1.Segurança de protocolos de rede

1.1 Segurança de porta com DHCP snooping

Segurança de Porta com DHCP Snooping (***DHCP Snooping Port Security***) é uma medida de segurança utilizada em redes para proteger contra ataques de Rogue DHCP. Rogue DHCP é um dispositivo malicioso que se faz passar por um servidor DHCP legítimo, distribuindo endereços IP incorretos e potencialmente comprometendo a rede.

O DHCP Snooping Port Security ajuda a proteger a rede contra ataques de Rogue DHCP, garantindo que apenas servidores DHCP legítimos possam atribuir endereços IP aos dispositivos conectados à rede. O funcionamento do DHCP Snooping Port Security é baseado em dois conceitos principais: a identificação de portas confiáveis e não confiáveis e a construção de uma tabela DHCP snooping.

Passo a passo:

1.2 Identificação de portas confiáveis e não confiáveis

- **Portas confiáveis:** São as portas onde estão conectados os servidores DHCP legítimos da rede. O DHCP Snooping não age nessas portas e permite que os pacotes DHCP sejam transmitidos sem restrições.
- **Portas não confiáveis:** São as portas onde estão conectados os dispositivos finais, como computadores, smartphones e impressoras. Nessas portas, o DHCP Snooping estará ativo e monitorando os pacotes DHCP.

1.3 Construção da tabela DHCP snooping

- O switch, ao receber pacotes DHCP vindos das portas não confiáveis, verifica o endereço MAC do remetente e o endereço IP fornecido.
- O switch constrói uma tabela que associa o endereço MAC à porta não confiável por onde o pacote foi recebido, juntamente com o endereço IP atribuído ao dispositivo.

1.4 Verificação de pacotes DHCP subsequentes

- Quando o switch recebe pacotes DHCP em portas não confiáveis, ele verifica a tabela DHCP snooping para garantir que o endereço MAC não tenha sido alterado em relação à porta por onde foi recebido anteriormente.
- Caso haja uma mudança, o pacote é tratado como suspeito e bloqueado, impedindo que um Rogue DHCP envie endereços IP maliciosos.

2.Domain Hijacking

É um tipo de ataque cibernético no qual um invasor obtém o controle de um domínio de internet sem a autorização do proprietário legítimo. Esse tipo de ataque pode ser prejudicial para a reputação, segurança e funcionamento de um site, pois o invasor pode

redirecionar o tráfego para outros lugares, roubar informações dos usuários ou até mesmo desativar completamente o site.

O ataque:

- **Identificação do domínio alvo:** O invasor escolhe um domínio específico como alvo, normalmente procurando por domínios populares ou de alto valor que possam ser explorados para ganhos financeiros ou outros fins maliciosos.
- **Roubo das credenciais de acesso:** O invasor tenta obter acesso às credenciais de administrador do domínio, que normalmente incluem o login e senha da conta do registrante ou do provedor de hospedagem do domínio.
- **Acesso à conta do registrante ou provedor:** Uma vez que as credenciais são obtidas, o invasor acessa a conta do registrante ou provedor de hospedagem do domínio e altera as informações de registro, como os servidores de nomes (DNS) associados ao domínio.
- **Transferência ou modificação de DNS:** Com controle sobre as configurações de DNS, o invasor pode transferir o domínio para outro registrante ou alterar os registros DNS para redirecionar o tráfego para servidores controlados pelo invasor.
- **Redirecionamento de tráfego:** O invasor pode redirecionar o tráfego do domínio sequestrado para um site falso ou malicioso, onde os usuários podem ser enganados ou induzidos a divulgar informações sensíveis.
- **Extorsão ou chantagem:** Em alguns casos, o invasor pode tentar extorquir dinheiro do proprietário legítimo do domínio em troca da restauração do controle sobre o domínio.
- **Monitoramento e ocultação:** O invasor monitora a situação do domínio sequestrado e pode ocultar suas atividades para evitar a detecção e dificultar o processo de recuperação.

3.DNS poisoning

É um tipo de ataque cibernético no qual um invasor compromete os servidores DNS para fornecer informações de mapeamento de nomes de domínio falsas. O objetivo principal desse ataque é redirecionar os usuários para sites maliciosos, controlados pelo invasor, em vez dos sites legítimos que eles pretendem acessar.

