



# Módulo 16: Atacando a Fundação



CyberOps Associate v1.0

Prof. Clemilson Oliveira

[clemilson.oliveira@edu.sc.senai.br](mailto:clemilson.oliveira@edu.sc.senai.br)



# Objetivos do módulo

**Título do módulo:**Atacando a Fundação

**Objetivo do Módulo:** Explique 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.

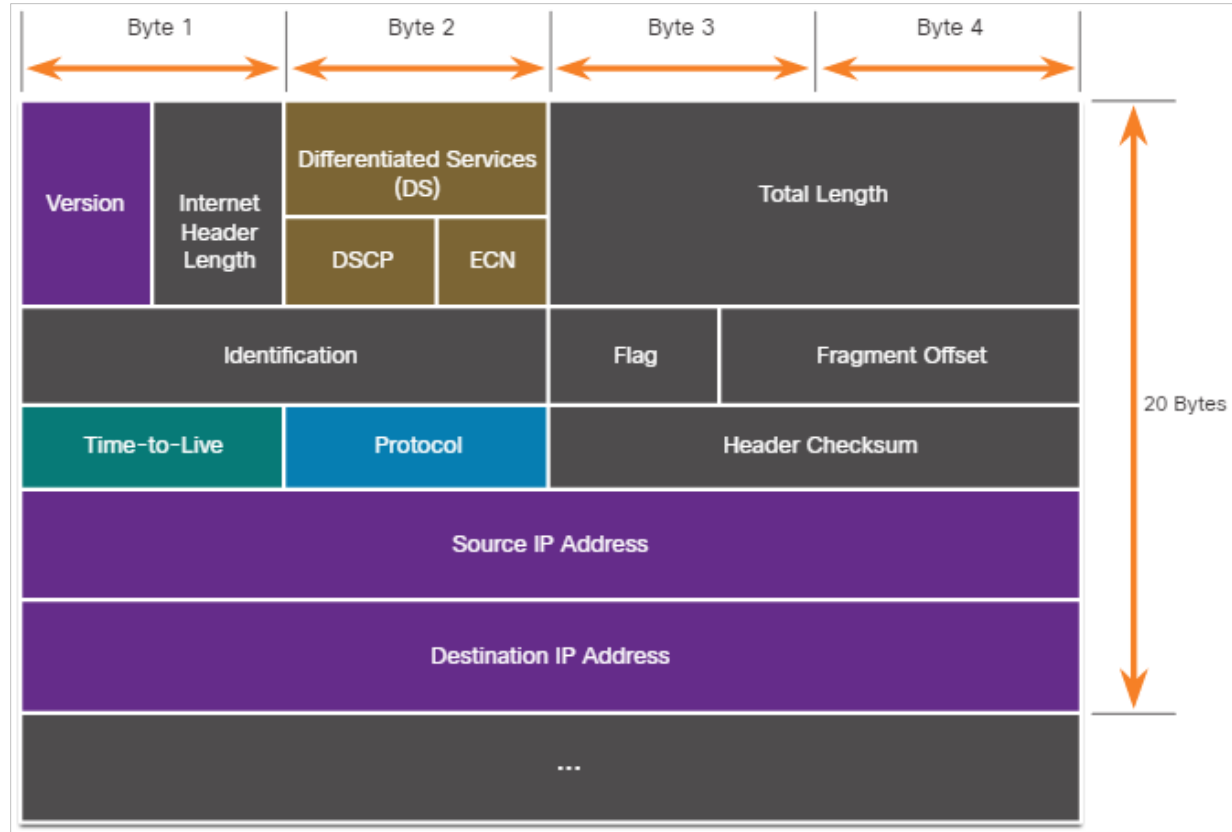
# 16.1 Detalhes da PDU IP

# IPv4 e IPv6

- 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 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.

# O Cabeçalho de Pacote IPv4

Os campos no cabeçalho do pacote IPv4 são mostrados na figura. Existem 10 campos no cabeçalho do pacote IPv4.



## O Cabeçalho de Pacote IPv4 (Cont.)

A tabela a seguir descreve os campos de cabeçalho IPv4:

Campo de cabeçalho IPv4	Descrição
Versão	<ul style="list-style-type: none"><li>• Contém um valor binário de 4 bits definido como 0100 que identifica isso como um pacote IPv4.</li></ul>
Comprimento do cabeçalho da Internet	<ul style="list-style-type: none"><li>• Um campo de 4 bits contendo o comprimento do cabeçalho IP.</li><li>• O comprimento mínimo de um cabeçalho IP é de 20 bytes.</li></ul>
Serviços diferenciados ou DiffServ (DS)	<ul style="list-style-type: none"><li>• 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.</li><li>• Os seis bits mais significativos do campo DiffServ são o Ponto de código de serviços diferenciados (DSCP).</li><li>• Os dois últimos bits são os bits de notificação de congestionamento explícito (ECN).</li></ul>
Comprimento total	<ul style="list-style-type: none"><li>• Especifica o comprimento do pacote IP, incluindo o cabeçalho IP e os dados do usuário.</li><li>• O campo de comprimento total é de 2 bytes, portanto, o tamanho máximo de um pacote IP é de 65.535 bytes.</li></ul>

