# Curso 3 de 8 - Redes de computadores e segurança de rede

# *Módulo 1*

## Introdução às redes de computadores

**Network(rede):** É um grupo de dispositivos conectados. Em casa, dispositivos conectados à rede podem ser um laptop, telefone e dispositivos inteligentes, como geladeira e ar condicionado.

Os dispositivos em uma rede podem se comunicar entre si por meio de cabos de rede ou conexões sem fio. Redes podem se comunicar com redes em outros locais e com os dispositivos nelas contidas.

Os dispositivos precisam se encontrar em uma rede para estabelecer comunicações, usando endereços ou identificadores exclusivos para se localizarem. Os identificadores garantem que a comunicação acontecerá com o dispositivo certo. Eles são chamados de endereços **IP** e **MAC**.

Os dispositivos podem se comunicar em dois tipos de redes: rede local (ou LAN) e uma rede de longa distância (WAN).

**Rede local (LAN):** É uma rede que abrange uma área pequena, como um prédio de escritórios, uma escola ou uma casa. Quando aparelhos domésticos como celulares, tablets e televisões se conecta ao wifi, eles formam uma LAN, que se conecta à internet.

**Rede de longa distância (WAN):** Abrange uma grande área geográfica, como uma cidade, estado ou país. Um exemplo de rede WAN é a internet.

**Hub:** É um dispositivo de rede que transmite informações para todos os dispositivos na rede.

**Switch:** É um dispositivo que faz conexões entre dispositivos específicos em uma rede ao enviar e receber dados entre eles. Ele é mais inteligente que um hub, pois só passa os dados para o destino pretendido, além de ser mais seguro e permitir o controle do fluxo do tráfego.

**Roteador:** É um dispositivo de rede que conecta múltiplas redes.

**Modem:** Conecta o roteador à internet e trás acesso à internet para a LAN.

**Ferramentas de virtualização:** São peças de software que realizam operações de rede que normalmente seriam concluídas por um hub, switch, roteador ou modem. São oferecidas por provedores de serviços em nuvem. Permitem reduzir custos e escalonabilidade.

**Computação em nuvem:** Prática de usar servidores remotos, aplicativos e serviços de rede hospedados na internet em vez de em dispositivos físicos locais.

**Rede em nuvem:** É uma coleção de servidores ou computadores que armazena recursos e dados em data centers remotos que podem ser acessados via internet.

**Provedores de serviços em nuvem(CSP):** Oferecem computação em nuvem para manter os aplicativos. Por exemplo:

- Armazenamento sob demanda
- Capacidade de processamento
- Análises comerciais e da web

**Três principais serviços oferecidos pelos CSPs:**

- **Software como serviço (SaaS)** refere-se a conjuntos de software operados pelo CSP que uma empresa pode usar remotamente sem hospedar o software.
- **Infraestrutura como serviço (IaaS)** refere-se ao uso de componentes de computador virtuais oferecidos pelo CSP. Eles incluem contenções virtuais e armazenamento que são configurados remotamente por meio da API ou do console da Web do CSP. Os serviços de computação e armazenamento em nuvem podem ser usados para operar aplicativos existentes e outras cargas de trabalho de tecnologia sem modificações significativas. Os aplicativos existentes podem ser modificados para aproveitar os recursos de disponibilidade, desempenho e segurança que são exclusivos dos serviços do provedor de nuvem.
- **Plataforma como serviço (PaaS)** refere-se a ferramentas que os desenvolvedores de aplicativos podem usar para projetar aplicativos personalizados para sua empresa. Os aplicativos personalizados são projetados e acessados na Nuvem e usados para as necessidades comerciais específicas de uma empresa.

**Ambiente de nuvem híbrida:** Quando as organizações usam os serviços de um CSP além de seus computadores, redes e armazenamento local.

**Ambiente de várias nuvens:** Quando as organizações usam mais de um CSP.

**Redes definidas por software(SDNs):** São compostas de dispositivos e serviços de rede virtuais. As SDNs fornecem switches virtuais, roteadores, firewalls e outros. Isso é possível por meio da virtualização de rede, onde os switches e roteadores físicos usam software para realizar o roteamento de pacotes. No caso da rede de computadores em nuvem, as ferramentas SDN são hospedadas em servidores localizados no data center do CSP.

