4. Seguridad de Redes

Ing. Pedro Escudero

Telf: 0994667184
Mail: pedro.escudero@unach.edu.ec
Web: https://www.researchgate.net/profile/Pedro-Escudero-3/research

Junio- 2025

Contents

Problemas de Seguridad de redes • IP

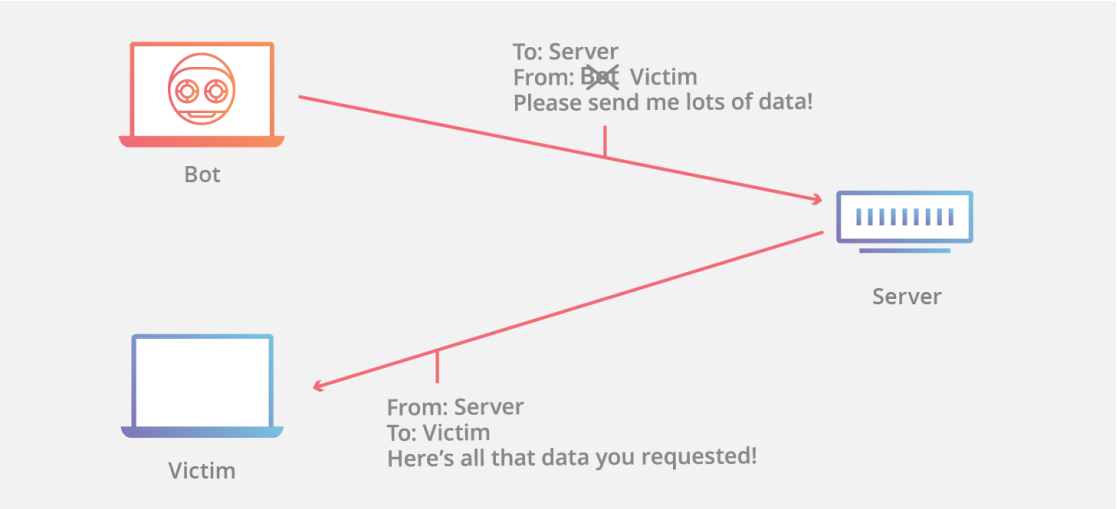
1. IP Spoofing
2. ARP spoofing
3. Ataques a protocolos de ruteo
4. TCP session Hijacking, SYN
5. Flooding
6. problemas DNS
7. Ataques VLAN

1. IP Spoofing

El **IP Spoofing** es una técnica utilizada en ciberataques para falsificar la dirección IP de origen en los paquetes enviados a través de una red. El objetivo es hacer que el tráfico parezca provenir de una fuente confiable en lugar del atacante.

Definición de IP Spoofing

El IP Spoofing es una técnica utilizada en ciberataques para falsificar la dirección IP de origen en los paquetes enviados a través de una red. El objetivo es hacer que el tráfico parezca provenir de una fuente confiable en lugar del atacante.



Cómo funciona el IP Spoofing

El atacante construye paquetes IP con una dirección IP de origen falsificada.
Los dispositivos receptores creen que los paquetes provienen de una dirección IP confiable.
Dependiendo del ataque, los paquetes pueden usarse para:

- Ocultar la identidad del atacante.
- Desviar tráfico.
- Ejecutar ataques como DoS o Man-in-the-Middle.

Tipos de ataques que emplean IP Spoofing

1. Ataque de Denegación de Servicio Distribuido (DDoS):
   Los atacantes usan direcciones IP falsificadas para enviar grandes cantidades de tráfico a un servidor, abrumándolo y causando interrupciones.

2. Ataque Man-in-the-Middle (MITM):
   El atacante usa IP Spoofing para interceptar o alterar datos entre dos partes confiables.

3. Sesión TCP Hijacking:
   El atacante falsifica la dirección IP para hacerse pasar por una parte en una sesión de comunicación, ganando acceso no autorizado.

Ejercicio práctico sobre IP Spoofing (en un entorno seguro)

Nota ética: Este ejercicio debe realizarse únicamente en un entorno controlado y con fines educativos. Cualquier uso fuera de este contexto es ilegal.

Requisitos:

- Un entorno de red virtualizado (como VirtualBox o VMware).
- Herramientas de análisis y manipulación de paquetes como Scapy (Python) o hping3 (Kali Linux).