## O Cabeçalho de Pacote IPv4 (Cont.)

Campo de cabeçalho IPv4	Descrição
Deslocamento de identificação, bandeira e fragmento	<ul style="list-style-type: none"><li>• À medida que um pacote IP se move, talvez seja necessário atravessar uma rota que não possa lidar com o tamanho do pacote. O pacote será dividido, ou fragmentado, em pacotes menores e remontado posteriormente.</li><li>• Esses campos são usados para fragmentar e remontar pacotes.</li></ul>
Tempo de Vida (TTL)	<ul style="list-style-type: none"><li>• Contém um valor binário de 8 bits que é usado para limitar a vida útil de um pacote.</li><li>• 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.</li><li>• 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.</li></ul>
Protocolos	<ul style="list-style-type: none"><li>• O campo é usado para identificar o protocolo de próximo nível.</li><li>• 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.</li><li>• Valores comuns incluem ICMP (1), TCP (6) e UDP (17).</li></ul>

## O Cabeçalho de Pacote IPv4 (Cont.)

Campo de cabeçalho IPv4	Descrição
Cabeçalho checksum	<ul style="list-style-type: none"><li>• Um valor calculado com base no conteúdo do cabeçalho IP.</li><li>• Usado para determinar se algum erro foi introduzido durante a transmissão.</li></ul>
Endereço IPv4 Origem	<ul style="list-style-type: none"><li>• Contém um valor binário de 32 bits que representa o endereço IPv4 de origem do pacote.</li><li>• O endereço de origem IPv4 é sempre um endereço unicast.</li></ul>
Endereço IPv4 de destino	<ul style="list-style-type: none"><li>• Contém um valor binário de 32 bits que representa o endereço IPv4 de destino do pacote.</li></ul>
Opções e Preenchimento	<ul style="list-style-type: none"><li>• Este é um campo que varia em comprimento de 0 a um múltiplo de 32 bits.</li><li>• 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.</li></ul>



## Video - Amostra de Cabeçalhos IPv4 no Wireshark

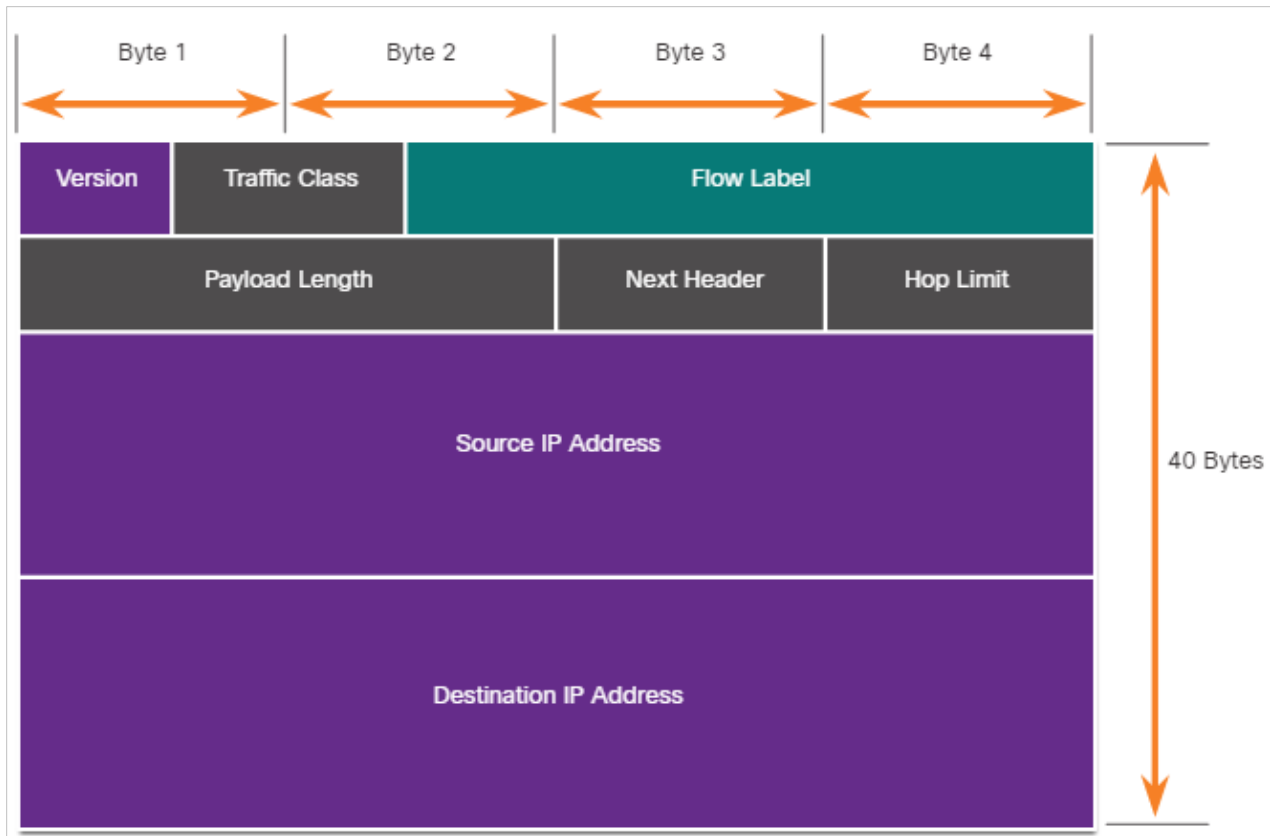
Clique em Reproduzir na figura para ver uma demonstração do exame de cabeçalhos IPv4 em uma captura do Wireshark.



direitos reservados.

