Fundamentos da Segurança da Informação

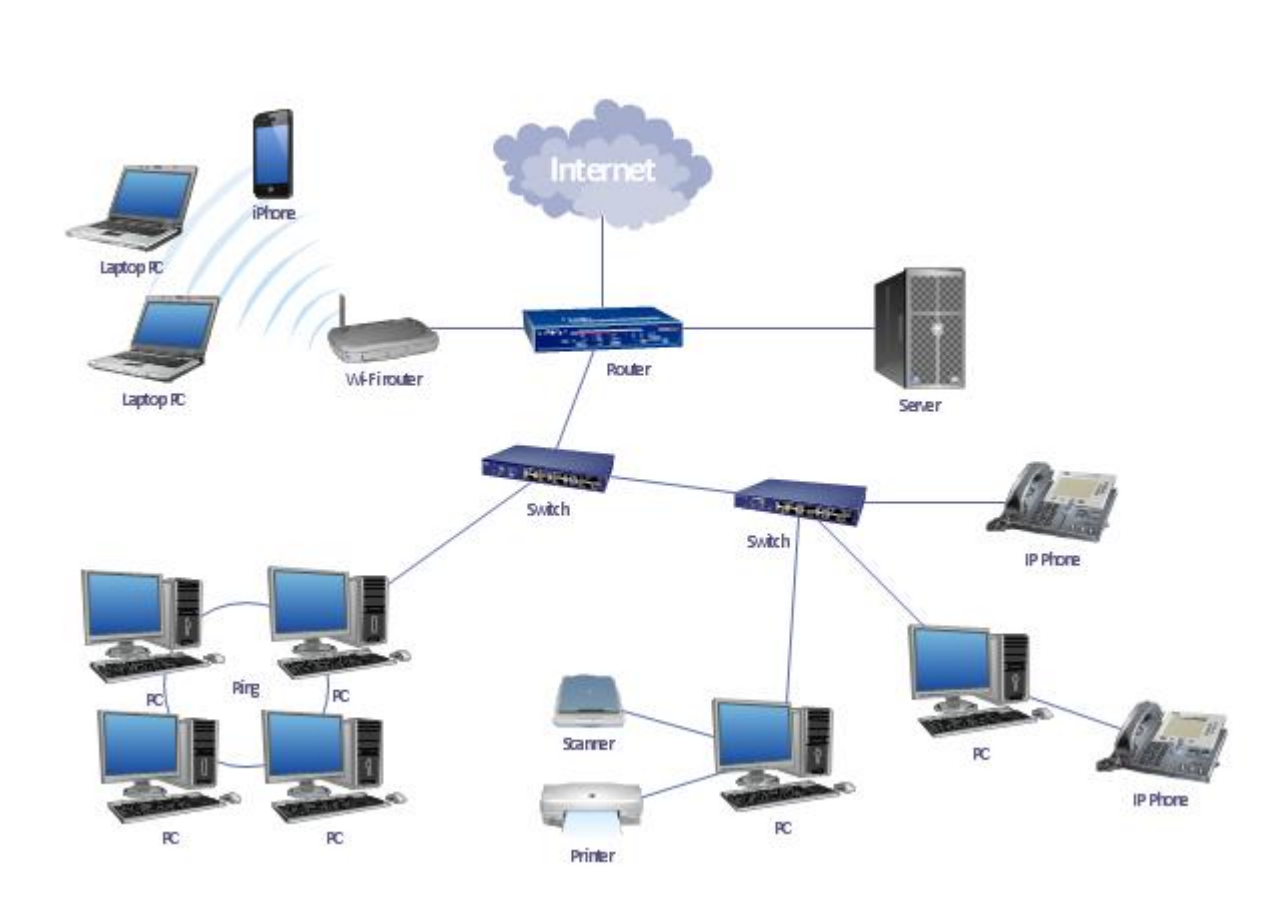
FABIANO GISBERT

Etapa 04

Estrutura de Rede e Vulnerabilidades

Rede LAN

Uma topologia padrão de uma Rede Corporativa

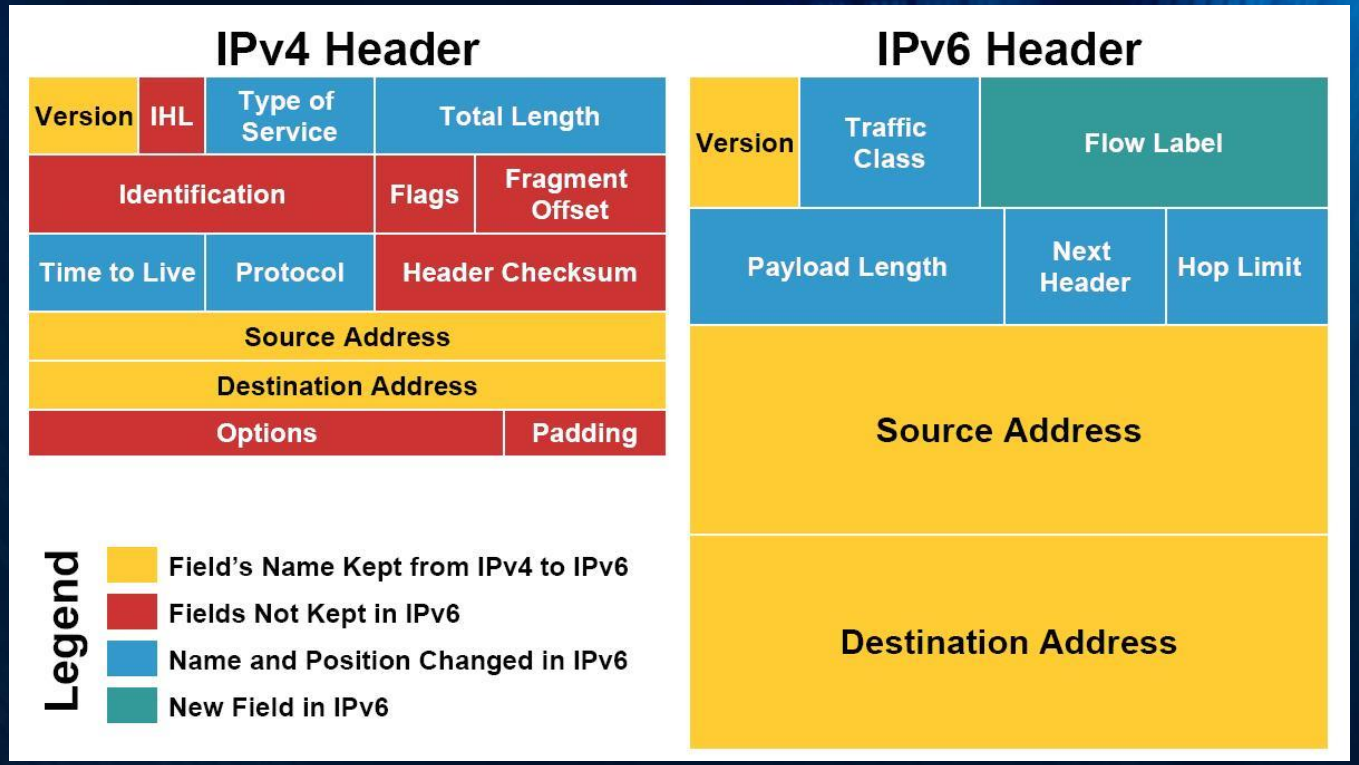


Itens Indispensáveis:

- Router (interno e Gateway externo se Internet)
- Switch (concentrador, distribuidores e Switches de borda)
- Servidores
- Endpoint (estações ou BYD)

Rede LAN

Pacote IP



O IP não valida se o endereço IP de origem contido em um pacote realmente veio dessa origem. Por esse motivo, os agentes de ameaças podem enviar pacotes usando um endereço IP de origem falsificado. Os atacantes também podem adulterar os outros campos do cabeçalho IP para realizar seus ataques.

Rede LAN

Ataques a Pacote IP

Ataques ICMP - Os agentes de ameaças usam pacotes de eco (pings) do protocolo de mensagens de controle da Internet (ICMP) para descobrir sub-redes e hosts em uma rede protegida, para gerar ataques de inundação DoS ou para alterar as tabelas de rotas.

- Solicitação de eco ICMP e resposta de eco: Usado para realizar verificação de host e ataques DoS.
- ICMP inacessível: Isso é usado para realizar o reconhecimento de rede e ataques de varredura.
- Resposta de máscara ICMP: usado para mapear uma rede IP interna.
- Redirecionamentos ICMP: usado para atrair um host alvo para enviar todo o tráfego através de um dispositivo comprometido e criar um ataque MITM.
- Descoberta de roteador ICMP: usado para injetar entradas de rota falsas na tabela de roteamento de um host de destino.