**Benefícios da computação em nuvem e das redes definidas por software:**

- **Confiabilidade:** Se baseia na disponibilidade dos serviços e recursos da nuvem, na segurança das conexões e na frequência com que os serviços são efetivamente executados. A computação em nuvem permite que os funcionários e clientes acessem os recursos de que precisam de forma consistente e com o mínimo de interrupção.
- **Redução de custos:** Como os CSPs têm data centers grandes, eles podem oferecer dispositivos e serviços de virtualização por uma fração do custo necessário para as empresas instalarem, corrigirem, atualizarem e gerenciarem a infraestrutura.
- **Aumento de escalonabilidade:** Os CSPs proporcionam um melhor aumento de escalonabilidade para as organizações, pois facilitam o consumo de serviços em um modelo de utilidade elástica, conforme necessário. As empresas pagam apenas pelo que precisam.

## Comunicação em rede

A comunicação em uma rede acontece quando os dados são transferidos de um ponto para outro. Partes de dados são, normalmente, chamados de pacotes de dados.

**Pacotes de dados:** Uma unidade básica de informação que viaja de um dispositivo para outro por meio de uma rede. Esse pacote contém informações sobre para onde o pacote está indo, de onde vem e o conteúdo da mensagem.

O pacote de dados possui uma estrutura dividade em três:

- **Cabeçalho:** Inclui o endereço do protocolo da internet, o endereço IP e o endereço de controle de acesso à mídia, ou MAC, do dispositivo

de destino. Também inclui um número de protocolo que informa ao dispositivo receptor o que fazer com as informações do pacote.
- **Corpo:** Contém a mensagem que precisa ser transmitida ao dispositivo receptor.
- **Rodapé:** Sinaliza ao dispositivo receptor que o pacote está concluído.

**Largura de banda:** Quantidade de dados que um dispositivo recebe a cada segundo. É possível calcular a largura de banda dividindo a quantidade de dados pelo tempo em segundos.

**Velocidade:** Taxa na qual os pacotes de dados são recebidos ou baixados.

**Packet sniffing (Detecção de pacotes):** Prática de capturar e inspecionar pacotes de dados na rede.

**Modelo TCP/IP:** Protocolo de controle de transmissão e protocolo de internet. É o modelo padrão usado para comunicação em rede.

**Protocolo de controle de transmissão (TCP):** É um protocolo de comunicação da internet que permite que dois dispositivos formem uma conexão e transmitam dados.

Inclui um conjunto de instruções para organizar os dados, para que possam ser enviados por uma rede. Garante que os pacotes cheguem ao destino apropriado.

**Protocolo de internet (IP):** Conjunto de padrões usados para rotear e endereçar pacotes de dados à medida que eles viajam entre dispositivos em uma rede.

Incluído no protocolo de internet está o endereço IP, que funciona como um endereço para cada rede privada.

Quando pacotes de dados são enviados e recebidos em uma rede, eles recebem uma porta

**Porta:** No sistema operacional de um dispositivo de rede, uma porta é um local baseado em software que organiza o envio e o recebimento de dados entre dispositivos em uma rede.

As portas dividem o tráfego da rede em segmentos com base no serviço que elas executarão entre os dispositivos.

As instruções dentro de um pacote de dados vem na forma de um número de porta, que permite que os computadores dividam o tráfego da rede e priorizem as operações que realizarão com os dados.