## O Cabeçalho de Pacote IPv6

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



## O Cabeçalho de Pacote IPv6 (Cont.)

A tabela a seguir descreve os campos de cabeçalho IPv6:

Campo de cabeçalho IPv6	Descrição
Versão	<ul style="list-style-type: none"><li>• Este campo contém um valor binário de 4 bits definido como 0110 que o identifica como um pacote IPv6.</li></ul>
Classe de tráfego	<ul style="list-style-type: none"><li>• Este campo de 8 bits é equivalente ao campo IPv4 Differentiated Services (DS).</li></ul>
Rótulo de fluxo	<ul style="list-style-type: none"><li>• Este campo de 20 bits sugere que todos os pacotes com o mesmo rótulo de fluxo recebem o mesmo tipo de tratamento pelos roteadores.</li></ul>
Tamanho da carga	<ul style="list-style-type: none"><li>• Este campo de 16 bits indica o comprimento da porção de dados ou carga útil do pacote IPv6.</li></ul>
Próximo cabeçalho	<ul style="list-style-type: none"><li>• Este campo de 8 bits é equivalente ao campo do protocolo IPv4.</li><li>• 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.</li></ul>

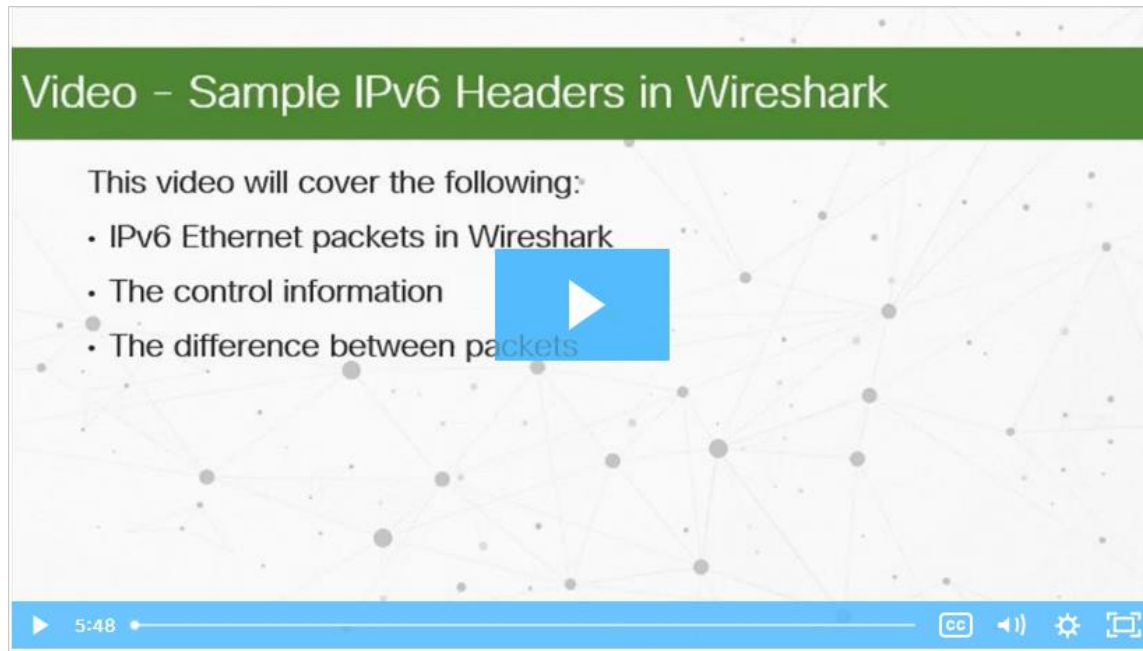
# O Cabeçalho de Pacote IPv6 (Cont.)

Campo de cabeçalho IPv6	Descrição
Limite de saltos	<ul style="list-style-type: none"><li>• Este campo de 8 bits substitui o campo TTL IPv4.</li><li>• Esse valor é subtraído de um por cada roteador que encaminha o pacote.</li><li>• 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.</li></ul>
Endereço IPv6 origem	<ul style="list-style-type: none"><li>• Este campo de 128 bits identifica o endereço IPv6 do host de envio.</li></ul>
Endereço IPv6 destino	<ul style="list-style-type: none"><li>• Este campo de 128 bits identifica o endereço IPv6 do host receptor.</li></ul>

- Um pacote IPv6 também contém 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.

## Video - Amostra de Cabeçalhos IPv6 no Wireshark

Clique em Reproduzir na figura para ver uma demonstração do exame de cabeçalhos IPv6 em uma captura do Wireshark.