O funcionamento do DNS Poisoning envolve a exploração de vulnerabilidades nos servidores DNS e pode ser realizado de diferentes maneiras:

- **Identificação do alvo:** O invasor escolhe um servidor DNS como alvo para o ataque. Isso pode ser um servidor específico de uma empresa, provedor de internet ou um servidor público usado por muitos usuários.
- **Interceptação do tráfego DNS:** O invasor intercepta o tráfego DNS entre o cliente (usuário) e o servidor DNS legítimo usando técnicas como o uso de redes Wi-Fi públicas não seguras ou a exploração de vulnerabilidades em roteadores e servidores.

- **Falsificação de respostas DNS:** Com o tráfego interceptado, o invasor responde às consultas DNS com informações falsas. Ele substitui os registros DNS legítimos com registros que apontam para endereços IP controlados pelo invasor.
- **Inserção de registros falsos no cache DNS:** Quando um servidor DNS responde a uma consulta, ele armazena temporariamente as informações em seu cache. O invasor pode inserir registros falsos no cache do servidor, de modo que futuras consultas para o mesmo domínio sejam redirecionadas para o site malicioso controlado pelo invasor.
- **Redirecionamento de tráfego:** Quando um usuário tenta acessar um site legítimo, o servidor DNS comprometido responde com informações falsas, redirecionando o tráfego para o site malicioso controlado pelo invasor.
- **Exploração do redirecionamento:** O usuário é redirecionado para o site malicioso, que pode ser uma cópia exata do site legítimo, mas com intenções maliciosas, como roubo de informações de login ou disseminação de malware.

4.DNS Security Extension (DNSSEC)

É uma extensão do protocolo DNS que visa aumentar a segurança e a integridade das respostas DNS, garantindo que os dados de mapeamento de nomes de domínio sejam autênticos e não tenham sido adulterados. **O DNSSEC fornece uma camada adicional de proteção contra ataques de envenenamento de cache DNS** (***DNS Poisoning***) e outras formas de manipulação maliciosa dos registros DNS.

O funcionamento do DNSSEC envolve a assinatura digital dos registros DNS, permitindo que os clientes verifiquem a autenticidade dos dados recebidos:

- **Assinatura digital dos registros DNS:** O servidor DNS responsável por um domínio assina digitalmente os registros DNS que contém informações sobre os endereços IP associados a esse domínio. A assinatura digital é gerada usando criptografia de chave pública e garante a autenticidade dos dados.
- **Cadeia de confiança:** O DNSSEC usa uma cadeia de confiança para verificar a autenticidade dos registros DNS. Os registros são assinados pelos servidores DNS de nível superior (como os servidores raiz) até o servidor DNS do domínio específico.
- **Armazenamento das chaves públicas:** As chaves públicas usadas para verificar as assinaturas digitais são armazenadas nos registros DNS em um tipo de registro chamado DNSKEY. Os clientes DNS podem acessar essas chaves públicas para verificar a autenticidade dos registros.
- **Resposta DNS com assinaturas:** Quando um cliente faz uma consulta DNS para um domínio protegido pelo DNSSEC, o servidor DNS responde com os registros DNS assinados digitalmente, juntamente com as chaves públicas necessárias para verificar as assinaturas.
- **Verificação das assinaturas:** O cliente DNS, ao receber a resposta, verifica as assinaturas digitais usando as chaves públicas contidas nos registros DNSKEY. Se as assinaturas forem válidas, o cliente pode ter confiança de que os dados de mapeamento de nomes de domínio são autênticos e não foram adulterados.

- **Indicação de suporte DNSSEC:** Os domínios protegidos pelo DNSSEC incluem um registro especial chamado DS (Delegation Signer) no registro de zona pai (por exemplo, os servidores raiz), indicando que o domínio usa DNSSEC.

5.LDAP Secure (LDAPS)

É uma extensão do protocolo Lightweight Directory Access Protocol (*LDAP*) que adiciona uma camada de segurança à comunicação entre os clientes e os servidores LDAP. O LDAPS utiliza criptografia para proteger os dados durante a transmissão, garantindo que as informações de autenticação e diretório fiquem protegidas contra acesso não autorizado e ataques de interceptação.