**Números de porta comuns:**

- **25** - Email
- **443** - Comunicação segura pela internet
- **20** - Trasnferência de arquivos grandes

**Modelo TCP/IP:** Framework usado para visualizar como os dados são organizados e transmitidos pela rede.

**Camadas do modelo TCP/IP:**

- **1 - Camada de acesso à rede:** Criação de pacotes de dados e sua transmissão pela rede. Inclui dispositivos de hardware conectados a cabos físicos e switches físicos que direcionam os dados para seu destino.
- **2 - Camada de internet:** Onde os endereços IP são anexados aos pacotes de dados para indicar a localização do remetente e do destinatário. Também se concentra em como as redes se conectam umas às outras.
- **3 - Camada de transporte:** Inclui protocolos para controlar o fluxo de tráfego em uma rede. Esses protocolos permitem ou negam a comunicação com outros dispositivos e incluem informações sobre o status da conexão. Envolve controle de erros.
- **4 - Camada de aplicativo:** Os protocolos determinam como os pacotes de dados interagirão com os dispositivos receptores. As funções incluem trasnferência de arquivos e serviços de e-mail.

## Comunicação em rede local e ampla

**Endereço de protocolo de internet (IP):** É uma String exclusiva de caracteres que identifica a localização de um dispositivo na internet. Cada dispositivo na internet possui um IP único.

**Tipos de endereço IP:**

- **IP versão 4 (IPv4):** Escritos como números de quatro com 1, 2  ou 3 dígitos separados por um ponto decimal (19.117.63.126)
- **IP versão 6 (IPv6):** Compostos de 32 caracteres, permitindo que mais dispositivos sejam conectados à internet sem ficar sem endereços tão rapidamente quanto o IPv4.

Os IPs podem ser públicos e privados. Os provedores de internet atribuem um endereço IP público que está conectado à localização geográfica da rede. Quando as comunicações de rede saem do dispositivo na internet, todos os

dispositivos têm o mesmo endereço público. Os IPs privados apenas são vistos por outros dispositivos na mesma rede local, significando que todos os dispositivos de uma rede podem se comunicar usando endereços IP exclusivos que o resto da internet não pode ver.

**Endereço MAC:** É um identificador alfanumérico único que é atribuído a cada dispositivo físico em uma rede.

## Glossário de revisão

**Largura de banda:** a capacidade máxima de transmissão de dados em uma rede, medida em bits por segundo
**Computação em nuvem:** A prática de usar servidores remotos, aplicativos e serviços de rede hospedados na Internet em vez de em dispositivos físicos locais
**Rede de computadores em nuvem:** Uma coleção de servidores ou computadores que armazenam recursos e dados em data centers remotos que podem ser acessados pela Internet
**Pacote de dados:** Uma unidade básica de informações que viaja de um dispositivo para outro em uma rede
**Hub:** Um dispositivo de rede que transmite informações para todos os dispositivos da rede
**Protocolo de Internet (IP):** Um conjunto de padrões usados para roteamento e endereçamento de pacotes de dados à medida que eles trafegam entre dispositivos em uma rede
**Endereço IP (Protocolo de Internet):** Uma sequência única de caracteres que identifica a localização de um dispositivo na Internet
**LAN (Local Area Rede, rede local):** Uma rede que abrange pequenas áreas, como um prédio de escritórios, uma escola ou uma casa
**Endereço de controle de acesso à mídia (MAC):** Um identificador alfanumérico Único que é atribuído a cada dispositivo físico em uma rede
**Modem:** Um dispositivo que conecta o roteador à Internet e leva o acesso à Internet para a LAN
**Rede:** Um grupo de dispositivos conectados
**Modelo OSI (Open Systems Interconnection, interconexão de sistemas abertos):** Um conceito padronizado que descreve as sete camadas que os computadores usam para se comunicar e enviar dados pela rede
**Interceptação de pacotes:** A prática de capturar e inspecionar pacotes de dados em uma rede
**Porta:** Um local baseado em software que organiza o envio e o recebimento de dados entre dispositivos em uma rede
**Roteador:** Um dispositivo de rede que conecta várias redes de computadores

**Velocidade:** a taxa na qual um dispositivo envia e recebe dados, medida em bits por segundo
**Switch:** Um dispositivo que faz conexões entre dispositivos específicos em uma rede, enviando e recebendo dados entre eles
**Modelo TCP/IP:** Uma estrutura usada para visualizar como os dados são organizados e transmitidos em uma rede
**Protocolo TCP (Transmission Control Protocol, Protocolo de Controle de Transmissão):** Um protocolo de comunicação da Internet que permite que dois dispositivos formem uma conexão e transmitam dados
**User Datagram Protocol (UDP):** Um protocolo sem conexão que não estabelece uma conexão entre dispositivos antes das transmissões
**Rede de longa distância (WAN):** Uma rede que abrange uma grande área geográfica, como uma cidade, um estado ou um país

# *Módulo 2*

## Introdução aos protocolos de rede

**Protocolos de rede:** Conjunto de regras usadas por dois ou mais dispositivos em uma rede que descreve a ordem de entrega e a estrutura dos dados.

