

Módulo 12 - Aulas 1 e 2

Módulo 12: Resposta a incidentes e protocolos seguros

Aula 1: Monitoramento de redes e redes sem fio

Objetivos

- ☒ Identificar e explicar os principais conceitos de monitoramento de redes.
- ☒ Demonstrar o uso de comandos de manipulação de arquivos.
- ☒ Explorar os conceitos de segurança em redes sem fio.

Conceitos

- ☒ Security Information and Event Management (SIEM) e User and Entity Behavior Analytics (UEBA).
- ☒ Wireless Access Point (WAP).
- ☒ Rogue Access Point e Evil Twin.

Introdução

Bem-vindos à aula de Monitoramento de redes e redes sem fio! Hoje, vamos mergulhar no emocionante mundo da proteção e análise de redes, explorando ferramentas e técnicas fundamentais para garantir a integridade e segurança dos sistemas. Durante nossa jornada, abordaremos conceitos essenciais como Network Monitor e Logs, que nos permitirão compreender a essência das ameaças e eventos que ocorrem em ambientes de rede.

Além disso, exploraremos o fascinante campo do Security Information and Event Management (SIEM) e o processo de Log Collection, que utiliza métodos como Agent-based, Collector e Sensor para garantir que informações valiosas sejam capturadas e analisadas adequadamente. Também aprenderemos sobre Log Aggregation e como esse processo contribui para a eficiência na detecção de incidentes e anomalias. Também desvendaremos os segredos das redes sem fio, discutindo tópicos como Wireless Access Point, SSID, WPA2, WPA3 e outras medidas de segurança, como IEEE 802.1X Authentication, Rogue Access Points e Evil Twins.

Monitoramento de redes

Network Monitor

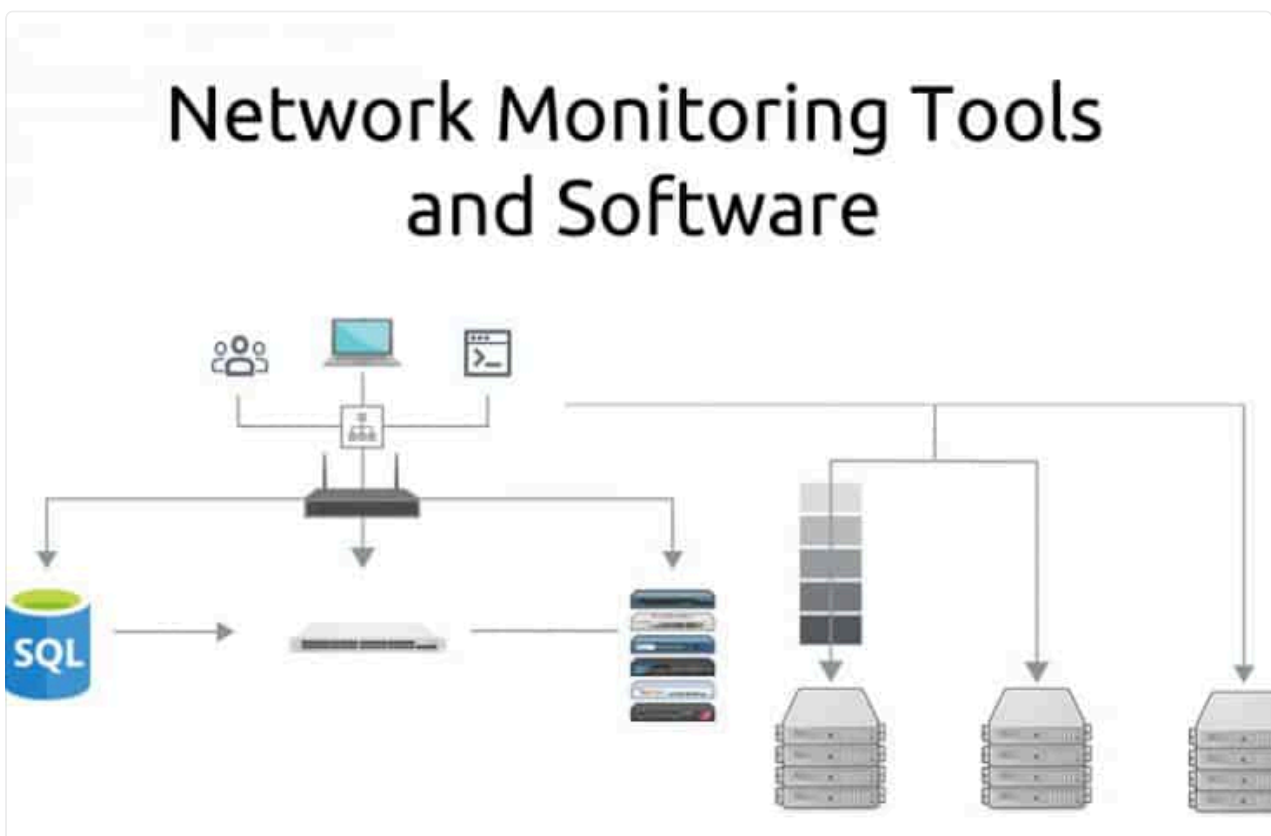
O Network Monitor, também conhecido como analisador de rede ou sniffer, é uma ferramenta utilizada para monitorar e analisar o tráfego de rede. Ele permite capturar pacotes de dados que circulam pela rede, tornando possível examinar em detalhes as comunicações entre dispositivos e os diferentes protocolos que estão sendo utilizados. O funcionamento do Network Monitor ocorre nas seguintes etapas:

- **Captura de pacotes:** O Network Monitor captura os pacotes de dados que trafegam na rede. Isso é realizado através de interfaces de rede dedicadas, como placas de rede ou adaptadores, que permitem ao analisador acessar o fluxo de informações que passa por elas.
- **Análise de pacotes:** Após a captura, os pacotes são analisados para extrair informações importantes. O Network Monitor pode decodificar os dados presentes nos pacotes, exibindo detalhes dos cabeçalhos dos protocolos utilizados, endereços IP, portas, informações de controle e carga útil dos pacotes.
- **Filtragem de dados:** Para tornar a análise mais eficiente, o Network Monitor permite aplicar filtros para selecionar pacotes específicos para visualização. Isso é especialmente útil em redes movimentadas, onde a quantidade de dados pode ser significativa. Filtros podem ser baseados em endereços IP, portas, protocolos, entre outros critérios.

-

Visualização e análise de tráfego: Os pacotes capturados são apresentados ao usuário em uma interface gráfica ou em formato de lista. O Network Monitor possibilita observar o tráfego em tempo real ou examinar capturas prévias. Essa visualização detalhada é fundamental para identificar padrões, detectar problemas e analisar o comportamento da rede.

- **Diagnóstico de problemas:** O Network Monitor é amplamente utilizado por administradores de rede e profissionais de segurança para diagnosticar problemas e investigar atividades suspeitas. Com ele, é possível identificar tráfego não autorizado, anomalias de rede, gargalos de desempenho e outros problemas que podem afetar a operação da rede.
- **Registro e exportação de dados:** O Network Monitor permite gravar as capturas em arquivos de registro para análises futuras. Além disso, os dados capturados podem ser exportados em diferentes formatos para compartilhamento com outros profissionais ou para análises posteriores em outras ferramentas.



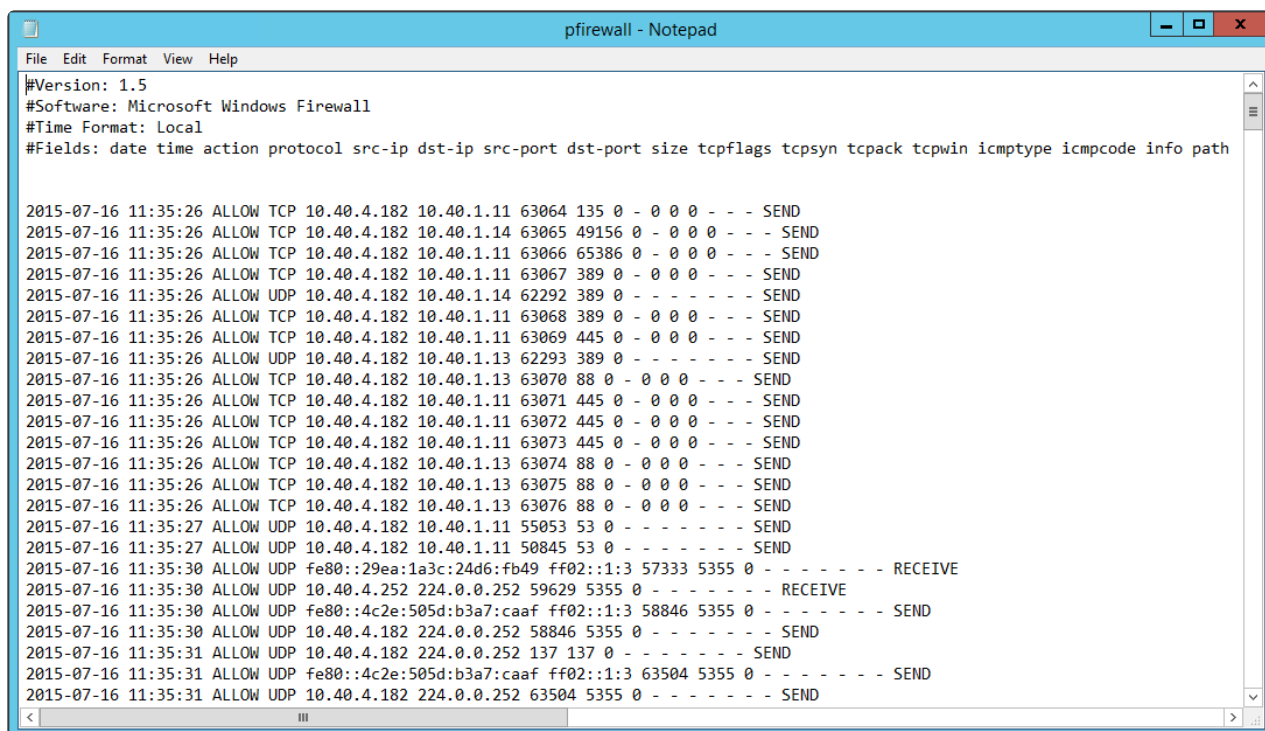
Network Monitor.

Logs

Logs são registros detalhados de eventos, atividades ou mensagens geradas por sistemas, aplicativos ou dispositivos. Eles têm o propósito de registrar informações

relevantes para análise, monitoramento, solução de problemas, auditoria e segurança. O funcionamento dos logs geralmente envolve os seguintes aspectos:

- **Geração de Logs:** Os sistemas e aplicativos geram logs automaticamente conforme eventos ocorrem. Isso pode incluir ações do usuário, erros, atividades de rede, processos iniciados ou encerrados, entre outros eventos importantes.
- **Formato e estrutura:** Os logs geralmente possuem um formato estruturado, com informações específicas sobre cada evento registrado. Essas informações podem incluir data e hora, nível de severidade (como informação, aviso ou erro), origem do evento, descrição do evento e outros detalhes relevantes.
- **Armazenamento e gerenciamento:** Os logs são armazenados em arquivos ou em um sistema centralizado de gerenciamento de logs. É importante que os logs sejam protegidos e devidamente gerenciados, especialmente para fins de auditoria e conformidade.
- **Análise e monitoramento:** Os logs são analisados regularmente para identificar possíveis problemas, anomalias ou tendências. O monitoramento contínuo dos logs ajuda a detectar atividades suspeitas ou comportamentos incomuns na rede ou nos sistemas.
- **Ferramentas de análise:** Existem ferramentas específicas, como SIEM (Security Information and Event Management) e sistemas de gerenciamento de logs, que auxiliam na análise, agregação e correlação dos logs de diferentes fontes. Essas ferramentas ajudam a simplificar o processo de identificação de eventos relevantes e a resposta a incidentes.



```
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmp type icmpcode info path

2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63064 135 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.14 63065 49156 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63066 65386 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63067 389 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW UDP 10.40.4.182 10.40.1.14 62292 389 0 - - - - - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63068 389 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63069 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW UDP 10.40.4.182 10.40.1.13 62293 389 0 - - - - - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63070 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63071 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63072 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.11 63073 445 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63074 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63075 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:26 ALLOW TCP 10.40.4.182 10.40.1.13 63076 88 0 - 0 0 0 - - - SEND
2015-07-16 11:35:27 ALLOW UDP 10.40.4.182 10.40.1.11 55053 53 0 - - - - - - - SEND
2015-07-16 11:35:27 ALLOW UDP 10.40.4.182 10.40.1.11 50845 53 0 - - - - - - - SEND
2015-07-16 11:35:30 ALLOW UDP fe80::29ea:1a3c:24d6:fb49 ff02::1:3 57333 5355 0 - - - - - - - RECEIVE
2015-07-16 11:35:30 ALLOW UDP 10.40.4.252 224.0.0.252 59629 5355 0 - - - - - - - RECEIVE
2015-07-16 11:35:30 ALLOW UDP fe80::4c2e:505d:b3a7:caaf ff02::1:3 58846 5355 0 - - - - - - - SEND
2015-07-16 11:35:30 ALLOW UDP 10.40.4.182 224.0.0.252 58846 5355 0 - - - - - - - SEND
2015-07-16 11:35:31 ALLOW UDP 10.40.4.182 224.0.0.252 137 137 0 - - - - - - - SEND
2015-07-16 11:35:31 ALLOW UDP fe80::4c2e:505d:b3a7:caaf ff02::1:3 63504 5355 0 - - - - - - - SEND
2015-07-16 11:35:31 ALLOW UDP 10.40.4.182 224.0.0.252 63504 5355 0 - - - - - - - SEND
```

Windows Firewall Logs.