Pasos:

1. **Configurar el entorno:**
   Crea una red virtual con al menos dos dispositivos: una víctima y un atacante.

2. **Falsificar paquetes con una dirección IP falsa (usando Scapy):**

En una máquina atacante, crea un script en Python para enviar paquetes con una dirección IP de origen falsificada:

```
from scapy.all import * ip = IP(src="192.168.1.100",
dst="192.168.1.101") # Dirección IP falsificada
icmp = ICMP()
packet = ip/icmp
send(packet, count=5) # Envía 5 paquetes ICMP
```

Pasos:

1. **Configurar el entorno:**
   Crea una red virtual con al menos dos dispositivos: una víctima y un atacante.

2. **Falsificar paquetes con una dirección IP falsa (usando Scapy):**

   En una máquina atacante, crea un script en Python para enviar paquetes con una dirección IP de origen falsificada:

```
from scapy.all import * ip = IP(src="192.168.1.100",
dst="192.168.1.101") # Dirección IP falsificada
icmp = ICMP()
packet = ip/icmp
send(packet, count=5) # Envía 5 paquetes ICMP
```

Cambia src por la IP que deseas falsificar y dst por la dirección IP de la víctima.

Pasos:

Observa el tráfico (opcional):

Usa Wireshark en la máquina víctima para capturar los paquetes y verificar que parecen venir de la dirección IP falsificada.

Mitigación del ataque:

- Configura filtrado de paquetes en los routers y firewalls para bloquear paquetes con direcciones IP de origen no válidas.
- Implementa Sistemas de Detección de Intrusos (IDS) para identificar y alertar sobre tráfico sospechoso.
- Utiliza técnicas como uRPF (Unicast Reverse Path Forwarding) en redes corporativas para verificar la legitimidad de las direcciones IP..

2. ARP Spoofing

ARP Spoofing

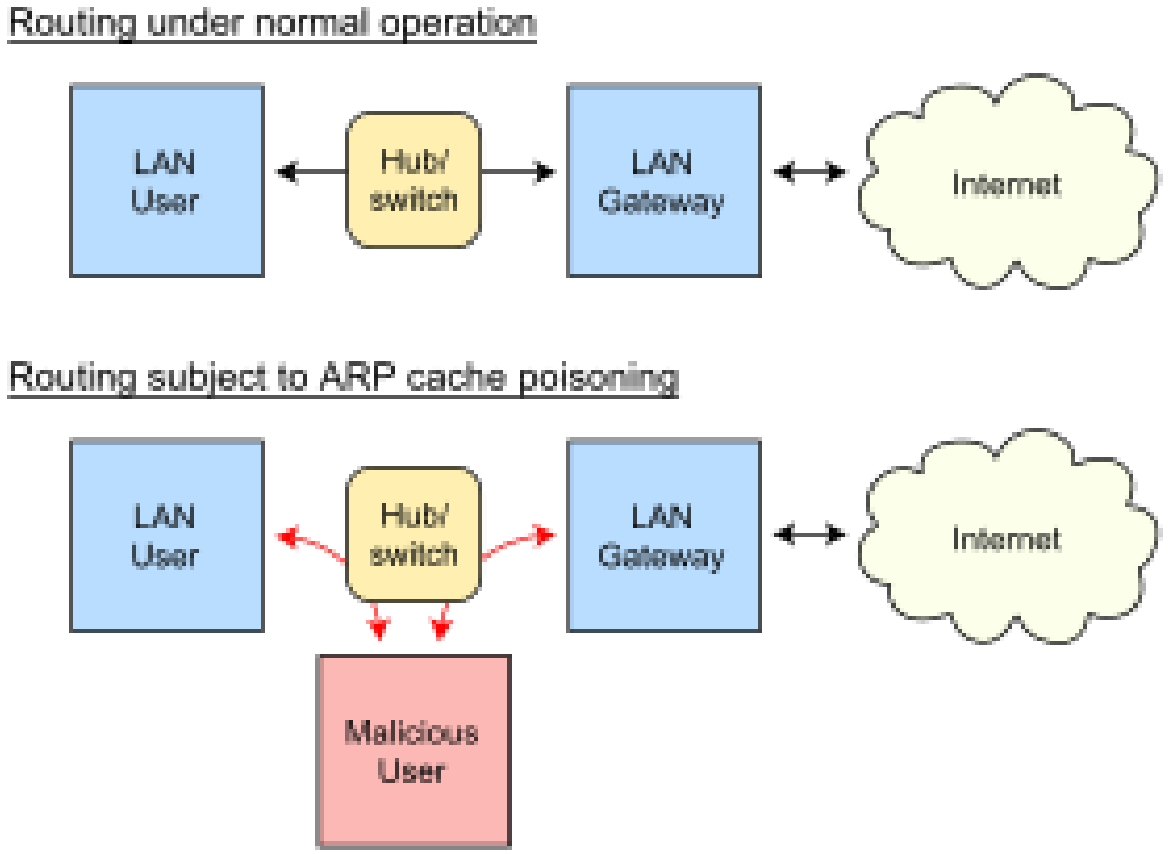
ARP Spoofing (también conocido como ARP Poisoning) es un ataque en redes de computadoras en el que un atacante envía mensajes ARP (Address Resolution Protocol) falsificados a una red local. Esto hace que los dispositivos conectados en esa red asocien la dirección MAC del atacante con la dirección IP de otro dispositivo legítimo (como un router o un servidor).