**Protocolo de controle de transmissão (TCP):** Protocolo de comunicação pela internet que permite que dois dispositivos formem uma conexão e transmitam dados. O TCP também verifica os dois dispositivos antes de permitir que outras comunicações ocorram, chamado de handshake.

**Protocolo de resolução de endereço (ARP):** Usado para determinar o endereço MAC do próximo roteador ou dispositivo no caminho, garantindo que os dados cheguem ao lugar correto.

**Protocolo de transferência de hipertexto seguro (HTTPS):** Protocolo de rede que fornece um método seguro de comunicação entre o cliente e os servidores do site. Permite que o navegador envie com segurança uma solicitação de uma página da web para o servidor.

**Sistema de nome de domínio (DNS):** Protocolo de rede que traduz nomes de domínio da internet em endereços IP. O protocolo DNS envia o nome do domínio e o endereço da web para um servidor DNS que recupera o endereço IP do site que se deseja acessar, incluindo o endereço IP como endereço de destino dos pacotes de dados que viajam para o servidor da web.

**Protocolos de segurança:**

- **HTTPS:** Criptografa dados usando a camada de soquetes seguros e a segurança da camada de transporte (TLS ou SSL/TLS).
- **TLS ou SSL/TLS**

**Protocolos e portas:**

- **DHCP:** Porta UP 67 (servidores) e porta UDP 68 (Clientes)
- **ARP:** Nenhuma
- **Telnet:** Porta TCP 23
- **SSH:** Porta TCP 22
- **POP3:** Porta TCP/UDP 110 (Não criptografada) e porta TCP/UDP 995 (criptografada, SSL/TLS)
- **IMAP:** Porta TCP 143 (não criptografada) e porta TCP 993 (criptografada, SSL/TLS)
- **SMTP:** Porta TCP/UDP 25 (não criptografada)
- **SMTPS:** Porta TCP/UDP 587 (criptografada, TLS)

**IEEE 802.11 (Wifi):** Conjunto de padrões que definem comunicações para LANs sem fio. IEEE significa Instituto de Engenheiros Elétricos e Eletrônicos, que é uma organização que mantém os padrões Wi-fi, e 802.11 é um conjunto de protocolos usados em comunicações sem fio.

**Wi-fi Protected Access (WPA):** Protocolo de segurança sem fio para dispositivos que se conectam à internet. Evoluiu para versões mais recentes, como WPA2 e WPA3, que incluem melhorias de segurança, como criptografia avançada.

**WEP:** Protocolo de segurança de rede sem fio projetado para fornecer o mesmo nível de privacidade de redes com fio em conexões de rede sem fio para o usuário. É o padrão de segurança sem fio mais antigo, sendo considerado ultrapassado e de alto risco para organizações.

## Identificação do sistema

**Firewall:** Dispositivo de segurança de rede que monitora o tráfego de e para sua rede. Ele permite o tráfego ou o bloqueia com base em um conjunto definido de regras de segurança.

**Filtragem de portas:** Função de um firewall que bloqueia ou permite que determinados números de porta limitem a comunicação indesejada.

**Tipos de firewall:**

- **Firewall de hardware:** Considerada a forma mais básica de se defender contra ameaças a uma rede. Inspeciona cada pacote de dados antes que possa entrar na rede.
- **Firewall de software:** Executa as mesmas funções de uma firewall de hardware, mas não é um dispositivo físico, e sim um programa de software instalado em um computador ou servidor. Geralmente custa menos do que comprar um dispositivo físico, mas como é um programa de software, ocupa carga de processamento nos dispositivos instalados.
- **Firewall baseado em nuvem:** Os provedores de serviços em Nuvem oferecem firewalls como serviços (ou FaaS) para organizações. São firewalls de software hospedados por um provedor de serviços em nuvem. Também protegem quaisquer recursos ou processos que uma organização possa estar usando na nuvem.