O funcionamento do LDAPS envolve a utilização do protocolo SSL/TLS para estabelecer uma conexão segura entre o cliente e o servidor LDAP. Veja como o LDAPS funciona:

- **Configuração do servidor LDAP:** O servidor LDAP é configurado para suportar a comunicação segura através do LDAPS. Para isso, ele precisa ter um certificado SSL/TLS instalado e configurado corretamente.
- **Solicitação de conexão segura:** O cliente LDAP que deseja se comunicar com o servidor envia uma solicitação para estabelecer uma conexão segura usando o LDAPS. Essa solicitação é feita através da porta TCP 636, que é a porta padrão utilizada para o LDAPS.
- **Estabelecimento da conexão segura:** Quando o servidor recebe a solicitação de conexão segura, ele responde e inicia o processo de estabelecimento de uma conexão criptografada. Isso é feito utilizando o protocolo SSL/TLS para negociar a segurança da comunicação.
- **Verificação do certificado:** Durante o processo de estabelecimento da conexão segura, o cliente verifica o certificado do servidor. Essa verificação é importante para garantir que o servidor seja legítimo e que o certificado tenha sido emitido por uma autoridade de certificação confiável.
- **Autenticação do cliente:** Se necessário, o cliente pode se autenticar junto ao servidor LDAP usando credenciais, como nome de usuário e senha. Essa autenticação também é realizada de forma segura através da conexão LDAPS criptografada.
- **Troca de dados criptografada:** Com a conexão segura estabelecida e as autenticações concluídas, o cliente e o servidor podem trocar dados de forma criptografada. Isso protege as informações transmitidas contra interceptação e garante a confidencialidade dos dados.

O LDAPS é amplamente utilizado em ambientes corporativos e de rede, especialmente em cenários onde a segurança da autenticação e do diretório é uma preocupação importante. A utilização do LDAPS garante que as informações do diretório, como senhas e informações de usuário, permaneçam protegidas durante a transmissão e ajuda a prevenir ataques de espionagem ou interceptação.

6.Network Time Protocol (NTP)

É um protocolo de rede usado para sincronizar os relógios de dispositivos em uma rede. Ele permite que os dispositivos obtenham a hora exata de servidores NTP, garantindo que todos os dispositivos na rede tenham o mesmo tempo de referência. Isso é essencial para a operação correta de sistemas distribuídos, aplicações em rede e atividades que dependem de marcações de tempo precisas.

Funcionamento:

- **Seleção de servidores NTP:** Os dispositivos configurados para usar o NTP selecionam um ou mais servidores NTP como referência de tempo. Esses servidores são responsáveis por fornecer a hora exata.
- **Sincronização inicial:** Quando um dispositivo é inicializado ou entra na rede, ele inicia uma solicitação para os servidores NTP selecionados para obter o tempo atual. O dispositivo pode calcular o atraso de rede e o desvio de tempo em relação aos servidores NTP para sincronizar seu relógio.
- **Atualização periódica:** O dispositivo continuará a fazer solicitações periódicas aos servidores NTP para ajustar o relógio e garantir que ele permaneça sincronizado com o tempo de referência.

7.Network Time Security (NTS)

É uma extensão do NTP que foi projetada para adicionar uma camada de segurança à sincronização de tempo em uma rede. O NTS usa criptografia para proteger as transações NTP, evitando ataques de spoofing, interceptação e manipulação de dados de tempo.

O NTS é especialmente importante em ambientes onde a precisão do tempo é crítica, como em sistemas financeiros, comunicações de rede sensíveis e infraestruturas críticas.

Funcionamento:

- **Estabelecimento de segurança:** Antes de iniciar a sincronização de tempo, o cliente NTP e o servidor NTP negociam uma conexão segura usando o protocolo Transport Layer Security (TLS), permitindo autenticação mútua e criptografia dos dados de tempo trocados.
- **Autenticação do servidor:** O servidor NTP apresenta um certificado digital durante o processo de negociação TLS para provar sua identidade. O cliente NTP verifica a autenticidade do certificado para garantir que está se comunicando com um servidor legítimo.
- **Proteção contra ataques de spoofing:** A troca de dados de tempo entre o cliente e o servidor é criptografada, o que impede que um invasor falsifique informações de tempo e realize ataques de spoofing.
- **Integridade dos dados de tempo:** A criptografia também garante a integridade dos dados de tempo, impedindo que um invasor manipule os dados durante a transmissão.
- **Sincronização segura:** Com a conexão segura estabelecida e a autenticação concluída, o cliente NTP pode sincronizar seu relógio com o servidor NTP de forma segura, garantindo que o tempo de referência seja preciso e confiável.

