resolvedor de DNS** | **Descrição** |
| **Ataques de envenenamento de cache DNS** | Atores de ameaças enviam informações falsas sobre recursos de registros falsificados (RR) para um resolvedor de DNS para redirecionar usuários de sites legítimos para sites maliciosos Sites Os ataques de envenenamento de cache DNS podem ser usados para informar o DNS resolvedor para usar um servidor de nome malicioso que está fornecendo RR informações para atividades maliciosas. |
| **Ataques de amplificação e reflexão de DNS** | Os agentes de ameaças usam ataques DoS ou DDoS em resolvedores abertos do DNS para aumentar o volume de ataques e ocultar a verdadeira fonte de um ataque. Os agentes de ameaças enviam mensagens DNS para os resolvedores abertos usando o endereço IP do host alvo. Esses ataques são possíveis porque o resolvedor aberto responderá às perguntas de qualquer pessoa que esteja questão. |
| **Ataques de utilização de recursos DNS** | Um ataque de DoS que consome os recursos dos resolvedores abertos do DNS. Esse ataque de DoS consome todos os recursos disponíveis para negativamente afetar as operações do resolvedor aberto do DNS. O impacto deste ataque DoS pode exigir que o resolvedor aberto do DNS seja reinicializado ou que serviços sejam parados e reiniciados. |

**Ataques furtivos de DNS**

Para ocultar sua identidade, os agentes de ameaças também usam as técnicas furtivas de DNS descritas na tabela para realizar seus ataques.

| Legenda da tabela | |
| --- | --- |
| **técnicas furtivas de DNS** | **Descrição** |
| **Fluxo Rápido** | Agentes de ameaças usam essa técnica para ocultar phishing e malware sites de entrega por trás de uma rede de dinâmica DNS comprometidos Hosts Os endereços IP do DNS são alterados continuamente em minutos. As redes de robôs geralmente empregam técnicas de fluxo rápido para efetivamente ocultar que servidores maliciosos sejam detectados. |
| **Fluxo de IP duplo** | Agentes de ameaças usam essa técnica para alterar rapidamente o nome do host para o endereço IP mapeados e também para alterar o servidor de nomes autoritativo. Isso aumenta a dificuldade de identificar a fonte do ataque. |
| **Algoritmos de geração de domínio** | Agentes de ameaças usam essa técnica em malware para gerar aleatoriamente nomes de domínio que podem ser usados como pontos de encontro para seus servidores de comando e controle (C&C). |

**Ataques de sombreamento de domínio DNS**

O sombreamento de domínio envolve o agente de ameaças coletando credenciais de conta de domínio para criar silenciosamente vários subdomínios a serem usados durante os ataques. Esses subdomínios normalmente apontam para servidores mal-intencionados sem alertar o proprietário real do domínio pai.

17.1.4

## Tunelamento DNS

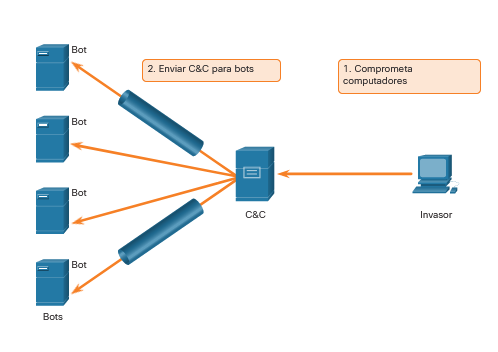
Botnets se tornaram um método de ataque popular de atores ameaçadores. Na maioria das vezes, os botnets são usados para espalhar malware ou iniciar ataques de DDoS e phishing.

O DNS na empresa às vezes é negligenciado como um protocolo que pode ser usado por botnets. Por isso, quando o tráfego DNS é determinado como parte de um incidente, o ataque geralmente já acabou. É necessário que o analista de segurança cibernética seja capaz de detectar quando um invasor está usando tunelamento DNS para roubar dados e prevenir e conter o ataque. Para isso, o analista de segurança deve implementar uma solução que possa bloquear as comunicações de saída dos hosts infectados.

Os agentes de ameaças que usam o tunelamento DNS colocam tráfego que não é de DNS, dentro do tráfego DNS. Esse método geralmente contorna soluções de segurança. Para que o agente da ameaça use o túnel DNS, os diferentes tipos de registros DNS, como TXT, MX, SRV, NULL, A ou CNAME, são alterados. Por exemplo, um registro TXT pode armazenar os comandos enviados para os bots de host infectados como respostas DNS. Um ataque de tunelamento DNS usando TXT funciona assim:

1. Os dados são divididos em vários blocos codificados.
2. Cada pedaço é colocado em um rótulo de nome de domínio de nível inferior na consulta DNS.
3. Como não há resposta do DNS local ou em rede para a consulta, a solicitação é enviada aos servidores DNS recursivos do ISP.
4. O serviço DNS recursivo encaminhará a consulta para o servidor de nomes autorizado do invasor.
5. O processo é repetido até que todas as consultas contendo os chunks sejam enviadas.
6. Quando o servidor de nomes autoritativo do invasor recebe as consultas DNS dos dispositivos infectados, ele envia respostas para cada consulta DNS, que contém os comandos encapsulados e codificados.
7. O malware no host comprometido recombina os pedaços e executa os comandos ocultos.

Para poder interromper o túnel DNS, um filtro que inspecione o tráfego DNS deve ser usado. Preste atenção especial às consultas DNS que são mais longas do que a média, ou aquelas que têm um nome de domínio suspeito. Além disso, as soluções de segurança de DNS, como Cisco Umbrella (anteriormente Cisco OpenDNS), bloqueiam grande parte do tráfego de túnel DNS ao identificar domínios suspeitos. Domínios associados a serviços DNS dinâmicos devem ser considerados altamente suspeitos



0

[Ir para o conteúdo](https://contenthub.netacad.com/cyberops/11.0.1?lng=pt-br#chunks-container)

*                            
*                                                           
*                     

1. Ataque ao trabalho
2. Serviços IP

# Serviços IP

17.1.1

## Vulnerabilidades ARP

Os hosts transmitem uma solicitação ARP para outros hosts no segmento de rede para determinar o endereço MAC de um host com um endereço IP específico. Todos os hosts na sub-rede recebem e processam a solicitação ARP. O host com o endereço IP correspondente na solicitação ARP envia uma resposta ARP.