**Firewall com estado:** Classe de firewall que monitora as informações que passam por ele e filtra proativamente as ameaças. Analisa o tráfego da rede em busca de características e comportamentos que pareçam suspeitos e impede que eles entrem na rede.

**Firewall sem estado:** Classe de firewall que opera baseado em regras predefinidas e não controla as informações dos pacotes de dados. Apenas age de acordo com as regras pré-configuradas definidas pelo administrador do firewall. Não armazena informações analisadas. São considerados menos seguros com os firewalls com estado.

**Firewall de última geração (NGFW):** Classe de firewall que oferece mais segurança do que um firewall com estado. Fornece inspeção de estado do tráfego de entrada e saída e executa funções de segurança mais aprofundadas, como:

- **Inspeção profunda de pacotes**
- **Proteção contra intrusões**
- **Serviços de inteligência de ameaças**

**Rede privada virtual (VPN):** Serviço de segurança de rede que altera o seu endereço de IP público e esconde sua localização virtual para que você mantenha os seus dados privados quando estiver usando uma rede pública como a internet.

As VPNs também criptografam seus dados enquanto eles viajam pela internet para preservar a confidencialidade. O serviço de VPN realiza o encapsulamento de seus dados de trânsito.

**Encapsulamento:** Processo realizado por um serviço de VPN que protege seus dados ao agrupar dados confidenciais em outros pacotes de dados.

**Segmentação de rede:** Técnica de segurança que divide a rede em segmentos.

**Zona de segurança:** Segmento de uma rede que protege a rede interna da internet. Faz parte de uma técnica de segurança chamada de segmentação de rede. Controlam quem pode acessar diferentes segmentos de uma rede. A rede de uma organização é classificada em dois tipos de zonas de segurança:

- **Zona não controlada:** Qualquer rede fora do controle da organização, como a internet.
- **Zona controlada:** Sub-rede que protege a rede interna de zonas não controladas.

**Áreas na zona controlada:**

- **Zona desmilitarizada:** Contém serviços voltados para o público que podem acessar a internet, como servidores web, servidores proxy e servidores DNS, além de servidores de e-mail e arquivos.
- **Rede interna:** Contém servidores e dados privados que a organização precisa proteger.
- **Zona restrita:** Existe dentro da rede interna e protege informações altamente confidenciais que só podem ser acessadas por funcionários com determinados privilégios.

**Servidor Proxy:** Servidor que atende à solicitação de um cliente encaminhando-a para outros servidores. É um servidor dedicado que fica entre a internet e o resto da rede, quando uma solicitação para se conectar à rede vem da internet, o servidor proxy determinará se a solicitação de conexão é segura. O servidor proxy é um endereço IP público diferente do resto da rede privada, ocultando o endereço IP da rede privada de agentes mal-intencionados na internet e adiciona uma camada de segurança.

**Tipos de servidores proxy:**

- **Servidor proxy direto:** Regula e restringe uma pessoa com acesso à internet.
- **Servidor proxy reverso:** Regula e restringe o acesso à internet a um servidor interno.
- **Servidor proxy de e-mail:** Filtra e-mails de spam verificando se o endereço do remetente foi falsificado, reduzindo o risco de ataques de

phishing que se fazem passar por pessoas conhecidas pela organização.