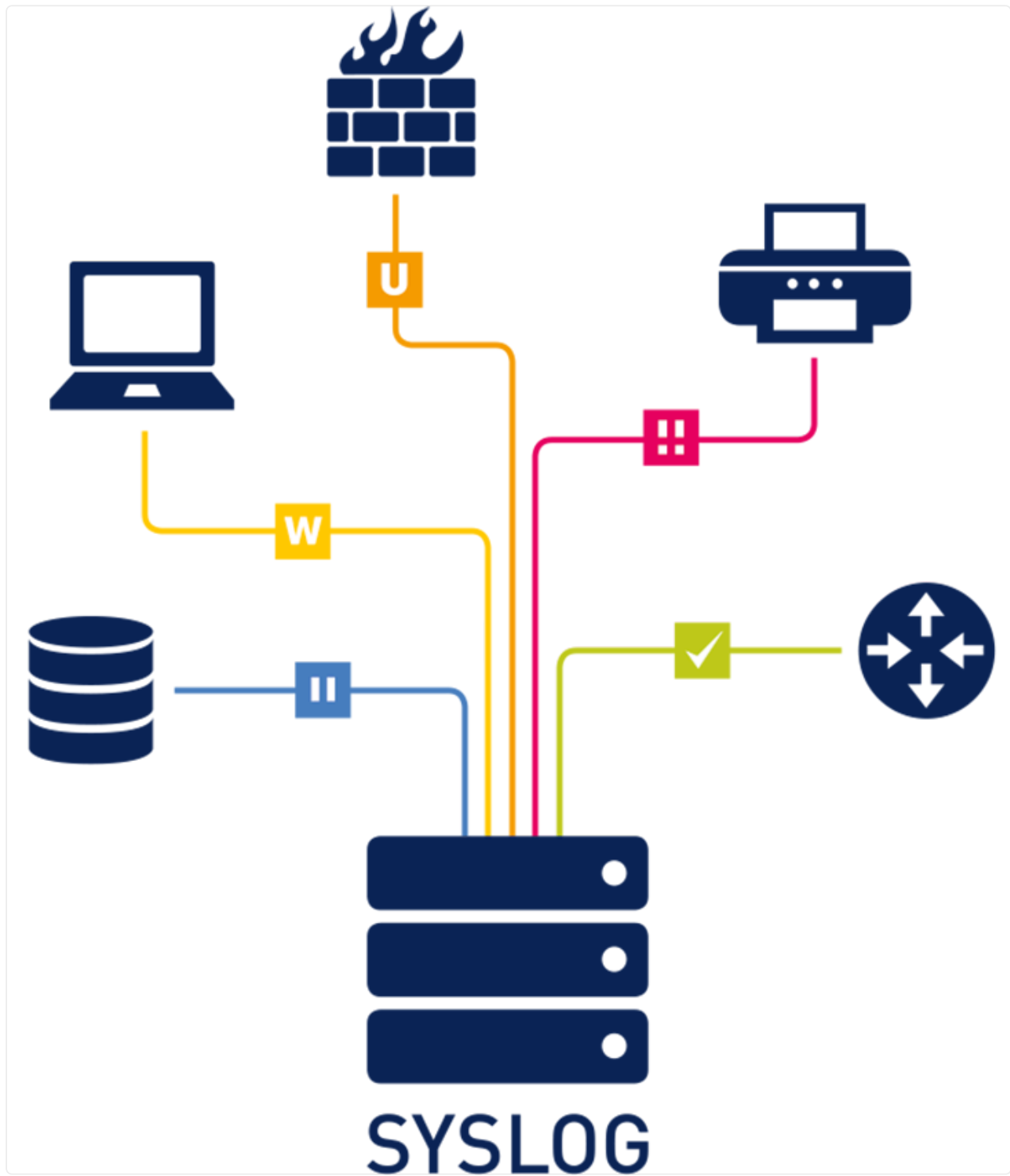
SysLog

SysLog é um protocolo padronizado amplamente utilizado para a geração, envio e recebimento de mensagens de registro de eventos em sistemas de computadores e dispositivos de rede. Criado originalmente em ambientes Unix-like, o SysLog tornou-se um dos métodos mais comuns para coletar informações sobre atividades e eventos relevantes que ocorrem nos sistemas e aplicativos.

O funcionamento do SysLog envolve a geração de mensagens de eventos pelos sistemas e sua posterior transmissão para um servidor SysLog centralizado ou outros dispositivos que estejam escutando em uma determinada porta. As mensagens SysLog são categorizadas em "facilities" (instalações) e "severidades", permitindo classificar a origem do evento e sua gravidade. O servidor SysLog centralizado consolida as mensagens de vários dispositivos em um único local, facilitando a análise, monitoramento e resposta a incidentes em toda a infraestrutura.

Além de ser uma ferramenta essencial para a manutenção e solução de problemas, o SysLog desempenha um papel fundamental na segurança da rede e dos sistemas, pois permite identificar atividades suspeitas, rastrear acessos não autorizados, detectar falhas de segurança e analisar tendências de eventos. Ele é

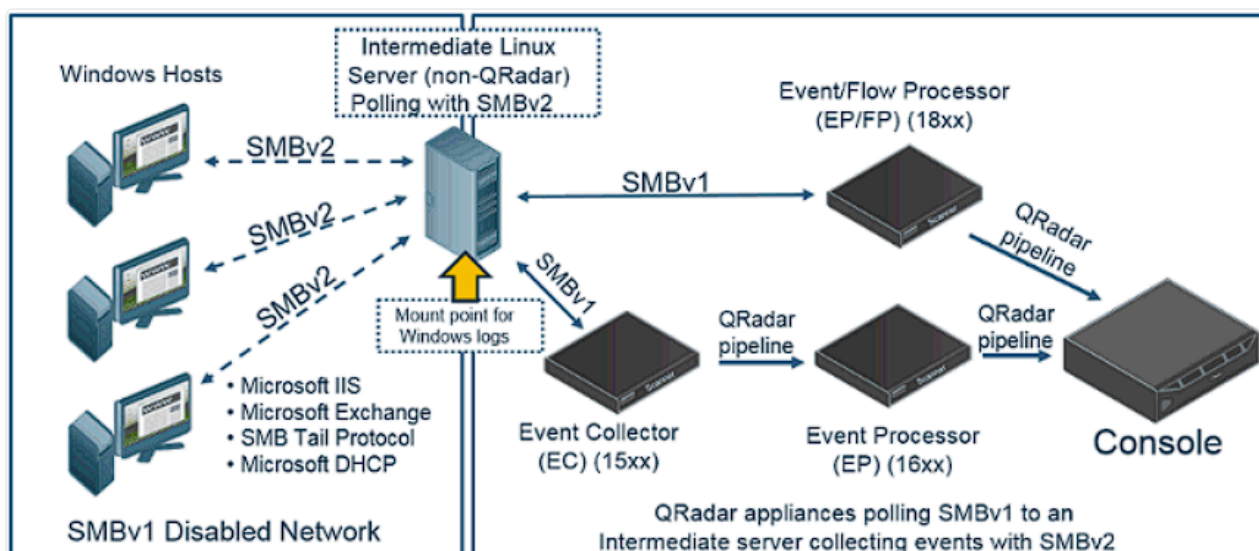
frequentemente utilizado em conjunto com ferramentas de análise e gerenciamento de logs, como SIEM (Security Information and Event Management), para proporcionar uma visão abrangente do ambiente de TI e auxiliar na proteção contra ameaças cibernéticas.



Coleta de Logs

A coleta de logs (Log Collection) é uma etapa essencial no processo de monitoramento e análise de eventos de segurança e atividades em uma rede ou sistema. Existem diferentes abordagens para a coleta de logs, cada uma com suas características específicas. As três principais abordagens são: Agent-based (baseada em agente), Collector e Sensor. Vamos detalhar cada uma delas:

1. **Agent-based (Baseada em Agente):** Na abordagem Agent-based, são instalados agentes (ou agentes de coleta de logs) nos dispositivos e sistemas que se deseja monitorar. Esses agentes são pequenos programas ou módulos que coletam e encaminham os logs relevantes para um servidor centralizado ou outro sistema de gerenciamento de logs. Cada agente é responsável por coletar os logs locais do dispositivo onde está instalado e pode ser configurado para filtrar ou selecionar os logs específicos que serão enviados para a centralização.
2. **Coletor (Collector):** Na abordagem do Collector, um dispositivo centralizado, conhecido como coletor de logs, é responsável por conectar-se a outros dispositivos, sistemas ou agentes de coleta de logs distribuídos na rede. O coletor recebe os logs enviados por esses dispositivos remotos e os armazena em um repositório central. Essa abordagem é especialmente útil em redes complexas, onde há uma grande quantidade de dispositivos e sistemas a serem monitorados. O Coletor ajuda a centralizar os logs e facilita a análise e correlação de eventos.
3. **Sensor:** A abordagem do Sensor é comumente usada em ambientes de rede, especialmente em sistemas de prevenção de intrusões (IPS) e firewalls. Os sensores são dispositivos dedicados que monitoram o tráfego de rede em busca de atividades suspeitas e eventos de segurança. Eles coletam logs de eventos específicos, como tentativas de intrusão, tráfego bloqueado, conexões de rede, entre outros, e os enviam para um sistema centralizado para análise e resposta a incidentes. Os sensores desempenham um papel importante na detecção proativa de ameaças e na proteção da rede contra ataques.



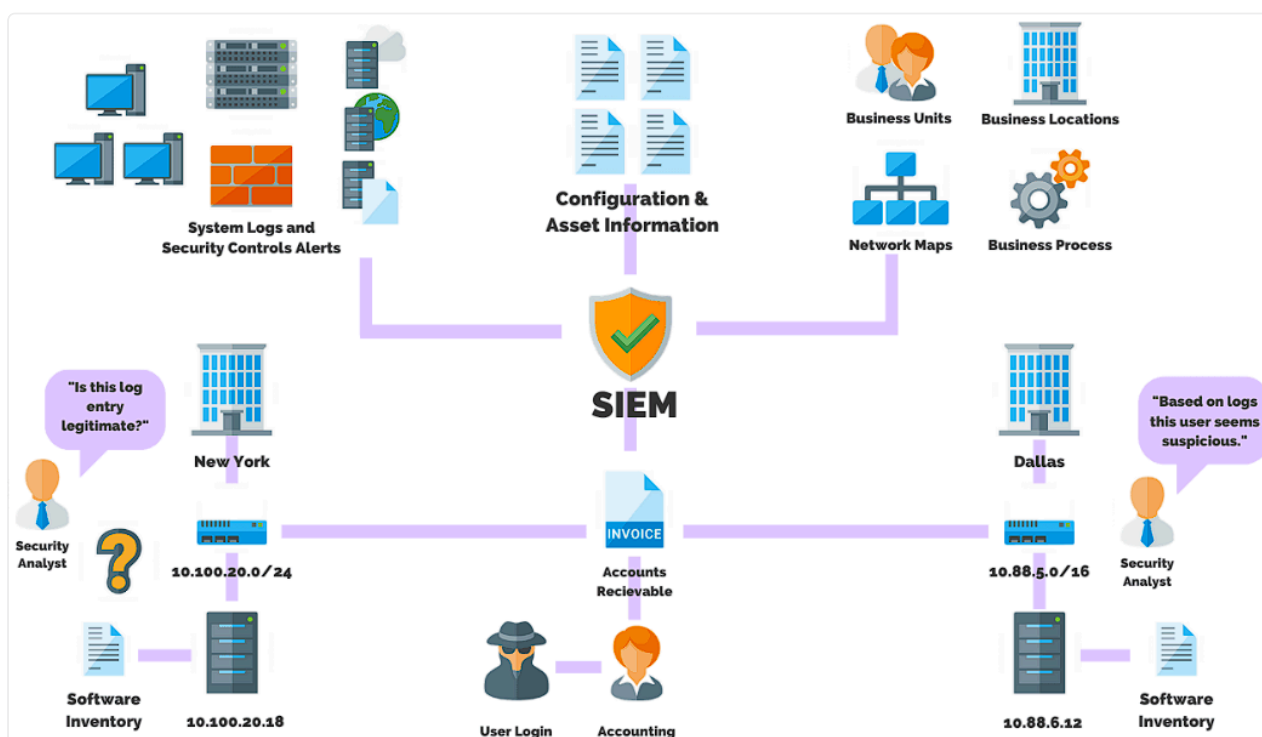
Coletores da ferramenta SIEM do QRadar da IBM.