El objetivo principal del ataque es:

1. **Interceptar tráfico:** El atacante puede redirigir y capturar datos transmitidos entre dispositivos.
2. **Modificar tráfico:** El atacante puede alterar la información transmitida.
3. **Interrumpir la comunicación:** A través de un ataque de denegación de servicio (DoS).

Pasos:

1. El atacante envía respuestas ARP falsas que contienen la dirección MAC del atacante, haciendo creer a las víctimas que esa es la dirección legítima para una IP específica.
2. Las víctimas actualizan su tabla ARP con la dirección MAC falsa, redirigiendo el tráfico hacia el atacante.
3. El atacante puede reenviar los datos hacia el destino legítimo (ataque "man-in-the-middle") o bloquearlos por completo.



Ejercicio práctico sobre ARP Spoofing:

Importante: Este ejercicio debe realizarse únicamente en un entorno controlado, como una red de laboratorio o un simulador, y con el permiso explícito de todos los involucrados. Utilizar estas técnicas fuera de estos contextos puede ser ilegal.

Objetivo:

Realizar una simulación de un ataque de ARP Spoofing en un entorno seguro para comprender su funcionamiento.

Requisitos:

- Un entorno de red virtualizado (como VirtualBox o VMware).
- Herramienta de pentesting, como **Cain & Abel**, **Ettercap**, o **arpspoof** (disponible en **Kali Linux** https://www.kali.org/).
- Mínimo 2 máquinas virtuales: una víctima y un atacante.
- Gateway (opcional): Maquina virtual con **pfSense**, o tambien se puede habilitar redirección de paquetes en Ubuntu

Ejercicio práctico sobre ARP Spoofing:

Pasos:

1. Configurar la red virtual:

- Crear una red local (LAN) con dos dispositivos: un cliente y un atacante.
- Asegurarte de que ambos dispositivos estén en la misma red.

2. Identificar las direcciones IP y MAC:

- En la máquina atacante, usa arp -a para listar los dispositivos en la red.
- Identifica la dirección IP y MAC de la víctima y el gateway (router).

3. Lanzar el ataque ARP Spoofing:

- En Kali Linux, ejecuta el siguiente comando con la herramienta arpspoof:

```
arpspoof -i <interface> -t <IP_de_la_victima> <IP_del_gateway>
```

- Esto enviará respuestas ARP falsas a la víctima, asociando la IP del gateway con la dirección MAC del atacante.

Ejercicio práctico sobre ARP Spoofing:

Pasos:

4. Capturar tráfico

Usa una herramienta como Wireshark para observar los paquetes interceptados durante el ataque.

5. Mitigar el ataque:

- Habilitar tablas ARP estáticas en la máquina víctima para prevenir modificaciones.
- Implementar herramientas como ARPwatch o switches con protección contra ARP Spoofing.

Pregunta para reflexionar:

¿Qué soluciones prácticas se pueden implementar en redes reales para mitigar este tipo de ataques?