## Glossário de revisão

**Protocolo de resolução de endereço (ARP):** um protocolo de rede usado para determinar o endereço MAC do próximo roteador ou dispositivo no caminho
**Firewalls baseados em nuvem:** Firewalls de software que são hospedados pelo provedor de serviços em nuvem
**Zona de controle:** Uma sub-rede que protege a rede interna da zona não controlada
**Sistema de Nomes de Domínio (DNS):** Um protocolo de rede que converte nomes de domínio da Internet em endereços IP
**Encapsulamento:** Um processamento realizado por um serviço de VPN que protege seus dados envolvendo dados confidenciais em outros pacotes de dados
**Firewall:** Um dispositivo de segurança de rede que monitora o tráfego de ou para a sua rede
**Servidor proxy de encaminhamento:** Um servidor que regula e restringe o acesso de uma pessoa à Internet
**Hypertext Transfer Protocol (HTTP):** Um protocolo da camada do aplicativo que fornece um método de comunicação entre clientes e servidores de sites
**Protocolo de transferência de hipertexto seguro (HTTPS):** Um protocolo de rede que fornece um método seguro de comunicação entre clientes e servidores
**IEEE 802.11 (Wi-Fi):** Um conjunto de padrões que define a comunicação para LANs sem fio
**Protocolos de rede:** Um conjunto de regras usadas por dois ou mais dispositivos em uma rede para descrever a ordem de entrega dos dados e a estrutura dos dados
**Segmentação de rede:** Uma técnica de segurança que divide a rede em segmentos
**Filtragem de portas:** Uma função do firewall que bloqueia ou permite determinados números de porta para limitar a comunicação indesejada
**Servidor proxy:** Um servidor que atende às solicitações de seus clientes encaminhando-as para outros servidores
**Servidor proxy reverso:** Um servidor que regula e restringe o acesso da Internet a um servidor interno
**Protocolo de Transferência de Arquivos (FTP):** Um protocolo seguro usado para transferir arquivos de um dispositivo para outro em uma rede
**Secure Shell (SSH):** Um protocolo de segurança usado para criar um shell em um sistema remoto.
**Zona de segurança:** Segmentação da rede de uma empresa que protege a rede interna da Internet
**Protocolo de gerenciamento de rede simples (SNMP):** um protocolo de rede usado para monitorar e gerenciar dispositivos em uma rede

**Estatal:** Uma classe de firewall que mantém o controle das informações que passam por ele e filtra proativamente as ameaças.
**Sem estado:** Uma classe de firewall que opera com base em regras predefinidas e não mantém o controle das informações dos pacotes de dados
**Subredes:** A subdivisão de uma rede em grupos lógicos chamados sub-redes
**Protocolo TCP (Transmission Control Protocol, Protocolo de Controle de Transmissão):** Um protocolo de comunicação da Internet que permite que dois dispositivos formem uma conexão e transmitam dados
**Zona não controlada:** A parte da rede fora da organização
**Rede privada virtual (VPN):** Um serviço de segurança de rede que muda seu endereço IP público e mascara sua localização virtual para que você possa manter seus dados privados quando estiver usando uma rede pública como a Internet
**Wi-Fi Protected Access (WPA):** Um protocolo de segurança IP para dispositivos que se conectam à Internet

# *Módulo 3*

## Introdução às táticas de intrusão na rede de computadores

**Ataques comuns de rede:**

- **Malware**
- **Spoofing**
- **Interceptação de pacotes**
- **Inundação de pacotes**

**Ataques podem prejudicar uma organização ao:**

- **Vazar informações valiosas ou confidenciais**
- **Prejudicar a reputação**
- **Impactar a retenção de clientes**
- **Custar dinheiro e tempo**

## Proteger as redes de computadores contra ataques de negação de serviços (DOS)

**Ataque de negação de serviço (DoS):** Ataque que tem como alvo uma rede ou servidor e o inunda com tráfego de rede. O objetivo do ataque de negação de serviço é interromper as operações comerciais normais sobrecarregando a rede de uma organização.

Os agentes mal-intencionados mandam tantas informações para um dispositivo de rede que ele falha ou não consegue responder a usuários legítimos. Com a interrupção dos serviços, a empresa perde tempo e dinheiro.

A falha na rede também pode deixá-la vulnerável a outras ameaças e ataques à segurança.

**Ataque distribuído de negação de serviço (DDoS):** Tipo de ataque DoS que usa vários dispositivos ou servidores em locais diferentes para inundar a rede alvo com tráfego indesejado.

O uso de vários dispositivos aumenta a probabilidade de que a quantidade total de tráfego enviado sobrecarregue o servidor de destino.