Security Information and Event Management (SIEM)

O Security Information and Event Management (SIEM) é uma solução de segurança cibernética que combina a funcionalidade de coleta, armazenamento, análise e correlação de eventos e informações de segurança em tempo real, provenientes de diversas fontes em uma rede. O objetivo principal do SIEM é oferecer uma visão abrangente e centralizada da postura de segurança da organização, permitindo identificar ameaças e responder a incidentes de forma mais eficiente. O funcionamento do SIEM pode ser dividido em etapas:

- **Coleta de dados:** O SIEM coleta dados de várias fontes, como logs de eventos de sistemas, aplicativos, dispositivos de rede, firewalls, IDS/IPS (Sistemas de Detecção e Prevenção de Intrusões), antivírus, entre outros. Esses dados são enviados para o SIEM por meio de agentes, sondas ou dispositivos de coleta.
- **Armazenamento centralizado:** Os dados coletados são armazenados em um repositório centralizado, o que facilita a busca, consulta e análise de informações relevantes. O armazenamento de longo prazo permite a análise histórica e a criação de relatórios de tendências.
- **Normalização e correlação:** O SIEM normaliza os dados recebidos para um formato comum, o que facilita a análise e correlação de eventos. A correlação é uma etapa importante em que o SIEM analisa os eventos coletados para identificar padrões e relacionamentos entre eles, permitindo detectar ameaças complexas que podem não ser evidentes em análises individuais.

- **Detecção de anomalias e ameaças:** O SIEM utiliza regras e algoritmos de detecção para identificar atividades suspeitas e potenciais ameaças à segurança. Ele pode disparar alertas em tempo real para que os analistas de segurança possam responder prontamente a incidentes.
- **Notificação e resposta:** Quando uma atividade maliciosa ou suspeita é detectada, o SIEM pode acionar notificações e alertas para a equipe de segurança. A resposta aos incidentes pode incluir ações como bloqueio de IPs, isolamento de máquinas comprometidas, análise forense, entre outras medidas de mitigação.
- **Relatórios e conformidade:** O SIEM gera relatórios detalhados sobre a atividade de segurança da organização, auxiliando na demonstração de conformidade com padrões regulatórios e políticas internas de segurança.
- **Integração com outras ferramentas:** O SIEM pode se integrar com outras ferramentas de segurança, como Sistemas de Gerenciamento de Vulnerabilidades e Sistemas de Gerenciamento de Incidentes, para proporcionar uma abordagem mais abrangente e colaborativa à segurança cibernética.



SIEM.

Agregação de Logs (Log Aggregation)

A Log Aggregation, ou agregação de logs, é um processo de coleta e centralização de logs de diferentes fontes em um único local. Essa técnica é utilizada para

facilitar a análise, monitoramento e correlação de eventos de segurança e atividades em uma rede ou sistema e é normalmente realizado no SIEM. Veja como funciona:

1. **Coleta de Logs de diferentes fontes:** O processo de Log Aggregation envolve a coleta de logs de diversas fontes, como sistemas operacionais, aplicativos, dispositivos de rede, bancos de dados, servidores, appliances de segurança, entre outros. Esses logs são originados de diferentes dispositivos e podem estar distribuídos por toda a infraestrutura.
2. **Centralização dos Logs:** Os logs coletados são enviados para um único local centralizado, conhecido como servidor de agregação de logs ou repositório central. Esse servidor é responsável por armazenar todos os logs coletados e disponibilizá-los para análise e monitoramento.
3. **Normalização dos dados:** Antes de armazenar os logs, o processo de agregação pode envolver a normalização dos dados para garantir que todos os logs sejam convertidos para um formato comum. Isso facilita a análise e correlação dos eventos, independentemente de sua origem e formato original.
4. **Análise e correlação de eventos:** Com os logs centralizados e normalizados, é possível realizar análises abrangentes e correlacionar eventos de diferentes fontes. A correlação de eventos permite identificar padrões e relacionamentos entre os logs, o que auxilia na detecção de atividades suspeitas e ameaças.
5. **Alertas e notificações:** A agregação de logs permite a configuração de regras e alertas para acionar notificações em tempo real quando eventos críticos ou suspeitos são identificados. Isso possibilita uma resposta rápida a incidentes de segurança.
6. **Armazenamento de longo prazo:** Além de possibilitar análises em tempo real, a agregação de logs também permite o armazenamento de longo prazo dos registros. Isso é útil para auditorias, conformidade com regulamentos e investigações forenses.
7. **Relatórios e inteligência de segurança:** A centralização e agregação de logs também possibilitam a geração de relatórios abrangentes e fornecem informações valiosas sobre a postura de segurança da organização. A análise dos logs agregados pode gerar inteligência de segurança que ajuda a melhorar a proteção da rede contra ameaças cibernéticas.



Log Aggregation.

User and Entity Behavior Analytics (UEBA)

User and Entity Behavior Analytics (UEBA), ou Análise de Comportamento de Usuários e Entidades, é uma abordagem avançada de segurança cibernética que utiliza técnicas de inteligência artificial e aprendizado de máquina para detectar ameaças e atividades maliciosas com base no comportamento de usuários e entidades (como dispositivos, aplicativos e sistemas) em uma rede. Geralmente trabalha em conjunto com o SIEM. O funcionamento do UEBA pode ser detalhado da seguinte forma:

1. **Coleta de dados de comportamento:** O UEBA coleta e analisa uma ampla variedade de dados de comportamento dos usuários e entidades na rede. Inclui atividades de login, padrões de acesso a recursos, horários e locais de acesso, atividades de usuários privilegiados, interações com aplicativos e dispositivos, entre outros. Esses dados são coletados de várias fontes, como logs de

eventos, registros de autenticação e dados de sistemas de gerenciamento de identidades.

2. **Perfil de comportamento baseline:** O UEBA cria um perfil de comportamento baseline para cada usuário e entidade na rede. Esse perfil representa o comportamento normal e esperado de cada entidade. Para isso, o UEBA analisa o histórico de atividades para identificar padrões regulares e comportamentos típicos.
3. **Deteção de anomalias:** O UEBA utiliza algoritmos de aprendizado de máquina para identificar anomalias no comportamento das entidades. Essas anomalias são indicativas de atividades incomuns ou suspeitas que podem representar ameaças de segurança, como acesso a recursos não autorizados, tentativas de autenticação suspeitas, atividades fora do horário comercial, entre outras.
4. **Correlação de eventos:** O UEBA também é capaz de correlacionar eventos aparentemente não relacionados para detectar comportamentos anômalos. Por exemplo, ele pode detectar se um usuário realiza uma ação de autenticação em um local geograficamente distante logo após ter se conectado localmente.
5. **Pontuação de risco:** Com base nas detecções de anomalias e correlações de eventos, o UEBA atribui pontuações de risco a cada usuário e entidade. Quanto maior a pontuação, maior a probabilidade de comportamento malicioso ou suspeito.
6. **Alertas e notificações:** Quando uma atividade suspeita é detectada e a pontuação de risco ultrapassa um limiar pré-definido, o UEBA dispara alertas e notificações para a equipe de segurança. Isso permite uma resposta rápida e pró-ativa a potenciais incidentes de segurança.
7. **Adaptação ao ambiente:** O UEBA é capaz de aprender com o ambiente e se adaptar a mudanças no comportamento das entidades ao longo do tempo. Isso evita falsos positivos e aumenta a eficácia na detecção de ameaças em constante evolução.

SIEM vs. UEBA

UEBA is an integrated part of the Modern SIEM to improve detection and response capabilities



SIEM

- Rule-based threat detection
- Used for a wealth of use cases within cybersecurity, compliance, IT operations and business analytics
- Can be tailored to meet specific analytics across all data
- Requires continuous tuning to ensure relevant analytics



UEBA

- Self-learning threat detection
- Uses unsupervised machine learning
- Automatically assigns risk scores to entities and users
- Great at detection insider threats
- Doesn't require tuning to ensure relevant analytics

SIEM x UEBA.

Security Orchestration, Automation, and Response (SOAR)

SOAR ou Orquestração, Automatização e Resposta de Segurança, é uma abordagem abrangente de segurança cibernética que combina a orquestração e automação de processos com a capacidade de resposta a incidentes em uma única plataforma integrada. O objetivo é melhorar a eficiência das equipes de segurança, reduzir o tempo de resposta a incidentes e simplificar a gestão de eventos de

segurança. Geralmente trabalha em conjunto com o SIEM e o UEBA. Veja como funciona:

- **Coleta e agregação de dados:** O SOAR integra-se a várias fontes de dados, como sistemas de gerenciamento de logs, soluções de detecção de intrusões (IDS/IPS), sistemas de gerenciamento de vulnerabilidades e outras ferramentas de segurança. Ele coleta e agrega informações relevantes em tempo real para ter uma visão abrangente da postura de segurança da organização.
- **Análise e correlação de eventos:** O SOAR utiliza técnicas avançadas de análise e correlação de eventos para identificar incidentes de segurança, detectar padrões e relacionamentos entre eventos e priorizar alertas. Ajuda a reduzir o volume de alertas falsos e permite que a equipe se concentre nas ameaças mais críticas.
- **Automatização de tarefas:** Com base nas análises e correlações, o SOAR pode automatizar tarefas de resposta a incidentes e procedimentos de segurança. Inclui ações como isolamento de máquinas comprometidas, bloqueio de IPs maliciosos, remediação de vulnerabilidades conhecidas, entre outras medidas.
- **Orquestração de fluxo de trabalho:** O SOAR permite criar fluxos de trabalho personalizados para orquestrar as ações de resposta a incidentes. Ele pode coordenar a execução de várias tarefas e a interação entre diferentes sistemas de segurança, criando um processo mais eficiente e consistente.
- **Integração com ferramentas de segurança:** O SOAR é altamente integrado com várias ferramentas de segurança existentes na organização, permitindo interações contínuas e troca de informações entre elas. Isso facilita a automação e a resposta coordenada a incidentes.
- **Geração de relatórios e métricas:** O SOAR oferece recursos de geração de relatórios e métricas para acompanhar o desempenho das equipes de segurança, avaliar a eficácia das medidas de resposta a incidentes e demonstrar a conformidade com políticas e regulamentos de segurança.



SOAR.

Manipulação de arquivos:

Os seguintes comandos permitem que os usuários extraiam informações relevantes, filtrem dados, registrem eventos e procurem padrões específicos em logs e outros arquivos de texto em sistemas Unix-like:

- **Comando Cat:** O comando cat (concatenate) é usado em sistemas Unix-like para exibir o conteúdo de um ou mais arquivos de texto no terminal. Ele também pode ser utilizado para combinar o conteúdo de vários arquivos em um único arquivo de saída. A sintaxe básica é `cat arquivo1 arquivo2 ...`, que exibirá o conteúdo do arquivo1, arquivo2 e assim por diante, consecutivamente, no terminal.
- **Comandos Head e Tail:** São usados para exibir as primeiras e últimas linhas de um arquivo de texto, respectivamente. A sintaxe do comando head é `head -n <número_de_linhas> arquivo`, onde <número_de_linhas> é o número de linhas iniciais que se deseja exibir. Já a sintaxe do comando tail é `tail -n <número_de_linhas> arquivo`, onde <número_de_linhas> é o número de linhas finais que se deseja exibir.

Comando Logger: É utilizado para registrar mensagens ou eventos no sistema de log do sistema operacional. Ele permite que os usuários e scripts adicionem entradas de log para registrar atividades importantes ou informações relevantes. A sintaxe do comando é simples, como por exemplo, logger "Mensagem de log".

- **Sintaxe de expressões regulares (Regex):** São padrões utilizados para identificar e extrair sequências de caracteres específicas em um texto. Elas são amplamente utilizadas em comandos e ferramentas de busca, substituição e filtragem de texto, como o comando grep. As expressões regulares podem incluir caracteres especiais e metacaracteres para definir padrões de busca mais complexos.
- **Comando Grep:** É uma ferramenta poderosa para busca e filtragem de texto baseada em expressões regulares. Ele permite procurar por padrões específicos em arquivos ou na saída de outros comandos. A sintaxe básica do comando é grep <padrão> arquivo, onde <padrão> é a expressão regular que você deseja buscar no arquivo.

```
ubuntu@ubuntu-VirtualBox:~/code$ cat products.txt
```

ID	Type	Brand	Size	Price
01	HDD	Samsung	1TB	\$70
02	Monitor	DELL	15"	\$60
03	Mouse	A4	N/A	\$04
04	Keyboard	Atech	Normal	\$10
05	Scanner	HP	N/A	\$50
06	Printer	Samsung	N/A	\$100
07	Adapter	A4	N/A	\$10
08	Monitor	Samsung	17"	\$90
09	HDD	Toshiba	500GB	\$45
10	Keyboard	Logitech	N/A	\$15

Exemplo do commando CAT.