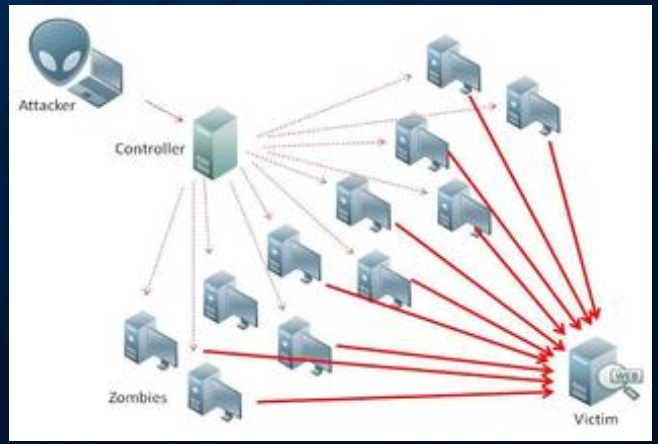
Rede LAN

Ataques a Pacote IP

ICMP Smurf - É um ataque distribuído de negação de serviço (DDoS) distribuído pela rede, com o nome do malware DDoS.Smurf que permite sua execução. Os ataques Smurf são um tipo de inundações por ping, já que ambos são realizados pelo envio de uma série de solicitação de pacotes ICMP (Internet Control Message Protocol)

Amplificação – O agente da ameaça encaminha mensagens de solicitação de eco ICMP para muitos hosts. Essas mensagens contêm o endereço IP de origem da vítima.

Reflexão – Todos esses hosts respondem ao endereço IP falsificado da vítima para sobrecarregá-lo.



Rede LAN

Ataques a Pacote IP

Ataques de falsificação de IP (ip spoofing) - Os ataques de falsificação de endereço IP ocorrem quando um agente de ameaça cria pacotes com informações de endereço IP de origem falsas para ocultar a identidade do remetente ou para se passar por outro usuário legítimo. O spoofing geralmente é incorporado a outro ataque, como um ataque de Smurf.

Spoofing não cego – O atacante pode ver o tráfego que está sendo enviado entre o host e o destino.

Spoofing cego – O atacante não pode ver o tráfego que está sendo enviado entre o host e o destino. A falsificação cega é usada em ataques DoS.