8.Simple Network Management Protocol (SNMP)

É um protocolo de gerenciamento de rede amplamente utilizado para monitorar e gerenciar dispositivos em uma rede. Ele permite que administradores obtenham informações e configurem dispositivos de rede, facilitando o diagnóstico de problemas, monitoramento de desempenho e gerenciamento eficiente de recursos.

Funcionamento:

- **Agentes SNMP:** Os dispositivos de rede que suportam SNMP, como roteadores, switches e servidores, são equipados com um componente chamado "agente SNMP". Esse agente é responsável por coletar informações sobre o dispositivo e disponibilizá-las para serem acessadas pelos gerenciadores SNMP.
- **Gerenciadores SNMP:** Os gerenciadores são os sistemas de monitoramento ou estações de gerenciamento que solicitam informações aos agentes SNMP e realizam ações de gerenciamento nos dispositivos de rede. Eles podem ser computadores, servidores ou ferramentas específicas de gerenciamento.
- **Management Information Base (MIB):** A MIB é uma estrutura de dados hierárquica que define as informações disponíveis para monitoramento e gerenciamento em um dispositivo. Cada dispositivo SNMP possui uma MIB que contém variáveis específicas que podem ser acessadas pelos gerenciadores.
- **Operações SNMP:** Os gerenciadores SNMP podem executar as seguintes quatro operações principais:
  a. Get: Solicita informações específicas do agente SNMP.
  b. Set: Configuração de variáveis no agente SNMP para alterar configurações.
  c. Trap: Notificação automática enviada pelos agentes SNMP para os gerenciadores quando ocorre um evento significativo.
  d. GetNext: Obtém a próxima variável disponível na MIB do agente.

SNMPv2 é uma atualização do SNMP original (SNMPv1) que adiciona algumas melhorias, mas ainda mantém algumas limitações de segurança:

- **Novas operações:** SNMPv2 adicionou novas operações como GetBulk e Inform, tornando mais eficiente a recuperação de grandes quantidades de informações e melhorando a notificação entre agentes e gerenciadores.
- **Tabelas de MIB:** SNMPv2 introduziu a capacidade de acessar e manipular tabelas de MIB, facilitando o gerenciamento de múltiplos itens de dados de uma só vez.
- **Community Strings:** Assim como SNMPv1, SNMPv2 também utiliza "community strings" para autenticação simples, o que representa uma limitação de segurança.

SNMPv3 é a versão mais segura do protocolo, introduzindo recursos avançados de autenticação e criptografia:

- **Autenticação e criptografia:** SNMPv3 suporta autenticação forte usando algoritmos como MD5 e SHA, além de criptografia de dados usando algoritmos como DES e AES.

Isso garante que as informações sejam transmitidas de forma segura entre agentes e gerenciadores.

- **Modelos de segurança:** SNMPv3 apresenta modelos de segurança que definem como a autenticação e a criptografia são realizadas. São três modelos: sem segurança (noAuthNoPriv), autenticação (authNoPriv) e autenticação e privacidade (authPriv).
- **Usuários e grupos:** SNMPv3 utiliza autenticação baseada em usuário e grupo para controlar o acesso aos dispositivos gerenciados. Isso permite uma gestão mais granular dos privilégios de acesso.

9.Secure Sockets Layer (SSL)

Secure Sockets Layer (***SSL***), que foi substituído pelo ***Transport Layer Security*** (***TLS***), é um protocolo de segurança criptográfica usado para estabelecer uma conexão segura entre um cliente (como um navegador da web) e um servidor. Seu objetivo principal é garantir que os dados transmitidos durante a comunicação sejam criptografados e protegidos contra interceptação por terceiros mal-intencionados.

10.Transport Layer Security (TLS)

O TLS é um protocolo de segurança criptográfica usado para proteger as comunicações na internet. Ele é uma evolução do antigo SSL e é amplamente utilizado para estabelecer conexões seguras entre clientes e servidores, garantindo que os dados transmitidos sejam confidenciais e protegidos contra interceptação e manipulação por terceiros mal-intencionados.