3. Ataques a protocolos de enrutamiento

Ataques a protocolos de enrutamiento

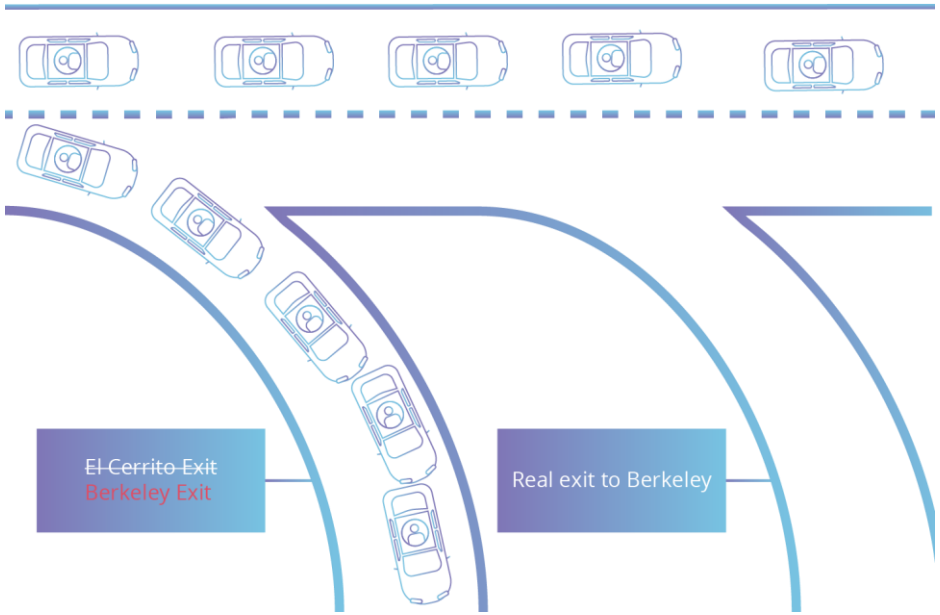
Los ataques a protocolos de enrutamiento buscan explotar vulnerabilidades en los protocolos utilizados para el intercambio de información entre routers, comprometiendo la integridad, disponibilidad o confidencialidad de la red. Estos ataques pueden afectar redes pequeñas y grandes, como las de los Proveedores de Servicios de Internet (ISP) y sistemas autónomos (AS).

Tipos:

1. Falsificación de rutas (Route Injection)

Descripción: Un atacante inyecta información de enrutamiento falsa en la red, desviando el tráfico hacia rutas incorrectas, interrumpiendo la conectividad o interceptando los datos.

Ejemplo: Un atacante que utiliza el protocolo BGP (Border Gateway Protocol) para anunciar prefijos de red falsos.



Ataques a protocolos de enrutamiento “Hijacking

Tipos:

2. Ataques de suplantación (Spoofing)

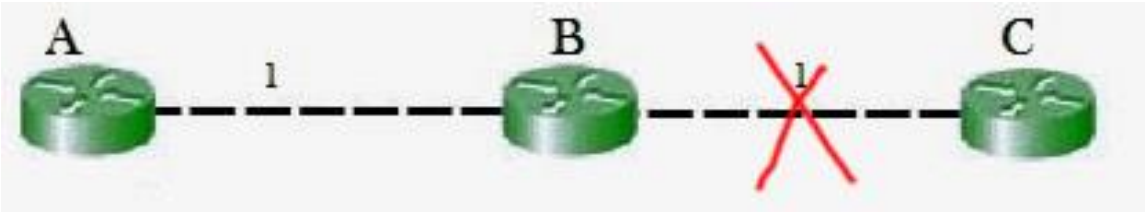
Descripción: El atacante falsifica su identidad para actuar como un router legítimo y participar en la comunicación de enrutamiento.

Ejemplo: Suplantar un router en un protocolo como OSPF (Open Shortest Path First) para modificar las rutas anunciadas.

3. Ataques de actualización maliciosa (Routing Table Poisoning)

Descripción: Se inyecta información incorrecta en la tabla de enrutamiento de los routers, causando que envíen tráfico a rutas no deseadas.

Ejemplo: Modificar las métricas de enlace en RIP (Routing Information Protocol) para preferir rutas menos eficientes.