Jogue na animação para ver o processo ARP em funcionamento.

This animation illustrates how a host will use A R P to discover the MAC address of a known I P address. O host H1 precisa enviar algumas informações para um host com endereço IP 192 ponto 168 ponto 1 ponto 7. No entanto, H1 não tem o endereço MAC para esse endereço. Therefore, it sends an A R P request to I P address 192.168.1.7. All hosts on the network will receive the A R P request. However, only host H4 with IP address 192.168.1.7 will send an A R P reply containing its MAC address. Então, o H1 pode enviar um envelope para o switch que vai diretamente para o H4.

Devo enviar uma solicitação ARP para saber o endereço MAC do host com o endereço IP 192.168.1.7.

Este não sou eu.

Este não sou eu.

Este sou eu. Enviarei meu endereço MAC de volta.

Agora tenho o MAC. Posso enviar minhas informações.

Obrigado. Recebi.

Qualquer cliente pode enviar uma resposta ARP não solicitada denominada "ARP gratuito". Isso geralmente é feito quando um dispositivo é inicializado para informar todos os outros dispositivos na rede local o endereço MAC do novo dispositivo. Quando um host envia um ARP gratuito, outros hosts na sub-rede armazenam o endereço MAC e o endereço IP contidos no ARP gratuito em suas tabelas ARP.

No entanto, esse recurso do ARP também significa que qualquer host pode reivindicar ser o proprietário de qualquer IP / MAC que escolher. Um ator de ameaça pode envenenar o cache ARP de dispositivos na rede local, criando um ataque MiTM para redirecionar o tráfego. O objetivo é associar o endereço MAC do ator de ameaça ao endereço IP do gateway padrão nos caches ARP dos hosts no segmento LAN. Isso posiciona o agente de ameaça entre a vítima e todos os outros sistemas fora da sub-rede local.

17.1.2

## Envenenamento de cache ARP

O envenenamento do cache ARP pode ser usado para iniciar vários ataques do tipo man-in-the-middle.

Clique em cada botão para obter uma ilustração e uma explicação do processo de envenenamento de cache do ARP.

Na figura, o agente da ameaça envia duas respostas ARP gratuitas falsificadas usando seu próprio endereço MAC para os endereços IP de destino indicados. O PC-A atualiza seu cache ARP com seu gateway padrão, que agora está apontando para o endereço MAC do host do agente da ameaça. O R1 também atualiza seu cache ARP com o endereço IP do PC-A apontando para o endereço MAC do agente da ameaça.

O host do ator de ameaça está executando um ataque de envenenamento ARP. O ataque de envenenamento ARP pode ser passivo ou ativo. O envenenamento ARP passivo é onde os atores de ameaças roubam informações confidenciais. O envenenamento ARP ativo é onde os agentes de ameaças modificam dados em trânsito ou injetam dados maliciosos.

A topologia de rede é a mesma descrita em 3.8.2-1. Ele mostra que o host do ator de ameaças enviou duas respostas ARP. O primeiro lê 192.168.10.1 tem EE:EE:EE:EE:EE:EE. O segundo lê 192.168.10.10 tem EE:EE:EE:EE:EE:EE. Isso fez com que o PC-A alterasse seu cache ARP para mapear o endereço IP 192.168.10.1 para o endereço MACEE:EE:EE:EE:EE:EE e R1 para alterar seu cache ARP para mapear o endereço IP 192.168.10.10 para MAC EE:EE:EE:EE:EE:EE. O cache ARP no host do agente de ameaças possui duas entradas; endereço IP 192.168.10.10 mapeado para endereço MAC AA:AA:AA:AA:AA:AA e endereço IP 192.168.10.1 mapeado para MAC A1:A1:A1:A1:A1:A1.

PC-A

R1

IP: 192.168.10.10  
MAC: AA:AA:AA:AA:AA:AAIP: 192.168.10.254  
MAC: EE:EE:EE:EE:EE:EEIP: 192.168.10.1  
MAC: A1:A1:A1:A1:A1:A1Agentes da ameaça**Resposta ARP:**   
192.168.10.1 tem EE:EE:EE:EE:EE:EE**Resposta ARP:**   
192.168.10.10 tem EE:EE:EE:EE:EE:EE

| ARP Cache no PC-A | |
| --- | --- |
| **ARP Cache no PC-A** | |
| **Endereço IP** | **Endereço MAC** |
| 192.168.10.1 | EE:EE:EE:EE:EE:EE |
| EMSP | EMSP |

| ARP Cache em R1 | |
| --- | --- |
| **ARP Cache em R1** | |
| **Endereço IP** | **Endereço MAC** |
| 192.168.10.10 | EE:EE:EE:EE:EE:EE |
| EMSP | EMSP |

| Cache ARP no host do agente de ameaças | |
| --- | --- |
| **Cache ARP no host do agente de ameaças** | |
| **Endereço IP** | **Endereço MAC** |
| 192.168.10.10 | AA:AA:AA:AA:AA:AA |
| 192.168.10.1 | A1:A1:A1:A1:A1:A1 |

**Nota**: Existem muitas ferramentas disponíveis na Internet para criar ataques ARP MiTM, incluindo dsniff, Cain & Abel, ettercap, Yersinia e outros.

17.1.3

## Ataques de DNS

O protocolo DNS (Domain Name System) define um serviço automatizado que corresponde a nomes de recursos, como [www.cisco.com](http://www.cisco.com), com o endereço de rede numérico necessário, como o endereço IPv4 ou IPv6. Ele inclui o formato para consultas, respostas e dados e usa os registros de recursos (RR) para identificar o tipo de resposta DNS.

A proteção do DNS geralmente é ignorada. No entanto, é crucial para a operação de uma rede e deve ser protegido adequadamente.