O TLS é amplamente utilizado em diversas aplicações e serviços na internet, incluindo navegação segura em sites (HTTPS), transações de comércio eletrônico, serviços de e-mail criptografados (SMTPS, POP3S, IMAPS), comunicações de mensagens instantâneas, transferências de arquivos seguras (SFTP e FTPS), acesso remoto seguro (SSH), serviços de VPN (Virtual Private Network) e em qualquer outra situação em que a confidencialidade, autenticação e integridade dos dados sejam fundamentais para proteger a privacidade e a segurança dos usuários.

Funcionamento:

- **TLS 1.1:**
  Lançado em 2006 como uma atualização do TLS 1.0.
  Oferece suporte a suites de criptografia mais seguras, como AES (Advanced Encryption Standard) e SHA-256 (Secure Hash Algorithm 256-bit).
  Corrige algumas vulnerabilidades de segurança encontradas no TLS 1.0.
  Ainda suporta algoritmos criptográficos mais antigos, que são considerados menos seguros em comparação com as versões mais recentes.
- **TLS 1.2:**
  Lançado em 2008, representa uma atualização significativa em relação ao TLS 1.1.
  Inclui novos algoritmos de criptografia, como AES-GCM (Galois/Counter Mode) e ECDHE (Elliptic Curve Diffie-Hellman Ephemeral).

Melhora a segurança em relação a ataques conhecidos, como BEAST (Browser Exploit Against SSL/TLS) e CRIME (Compression Ratio Info-leak Made Easy).
Remove suporte para algoritmos criptográficos mais antigos e inseguros, tornando-o mais seguro que o TLS 1.1.

- **TLS 1.3:**
  Lançado em 2018, é a versão mais recente e avançada do protocolo TLS.
  Apresenta melhorias significativas em termos de velocidade, eficiência e segurança.
  Remove suporte para versões antigas e inseguras de algoritmos criptográficos, focando em algoritmos mais modernos e seguros.
  Reduz o número de etapas do Handshake, acelerando a negociação da conexão segura e diminuindo o tempo de latência.
  Introduz suporte para criptografia de curva elíptica por padrão, melhorando a segurança dos algoritmos de chave pública.

11.SSH FTP (SFTP)

- **Conexão segura:** O SFTP utiliza o protocolo SSH (Secure Shell), na porta 22 TCP, para estabelecer uma conexão segura entre o cliente e o servidor. O SSH fornece autenticação e criptografia, garantindo a segurança da comunicação.
- **Autenticação:** Antes de iniciar a transferência de arquivos, o cliente é autenticado no servidor SSH usando chaves públicas ou senhas, garantindo que apenas usuários autorizados tenham acesso ao servidor.
- **Criptografia da transferência:** Durante a transferência de arquivos, todos os dados são criptografados, protegendo os dados sensíveis contra interceptação e espionagem.
- **Integração com o sistema de arquivos:** O SFTP permite ao cliente navegar no sistema de arquivos remoto, realizar operações de listagem, upload e download de arquivos, além de executar operações de gerenciamento de diretórios.

12.FTP Over SSL (FTPS)

- **Início da conexão:** O FTPS utiliza o protocolo FTP como base para a transferência de arquivos, mas adiciona uma camada de segurança através do uso de SSL/TLS.
- **Estabelecimento da conexão segura:** Antes da transferência de arquivos, o cliente e o servidor negociam uma conexão segura através do SSL/TLS. Essa negociação envolve a troca de certificados digitais e a definição dos parâmetros de criptografia.
- **Autenticação:** O cliente é autenticado no servidor FTPS usando certificados digitais ou senhas, garantindo a identidade do cliente e protegendo contra acessos não autorizados.
- **Criptografia da transferência:** Durante a transferência de arquivos, todos os dados são criptografados usando o SSL/TLS, garantindo a confidencialidade dos dados e protegendo contra interceptação.
- **Modos de transferência:** O FTPS suporta dois modos de transferência: o modo explícito (explicit FTPS) e o modo implícito (implicit FTPS). No modo explícito, a segurança é negociada pelo cliente e pelo servidor após a conexão inicial. No modo implícito, a segurança é estabelecida logo no início da conexão.

- **Portas:** Depende do modo de conexão. O FTPS explícito usa a porta TCP 21 para iniciar uma conexão segura. O FTPS implícito usa a porta TCP 990 para iniciar uma conexão segura diretamente.