# 16.2 Vulnerabilidades de IP

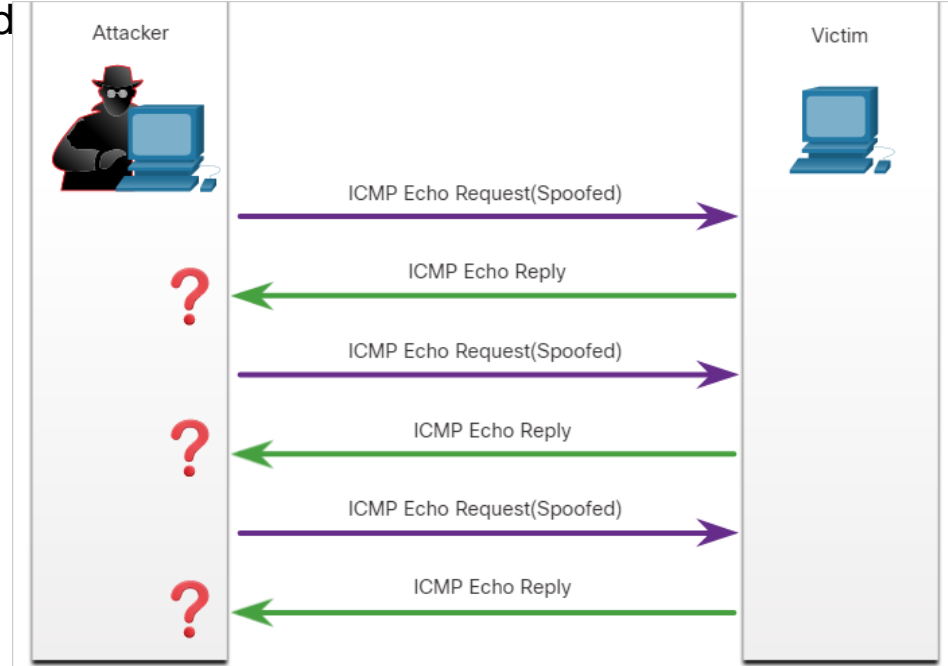
# Vulnerabilidadesde IP

A tabela a seguir lista alguns dos ataques 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 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.

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



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



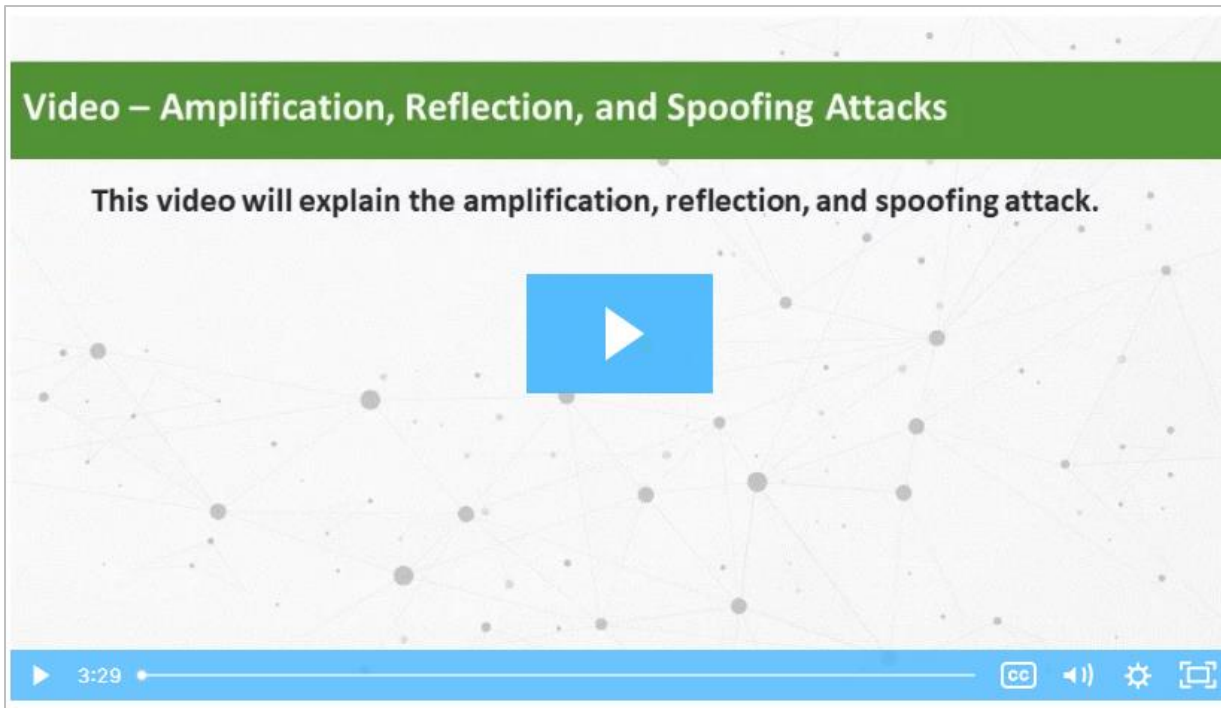
## Ataques ICMP (Cont.)

- 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.
- A tabela a seguir lista as 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 desviar o tráfego um host de destino a enviar 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.