Segurança em redes sem fio

Wireless Access Point (WAP)

Também conhecido como Ponto de Acesso sem Fio, é um dispositivo de rede que permite a conexão de dispositivos sem fio, como laptops, smartphones, tablets e outros dispositivos habilitados para Wi-Fi, a uma rede com fio. O WAP atua como uma ponte entre os dispositivos sem fio e a rede cabeada, permitindo a comunicação sem fio entre eles. O funcionamento do WAP é mostrado a seguir:

- **Conexão à rede com fio:** O WAP é conectado a uma rede cabeada através de um cabo Ethernet. Esse cabo é conectado a uma porta LAN (Local Area Network) do WAP, fornecendo conectividade à rede.
- **Criação de rede sem fio:** O WAP transmite um sinal de rádio para criar uma rede sem fio. Esse sinal é utilizado pelos dispositivos sem fio próximos para se conectarem ao WAP e obterem acesso à rede com fio.
- **SSID e autenticação:** O WAP possui um nome de rede, conhecido como SSID (Service Set Identifier), que identifica a rede sem fio. Quando os dispositivos sem fio estão dentro do alcance do WAP, eles detectam o SSID e podem se conectar à rede. O WAP pode exigir uma senha ou outras formas de autenticação para garantir que apenas dispositivos autorizados possam acessar a rede.
- **Comutação de pacotes:** O WAP é capaz de receber e transmitir pacotes de dados entre os dispositivos sem fio e a rede cabeada. Ele atua como uma espécie de "ponte" ou "gateway" que encaminha os pacotes de e para os dispositivos sem fio e a rede com fio.
- **Gerenciamento de conexões:** O WAP é responsável por gerenciar as conexões dos dispositivos sem fio. Ele pode permitir um número máximo de dispositivos conectados simultaneamente (chamado de limite de clientes) e garantir que a largura de banda seja distribuída de maneira adequada entre os dispositivos.
- **Segurança:** A segurança é uma consideração importante no funcionamento do WAP. É essencial que o WAP esteja configurado corretamente com criptografia forte (como WPA2 ou WPA3) para proteger as comunicações sem fio contra acessos não autorizados e ataques de intrusos.
- **Gestão e monitoramento:** O WAP pode ser gerenciado e monitorado remotamente por meio de interfaces de gerenciamento, como uma interface web ou um aplicativo. Isso permite que os administradores de rede controlem as configurações, monitorem o desempenho e apliquem atualizações de segurança no WAP.

WAC104 802.11ac

NETGEAR®



NETGEAR WAC104 802.11ac Wireless Access Point

WAP.

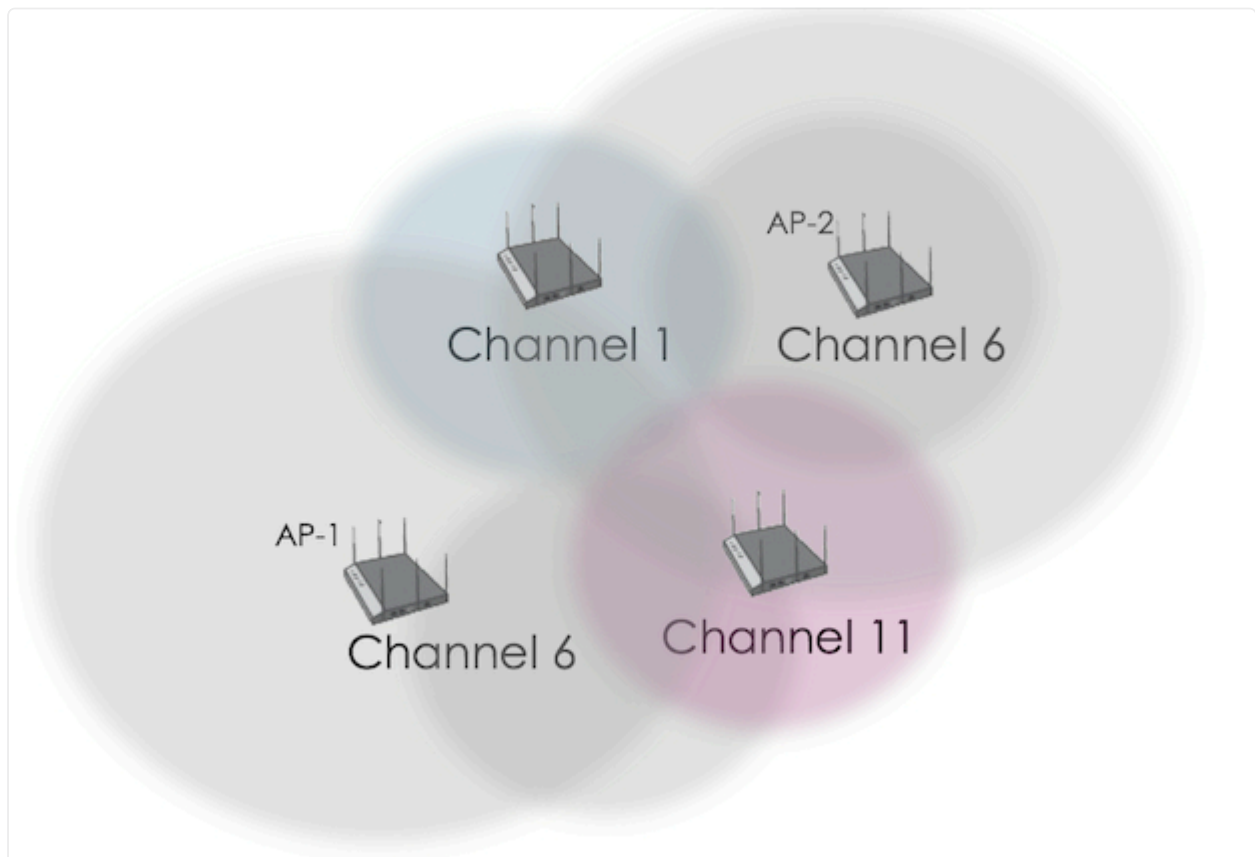
Interferência de Canal Compartilhado

A Co-channel Interference (CCI) ou Interferência de Canal Compartilhado é um fenômeno que ocorre em redes sem fio, especialmente em redes Wi-Fi, quando dois ou mais pontos de acesso sem fio (APs) operam no mesmo canal de frequência. Quando APs diferentes compartilham o mesmo canal, eles competem pelo espectro de rádio disponível, resultando em interferência mútua que pode afetar negativamente o desempenho e a confiabilidade da rede. O fenômeno CCI é detalhado a seguir:

1. **Canais de frequência:** As redes Wi-Fi operam em faixas de frequência não licenciadas, como as faixas de 2,4 GHz e 5 GHz. Cada faixa é dividida em canais, e os APs podem ser configurados para operar em um canal específico dentro dessas faixas.
2. **Sobreposição de canais:** Em ambas as faixas (2,4 GHz e 5 GHz), existem canais que se sobrepõem, o que significa que eles têm parte de sua largura de banda em comum. Por exemplo, nos canais de 2,4 GHz, os canais 1, 6 e 11 não se sobrepõem, mas outros canais têm sobreposição parcial.
3. **Canais não sobrepostos e Canais sobrepostos:** Os canais não sobrepostos são aqueles que não compartilham parte de sua largura de banda com outros canais adjacentes. Esses canais podem ser usados simultaneamente sem causar

interferência um no outro. Já os canais sobrepostos são aqueles que compartilham parte de sua largura de banda, o que pode levar à interferência quando vários APs operam nesses canais ao mesmo tempo.

4. **Concorrência por largura de banda:** Quando dois ou mais APs operam no mesmo canal sobreposto, eles competem pela mesma largura de banda, causando interferência. Essa interferência pode levar a perdas de pacotes, latência aumentada, redução da taxa de transferência e instabilidade na conexão de dispositivos sem fio.
5. **Gerenciamento de canais:** Para reduzir a CCI, é importante realizar um planejamento adequado dos canais utilizados pelos APs. Administradores de rede devem configurar os APs para operarem em canais não sobrepostos sempre que possível e, quando necessário, escolher canais com menor interferência para minimizar os efeitos da CCI.
6. **Controle de potência:** O controle de potência dos APs também pode ajudar a reduzir a CCI. Ao ajustar a potência de transmissão dos APs, é possível evitar que APs próximos operem em níveis muito altos de potência, o que pode agravar a interferência.



CCI.

WPA2 (Wi-Fi Protected Access 2) e WPA3 (Wi-Fi Protected Access 3) são padrões de segurança utilizados em redes Wi-Fi para proteger a comunicação entre os dispositivos sem fio e o ponto de acesso (AP) ou roteador. Ambos foram desenvolvidos para substituir o padrão WEP (Wired Equivalent Privacy), que era inseguro e foi amplamente comprometido. Veja como funciona o WPA2:

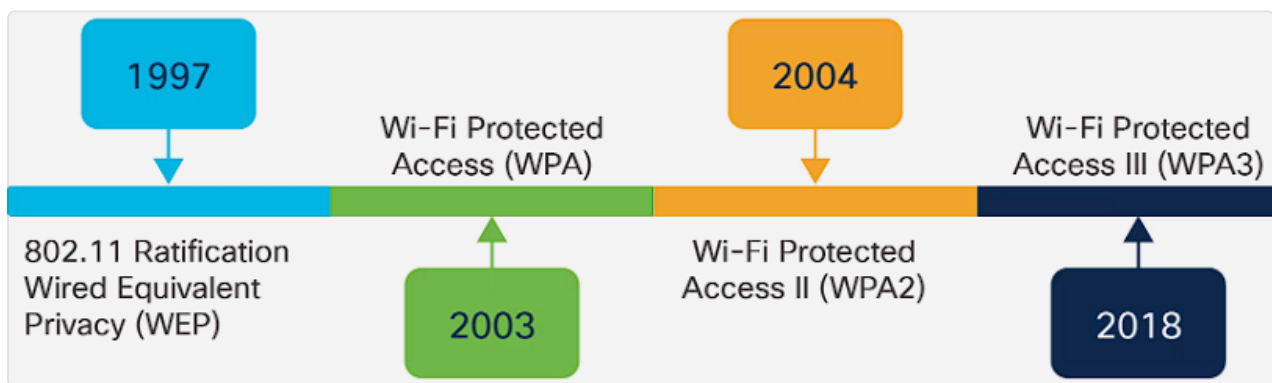
1. **Autenticação:** O WPA2 utiliza o protocolo de autenticação 802.1X/EAP (Extensible Authentication Protocol) para autenticar os dispositivos na rede. Esse protocolo requer a apresentação de credenciais, como senhas, certificados ou outras formas de autenticação, antes que um dispositivo seja autorizado a se conectar à rede.
2. **Criptografia:** O WPA2 utiliza o padrão de criptografia AES (Advanced Encryption Standard) para proteger a comunicação entre os dispositivos e o ponto de acesso. O AES é um algoritmo de criptografia forte e amplamente reconhecido por sua segurança.
3. **Modos de operação:** O WPA2 oferece dois modos de operação: WPA2-Personal (ou WPA2-PSK) e WPA2-Enterprise. No modo WPA2-Personal, também conhecido como WPA2 com chave pré-compartilhada (PSK), todos os dispositivos compartilham uma senha comum para se conectar à rede. No modo WPA2-Enterprise, a autenticação é baseada em um servidor de autenticação externo, como um servidor RADIUS, tornando-o mais adequado para redes corporativas.

Veja como funciona o WPA3:

1. **Autenticação individualizada:** O WPA3 introduz o conceito de autenticação individualizada, onde cada dispositivo tem uma chave única para a autenticação, tornando mais difícil para atacantes obterem acesso à rede mesmo que conheçam a senha de autenticação.
2. **Criptografia de 192 bits:** O WPA3 utiliza a criptografia de 192 bits do padrão SAE (Simultaneous Authentication of Equals) para proteger a autenticação entre o dispositivo e o ponto de acesso. Esse método de autenticação é mais seguro e resiliente a ataques de força bruta.
3. **Proteção contra ataques de força bruta:** O WPA3 incorpora uma proteção contra ataques de força bruta para evitar tentativas repetidas de adivinhar a senha de autenticação.

4. **Resistência a ataques de dicionário:** O WPA3 também oferece maior resistência a ataques de dicionário, tornando mais difícil para os atacantes descobrirem senhas comuns usando listas de palavras.
5. **Transições de segurança:** O WPA3 é projetado para ser retrocompatível com dispositivos mais antigos, permitindo que eles se conectem à rede com segurança, mesmo que não suportem os recursos mais avançados do WPA3.

O WPA3 traz aprimoramentos significativos em relação ao WPA2, tornando-o mais resistente a ataques e proporcionando uma camada adicional de segurança para redes Wi-Fi. À medida que a adoção do WPA3 cresce, é esperado que se torne o novo padrão de segurança preferencial para redes Wi-Fi em diversos ambientes, desde ambientes domésticos até redes empresariais e públicas.



WPA2 e WPA3.

Wi-Fi Protected Setup (WPS)

É um recurso criado para facilitar a configuração de redes Wi-Fi seguras, especialmente em ambientes domésticos e pequenos escritórios. Ele permite que os dispositivos se conectem à rede sem fio com segurança sem a necessidade de inserir a senha da rede manualmente. Veja como funciona:

- **Métodos de configuração:** O WPS oferece dois métodos de configuração: o método de botão de pressão (Push Button) e o método PIN (Personal Identification Number).

Método de Botão de Pressão: Neste método, o usuário pressiona um botão físico no roteador ou no ponto de acesso (AP) e, em seguida, ativa a função WPS no dispositivo que deseja se conectar à rede Wi-Fi. Os dois dispositivos

(roteador/AP e dispositivo cliente) trocam informações automaticamente, configurando a conexão sem fio de forma segura.