13.Secure SMTP (SMTPS)

- O SMTPS é uma versão segura do protocolo Simple Mail Transfer Protocol (SMTP) que utiliza criptografia SSL/TLS para proteger a comunicação entre o cliente de e-mail e o servidor de envio de e-mails SMTP.
- Utiliza a porta TCP 465 para estabelecer a conexão segura entre o cliente e o servidor.
- O SMTPS é amplamente utilizado para enviar e-mails de forma segura, garantindo que as informações de login e os dados do e-mail sejam criptografados e protegidos contra interceptação.

14.Secure POP (POP3S)

- O POP3S é uma versão segura do protocolo Post Office Protocol version 3 (POP3) que utiliza criptografia SSL/TLS para proteger a comunicação entre o cliente de e-mail e o servidor de recebimento de e-mails (POP3).
- Utiliza a porta TCP 995 para estabelecer a conexão segura entre o cliente e o servidor.
- O POP3S permite que o cliente baixe e-mails de forma segura do servidor, garantindo que os dados do e-mail e as informações de autenticação sejam confidenciais e protegidos.

15.Secure IMAP (IMAPS)

- O IMAPS é uma versão segura do protocolo Internet Message Access Protocol (IMAP) que utiliza criptografia SSL/TLS para proteger a comunicação entre o cliente de e-mail e o servidor de correio (IMAP).
- Utiliza a porta TCP 993 para estabelecer a conexão segura entre o cliente e o servidor.
- O IMAPS permite que o cliente acesse e-mails armazenados no servidor de forma segura, garantindo que os dados do e-mail e as credenciais de acesso sejam criptografados e seguros.

16.Secure/Multipurpose Internet Mail Extensions (S/MIME)

- S/MIME é um padrão de criptografia e assinatura digital utilizado para garantir a segurança e autenticidade dos e-mails.
- Permite que os usuários criptografem e assinem digitalmente seus e-mails, garantindo a confidencialidade das informações e a verificação da autenticidade do remetente.
- Os e-mails criptografados com S/MIME só podem ser lidos pelo destinatário com a chave privada correspondente à chave pública usada para criptografar o e-mail, garantindo a privacidade das comunicações.
- A assinatura digital permite que o destinatário verifique a integridade do e-mail e a autenticidade do remetente, garantindo que o e-mail não tenha sido alterado e que o remetente seja quem afirma ser.

17.Transport Layer Security VPN

Transport Layer Security Virtual Private Network (***TLS VPN***) é um tipo de VPN que utiliza o protocolo TLS (Transport Layer Security) para criar uma conexão segura entre dispositivos e redes através da internet. A TLS VPN oferece criptografia e autenticação para garantir a confidencialidade, integridade e autenticidade dos dados transmitidos durante a comunicação.

Funcionamento:

- **Handshake TLS:** O processo de estabelecimento da conexão começa com o Handshake TLS, onde o cliente e o servidor negociam os parâmetros de segurança, autenticação e criptografia a serem utilizados na comunicação.
- **Autenticação:** Durante o Handshake, os dispositivos envolvidos na conexão TLS VPN se autenticam mutuamente por meio de certificados digitais, senhas ou outras formas de autenticação, garantindo que apenas dispositivos autorizados tenham acesso à VPN.
- **Criptografia:** Após o Handshake, a comunicação entre os dispositivos é criptografada usando algoritmos de criptografia seguros, como AES (Advanced Encryption Standard) ou TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, garantindo que os dados transmitidos sejam confidenciais e protegidos contra interceptação.
- **VPN tunneling:** A TLS VPN estabelece um túnel seguro entre os dispositivos, encapsulando os pacotes de dados em uma camada adicional de cabeçalho, protegendo-os de ameaças externas durante a transmissão.
- **Roteamento seguro:** Os dispositivos configurados para a TLS VPN roteiam seus pacotes através do túnel seguro, permitindo que a comunicação ocorra como se estivessem diretamente conectados em uma rede local, mesmo estando fisicamente em diferentes locais geográficos.
- **Acesso remoto e conexões site-to-site:** A TLS VPN pode ser utilizada para oferecer acesso remoto seguro a uma rede corporativa, permitindo que funcionários acessem recursos internos de forma segura de qualquer local. Além disso, a TLS VPN também pode ser configurada para criar conexões seguras entre diferentes filiais ou escritórios de uma mesma organização, conhecidas como conexões site-to-site.