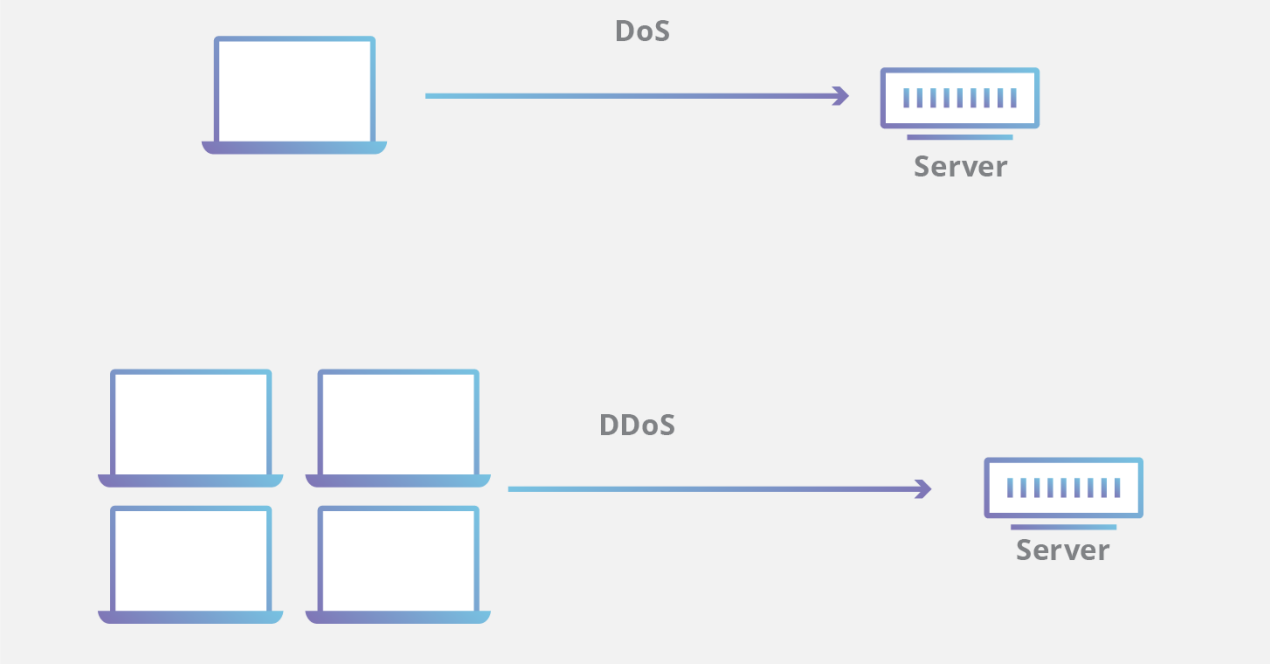
Ataques a protocolos de enrutamiento

Tipos:

4. Ataques de denegación de servicio (DoS/DDoS)

Descripción: Los atacantes generan un gran volumen de tráfico dirigido a los routers o al protocolo de enrutamiento, agotando sus recursos y provocando fallos en la red.

Ejemplo: Saturar un router con actualizaciones de enrutamiento falsas.