Método PIN: Neste método, o usuário insere um PIN (número de identificação pessoal) de oito dígitos fornecido pelo roteador ou AP no dispositivo cliente. Esse PIN é usado para estabelecer a conexão Wi-Fi com segurança.

- **Temporização do PIN:** Para aumentar a segurança do método PIN, o WPS possui um recurso de bloqueio temporário. Após várias tentativas fracassadas de inserção do PIN, o WPS entra em um estado de bloqueio temporário, tornando mais difícil para um atacante tentar forçar a conexão através de ataques de força bruta.
- **Chaves de criptografia:** O WPS gera chaves de criptografia temporárias e exclusivas para a conexão entre o dispositivo cliente e o roteador/AP. Essas chaves são usadas para proteger a comunicação sem fio e são modificadas periodicamente para garantir a segurança contínua.
- **Ativação e desativação:** A maioria dos dispositivos roteadores e clientes possui suporte ao WPS. No entanto, por motivos de segurança, muitos fabricantes desativam o WPS por padrão em seus roteadores, pois alguns ataques demonstraram vulnerabilidades na implementação do WPS.
- **Segurança:** Embora o WPS tenha sido projetado para facilitar a configuração de redes Wi-Fi seguras, algumas implementações do WPS foram criticadas por suas vulnerabilidades de segurança. Isso inclui ataques conhecidos como "ataque de força bruta de PIN" e "ataque de registro externo". Como resultado, muitos especialistas em segurança recomendam desativar o WPS em roteadores e dispositivos que suportam esse recurso.



WPS.

Engenharia social em Wi-Fi

Os seguintes ataques podem ser implementados em redes Wi-Fi para descobrir dados confidenciais:

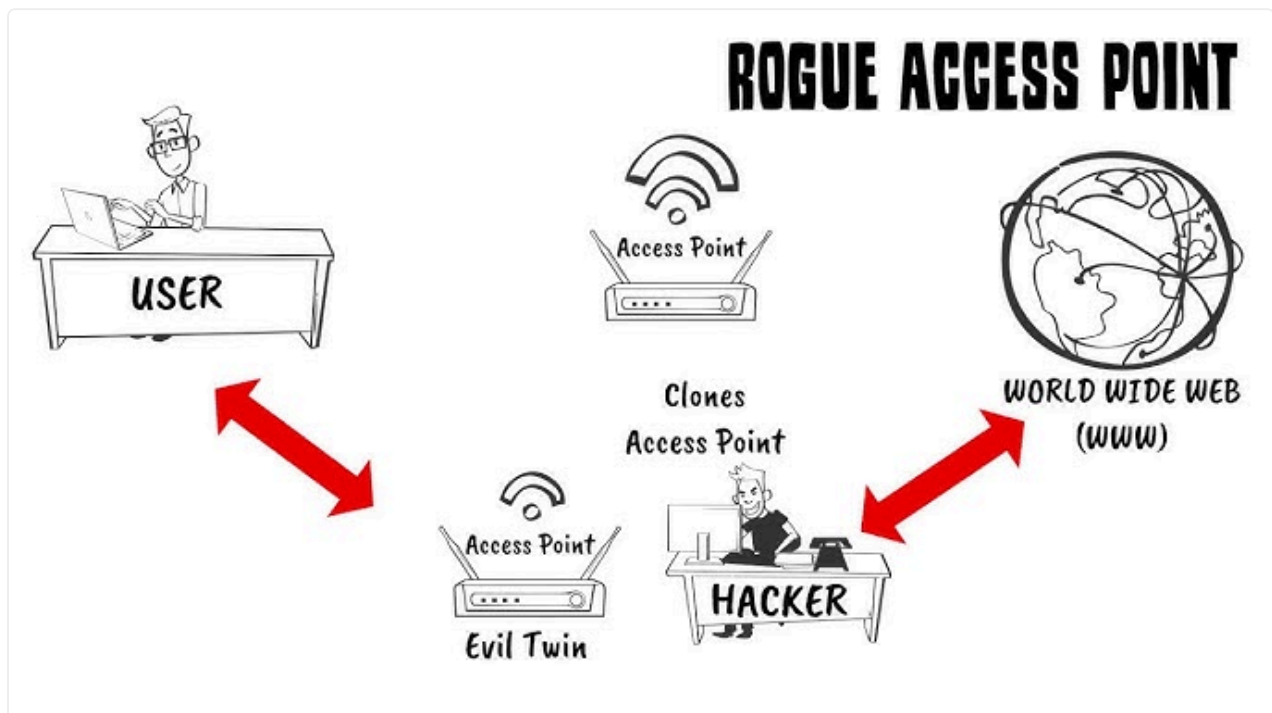
Rogue Access Point (Ponto de Acesso Falso) O Rogue Access Point (RAP) é um dispositivo de rede não autorizado que se disfarça como um ponto de acesso legítimo em uma rede Wi-Fi. Ele é configurado e controlado por um atacante com o objetivo de enganar dispositivos sem fio e fazê-los se conectar ao RAP em vez do ponto de acesso legítimo. O funcionamento do Rogue Access Point pode ser detalhado da seguinte forma:

1. **Criação da rede falsa:** O atacante configura o RAP para transmitir um sinal Wi-Fi com um SSID (nome da rede) similar ou idêntico ao da rede legítima. Isso faz com que dispositivos sem fio próximos detectem a rede falsa como uma opção de conexão.
2. **Enganando dispositivos:** Quando os dispositivos sem fio tentam se conectar à rede, eles podem ser enganados a escolher o RAP em vez do ponto de acesso legítimo, especialmente se o sinal do RAP for mais forte ou estiver mais próximo dos dispositivos.
3. **Captura de tráfego:** Uma vez que os dispositivos se conectam ao RAP, todo o tráfego da rede passa por ele. O atacante pode capturar e analisar o tráfego, incluindo informações confidenciais, senhas, dados de autenticação e outras comunicações sensíveis.
4. **Ataques Man-in-the-Middle:** O RAP também pode ser usado para realizar ataques Man-in-the-Middle (MITM), onde o atacante intercepta e manipula o tráfego entre os dispositivos e a rede legítima. Isso permite que o atacante veja, modifique ou injete dados no tráfego de rede.

Evil Twin (Gêmeo Malicioso)

O Evil Twin (Gêmeo Malicioso) é uma forma específica de Rogue Access Point em que o atacante configura um ponto de acesso falso que se disfarça como o ponto de acesso legítimo de uma rede Wi-Fi conhecida. O funcionamento do Evil Twin é semelhante ao do Rogue Access Point, mas sua característica distintiva é a tentativa de enganar os usuários ao criarem uma rede com um SSID idêntico ou muito semelhante ao da rede legítima. Isso pode levar os usuários a se conectarem

inadvertidamente ao Evil Twin sem perceberem que não estão conectados à rede real.



Evil Twin.

Conclusão

Nesta aula, exploramos conceitos fundamentais para o monitoramento e segurança de redes. Através do Network Monitor, aprendemos a coletar e analisar dados de tráfego, permitindo detectar comportamentos suspeitos e ameaças potenciais. Os Logs se mostraram essenciais para registrar eventos relevantes e facilitar a investigação de incidentes de segurança. Também discutimos o papel crucial do SIEM na centralização e correlação de informações para uma visão abrangente da postura de segurança da organização.

Aprofundando-nos na coleta de logs, exploramos as diferentes abordagens, como Agent-based, Collector e Sensor. A prática da Log Aggregation nos permitiu consolidar dados dispersos em um único repositório, facilitando a análise e o rastreamento de atividades maliciosas. A abordagem inovadora de User and Entity Behavior Analytics (UEBA) se mostrou promissora ao identificar padrões de comportamento anômalos, contribuindo para uma resposta mais proativa a ameaças em potencial.

Em seguida, conhecemos o poder do Security Orchestration, Automation, and Response (SOAR), que nos possibilitou automatizar tarefas de resposta a incidentes, melhorando a eficiência da equipe de segurança. No contexto da File Manipulation, aprendemos os comandos essenciais, como Cat, Head, Tail, Logger e Grep, ferramentas valiosas para filtrar e manipular informações em arquivos. Por fim, abordamos questões cruciais em redes sem fio, compreendendo os desafios do Wireless Access Point (WAP) e os riscos associados à Co-channel Interference (CCI), bem como as melhorias de segurança do WPA2, WPA3 e Wi-Fi Protected Setup (WPS), enfatizando a importância de proteger-se contra ameaças como Rogue Access Points e Evil Twins.

Parabéns por ter finalizado esta aula de monitoramento de redes e segurança em redes sem fio!

Aula 2: Protocolos seguros

Objetivos

- ☒ Conhecer os principais protocolos de rede que têm implementações com versões seguras.
- ☒ Explorar as diferenças entre Secure Shell (SSH) e outros protocolos de transferência de arquivos.
- ☒ Conhecer ataques que exploram versões de protocolos de redes sem versão segura.

Conceitos

- ☒ DNS Security Extensions (DNSSEC).
- ☒ SSH FTP (SFTP) e FTP Over SSL (FTPS).
- ☒ Secure Shell (SSH).

Introdução

Nesta aula de protocolos seguros, abordaremos desde os riscos associados a ataques como Domain Hijacking e DNS Poisoning, até a importância de implementar protocolos como DHCP Snooping Port Security e DNS Security Extensions (DNSSEC) para mitigar vulnerabilidades. Ao longo da aula, exploraremos conceitos fundamentais relacionados ao Secure Sockets Layer (SSL) e Transport Layer Security (TLS) em suas várias versões, entendendo como esses protocolos podem fortalecer as conexões seguras. Além disso, discutiremos as funcionalidades do Secure Shell (SSH) e suas aplicações no contexto de FTP (SFTP) e FTP Over SSL (FTPS), bem como o uso de criptografia em serviços de email, como Secure SMTP, Secure POP e Secure IMAP, incluindo o emprego do S/MIME.

Ataques de rede e protocolos seguros

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. Veja o processo passo a passo:

1. 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.
-

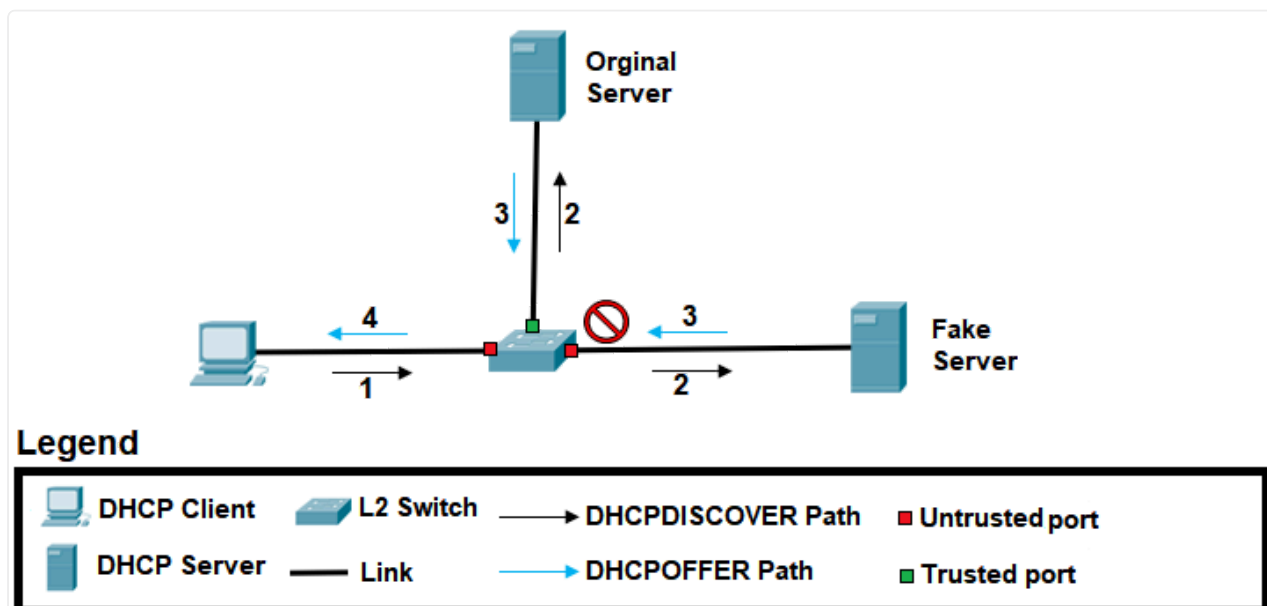
Portas não confiáveis: São as portas onde estão conectados os dispositivos finais, como computadores, smartphones e impressoras. Nessas portas, o DHCP Snooping estará ativo e monitorando os pacotes DHCP.

2. 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.

3. 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.