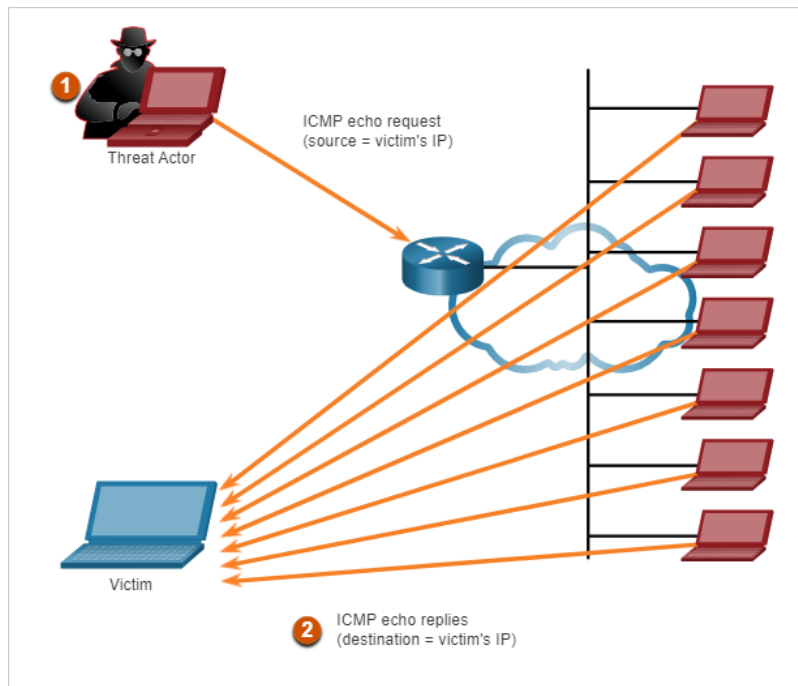
## Video - Ataques de Amplificação, Reflexão e Falsificação

Clique em Reproduzir na figura para ver um vídeo de amplificação, reflexão e ataques de spoofing.



# Ataques de Amplificação e Reflexão

- Os agentes de ameaças geralmente usam técnicas de amplificação e reflexão para criar ataques de negação de serviço (DoS).
- A figura mostra como uma técnica de amplificação e reflexão chamada de ataque Smurf é usada para oprimir um host alvo.
  - Amplificação** - O ator da ameaça encaminha mensagens de solicitação de eco ICMP para muitos hosts. Essas mensagens contêm o endereço IP de origem da vítima.
  - Reflexão** - Todos esses hosts respondem ao endereço IP falsificado da vítima para sobrecarregá-lo.
- Os agentes de ameaças também usam ataques de exaustão de recursos.



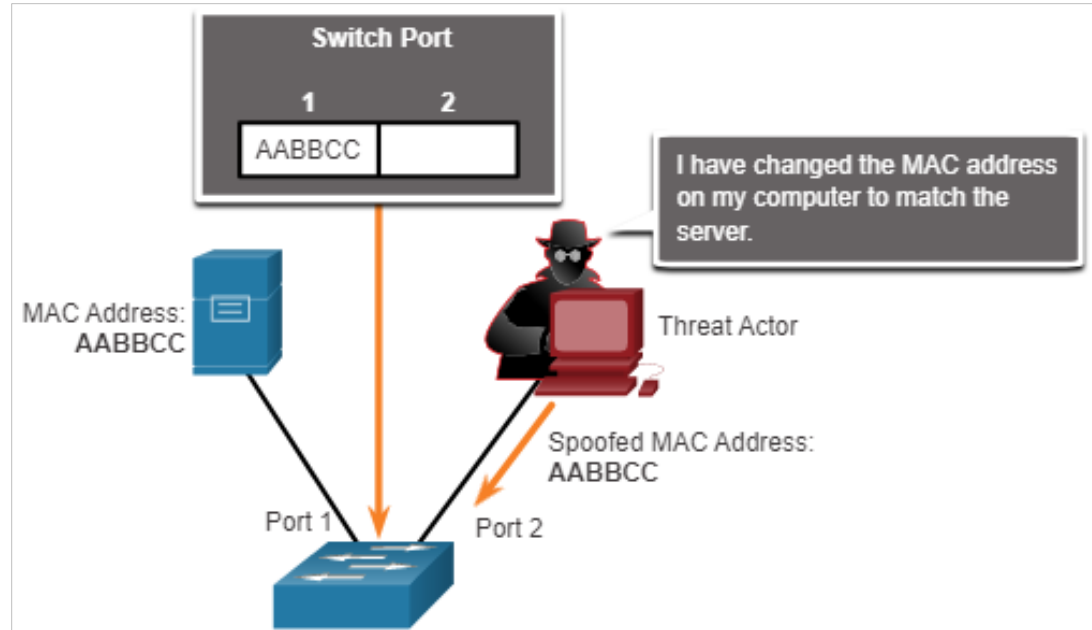
**Nota:** Novas formas de ataques de amplificação e reflexão, como ataques de reflexão e amplificação com base no DNS e ataques de amplificação do Network Time Protocol (NTP), agora estão sendo usados.

## Ataques de Falsificação de Endereço

- 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:
  - **Spoofing não cego** - O ator 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.