Rede LAN

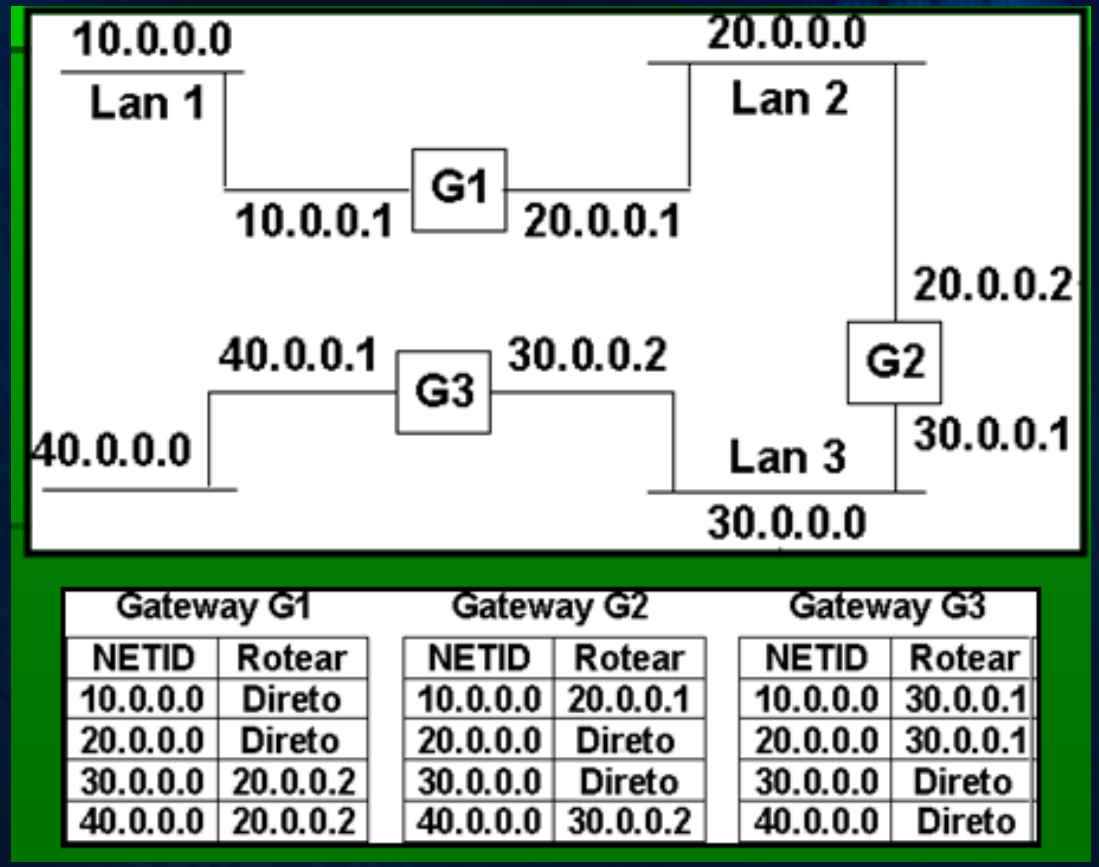
Ataques a Pacote IP

Ataques de falsificação de IP (ip spoofing) - Os agentes de ameaças falsificam o endereço IP de origem em um pacote IP para executar falsificação cega ou não cega.

Ataque man-in-the-middle (MITM) Os atores da ameaça se posicionam entre uma origem e um destino para monitorar, capturar e controlar a comunicação de forma transparente. Eles podiam espionar inspecionando pacotes capturados ou alterar pacotes e encaminhá-los para seu destino original.

Rede LAN

Roteador



Gateway G1	
NETID	Rotear
10.0.0.0	Direto
20.0.0.0	Direto
30.0.0.0	20.0.0.2
40.0.0.0	20.0.0.2

Gateway G2	
NETID	Rotear
10.0.0.0	20.0.0.1
20.0.0.0	Direto
30.0.0.0	Direto
40.0.0.0	30.0.0.2

Gateway G3	
NETID	Rotear
10.0.0.0	30.0.0.1
20.0.0.0	30.0.0.1
30.0.0.0	Direto
40.0.0.0	Direto

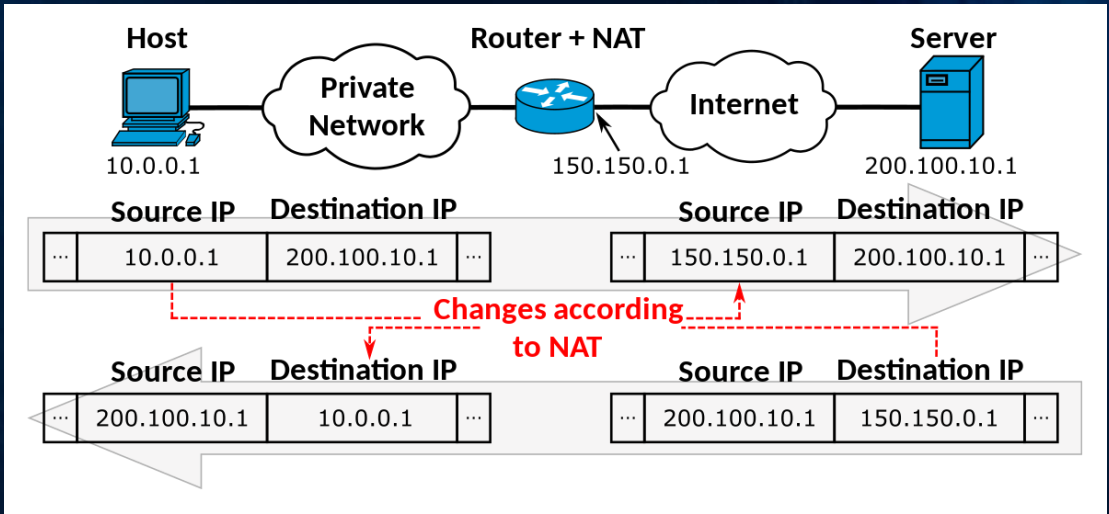
Tabela de Rotas

Uma tabela de rotas contém um conjunto de regras, chamado de rotas, que determinam para onde o tráfego de rede de sua sub-rede ou gateway é direcionado.

Cada tabela contém uma lista de destinos com prefixos de endereços IP para os quais o pacote pode ser encaminhado. O atacante que obtém controle do Router tem acesso para editar a tabela e incluir rotas para serviços protegidos.