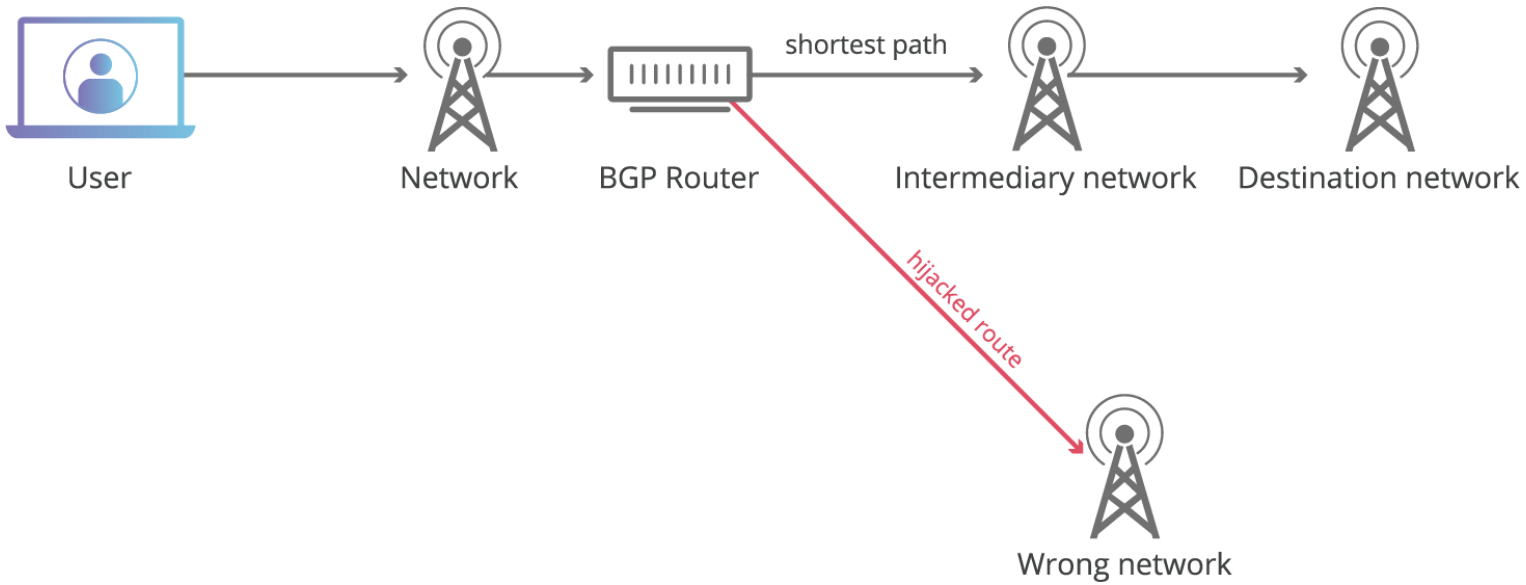
Ataques a protocolos de enrutamiento

Tipos:

5. Secuestro de rutas (Route Hijacking)

Descripción: Un atacante anuncia de forma maliciosa un prefijo de red legítimo como propio, redirigiendo el tráfico.

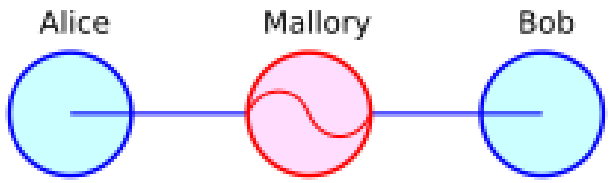
Ejemplo: Un router malicioso anuncia un prefijo IP de un cliente legítimo a través de BGP, interceptando tráfico global.



Ataques a protocolos de enrutamiento

Tipos:

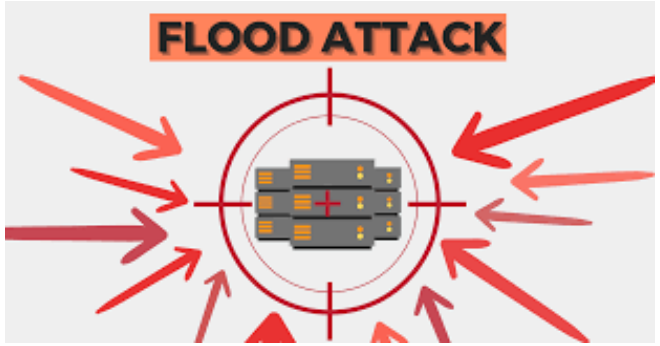
6. Ataques de hombre en el medio (MITM)



Descripción: Un atacante intercepta el tráfico enrutado y lo redirige a su dispositivo antes de enviarlo al destino legítimo.

Ejemplo: En redes que usan OSPF, un atacante podría modificar los enlaces para colocarse como puente entre routers.

7. Ataques de saturación de actualizaciones (Update Flooding)



Descripción: Un atacante envía grandes cantidades de actualizaciones de enrutamiento no válidas, sobrecargando la capacidad de procesamiento de los routers.

Ejemplo: Enviar actualizaciones constantes en RIP para obligar al router a recalcular rutas continuamente.

Protocolos de enrutamiento vulnerables

1. **RIP (Routing Information Protocol):**

   Basado en distancia; fácil de manipular por la falta de autenticación robusta.

2. **OSPF (Open Shortest Path First):**

   Más seguro que RIP, pero puede ser vulnerable a ataques si se omiten medidas de autenticación.

3. **BGP (Border Gateway Protocol):**

   Usado entre sistemas autónomos; particularmente vulnerable a secuestro de rutas y falsificación de anuncios.

4. **EIGRP (Enhanced Interior Gateway Routing Protocol):**

   Tiene mejores medidas de autenticación, pero puede ser explotado si estas no se configuran correctamente.

Medidas de mitigación

Autenticación robusta:

Implementar autenticación mediante contraseñas seguras o algoritmos criptográficos (MD5, SHA) en protocolos como OSPF y BGP.

Filtros de prefijos:

Restringir los prefijos que los routers pueden anunciar para evitar inyecciones de rutas maliciosas.