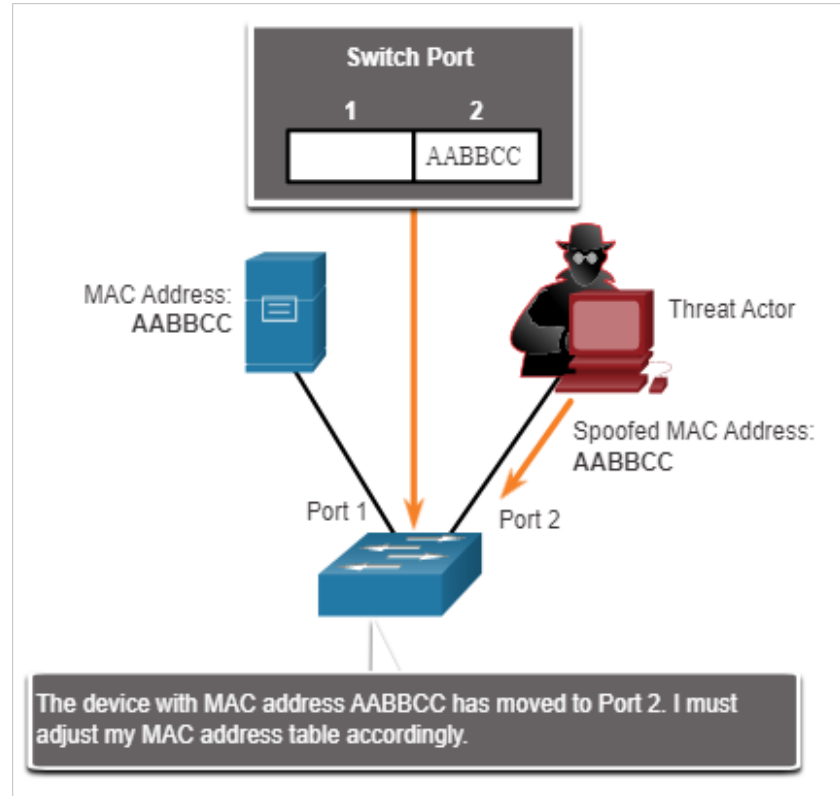
## Ataques de Falsificação de Endereço (Cont.)

- 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.



## Ataques de Falsificação de Endereço (Cont.)

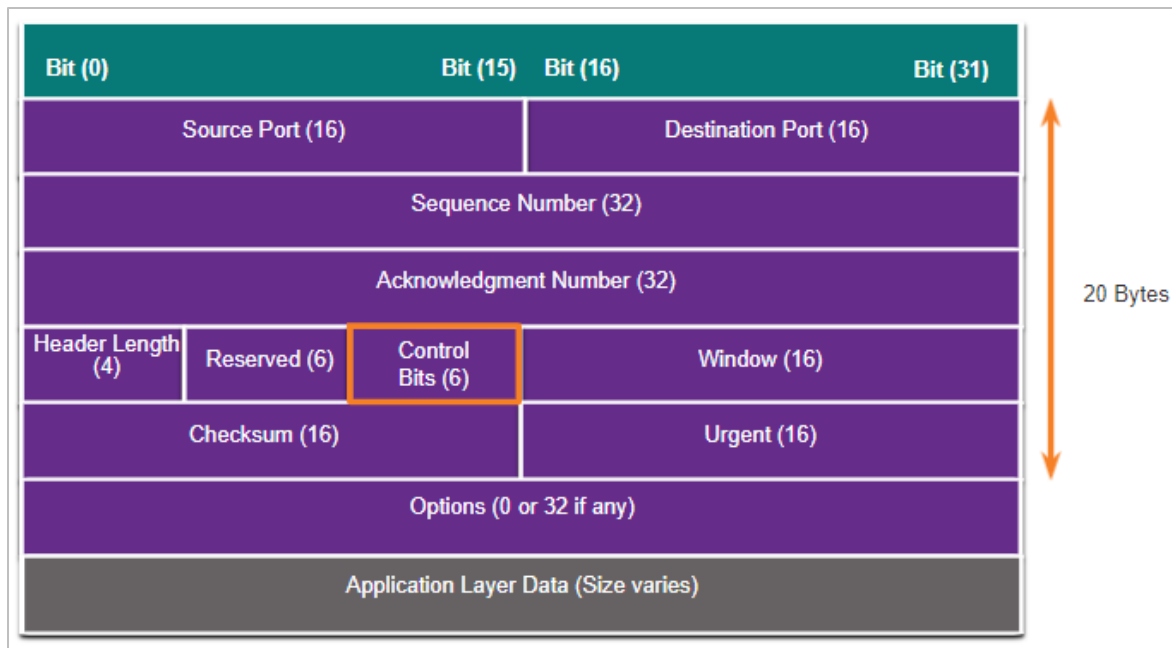
- O switch substitui a entrada atual da tabela CAM e atribui o endereço MAC à nova porta, como mostrado na figura.
- Em seguida, encaminha os quadros destinados ao host de destino para o host atacante.
- A falsificação de aplicativos ou serviços é outro exemplo de falsificação. Um agente de ameaça pode conectar um servidor DHCP não autorizado para criar uma condição MiTM.



# 16.3 Vulnerabilidades de TCP e UDP

## Cabeçalho de segmento TCP

- 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.
- A seguir, os seis bits de controle do segmento TCP:
  - **URG** - Campo indicador de urgência
  - **ACK** - Campo de Reconhecimento Significativo
  - **PSH** - Função Push
  - **RST** - Restabelecer a conexão
  - **SYN** - Sincronizar números de sequência
  - **FIN** - Não há mais dados do remetente





## Serviços TCP

O TCP fornece estes serviços:

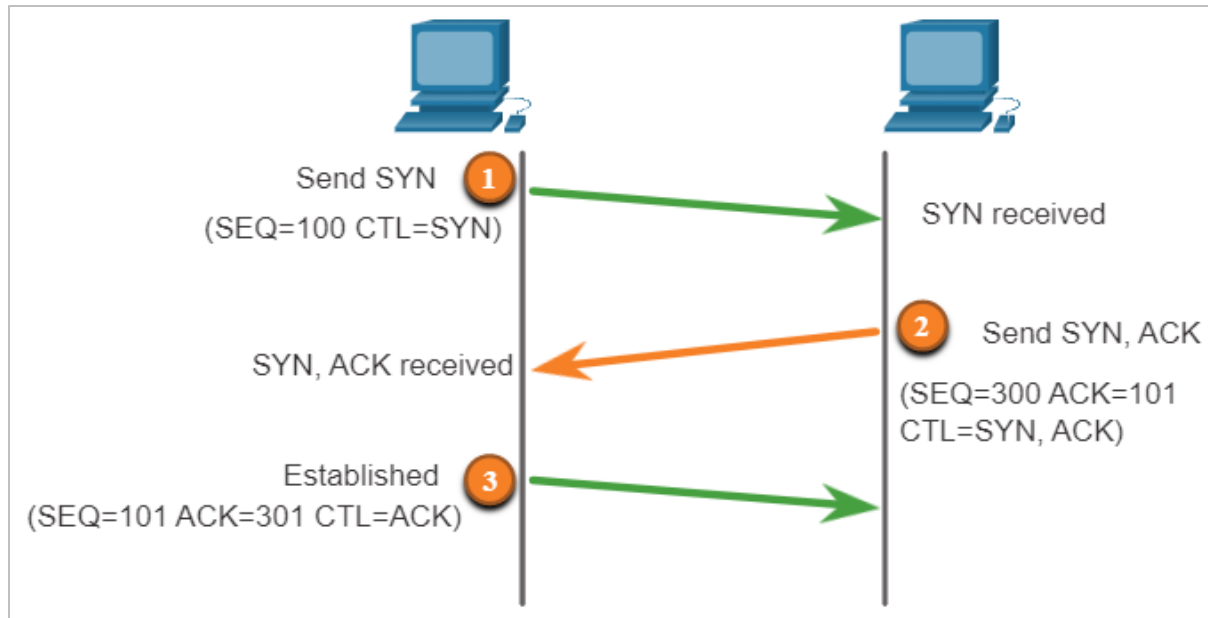
- **Entrega Confiável** - O TCP incorpora confirmações para garantir a entrega, em vez de depender de protocolos da camada superior para detectar e resolver erros. Se uma confirmação não for recebida à tempo, o remetente retransmitirá os dados. Exigir reconhecimentos dos dados recebidos pode causar atrasos 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 Stateful** - A comunicação com monitoração de estado TCP entre duas partes ocorre durante o handshake TCP de três vias. Antes que os dados possam ser transferidos usando TCP, um handshake de três vias abre a conexão TCP. Se ambos os lados concordarem com a conexão TCP, os dados poderão ser enviados e recebidos por ambas as partes usando o TCP.

## Serviços TCP (Cont.)

### Análise do Aperto de mãos Triplo do TCP

Uma conexão TCP é estabelecida em três etapas:

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

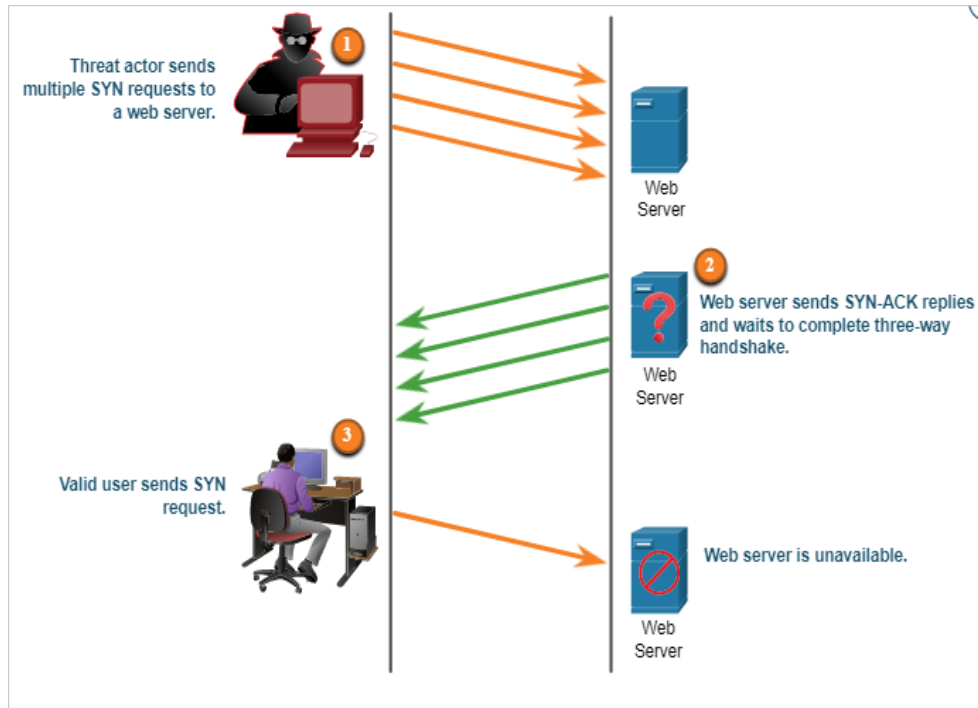


# Ataques TCP

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

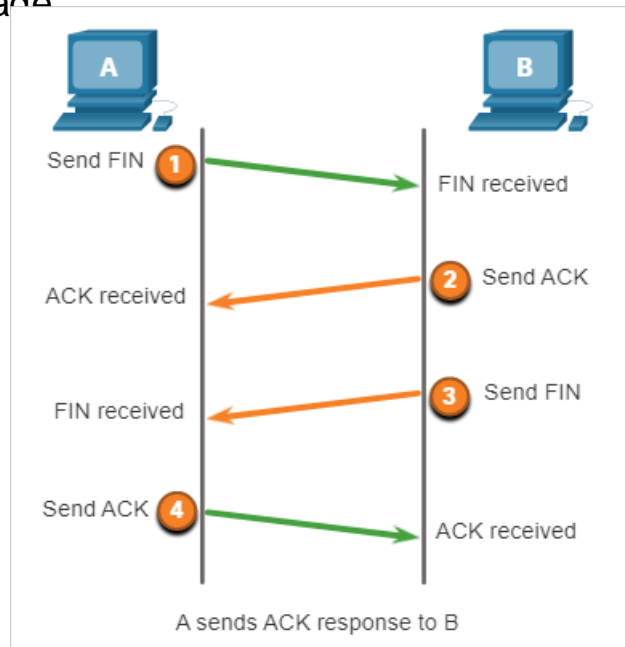
- O ataque de inundação SYN TCP explora o aperto de mãos triplo do TCP.
- A figura mostra um agente de ameaça enviando continuamente pacotes de solicitação de sessão TCP SYN com um endereço IP de origem falsificado aleatoriamente para um destino.
- O destino responde com um pacote TCP SYN-ACK ao endereço IP falsificado e espera por um pacote TCP ACK. Essas respostas nunca chegam.
- O host de destino tem muitas conexões TCP semiabertas e serviços TCP negados a usuários legítimos.



## Ataques TCP (Cont.)

### Ataque de redefinição de TCP

- Um ataque de redefinição de TCP pode ser usado para encerrar as comunicações TCP entre dois hosts.
- 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.
- O encerramento de uma sessão TCP usa o seguinte processo de troca de quatro vias:
  - Quando o cliente não tem mais dados para enviar no fluxo, ele envia um segmento com um flag FIN ligado.
  - O servidor envia ACK para confirmar o recebimento de FIN para encerrar a sessão do cliente com o servidor.
  - O servidor envia um FIN ao cliente para encerrar a sessão do servidor-para-cliente.
  - O cliente responde com um ACK para reconhecer o FIN do servidor.



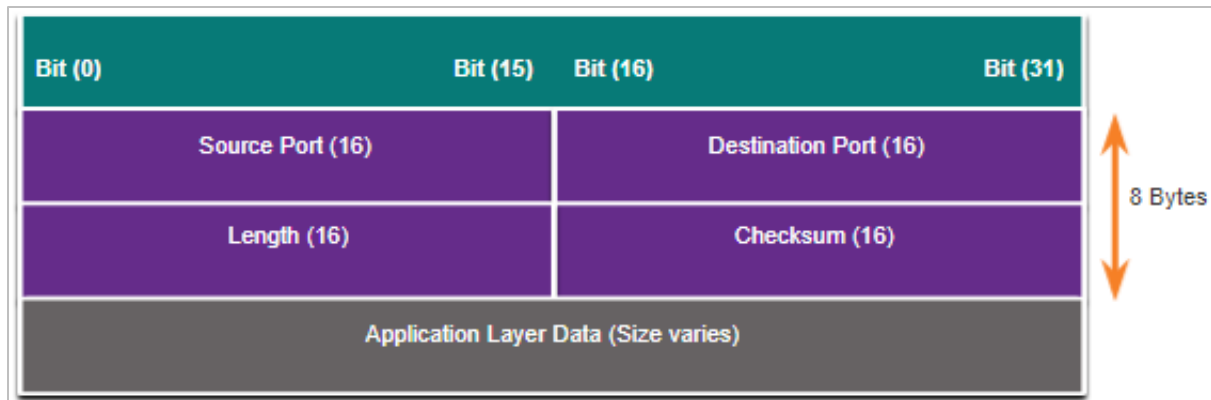
## Ataques TCP (Cont.)

### Sequestro de sessão TCP

- Sequestro de sessão TCP é outra vulnerabilidade do TCP.
- Um ator de ameaça assume o controle de um host já autenticado à medida que 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.

# Cabeçalho e operação de 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.
- A estrutura do segmento UDP, mostrada na figura, é muito menor que o TCP.
- Embora o UDP normalmente seja chamado de não confiável, isso não significa que os aplicativos que usam UDP sejam sempre não confiáveis. 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.



### Ataques TCP

- O UDP não está protegido por nenhuma criptografia. A criptografia pode ser adicionada 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.

### Ataques 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 há muitas portas fechadas no servidor, isso cria muito tráfego no segmento, que usa a maior parte da largura de banda. O resultado é muito semelhante a um ataque DoS.

# 16.4 Resumo do ataque à base



## O que eu aprendi neste módulo?

- 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.
- 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 que eu aprendi neste módulo? (Continuação)

- O ICMP foi desenvolvido para transportar mensagens de diagnóstico e relatar condições de erro quando rotas, hosts e portas não estão disponíveis.
- 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.
- 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.