Os ataques de DNS incluem os seguintes:

* Ataques de resolvedor aberto de DNS
* Ataques furtivos de DNS
* Ataques de sombreamento de domínio DNS
* Ataques de tunelamento de DNS

**Ataques de resolvedor aberto de DNS**

Muitas organizações usam os serviços de servidores DNS abertos ao público, como o GoogleDNS (8.8.8.8), para fornecer respostas às consultas. Esse tipo de servidor DNS é chamado de resolvedor aberto. Um resolvedor aberto de DNS responde a consultas de clientes fora de seu domínio administrativo. Os resolvedores abertos de DNS são vulneráveis a várias atividades maliciosas descritas na tabela.

| Legenda da tabela | |
| --- | --- |
| **Vulnerabilidades de resolvedor de DNS** | **Descrição** |
| **Ataques de envenenamento de cache DNS** | Atores de ameaças enviam informações falsas sobre recursos de registros falsificados (RR) para um resolvedor de DNS para redirecionar usuários de sites legítimos para sites maliciosos Sites Os ataques de envenenamento de cache DNS podem ser usados para informar o DNS resolvedor para usar um servidor de nome malicioso que está fornecendo RR informações para atividades maliciosas. |
| **Ataques de amplificação e reflexão de DNS** | Os agentes de ameaças usam ataques DoS ou DDoS em resolvedores abertos do DNS para aumentar o volume de ataques e ocultar a verdadeira fonte de um ataque. Os agentes de ameaças enviam mensagens DNS para os resolvedores abertos usando o endereço IP do host alvo. Esses ataques são possíveis porque o resolvedor aberto responderá às perguntas de qualquer pessoa que esteja questão. |
| **Ataques de utilização de recursos DNS** | Um ataque de DoS que consome os recursos dos resolvedores abertos do DNS. Esse ataque de DoS consome todos os recursos disponíveis para negativamente afetar as operações do resolvedor aberto do DNS. O impacto deste ataque DoS pode exigir que o resolvedor aberto do DNS seja reinicializado ou que serviços sejam parados e reiniciados. |

**Ataques furtivos de DNS**

Para ocultar sua identidade, os agentes de ameaças também usam as técnicas furtivas de DNS descritas na tabela para realizar seus ataques.

| Legenda da tabela | |
| --- | --- |
| **técnicas furtivas de DNS** | **Descrição** |
| **Fluxo Rápido** | Agentes de ameaças usam essa técnica para ocultar phishing e malware sites de entrega por trás de uma rede de dinâmica DNS comprometidos Hosts Os endereços IP do DNS são alterados continuamente em minutos. As redes de robôs geralmente empregam técnicas de fluxo rápido para efetivamente ocultar que servidores maliciosos sejam detectados. |
| **Fluxo de IP duplo** | Agentes de ameaças usam essa técnica para alterar rapidamente o nome do host para o endereço IP mapeados e também para alterar o servidor de nomes autoritativo. Isso aumenta a dificuldade de identificar a fonte do ataque. |
| **Algoritmos de geração de domínio** | Agentes de ameaças usam essa técnica em malware para gerar aleatoriamente nomes de domínio que podem ser usados como pontos de encontro para seus servidores de comando e controle (C&C). |

**Ataques de sombreamento de domínio DNS**

O sombreamento de domínio envolve o agente de ameaças coletando credenciais de conta de domínio para criar silenciosamente vários subdomínios a serem usados durante os ataques. Esses subdomínios normalmente apontam para servidores mal-intencionados sem alertar o proprietário real do domínio pai.

17.1.4

## Tunelamento DNS

Botnets se tornaram um método de ataque popular de atores ameaçadores. Na maioria das vezes, os botnets são usados para espalhar malware ou iniciar ataques de DDoS e phishing.

O DNS na empresa às vezes é negligenciado como um protocolo que pode ser usado por botnets. Por isso, quando o tráfego DNS é determinado como parte de um incidente, o ataque geralmente já acabou. É necessário que o analista de segurança cibernética seja capaz de detectar quando um invasor está usando tunelamento DNS para roubar dados e prevenir e conter o ataque. Para isso, o analista de segurança deve implementar uma solução que possa bloquear as comunicações de saída dos hosts infectados.

Os agentes de ameaças que usam o tunelamento DNS colocam tráfego que não é de DNS, dentro do tráfego DNS. Esse método geralmente contorna soluções de segurança. Para que o agente da ameaça use o túnel DNS, os diferentes tipos de registros DNS, como TXT, MX, SRV, NULL, A ou CNAME, são alterados. Por exemplo, um registro TXT pode armazenar os comandos enviados para os bots de host infectados como respostas DNS. Um ataque de tunelamento DNS usando TXT funciona assim:

1. Os dados são divididos em vários blocos codificados.
2. Cada pedaço é colocado em um rótulo de nome de domínio de nível inferior na consulta DNS.
3. Como não há resposta do DNS local ou em rede para a consulta, a solicitação é enviada aos servidores DNS recursivos do ISP.
4. O serviço DNS recursivo encaminhará a consulta para o servidor de nomes autorizado do invasor.
5. O processo é repetido até que todas as consultas contendo os chunks sejam enviadas.
6. Quando o servidor de nomes autoritativo do invasor recebe as consultas DNS dos dispositivos infectados, ele envia respostas para cada consulta DNS, que contém os comandos encapsulados e codificados.
7. O malware no host comprometido recombina os pedaços e executa os comandos ocultos.

Para poder interromper o túnel DNS, um filtro que inspecione o tráfego DNS deve ser usado. Preste atenção especial às consultas DNS que são mais longas do que a média, ou aquelas que têm um nome de domínio suspeito. Além disso, as soluções de segurança de DNS, como Cisco Umbrella (anteriormente Cisco OpenDNS), bloqueiam grande parte do tráfego de túnel DNS ao identificar domínios suspeitos. Domínios associados a serviços DNS dinâmicos devem ser considerados altamente suspeitos.

A figura mostra um invasor p c à direita com uma seta apontando para um servidor C & C à esquerda do p c. O servidor C & C tem 4 servidores à esquerda dele. Sob todos os servidores está a palavra bots. Ao lado de cada servidor está a palavra bot. Uma seta com um tubo sobre ele vai do servidor C & C para os servidores superior e inferior. Uma linha normal com uma seta no final vai do servidor C & C apontando para os dois servidores intermediários. Palavras acima são 1. comprometimento computadores. 2. enviar C & C para bots.