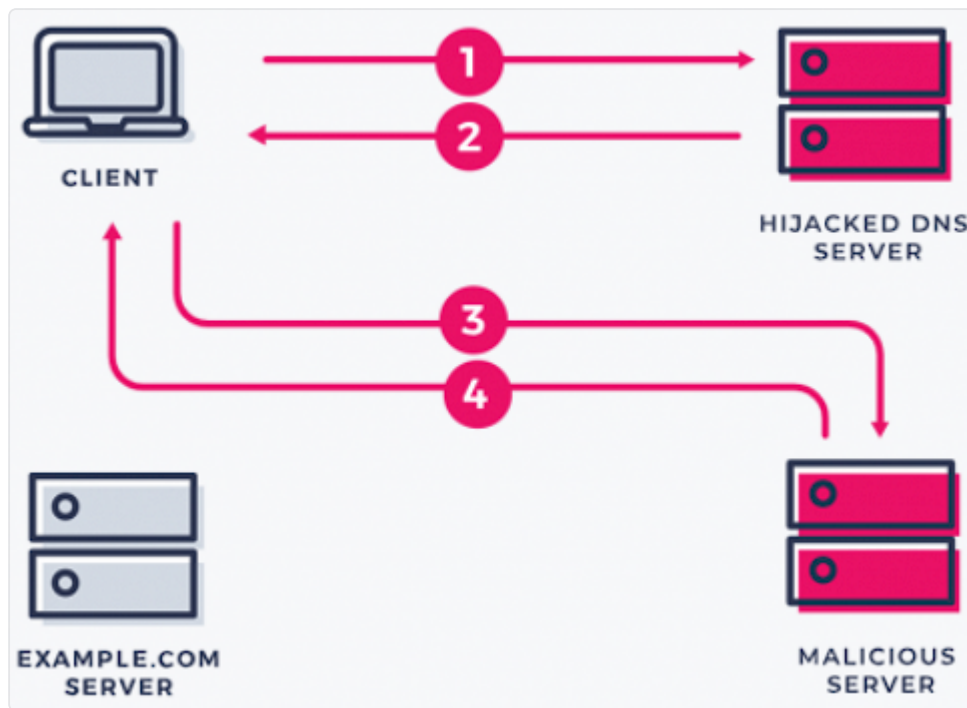
DHCP snooping.

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. Veja como o ataque é executado:

1. **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.
2. **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.
3. **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.
4. **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.
5. **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.
6. **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.
7. **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.



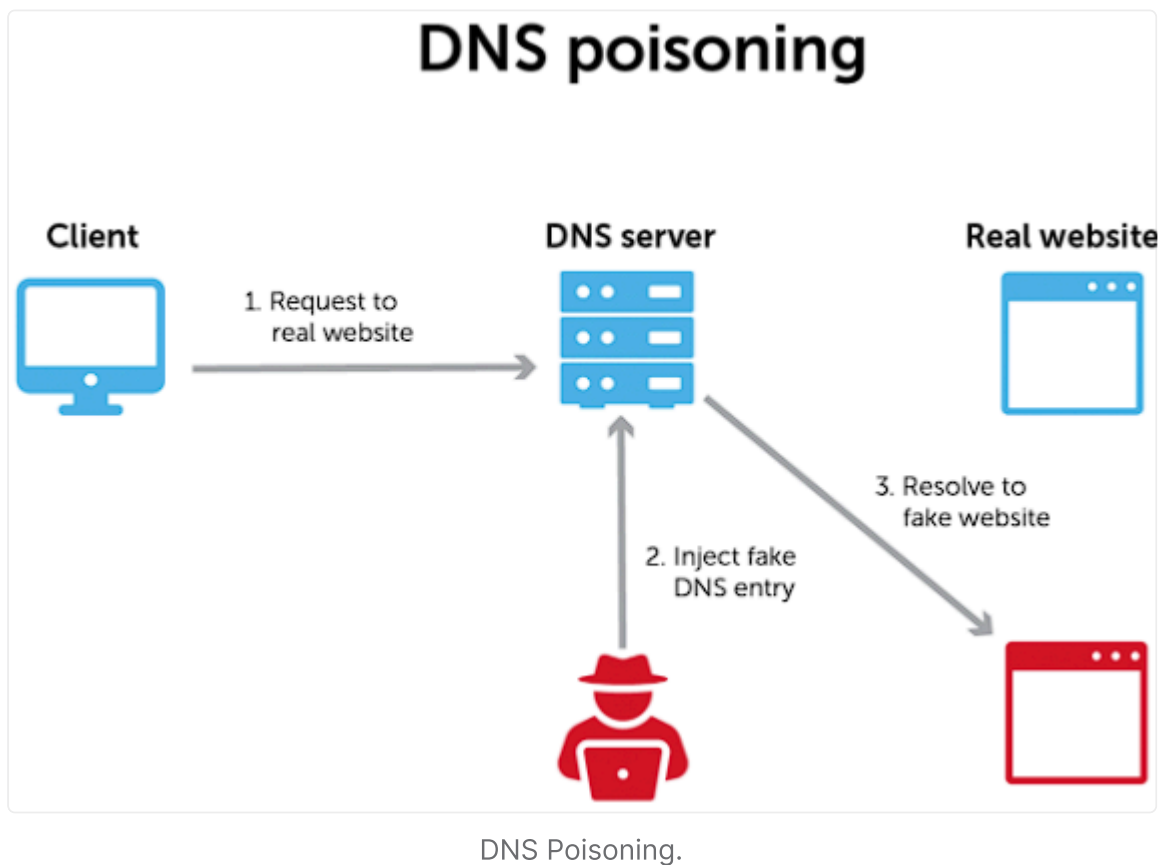
Domain hijacking.

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:

1. **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.
2. **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.
3. **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.

4. **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.
5. **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.
6. **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.

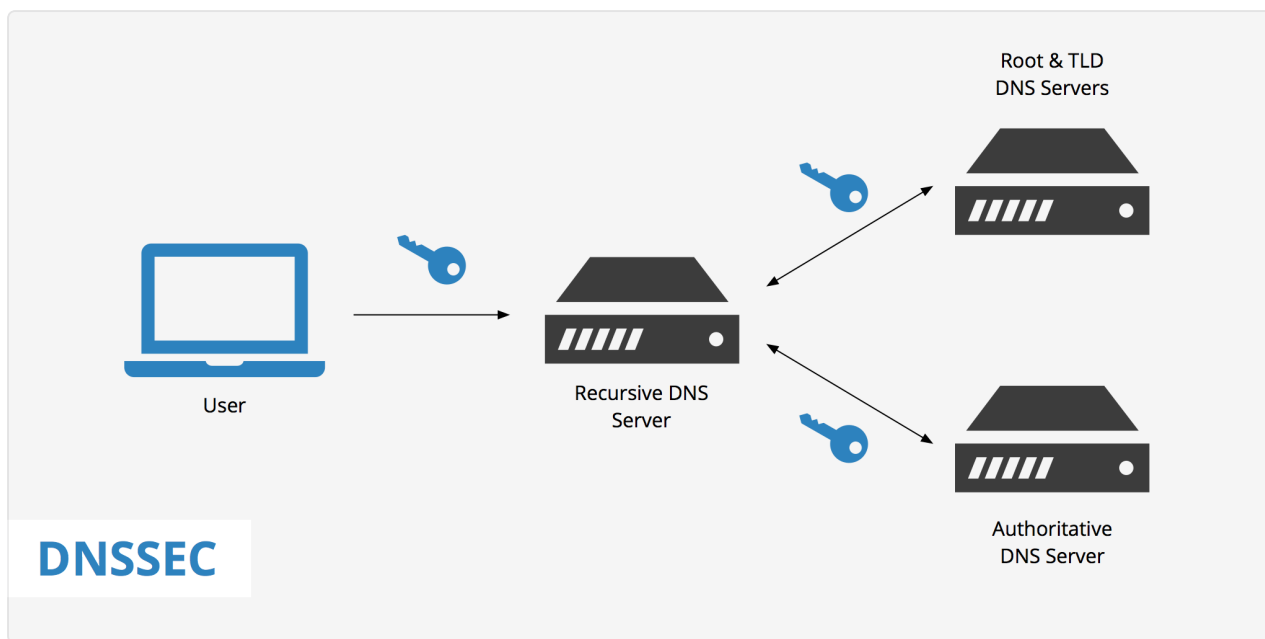


DNS Security Extensions (DNSSEC)

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:

1. **Assinatura digital dos registros DNS:** O servidor DNS responsável por um domínio assina digitalmente os registros DNS que contêm 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.
2. **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.
3. **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.
4. **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.
5. **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.
6. **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.



DNSSEC.

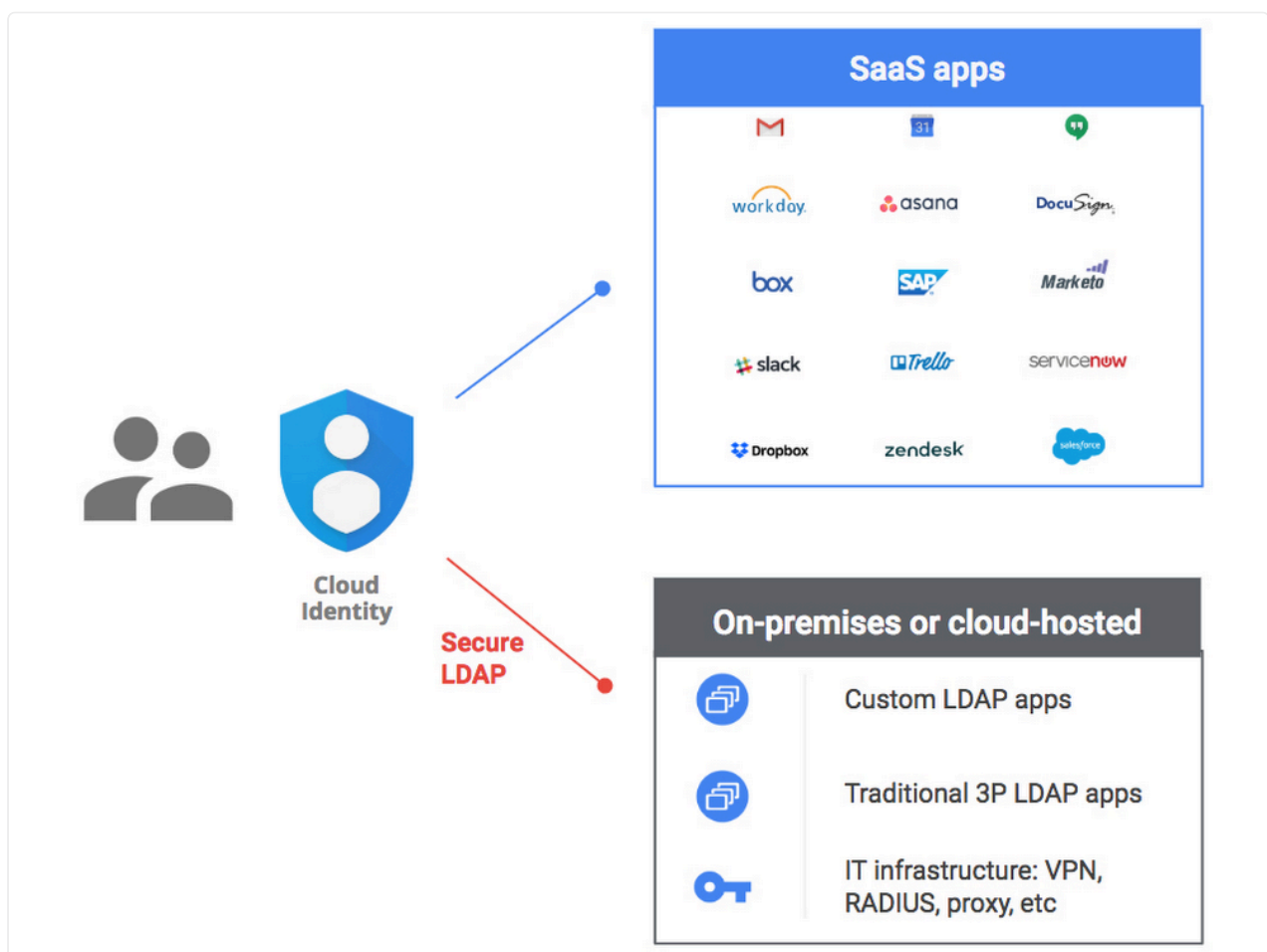
LDAP Secure (LDAPS)

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:

1. **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.
2. **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.
3. **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.

4. **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.
5. **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.
6. **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.

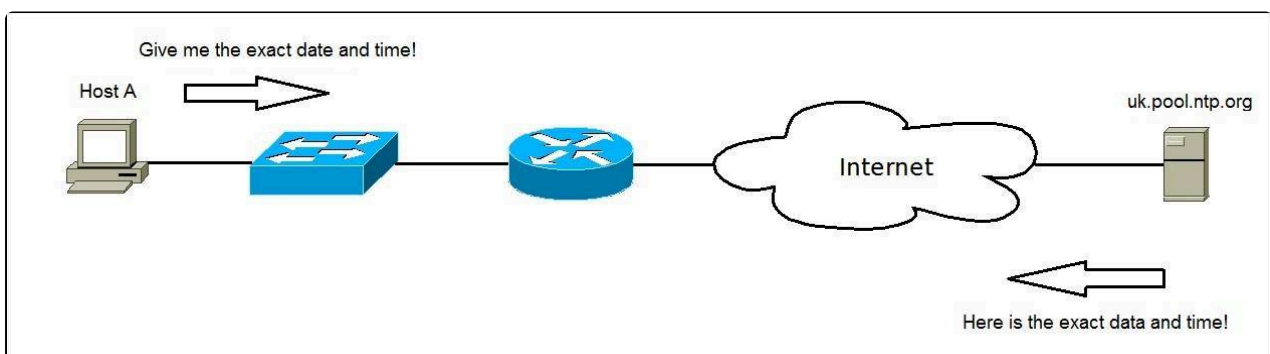


LDAPS.