Monitoreo continuo:

Usar herramientas para detectar anomalías en el tráfico o las rutas anunciadas.

Segregación de redes:

Aislar redes críticas para evitar que ataques en una red afecten a otras.

Actualizaciones de firmware y software:

Mantener los routers actualizados con los últimos parches de seguridad.

Implementación de RPKI (Resource Public Key Infrastructure):

Validar que las rutas anunciadas por BGP provengan de fuentes legítimas.

Ejercicio práctico: Simulación de un ataque BGP Hijacking en un entorno controlado

Objetivo:

Comprender cómo un atacante puede secuestrar rutas y redirigir tráfico en redes BGP.

Guía práctica: GSR-GP_4-3 – BGP Hijacking.pdf

4. TCP session Hijacking, SYN

TCP session Hijacking, SYN

TCP Session Hijacking es un ataque en el que un atacante intercepta o toma el control de una sesión activa entre un cliente y un servidor en una conexión TCP. El atacante explota la confianza entre ambos extremos de la comunicación, engañando a una de las partes para que piense que sigue hablando con la contraparte legítima.

Pasos de un ataque de TCP Session Hijacking

1. **Monitorización del tráfico (Sniffing):**
   El atacante captura los paquetes de la conexión TCP para obtener información clave, como direcciones IP, puertos y números de secuencia (sequence numbers).

2. **Predicción del número de secuencia:**
   El atacante debe calcular o adivinar el número de secuencia actual en la sesión, que es crítico para enviar paquetes válidos.

3. **Inyección de paquetes:**
   Una vez que el atacante predice correctamente el número de secuencia, puede enviar paquetes maliciosos que parecen venir del cliente o el servidor.

4. **Finalización de la conexión original:**
   En algunos casos, el atacante envía paquetes RST (Reset) o FIN (Finish) para desconectar al cliente legítimo y tomar control total de la sesión.

SYN Attack y Relación con TCP Session Hijacking

Un ataque SYN (también llamado SYN Flood) está relacionado con el inicio de las conexiones TCP, pero tiene un objetivo diferente. Mientras que el TCP Session Hijacking busca apoderarse de una sesión establecida, el ataque SYN busca explotar el proceso de establecimiento de la conexión TCP.

1. **Proceso de conexión TCP (Three-Way Handshake):**
   - El cliente envía un paquete SYN al servidor.
   - El servidor responde con un SYN-ACK.
   - El cliente completa el handshake enviando un ACK.

2. **Ataque SYN Flood:**
   - El atacante envía una gran cantidad de solicitudes SYN sin completar el handshake.
   - Esto consume los recursos del servidor, causando una denegación de servicio (DoS).

Nota: Aunque el SYN Flood y el TCP Session Hijacking son distintos, ambos explotan debilidades en el protocolo TCP

Demostración práctica de TCP Session Hijacking

Entorno requerido:

- Dos máquinas virtuales (cliente y servidor) configuradas en una red local.
- Una máquina del atacante con herramientas como Wireshark (para sniffing) y Scapy (para inyección de paquetes) en Linux.

Ejercicio:

Objetivo: Simular un ataque de TCP Session Hijacking en un entorno seguro.

Paso 1: **Captura de tráfico**

- Usa Wireshark en la máquina del atacante para capturar paquetes en la red.
- Filtra el tráfico para identificar la comunicación TCP entre el cliente y el servidor.

Paso 2: Predicción del número de secuencia

- Observa los números de secuencia en los paquetes capturados.
- Estima el próximo número de secuencia del cliente

Demostración práctica de TCP Session Hijacking

Paso 3: Inyección de paquetes

- Usa Scapy para crear y enviar un paquete TCP con el número de secuencia correcto.
- Incluye un mensaje malicioso o comandos en el payload.

Paso 4: Verifica el control

- Observa si el servidor responde al atacante en lugar del cliente legítimo.
- Verifica si el cliente original pierde la conexión.

Precaución:

Este ejercicio debe realizarse únicamente en un entorno controlado y con fines educativos. Los ataques de TCP Session Hijacking están prohibidos en redes no autorizadas.