Bots2. Enviar C&C para bots1. Comprometa computadoresC&CInvasorBotBotBotBot

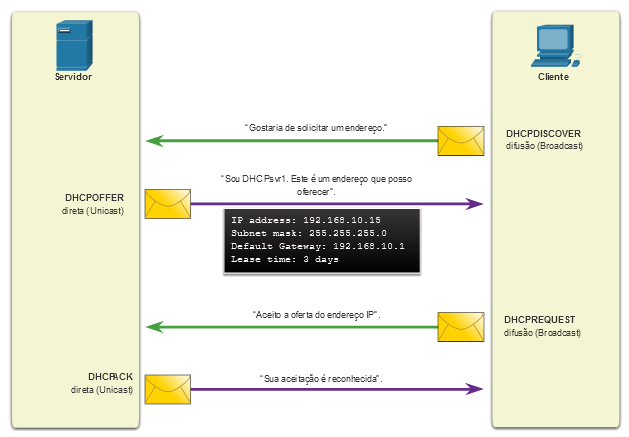
17.1.5

## DHCP

Os servidores DHCP fornecem dinamicamente informações de configuração de IP aos clientes. A figura mostra a sequência típica de uma troca de mensagens DHCP entre cliente e servidor.

O gráfico mostra a troca de mensagens entre um cliente e um servidor DHCP durante operações normais do DHCP. Primeiro, o cliente envia uma mensagem de difusão (broadcast) DHCPDISCOVER para o servidor com a mensagem. Gostaria de solicitar um endereço. O servidor responde com uma mensagem direta (unicast) DHCPOFFER dizendo: Eu sou DHCPsvr1. Este é um endereço que posso oferecer. As informações nesta mensagem são: Endereço IP 192.168.10.15, Máscara de sub-rede 255.255.255.0, Gateway padrão 192.168.10.1 e tempo de concessão de 3 dias. O cliente responde com uma mensagem de difusão (broadcast) DHCPREQUEST dizendo: Aceito o endereço IP ofertado. O servidor responde com uma mensagem direta (unicast) DHCPACK dizendo: Seu aceite está confirmado.

### Operação normal do DHCP



IP address: 192.168.10.15Subnet mask: 255.255.255.0Default Gateway: 192.168.10.1Lease time: 3 days

ServidorCliente**DHCPOFFER**  
direta (Unicast)**DHCPACK**  
direta (Unicast)**DHCPDISCOVER**  
difusão (Broadcast)**DHCPREQUEST**  
difusão (Broadcast)“Gostaria de solicitar um endereço.”“Sou DHCPsvr1. Este é um endereço que posso oferecer”.“Aceito a oferta do endereço IP”.“Sua aceitação é reconhecida”.

Na figura, um cliente transmite uma mensagem de descoberta DHCP. O servidor DHCP responde com uma oferta direta (unicast) que inclui informações de endereçamento que o cliente pode usar. O cliente transmite em difusão (broadcast) uma solicitação DHCP para informar ao servidor que aceita a oferta. O servidor responde com uma confirmação de direta (unicast) aceitando a solicitação.

17.1.6

## Ataques à DHCP

**Ataque de falsificação de DHCP**

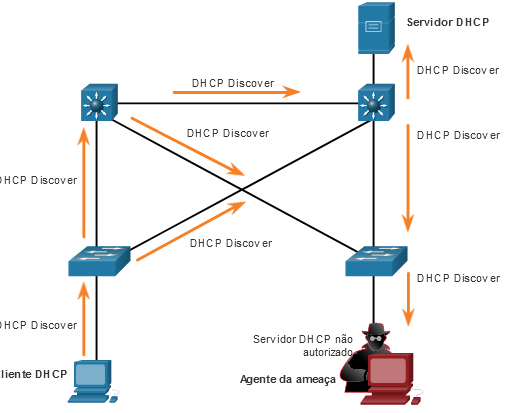
Um ataque de spoofing de DHCP ocorre quando um servidor DHCP invasor está conectado à rede e fornece falsos parâmetros de configuração IP aos clientes legítimos. Um servidor não autorizado pode fornecer uma variedade de informações enganosas:

* **Gateway padrão errado** - o ator da ameaça fornece um gateway inválido ou o endereço IP de seu host para criar um ataque MiTM. Isso pode não ser totalmente detectado, pois o invasor intercepta o fluxo de dados pela rede.
* **servidor DNS errado** - O agente de ameaças fornece um endereço de servidor DNS incorreto, apontando o usuário para um site malicioso.
* **endereço IP errado**- O agente de ameaças fornece um endereço IP inválido, um endereço IP de gateway padrão inválido ou ambos. O agente de ameaça cria um ataque de negação de serviço no cliente DHCP.

Suponha que um agente de ameaça tenha conectado com êxito um servidor DHCP não autorizado a uma porta de switch na mesma sub-rede que os clientes de destino. O objetivo do servidor não autorizado é fornecer aos clientes informações falsas de configuração de IP.

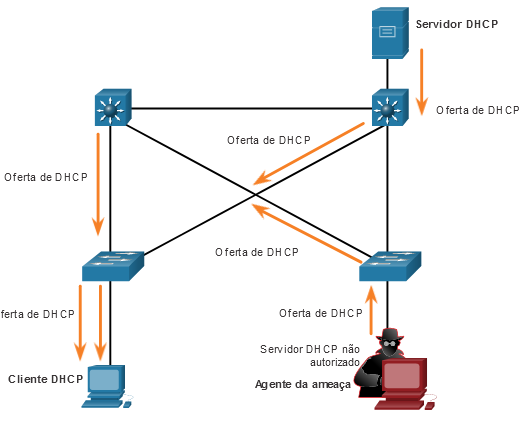
**Cliente transmite mensagens de descoberta DHCP**

Na figura, um cliente legítimo se conecta à rede e requer parâmetros de configuração de IP. O cliente transmite uma solicitação de descoberta de DHCP procurando uma resposta de um servidor DHCP. Ambos os servidores recebem a mensagem.



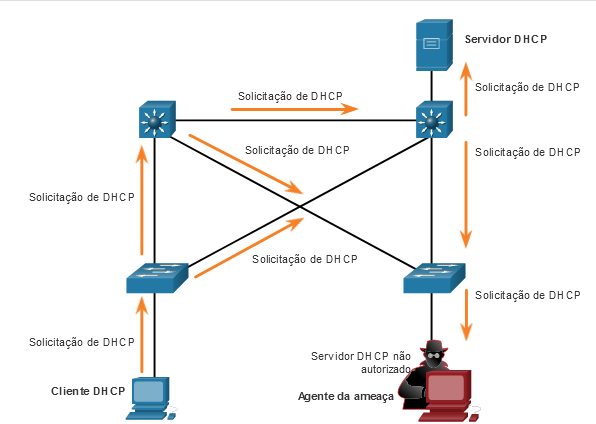
**Servidores DHCP respondem com ofertas**

A figura mostra como os servidores DHCP legítimos e o não autorizado, respondem com parâmetros de configuração de IP válidos. O cliente responde à primeira oferta recebida.