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. Veja como funciona:

1. **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.
2. **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.
3. **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.



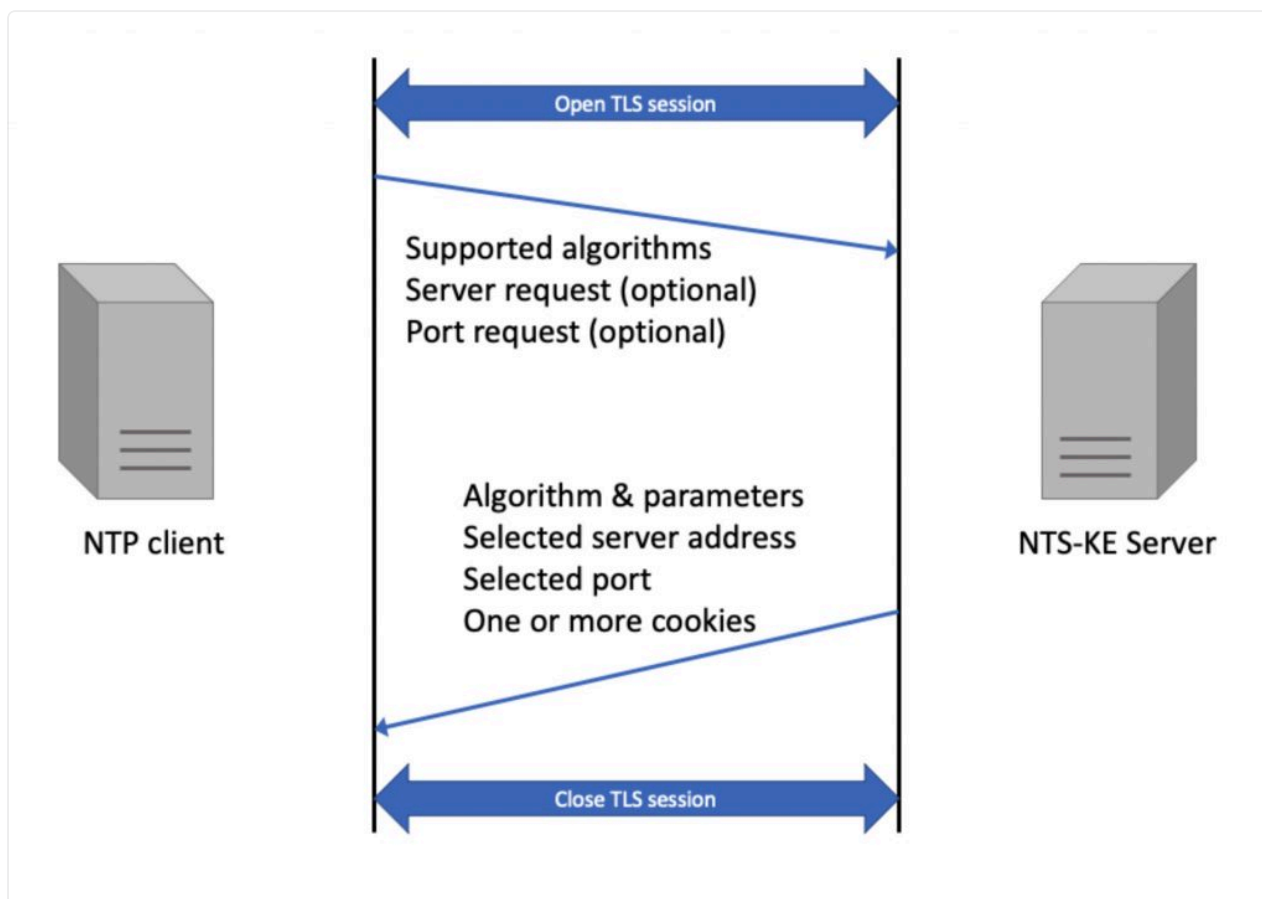
NTP.

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 do Network Time Security (NTS):

1. **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.
2. **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.
3. **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.
4. **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.
5. **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.



NTS.

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. Veja como funciona a primeira versão do SNMP:

- **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.

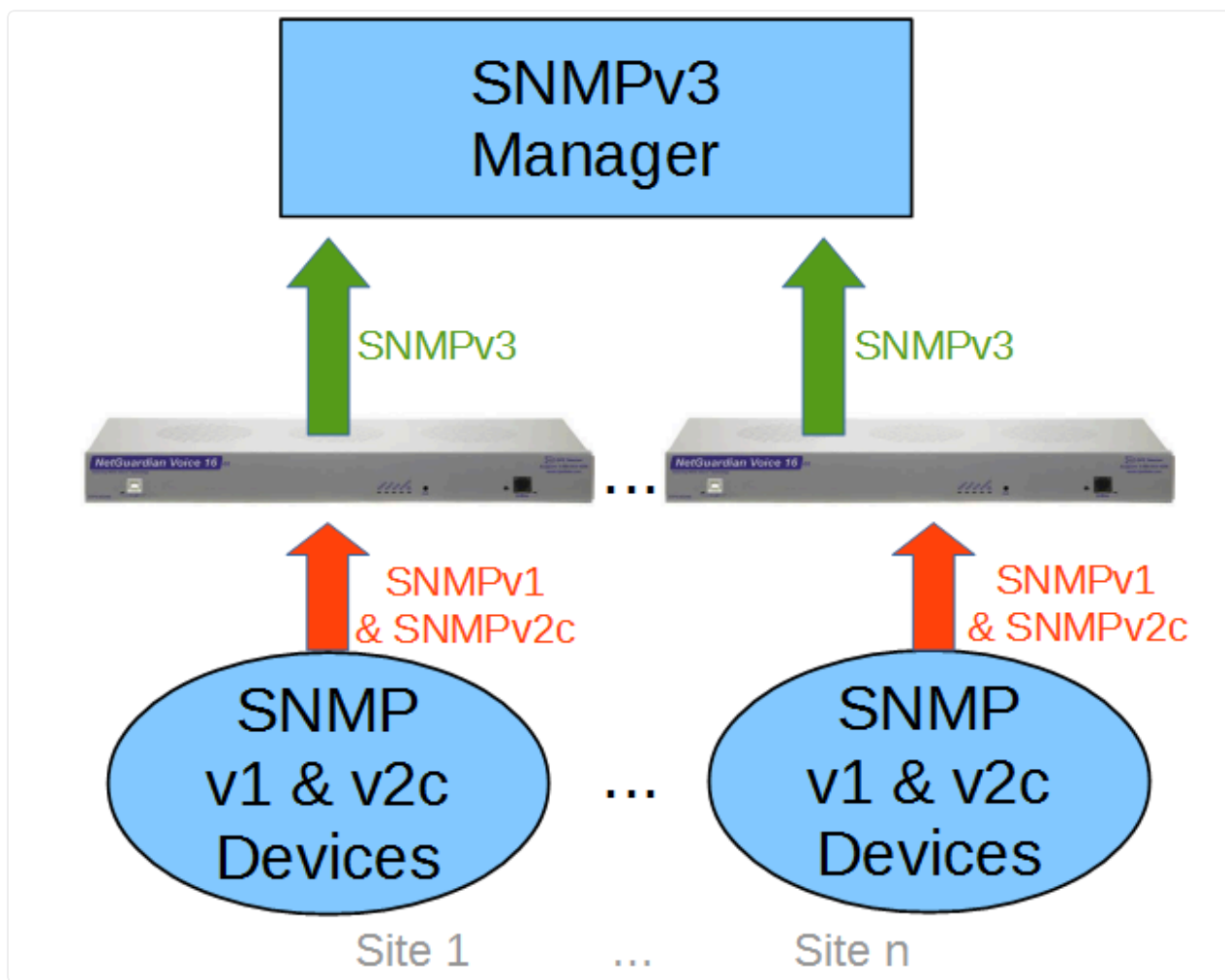
- **Operações SNMP:** Os gerenciadores SNMP podem executar as seguintes quatro operações principais. a. Get: Solicita informações específicas do agente SNMP. b. Set: Configuração de variáveis no agente SNMP para alterar configurações. c. Trap: Notificação automática enviada pelos agentes SNMP para os 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.



SNMPv3.

Secure Sockets Layer (SSL) e Transport Layer Security (TLS)

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.

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. Veja as principais versões do TLS:

1. **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.

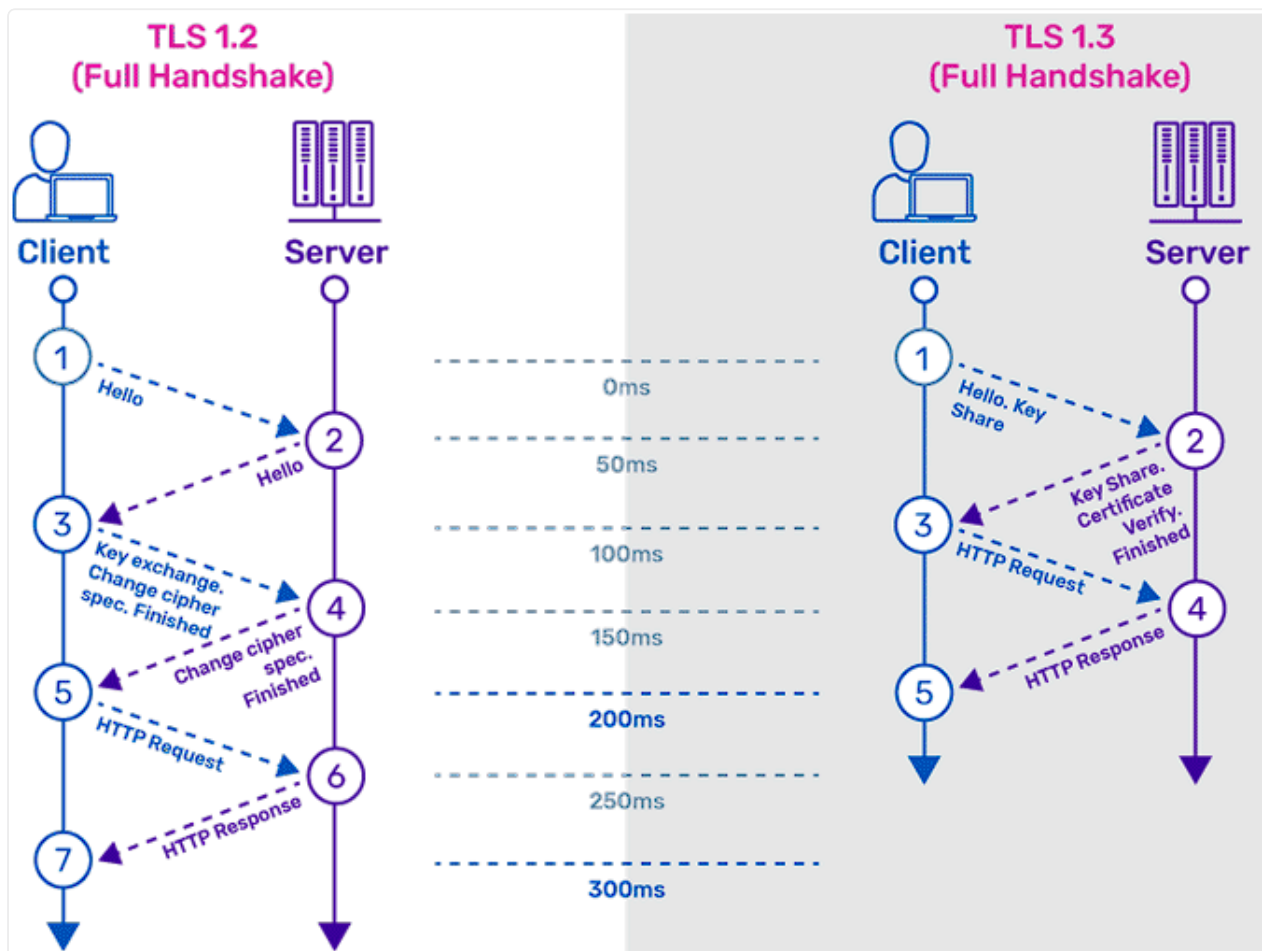
2. **TLS 1.2:**

- 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.

3. **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.



TLS 1.2 x TLS 1.3.

SSH FTP (SFTP) e FTP Over SSL (FTPS)

São protocolos de transferência de arquivos seguros que utilizam técnicas diferentes para proteger a confidencialidade e a integridade dos dados transmitidos durante o processo de transferência de arquivos.