Rede LAN

Roteador



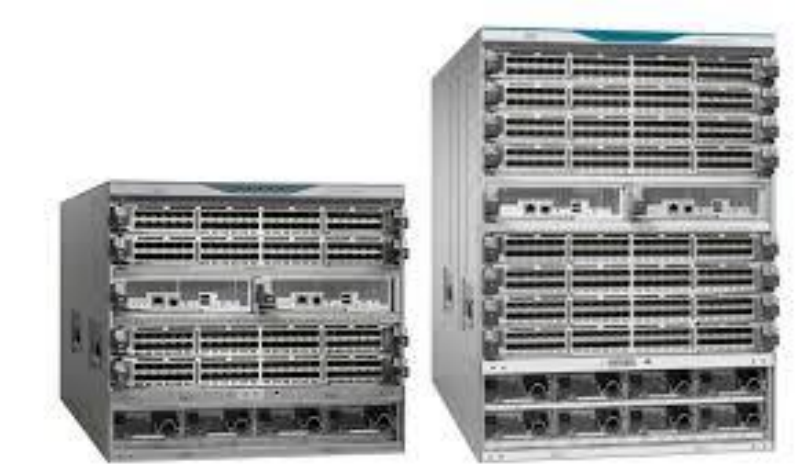
NAT

NAT (Network Address Translation) é um recurso que permite que uma mesma conexão e endereço IP sejam compartilhados com diversos computadores de forma transparente. Toda a conexão dos clientes irá passar pelo servidor NAT (que também é chamado de Gateway).

O Atacante pode redirecionar as respostas do servidor.

Rede LAN

Switch Concentrador



Switch core é o termo associado aos comutadores centrais de grandes infraestruturas de TI, ou seja, aqueles que centralizam o tráfego de dados de outros switches.

Esses equipamentos podem concentrar o tráfego de centenas (ou milhares) de dispositivos conectados (end-points), por isso precisam de funcionalidades específicas como operar em Layer 3 (Camada 3)

Rede LAN

Switch Distribuidor

O switch de distribuição é um elemento intermediário entre os switches core e os switches de borda. Esses equipamentos normalmente são utilizados em redes locais de empresas de grande porte, geralmente com múltiplos prédios e centenas de dispositivos conectados. Os switches de distribuição são adicionados em redes maiores, que necessitam de mais uma camada de comutação e tem como papel principal limitar a quantidade de conexões de um switch core.

Rede LAN

Switch de Borda

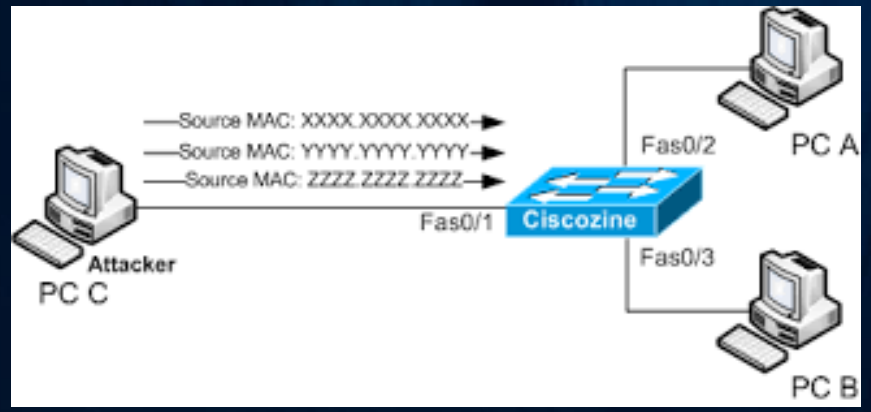
O switch de borda ou de acesso é o único comutador que interage diretamente com dispositivos operados por usuários finais como computadores, câmeras CFTV e impressoras. Esse tipo de switch é o responsável pela conexão de todos os end-points ao backbone da rede.

Geralmente esses Switchs são apenas redirecionadores na camada 2 e gerenciados pelos distribuidores ou core.

Rede LAN

Ataques a Switch

MAC flooding - Subir endereços MAC falsos em um Switch é uma técnica utilizada para realizar um ataque conhecido como "encher a memória do Switch". Esse ataque faz com que o Switch atue como um Hub, o que permite que todas as informações que passam por ele sejam acessíveis a todos os usuários conectados.



Rede LAN

Ataques a Switch

MAC spoofing - Um ataque de MAC spoofing consiste em alterar o endereço MAC de um dispositivo de rede (placa de rede). Como resultado, um invasor pode redirecionar dados enviados para um dispositivo para outro dispositivo e obter acesso a esses dados. Ataques de falsificação de endereço MAC são usados quando os atores da ameaça têm acesso à rede interna.

Os atacantes alteram o endereço MAC de seu host para corresponder a outro endereço MAC conhecido de um host de destino. O host de ataque então envia um quadro por toda a rede com o endereço MAC recém-configurado. Quando o switch recebe o quadro, ele examina o endereço MAC de origem. O switch sobrescreve a entrada da tabela CAM atual e atribui o endereço MAC à nova porta.

Etapa 04