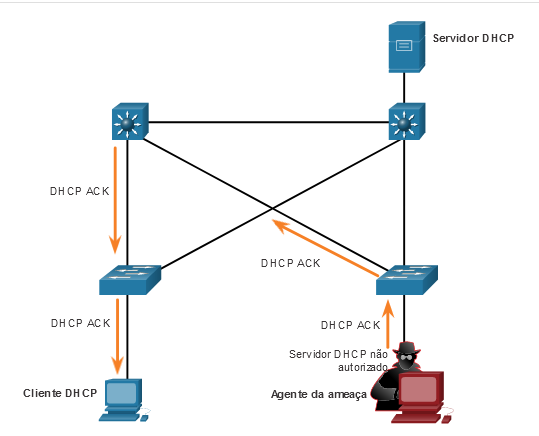
**Cliente aceita solicitação DHCP não autorizada**

Nesse cenário, o cliente recebeu a oferta não autorizada primeiro. Ele transmite uma solicitação DHCP, aceitando os parâmetros do servidor não autorizado, conforme mostrado na figura. Cada servidor legítimo e não autorizado recebem a solicitação.



**DHCP não autorizado confirma a solicitação**

No entanto, apenas o servidor não autorizado envia uma resposta ao cliente para confirmar sua solicitação, conforme mostrado na figura. O servidor legítimo para de se comunicar com o cliente porque a solicitação já foi confirmada.



# Serviços Corporativos

17.2.1

## HTTP e HTTPS

Os navegadores da Internet são usados por quase todos. Bloquear completamente a navegação na Web não é uma opção porque as empresas precisam de acesso à Web, sem comprometer a segurança da Web.

Para investigar ataques baseados na Web, os analistas de segurança devem ter uma boa compreensão de como funciona um ataque padrão baseado na Web. Estes são os estágios comuns de um ataque típico da web:

1. A vítima visita inconscientemente uma página web que foi comprometida por malware.
2. A página Web comprometida redireciona o usuário, muitas vezes através de muitos servidores comprometidos, para um site contendo código malicioso.
3. O usuário visita este site com código malicioso e seu computador fica infectado. Isso é conhecido como uma unidade por download. Quando o usuário visita o site, um kit de exploração verifica o software em execução no computador da vítima, incluindo o sistema operacional, Java ou Flash player que procura uma exploração no software. O kit de exploração geralmente é um script PHP e fornece ao invasor um console de gerenciamento para gerenciar o ataque.
4. Depois de identificar um pacote de software vulnerável em execução no computador da vítima, o kit de exploração entra em contato com o servidor do kit de exploração para baixar código que pode usar a vulnerabilidade para executar código mal-intencionado no computador da vítima.
5. Depois que o computador da vítima foi comprometido, ele se conecta ao servidor de malware e baixa uma carga útil. Isso pode ser malware ou um serviço de download de arquivos que baixa outro malware.
6. O último pacote de malware é executado no computador da vítima.

Independente do tipo de ataque que está sendo usado, o objetivo principal do ator da ameaça é garantir que o navegador da Web da vítima acabe na página da web do ator da ameaça, que, em seguida, serve a exploração maliciosa para a vítima.

Alguns sites mal-intencionados aproveitam plug-ins vulneráveis ou vulnerabilidades do navegador para comprometer o sistema do cliente. Redes maiores dependem de IDSs para verificar arquivos baixados em busca de malware. Se detectado, o IDS emite alertas e registra o evento em arquivos de log para análise posterior.

Os logs de conexão do servidor geralmente podem revelar informações sobre o tipo de varredura ou ataque. Os diferentes tipos de códigos de status de conexão estão listados aqui:

* **Informativo 1xx** — Esta é uma resposta provisória, consistindo apenas na Linha de Status e cabeçalhos opcionais. É encerrado por uma linha vazia. Não há cabeçalhos necessários para esta classe de código de status. Servidores NÃO DEVE enviar uma resposta 1xx para um cliente HTTP/1.0, exceto em condições experimentais.
* **2xx bem-sucedido** — A solicitação do cliente foi recebida, compreendida e aceita com êxito.
* **Redirecionamento 3xx** — Outras ações devem ser tomadas pelo agente do usuário para atender a solicitação. Um cliente DEVE detectar loops de redirecionamento infinitos, porque esses loops geram tráfego de rede para cada redirecionamento.
* **Erro de cliente 4xx** — Para casos em que o cliente parece ter errado. Exceto quando responder a uma solicitação HEAD, o servidor DEVE incluir uma entidade contendo uma explicação da situação, e se ela é temporária. Agentes de usuário DEVE exibir qualquer entidade incluída para o usuário.
* **Erro de servidor 5xx** — Para casos em que o servidor está ciente de que ele errou ou não pode executar a solicitação. Exceto quando responder a uma solicitação HEAD, o servidor DEVE incluir uma entidade contendo uma explicação da situação de erro, e se ela é temporária. Agentes de usuário DEVE exibir qualquer entidade incluída para o usuário.

Para se defender contra ataques baseados na web, as seguintes contramedidas devem ser usadas:

* Sempre atualize o sistema operacional e os navegadores com patches e atualizações atuais.
* Use um proxy da Web como o Cisco Cloud Web Security ou o Cisco Web Security Appliance para bloquear sites mal-intencionados.
* Use as melhores práticas de segurança do Open Web Application Security Project (OWASP) ao desenvolver aplicativos Web.
* Educar os usuários finais mostrando-lhes como evitar ataques baseados na Web.

O OWASP Top 10 Riscos de Segurança de Aplicativos Web foi projetado para ajudar as organizações a criar aplicativos Web seguros. É uma lista útil de potenciais vulnerabilidades que são comumente exploradas por atores de ameaças.