**Handshake do protocolo TCP:** No protocolo TCP, uma conexão entre dispositivos e servidores é realizada antes que os arquivos sejam enviados, chamada de handshake.

O primeiro dispositivo envia um uma solicitação SYN (ou sincronize) para o servidor, em seguida, o servidor responde com um pacote SYN/ACK de volta para o dispositivo para confirmar o recebimento da solicitação e deixa uma porta aberta para a etapa final do handshake. Após o servidor receber o pacote ACK final do dispositivo, a conexão TCP é estabelecida.

**Ataque de inundação sincronizado (SYN):** Tipo de ataque DoS que simula a conexão TCP e inunda o servidor com pacotes SYN. Inunda o servidor com solicitações de pacotes SYN na primeira parte do handshake do TCP, se o número de solicitações SYN for maior do que o número de portas disponíveis no servidor, ele ficará sobrecarregado e incapaz de funcionar.

**Protocolo de Mensagens de Controle da Internet (ICMP):** Protocolo de internet usado por dispositivos para informar uns aos outros sobre erros de transmissão de dados pela rede.

**Ataque de inundação de IMCP:** Tipo de ataque DoS realizado por um invasor que envia repetidamente pacotes ICMP para um servidor de rede. Isso força o servidor a mandar um pacote ICMP, eventualmente consumindo toda a largura de banda para tráfego de entrada e saída e faz com que o servidor falhe.

**Ping of death:** Tipo de ataque DoS causado quando um hacker executa um ping em um sistema enviando a ele um pacote ICMP enorme com mais de 64 KB, o tamanho máximo para um pacote ICMP formado corretamente.

## Táticas de ataque e defesa da rede de computadores

**Interceptação de pacotes passiva:** Tipo de ataque em que os pacotes de dados são lidos em trânsito.

**Interceptação de pacotes ativa:** Tipo de ataque onde os pacotes de dados são manipulados em trânsito. Envolve o redirecionamento do pacote por injeção de protocolos de internet ou a alteração das informações do pacote.

**Spoofing de IP:** Ataque de rede realizado quando um invasor altera o ip de origem de um pacote de dados para se passar por um sistema autorizado e obter acesso a uma rede. Tipos de ataques de spoofing:

- **Ataques on-path:** Ataque em que o agente mal-intencionado se coloca no meio de uma conexão autorizada e intercepta ou altera os dados em trânsito.
- **Ataques de repetição:** Ataque de rede realizado quando um agente mal-intencionado intercepta um pacote de dados em trânsito e o atrasa ou repete em outro momento.
- **Ataques smurf:** Cominação de um ataque DDoS e um ataque de spoofing de IP. O atacante detecta o endereço IP de um usuário autorizado e o inunda com pacotes.

## Glossário de revisão

**Interceptação ativa de pacotes:** Um tipo de ataque em que os pacotes de dados são manipulados em trânsito
**Botnet:** Uma coleção de computadores infectados por malware que estão sob o controle de um único agente de ameaça, conhecido como "bot-herder"
**Ataque de negação de serviço (DoS):** Um ataque que visa uma rede ou servidor e o inunda com tráfego de rede
**Ataque distribuído de negação de serviço (DDoS):** Um tipo de ataque de negação de serviço que usa vários dispositivos ou servidores localizados em diferentes locais para inundar a rede-alvo com tráfego indesejado
**Protocolo de controle de transmissão/protocolo de Internet (TCP/IP):** um protocolo de Internet usado por dispositivos para informar uns aos outros sobre erros de transmissão de dados na rede
**Inundação do Protocolo de Mensagens de Controle da Internet (ICMP):** Um tipo de ataque DoS realizado por um invasor que envia repetidamente pacotes de solicitação ICMP a um servidor de rede
**IP spoofing (falsificação de IP):** Um ataque à rede realizado quando um invasor muda o IP de origem de um pacote de dados para se passar por um sistema autorizado e obter acesso a uma rede