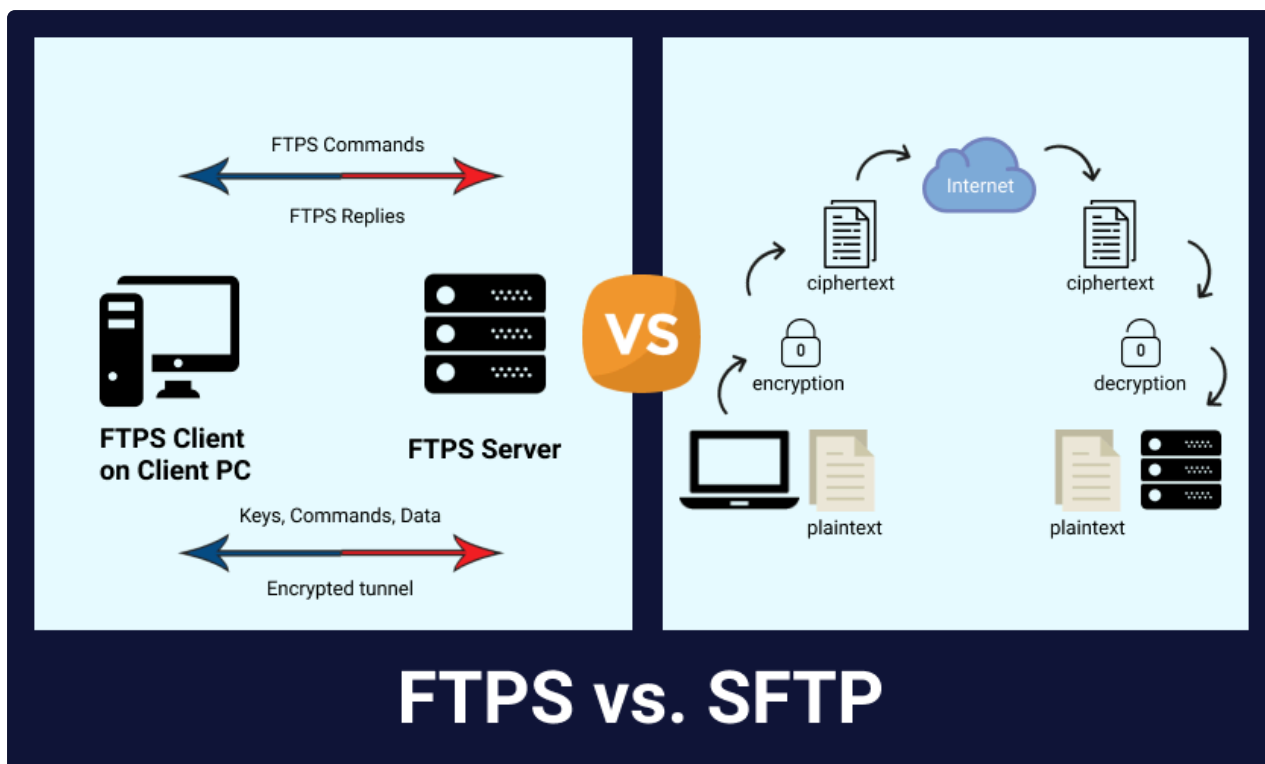
1. Funcionamento do SFTP:

- **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.

2. Funcionamento do 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.



FTPS x SFTP.

Secure SMTP (SMTPS), Secure POP (POP3S), Secure IMAP (IMAPS) e Secure/Multipurpose Internet Mail Extensions (S/MIME)

São mecanismos de segurança utilizados para proteger as comunicações de e-mail, garantindo que os dados sejam transmitidos de forma criptografada e segura. Veja como funcionam:

1. 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.

2. 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).

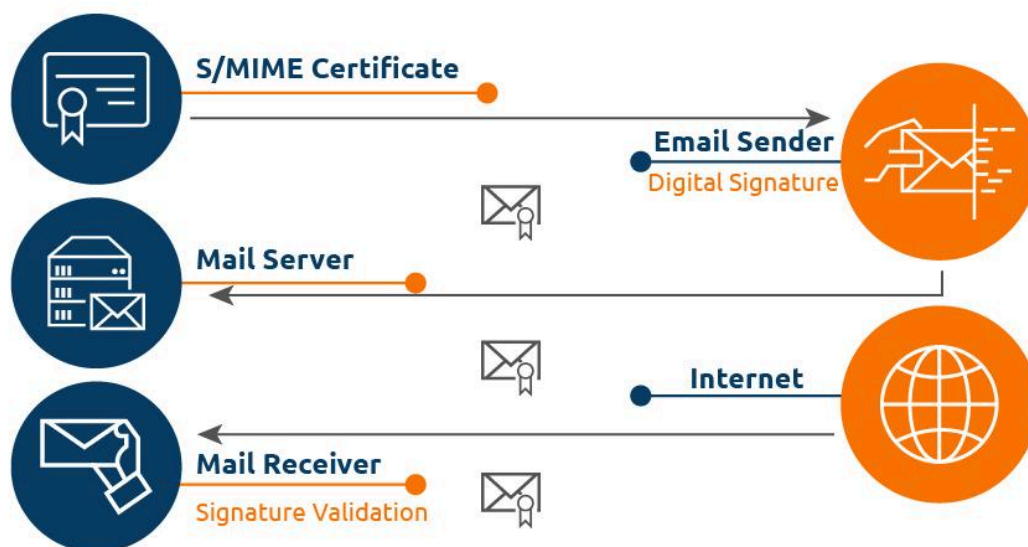
- Utiliza a porta TCP 995 para estabelecer a conexão segura entre o cliente e o servidor.
- O POP3S permite que o cliente baixe e-mails de forma segura do servidor, garantindo que os dados do e-mail e as informações de autenticação sejam confidenciais e protegidos.

3. **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.

4. **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.



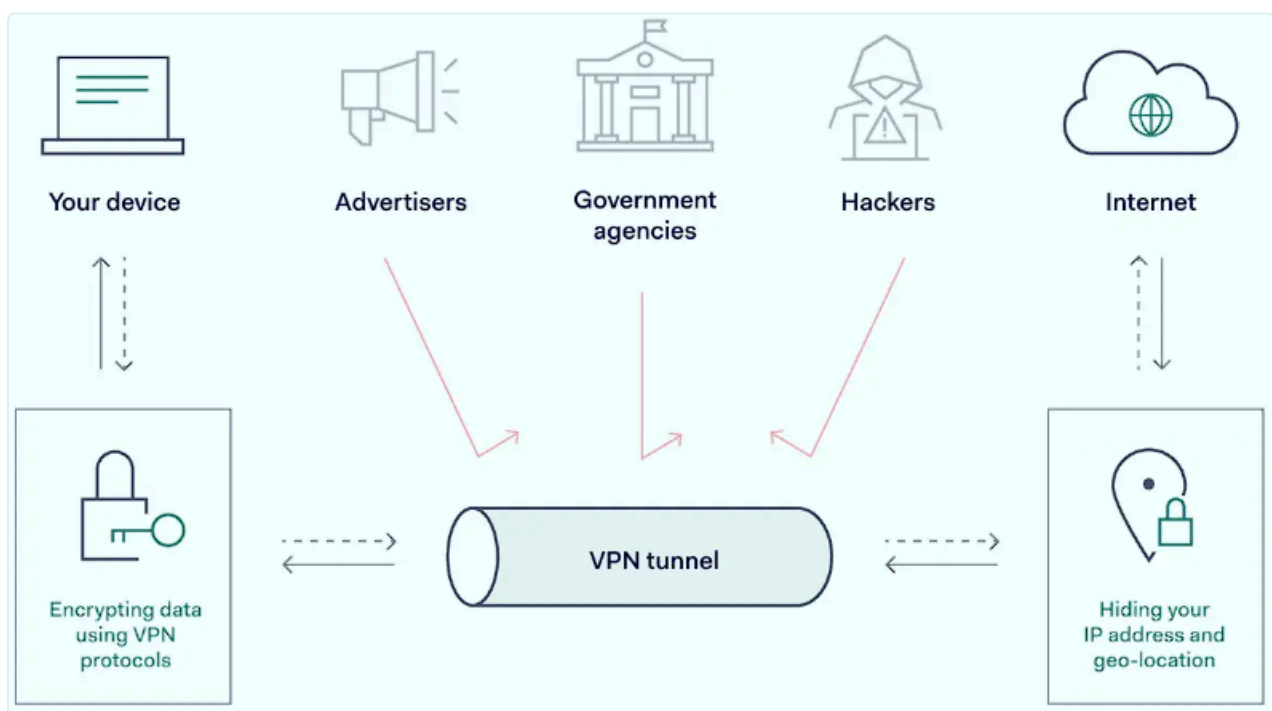
S/MIME.

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. Veja como funciona:

1. **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.
2. **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.
3. **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.
4. **Túnel VPN:** 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.

5. **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.
6. **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.



TLS VPN.

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). Ambos são usados para proteger pacotes IP, mas diferem em suas funcionalidades específicas:

1. **Authentication Header (AH):**

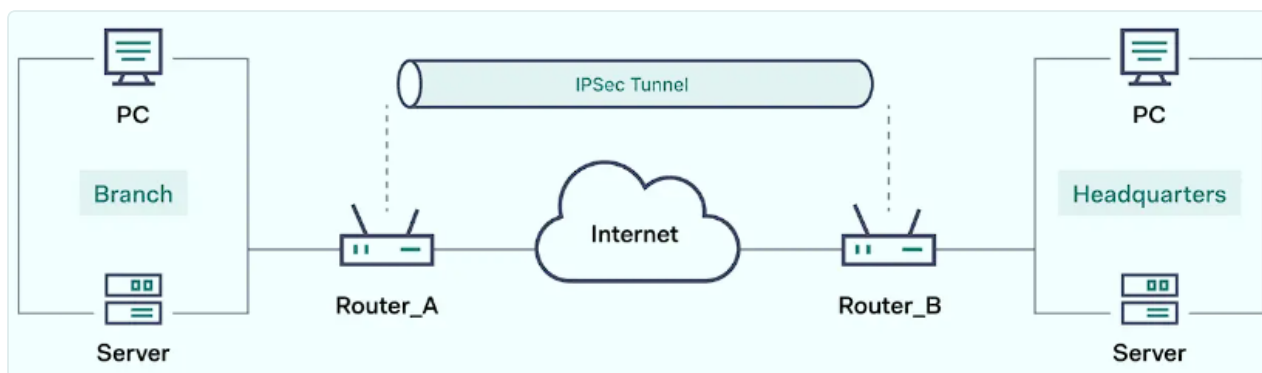
- O AH é um dos protocolos do IPSec que fornece autenticação e integridade dos dados transmitidos.
- Ele adiciona um cabeçalho ao pacote IP, contendo um valor de hash (MAC - Message Authentication Code) calculado a partir dos dados originais e de uma chave secreta compartilhada entre os dispositivos 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.

2. **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 do IPSec:

- 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.



IPSec.

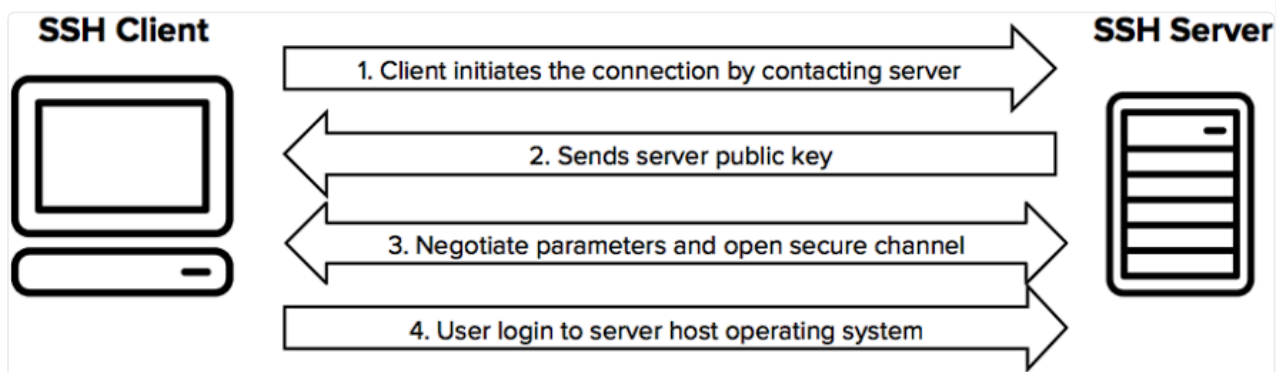
Secure Shell (SSH)

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. O SSH funciona da seguinte maneira:

- **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 descryptografia.

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.



SSH.

Conclusão

Nesta aula, exploramos uma variedade de tópicos essenciais em segurança de redes e comunicações, abrangendo desde ataques de DHCP não autorizados até protocolos de criptografia robustos. Aprendemos sobre os riscos associados a ataques de DHCP rogue e como mitigá-los usando DHCP snooping port security. Adicionalmente, compreendemos os perigos do domain hijacking e DNS poisoning, bem como a importância do DNSSEC para garantir a autenticidade e integridade dos registros DNS.

Também exploramos a segurança em protocolos como LDAP Secure (LDAPS), Network Time Protocol (NTP) com Network Time Security e SNMP v3, entre outros. Também examinamos a criptografia segura fornecida pelo SSL/TLS 1.1, 1.2 e 1.3, além das opções seguras para transferência de arquivos, como SFTP e FTPS. Essa ampla gama de tópicos demonstra a importância de uma abordagem abrangente de segurança para proteger redes e comunicações contra ameaças em constante evolução, enfatizando a necessidade contínua de implementar medidas de segurança sólidas.

Parabéns por ter finalizado a aula de Protocolos seguros! Agora, você sabe identificar a versão segura dos principais protocolos de rede!