17.2.2

## Explorações HTTP comuns

**IFrames maliciosos**

Os atores de ameaças costumam usar quadros inline maliciosos (iFrames). Um iFrame é um elemento HTML que permite que o navegador carregue outra página da Web a partir de outra fonte. Os ataques de iFrame tornaram-se muito comuns, pois são frequentemente usados para inserir anúncios de outras fontes na página. Os atores de ameaças comprometem um servidor da Web e modificam páginas da Web adicionando HTML para o iFrame malicioso. O HTML vincula ao servidor da web do ator da ameaça. Em alguns casos, a página IFrame carregada consiste em apenas alguns pixels. Isso torna muito difícil para o usuário ver. Como o iFrame é executado na página, ele pode ser usado para fornecer uma exploração mal-intencionada, como publicidade de spam, um kit de exploração e outros malwares.

Estas são algumas das maneiras de prevenir ou reduzir iFrames maliciosos:

* Use um proxy da Web para bloquear sites mal-intencionados.
* Como os invasores geralmente alteram o HTML de origem do iFrame em um site comprometido, verifique se os desenvolvedores da Web não usam iFrames. Isso isolará qualquer conteúdo de sites de terceiros e facilitará a localização de páginas modificadas.
* Use um serviço como o Cisco Umbrella para impedir que os usuários naveguem para sites conhecidos por serem mal-intencionados.
* Certifique-se de que o usuário final entenda o que é um iFrame. Os atores de ameaças costumam usar esse método em ataques baseados na Web.

**Amortecimento HTTP 302**

Outro tipo de ataque HTTP é o ataque de amortecimento HTTP 302. Os atores de ameaças usam o código de status de resposta 302 Found HTTP para direcionar o navegador da Web do usuário para um novo local. Os atores de ameaças costumam usar funções HTTP legítimas, como redirecionamentos HTTP para realizar seus ataques. HTTP permite que os servidores redirecionem a solicitação HTTP de um cliente para um servidor diferente. O redirecionamento HTTP é usado, por exemplo, quando o conteúdo da Web é movido para um URL ou nome de domínio diferente. Isso permite que URLs e marcadores antigos continuem a funcionar. Portanto, os analistas de segurança devem entender como uma função como o redirecionamento HTTP funciona e como ela pode ser usada durante ataques.

Quando a resposta do servidor é um status 302 Encontrado, ele também fornece a URL no campo de localização. O navegador acredita que o novo local é o URL fornecido no cabeçalho. O navegador é convidado a solicitar este novo URL. Esta função de redirecionamento pode ser usada várias vezes até que o navegador finalmente pouse na página que contém o exploit. Os redirecionamentos podem ser difíceis de detectar devido ao fato de que redirecionamentos legítimos ocorrem frequentemente na rede.

Estas são algumas maneiras de evitar ou reduzir ataques de amortecimento HTTP 302:

* Use um proxy da Web para bloquear sites mal-intencionados.
* Use um serviço como o Cisco Umbrella para impedir que os usuários naveguem para sites conhecidos por serem mal-intencionados.
* Certifique-se de que o usuário final entenda como o navegador é redirecionado por meio de uma série de redirecionamentos HTTP 302.

**Sombreamento de domínio**

Quando um ator de ameaça deseja criar um ataque de sombreamento de domínio, o ator de ameaça deve primeiro comprometer um domínio. Em seguida, o ator de ameaça deve criar vários subdomínios desse domínio para ser usado para os ataques. Logins de registro de domínio seqüestrados são usados para criar os muitos subdomínios necessários. Depois que esses subdomínios tiverem sido criados, os invasores podem usá-los como quiserem, mesmo que sejam encontrados domínios mal-intencionados. Eles podem simplesmente fazer mais do domínio pai. A sequência a seguir é normalmente usada por atores de ameaça:

1. Um site fica comprometido.
2. O amortecimento HTTP 302 é usado para enviar o navegador para sites maliciosos.
3. O sombreamento de domínio é usado para direcionar o navegador para um servidor comprometido.
4. Uma página inicial do kit de exploração é acessada.
5. Downloads de malware da página inicial do kit de exploração.

Estas são algumas maneiras de prevenir ou reduzir ataques de sombreamento de domínio:

* Proteja todas as contas de proprietário do domínio. Use senhas fortes e use autenticação de dois fatores para proteger essas contas poderosas.
* Use um proxy da Web para bloquear sites mal-intencionados.
* Use um serviço como o Cisco Umbrella para impedir que os usuários naveguem para sites conhecidos por serem mal-intencionados.
* Certifique-se de que os proprietários de domínio validem as suas contas de registo e procure quaisquer subdomínios que não tenham autorizado.

17.2.3

## E-mail

Nos últimos 25 anos, o email evoluiu de uma ferramenta usada principalmente por profissionais técnicos e de pesquisa para se tornar a espinha dorsal das comunicações corporativas. A cada dia, mais de 100 bilhões de mensagens de e-mail corporativo são trocadas. À medida que o nível de uso aumenta, a segurança torna-se uma prioridade maior. A maneira como os usuários acessam o email hoje também aumenta a oportunidade de a ameaça de malware ser introduzida. Costumava ser que os usuários corporativos acessavam e-mails baseados em texto a partir de um servidor corporativo. O servidor corporativo estava em uma estação de trabalho protegida pelo firewall da empresa. Hoje, as mensagens HTML são acessadas a partir de muitos dispositivos diferentes que muitas vezes não são protegidos pelo firewall da empresa. HTML permite mais ataques devido à quantidade de acesso que às vezes pode ignorar diferentes camadas de segurança.

Veja a seguir exemplos de ameaças de email:

* **Ataques baseados em anexos** — os agentes de ameaças incorporam conteúdo malicioso em arquivos de negócios, como um e-mail do departamento de TI. Usuários legítimos abrem conteúdo malicioso. O malware é usado em ataques amplos, muitas vezes visando uma vertical de negócios específica para parecer legítima, atraindo usuários que trabalham nessa vertical para abrir anexos ou clicar em links incorporados.
* **Falsificação de e-mails** — os atores de ameaças criam mensagens de e-mail com um endereço de remetente falsificado que visa enganar o destinatário a fornecer dinheiro ou informações confidenciais. Por exemplo, um banco envia um e-mail solicitando que você atualize suas credenciais. Quando este e-mail exibe o logotipo do banco idêntico ao e-mail que você abriu anteriormente e que era legítimo, ele tem uma maior chance de ser aberto, ter anexos abertos e links clicados. O e-mail falsificado pode até pedir que você verifique suas credenciais para que o banco tenha certeza de que você é você, expondo suas informações de login.
* **E-mail de spam** — Os agentes de ameaças enviam e-mails não solicitados contendo anúncios ou arquivos mal-intencionados. Esse tipo de e-mail é enviado com mais frequência para solicitar uma resposta, informando ao ator da ameaça que o e-mail é válido e que um usuário abriu o spam.
* **Servidor de retransmissão de email aberto** — os atores de ameaças aproveitam os servidores corporativos configurados incorretamente como retransmissores de email abertos para enviar grandes volumes de spam ou malware para usuários desavisados. O retransmissor de email aberto é um servidor SMTP que permite que qualquer pessoa na internet envie e-mails. Como qualquer pessoa pode usar o servidor, eles são vulneráveis a spammers e worms. Volumes muito grandes de spam podem ser enviados usando um retransmissor de email aberto. É importante que os servidores de e-mail corporativos nunca sejam configurados como uma retransmissão aberta. Isso reduzirá consideravelmente a quantidade de e-mails não solicitados.
* **Homoglifos** — os atores de ameaças podem usar caracteres de texto muito semelhantes ou até mesmo idênticos aos caracteres de texto legítimos. Por exemplo, pode ser difícil distinguir entre um O (letra maiúscula O) e um 0 (número zero) ou um l (minúsculo “L”) e um 1 (número um). Eles podem ser usados em e-mails de phishing para torná-los muito convincentes. No DNS, esses caracteres são muito diferentes do real. Quando o registro DNS é pesquisado, um URL completamente diferente é encontrado quando o link com o homoglifo é usado na pesquisa.

Assim como qualquer outro serviço que esteja escutando uma porta para conexões de entrada, os servidores SMTP também podem ter vulnerabilidades. Mantenha sempre o software SMTP atualizado com patches e atualizações de segurança e software. Para evitar que os atores da ameaça completem sua tarefa de enganar o usuário final, implemente contramedidas. Use um Security Appliance específico para e-mail, como o Cisco Email Security Appliance. Isso ajudará a detectar e bloquear muitos tipos conhecidos de ameaças, como phishing, spam e malware. Além disso, eduque o usuário final. Quando os ataques fazem isso pelas medidas de segurança em vigor, e eles vão às vezes, o usuário final é a última linha de defesa. Ensine-os a reconhecer spam, tentativas de phishing, links e URLs suspeitos, homoglifos e a nunca abrir anexos suspeitos.

17.2.4

**Bancos de dados expostos pela Web**

Aplicativos Web geralmente se conectam a um banco de dados relacional para acessar dados. Como os bancos de dados relacionais geralmente contêm dados confidenciais, os bancos de dados são um alvo freqüente para ataques.

**Injeção de código**

Os atacantes podem executar comandos no sistema operacional de um servidor Web através de uma aplicação Web vulnerável. Isso pode ocorrer se o aplicativo Web fornecer campos de entrada para o invasor para inserir dados mal-intencionados. Os comandos do intruso são executados através da aplicação Web e têm as mesmas permissões que a aplicação Web. Este tipo de ataque é usado porque muitas vezes não há validação insuficiente de entrada. Um exemplo é quando um ator ameaça injeta código PHP em um campo de entrada inseguro na página do servidor.

**Injeção de SQL**

SQL é a linguagem usada para consultar um banco de dados relacional. Os atores de ameaças usam injeções SQL para violar o banco de dados relacional, criar consultas SQL mal-intencionadas e obter dados confidenciais do banco de dados relacional.

Um dos ataques de banco de dados mais comuns é o ataque de injeção SQL. O ataque de injeção SQL consiste em inserir uma consulta SQL através dos dados de entrada do cliente para o aplicativo. Uma exploração de injeção SQL bem-sucedida pode ler dados confidenciais do banco de dados, modificar dados do banco de dados, executar operações de administração no banco de dados e, às vezes, emitir comandos para o sistema operacional.

A menos que um aplicativo use validação rigorosa de dados de entrada, ele será vulnerável ao ataque de injeção SQL. Se um aplicativo aceitar e processar dados fornecidos pelo usuário sem qualquer validação de dados de entrada, um ator de ameaça poderá enviar uma string de entrada criada com intuito malicioso para acionar o ataque de injeção SQL.

Os analistas de segurança devem ser capazes de reconhecer consultas SQL suspeitas para detectar se o banco de dados relacional foi submetido a ataques de injeção SQL. Eles precisam ser capazes de determinar qual ID de usuário foi usado pelo ator da ameaça para fazer login e, em seguida, identificar qualquer informação ou acesso adicional que o ator da ameaça poderia ter aproveitado após um login bem-sucedido.

17.2.5

## Scripts do lado do cliente

**Scripting através de sites**

Nem todos os ataques são iniciados do lado do servidor. Cross-Site Scripting (XSS) é onde as páginas da Web executadas no lado do cliente, dentro de seu próprio navegador da Web, são injetadas com scripts mal-intencionados. Esses scripts podem ser usados pelo Visual Basic, JavaScript e outros para acessar um computador, coletar informações confidenciais ou implantar mais ataques e espalhar malware. Tal como acontece com a injeção de SQL, isso é muitas vezes devido ao invasor postar conteúdo em um site confiável com falta de validação de entrada. Os futuros visitantes do Web site fidedigno serão expostos ao conteúdo fornecido pelo intruso.

Estes são os dois tipos principais de XSS:

* **Armazenado (persistente)** — Isso é armazenado permanentemente no servidor infectado e é recebido por todos os visitantes da página infectada.
* **Refletido (não persistente)** — Isso requer apenas que o script mal-intencionado esteja localizado em um link e os visitantes devem clicar no link infectado para se infectarem.

Estas são algumas maneiras de prevenir ou reduzir ataques XSS:

* Certifique-se de que os desenvolvedores de aplicativos da Web estejam cientes das vulnerabilidades XSS e de como evitá-las.
* Use uma implementação IPS para detectar e evitar scripts mal-intencionados.
* Use um proxy da Web para bloquear sites mal-intencionados.
* Use um serviço como o Cisco Umbrella para impedir que os usuários naveguem para sites conhecidos por serem mal-intencionados.
* Tal como acontece com todas as outras medidas de segurança, certifique-se de educar os usuários finais. Ensine-os a identificar ataques de phishing e notificar o pessoal da Infosec quando suspeitar de qualquer coisa relacionada à segurança.