**Ataque no caminho:** Um ataque em que um agente mal-intencionado se coloca no meio de uma conexão autorizada e intercepta ou altera os dados em trânsito
**Interceptação de pacotes:** A prática de capturar e inspecionar pacotes de dados em uma rede
**Interceptação passiva de pacotes:** Um tipo de ataque em que um agente mal-intencionado se conecta a um hub de rede e observa todo o tráfego na rede
**Ping of death (ping da morte):** Um tipo de ataque DoS causado quando um hacker faz ping em um sistema enviando a ele um pacote ICMP superdimensionado, com mais de 64 KB
**Ataque de repetição:** Um ataque de rede realizado quando um agente mal-intencionado intercepta um pacote de dados em trânsito e o atrasa ou o repete em outro momento
**Ataque Smurf:** Ataque de rede realizado quando um invasor descobre o endereço IP de um usuário autorizado e o inunda com pacotes ICMP
**Ataque de inundação de SYN (Synchronize):** Um tipo de ataque DoS que simula uma conexão TCP/IP e inunda um servidor com pacotes SYN

# *Módulo 4*

## Introdução ao fortalecimento da segurança

**Fortalecimento de segurança:** Processo de fortalecer um sistema para reduzir sua vulnerabilidade e superfície de ataque.

**Superfície de ataque:** Todas as vulnerabilidades potenciais que um agente de ameaças pode utilizar.

**Fortalecimento de segurança pode ser feito em:**

- **Hardware**
- **Sistemas operacionais**
- **Aplicativos**
- **Redes**
- **Banco de dados**

**Teste de penetração:** Ataque simulado que ajuda a identificar vulnerabilidades em sistemas, redes, sites, aplicativos e processamentos. Os pen testers documentam suas descobertas em um relatório.

## Fortalecimento do sistema operacional

**Sistema operacional:** Interface entre o hardware do computador e o usuário.

**Atualização de patch:** Atualização de software e sistema operacional que soluciona vulnerabilidades de segurança em um programa ou produto.

**Configuração básica (imagem básica):** Conjunto documentado de especificações em um sistema que é usado como base para futuras compilações, lançamentos e atualizações. Pode conter uma regra de firewall com uma lista de portas de rede permitidas e não permitidas.

**Outras medidas de segurança:** Descarte de hardware e software, excluir aplicativos de software não utilizados e a implementação de políticas de senhas fortes.

## Fortalecimento de rede

**Fortalecimento de segurança da rede:**

- **Filtragem de portas**
- **Privilégios de acesso à rede**
- **Criptografia**

**Tarefas regulares de fortalecimento:**

- **Manutenção de regras de firewall**
- **Análise de logs de rede**
- **Atualizações de patches**
- **Backups de servidores**

**Tarefas únicas de fortalecimento:**

- **Filtragem de portas em firewalls**
- **Privilégios de acesso à rede**
- **Criptografia para comunicação**

## Glossário de revisão

**Configuração da linha de base (imagem da linha de base):** Um conjunto documentado de especificações em um sistema que é usado como base para futuras compilações, liberações e atualizações

**Hardware:** Os componentes físicos de um computador
**Autenticação multifator (MFA):** Uma medida de segurança que exige que o usuário verifique sua identidade de duas ou mais maneiras para acessar um sistema ou uma rede
**Análise de registros de rede:** O processamento do exame dos registros de rede para identificar eventos de interesse.
**Sistema operacional (SO):** A interface entre o hardware do computador e o usuário
**Atualização de patch:** uma atualização de software e sistema operacional que aborda vulnerabilidades de segurança em um programa ou produto
**Teste de penetração (pen test):** Um ataque simulado que ajuda a identificar vulnerabilidades em sistemas, redes de computadores, sites, aplicativos e processos
**Fortalecimento da segurança:** O processamento de fortalecimento de um sistema para reduzir suas vulnerabilidades e superfície de ataque
**Gerenciamento de eventos e informações de segurança (SIEM):** Um aplicativo que coleta e analisa dados de registros para monitorar atividades críticas de uma organização
**Arquivo gravável em escala mundial:** Um arquivo que pode ser alterado por qualquer pessoa no mundo

**FINALIZADO!**