18.Internet Protocol Security (IPSec)

É um conjunto de protocolos de segurança utilizado para proteger as comunicações de rede através da internet ou de redes privadas. Ele oferece autenticação, integridade e confidencialidade dos dados transmitidos. O IPSec é composto por dois principais protocolos: ***Authentication Header*** (***AH***) e ***Encapsulation Security Payload*** (***ESP***).

19.Authentication Header (AH)

- O AH é um dos protocolos do IPSec que fornece autenticação e integridade dos dados transmitidos.

- Ele adiciona um cabeçalho ao pacote IP, contendo um valor de hash (MAC - Message Authentication Code) calculado a partir dos dados originais e de uma chave secreta compartilhada entre os dispositivos envolvidos na comunicação.
- A verificação do valor de hash no cabeçalho AH no destino permite ao receptor confirmar que os dados não foram modificados e que o pacote é autêntico, ou seja, originado do remetente esperado.

20.Encapsulation Security Payload (ESP)

- O ESP é outro protocolo do IPSec que fornece confidencialidade, integridade e autenticação dos dados.
- Ele encapsula o pacote IP original e criptografa seus dados, protegendo-os contra interceptação e leitura por terceiros não autorizados.
- O ESP também adiciona um valor de hash para verificar a integridade dos dados e garantir que não foram alterados durante a transmissão.
- O ESP pode fornecer autenticação usando autenticação de chave pública (digital) ou autenticação pré-compartilhada, garantindo que o pacote seja de origem legítima.

Funcionamento:

- O IPSec é frequentemente implementado em duas formas: modo de túnel e modo de transporte.
- No modo de túnel, todo o pacote IP original é encapsulado em um novo pacote IP com os cabeçalhos AH e/ou ESP adicionados, é comumente utilizado em conexões site-to-site VPN, protegendo o tráfego entre redes remotas.
- No modo de transporte, apenas o payload dos pacotes IP é encapsulado com os cabeçalhos AH e/ou ESP, deixando os cabeçalhos originais intactos. Isso é mais utilizado para conexões ponto-a-ponto, como acesso remoto VPN.
- O IPSec é transparente para as aplicações e não requer modificações no código das mesmas, tornando-o uma solução de segurança de rede amplamente utilizada e eficiente para garantir a proteção das comunicações de rede contra ameaças de interceptação, alteração e falsificação de dados.

21.Secure Shell (SSH)

O SSH é um protocolo de rede utilizado para estabelecer conexões seguras e criptografadas entre dispositivos através de uma rede não confiável, como a internet. Ele oferece autenticação e criptografia para proteger as comunicações, permitindo que os usuários realizem operações remotas de forma segura em servidores e dispositivos.

Funcionamento:

- **Conexão segura:** O SSH utiliza criptografia para estabelecer uma conexão segura entre o cliente e o servidor, evitando que terceiros interceptem ou leiam as informações transmitidas durante a comunicação.
- **Autenticação:** Antes de estabelecer a conexão, o cliente e o servidor precisam se autenticar mutuamente. O SSH suporta diferentes métodos de autenticação, como

autenticação por senha, autenticação por chave pública ou autenticação por chave de host. Esses métodos garantem que apenas usuários autorizados tenham acesso ao servidor.

- **Chaves criptográficas:** A autenticação por chave pública utiliza pares de chaves criptográficas, uma pública e uma privada. O cliente possui a chave privada e o servidor possui a chave pública correspondente. Quando o cliente se conecta ao servidor, ele prova sua identidade ao assinar um desafio enviado pelo servidor com sua chave privada. O servidor verifica a assinatura usando a chave pública do cliente.
- **Criptografia de dados:** Após a autenticação, a comunicação entre o cliente e o servidor é criptografada. Ou seja, qualquer dado transmitido entre os dois é codificado de tal forma que apenas o cliente e o servidor possam decifrá-lo. Dessa forma, mesmo que alguém intercepte os dados, não conseguirá compreendê-los sem a chave de descriptografia.
- **Operações remotas:** Uma vez estabelecida a conexão segura, os usuários podem executar operações remotas no servidor, como acesso ao sistema de arquivos, execução de comandos e transferência de arquivos.
- **Porta padrão:** A porta padrão usada pelo SSH é a TCP 22. Isso significa que, por padrão, o servidor SSH escuta conexões na porta 22. Entretanto, é possível configurar o servidor para escutar em portas diferentes, o que pode ser útil para aumentar a segurança e evitar ataques automatizados.