17.2.6

**Laboratório - Atacando um banco de dados MySQL**

Neste laboratório, você visualizará um arquivo PCAP de um ataque anterior contra um banco de dados SQL.

17.2.7

## Laboratório - Leitura de logs do servidor

Neste laboratório, você completará os seguintes objetivos:

* Lendo arquivos de log ….
* Arquivos de log e Syslog
* Log Files and **jornalctl**

# Resumo do ataque ao que fazemos

17.3.1

## O que aprendi neste módulo?

**Serviços IP**

Os hosts transmitem uma solicitação ARP para outros hosts no segmento de rede para determinar o endereço MAC de um host com um endereço IP específico. Qualquer cliente pode enviar uma resposta ARP não solicitada denominada "ARP gratuito". Esse recurso do ARP também significa que qualquer host pode reivindicar ser o proprietário de qualquer IP / MAC que escolher. Um ator de ameaça pode envenenar o cache ARP de dispositivos na rede local, criando um ataque MiTM para redirecionar o tráfego.

O protocolo Domain Name System (DNS) define um serviço automatizado que combina nomes de recursos com o endereço de host IP numérico necessário. Inclui o formato da mensagem para consultas, respostas e dados. Ele usa registros de recursos (RR) para identificar o tipo de resposta DNS. O DNS é crucial para a operação de uma rede e deve ser protegido de acordo. Muitas organizações usam os serviços de servidores DNS abertos publicamente para fornecer respostas às consultas. Os resolvedores abertos DNS são vulneráveis a várias atividades mal-intencionadas, incluindo envenenamento de cache DNS, em que registros falsificados são fornecidos ao resolvedor aberto. Ataques de amplificação e reflexão DNS são outro tipo de ataque no qual a natureza benigna do protocolo DNS é explorada para causar ataques DOS/DDoS. Em ataques de utilização de recursos DNS, um ataque DoS é iniciado contra o próprio servidor DNS. Os atores de ameaças geralmente se escondem usando técnicas furtivas de DNS, como Fast Flux, em que servidores mal-intencionados mudam rapidamente seu endereço IP. Os atores de ameaças usam o Double IP Flux, no qual os atores de ameaças mudarão rapidamente seu nome de domínio para mapeamento IP e seu servidor de nomes autoritativo. Os agentes de ameaças também podem usar o domínio sombreado para ocultar a origem de seus ataques, reunindo credenciais de contas de domínio para criar silenciosamente vários subdomínios a serem usados durante os ataques. O DNS na empresa às vezes é negligenciado como um protocolo que pode ser usado por botnets. Os agentes de ameaças que usam o tunelamento DNS colocam tráfego que não é de DNS, dentro do tráfego DNS. Esse método geralmente contorna soluções de segurança. Para poder interromper o túnel DNS, um filtro que inspecione o tráfego DNS deve ser usado. Os servidores DNS dinâmicos são populares entre os atores de ameaças e o tráfego que usa DNS dinâmico deve ser uma preocupação especial do analista de segurança cibernética.

O DHCP usa uma simples troca de mensagens broadcast e unicast para fornecer aos hosts informações de endereçamento. Um ataque de spoofing de DHCP ocorre quando um servidor DHCP invasor está conectado à rede e fornece falsos parâmetros de configuração IP aos clientes legítimos. O servidor não autorizado pode fornecer informações incorretas do gateway, informações do servidor DNS ou informações de endereçamento IP.

**Serviços Corporativos**

Os navegadores da World Wide Web são usados por quase todos. Bloquear completamente a navegação na Web não é uma opção porque as empresas precisam de acesso à Web. Os analistas de segurança cibernética devem ter uma boa compreensão de como um ataque padrão baseado na Web funciona. Os estágios comuns de um ataque típico da Web incluem a vítima, sem saber, visitar uma página da Web que foi comprometida por malware. A página Web comprometida redireciona o usuário para um site que hospeda códigos mal-intencionados. O navegador é feito para visitar este site e código malicioso infecta seu computador. Isso é conhecido como um drive-by download. Independentemente do tipo de ataque que está sendo usado, o objetivo principal do ator da ameaça é garantir que o navegador da Web da vítima acabe na página da web do ator da ameaça, que, em seguida, serve o exploit malicioso para a vítima. Alguns sites mal-intencionados aproveitam plug-ins vulneráveis ou vulnerabilidades do navegador para comprometer o sistema do cliente. Redes maiores dependem de IDSs para verificar arquivos baixados em busca de malware. Se detectado, o IDS emite alertas e registra o evento em arquivos de log para análise posterior. Os logs de conexão do servidor geralmente podem revelar informações sobre o tipo de varredura ou ataque. Os diferentes grupos de códigos de status de conexão incluem **informações 1xx**, 2xx **bem-sucedido**, **redirecionamento 3xx**, erro de **cliente 4xx**e erro de **servidor 5xx**. Para se defender contra ataques baseados na Web, as contramedidas que devem ser usadas incluem sempre atualizar o sistema operacional e os navegadores com patches e atualizações atuais, usar um proxy da Web para bloquear sites mal-intencionados, usar as melhores práticas de segurança do Open Web Application Security Project (OWASP) ao desenvolver a Web e educando os usuários finais mostrando-lhes como evitar ataques baseados na Web.

Há uma série de ataques que usam e-mail para transportar cargas de malware ou para phish para obter informações pessoais. Os servidores SMTP também podem ter vulnerabilidades e devem ser mantidos atualizados com patches. Os appliances de segurança de e-mail podem detectar e bloquear muitos tipos de ameaças de e-mail conhecidas, incluindo phishing, spam e malware.

Aplicativos Web geralmente se conectam a bancos de dados. Como esses bancos de dados podem conter informações confidenciais, eles são um alvo freqüente de ataques. Os ataques de injeção de código e injeção SQL exploram campos de entrada insuficientemente validados para enviar comandos para bancos de dados ou outros aplicativos, a fim de obter acesso a informações privadas. Os ataques XSS (Cross-Site Scripting) ocorrem quando os navegadores executam scripts mal-intencionados no cliente e fornecem aos agentes da ameaça acesso a informações confidenciais no host local.

O OWASP Top 10 Riscos de Segurança de Aplicativos Web foi projetado para ajudar as organizações a criar aplicativos Web seguros. É uma lista útil de potenciais vulnerabilidades que são comumente exploradas por atores de ameaças.