Prevención de TCP Session Hijacking

1. **Cifrado del tráfico:**
    - Implementa SSL/TLS para proteger las sesiones TCP.
    - Esto hace que los datos interceptados sean ininteligibles para el atacante.
2. **Uso de firewalls y sistemas IDS/IPS:**
    - Monitorean la red en busca de patrones anómalos.
3. **Gestión adecuada de números de secuencia:**
    - Modernos sistemas operativos utilizan números de secuencia aleatorios.
4. **Autenticación adicional:**
    - Protocolos como SSH incluyen autenticación para validar cada comando enviado.

4. Problemas DNS

Problemas DNS

Los ataques de seguridad relacionados con DNS son una preocupación crítica, ya que pueden comprometer la integridad, disponibilidad y confidencialidad de las comunicaciones en línea.

1. Tipos de Ataques de Seguridad DNS

a) DNS Spoofing (DNS Cache Poisoning)

Descripción: Un atacante manipula las respuestas DNS para redirigir a los usuarios a sitios web maliciosos.

Método:

- Inserta información falsa en la caché DNS de un servidor.
- Usa respuestas no autenticadas para reemplazar registros legítimos.

Impacto: Redirige a víctimas a sitios fraudulentos para robo de datos o distribución de malware.

Prevención:

- Implementar DNSSEC (DNS Security Extensions) para verificar la autenticidad de las respuestas DNS.
- Configurar servidores DNS para no aceptar respuestas no solicitadas.

Problemas DNS

b) Hijacking de DNS

Descripción: El atacante toma el control de los registros DNS de un dominio para desviar el tráfico.

Método:

- Compromete credenciales de acceso al registrador del dominio.
- Modifica los registros DNS (A, CNAME, MX, etc.).

Impacto: Redirige tráfico legítimo a sitios maliciosos o interrumpe servicios.

Prevención:

- Habilitar la autenticación de dos factores (2FA) en el registrador de dominio.
- Monitorear y auditar regularmente los cambios en los registros DNS.
- Usar bloqueos de dominio en el registrador para evitar modificaciones no autorizadas.

Problemas DNS

c) Ataques DDoS en DNS

Descripción: Un atacante satura un servidor DNS con grandes volúmenes de tráfico para hacerlo inaccesible.

Método:

- Uso de bots para enviar consultas masivas.
- Ampliación del tráfico mediante DNS Amplification.

Impacto: Interrumpe la resolución DNS, dejando inactivos servicios y sitios web.

Prevención:

- Usar servicios de DNS con protección DDoS, como Cloudflare o AWS Route 53.
- Configurar límites de tráfico en el servidor DNS.
- Habilitar medidas de rate-limiting en los firewalls.

Problemas DNS

d) Tunneling DNS

Descripción: Se utiliza el protocolo DNS para transmitir datos maliciosos o robar información de la red.

Método:

- Codificación de datos en las consultas/respuestas DNS.

Impacto: Exfiltración de datos confidenciales sin detección.

Prevención:

- Monitorear el tráfico DNS en busca de patrones inusuales.
- Restringir el uso de servidores DNS externos en la red.
- Utilizar herramientas para detectar y bloquear tunneling, como firewalls de próxima generación (NGFW).

Problemas DNS

e) NXDOMAIN Attack

Descripción: Un atacante envía múltiples consultas DNS para dominios inexistentes, sobrecargando el servidor.

Método:

- Genera consultas DNS para dominios aleatorios que no existen.

Impacto: Agota recursos del servidor y reduce la calidad del servicio.

Prevención:

- Implementar listas de bloqueo (blacklists) y configuraciones para limitar el impacto de dominios inexistentes.
- Usar servicios DNS de alta disponibilidad.

2. Contramedidas Generales contra Ataques DNS

1. **Habilitar DNSSEC:**

   Autentica la información DNS mediante firmas digitales.

2. **Configurar Firewalls y IDS/IPS:**

   Monitorean y bloquean tráfico DNS sospechoso.

3. **Usar Servidores DNS Confiables:**

   Utiliza servicios DNS robustos y seguros como Google DNS, Cloudflare o Quad9.

4. **Actualizar Software DNS:**

   Asegúrate de que el servidor DNS esté actualizado para corregir vulnerabilidades conocidas.

5. **Implementar Monitoreo de Tráfico:**

   Usa herramientas como Wireshark o Splunk para analizar el tráfico DNS en busca de anomalías.

6. **Educación y Buenas Prácticas:**

   Capacita a los administradores y usuarios para identificar posibles señales de ataques y proteger sus credenciales.

3. Ejemplo Práctico: DNS Spoofing

Simulación de un Ataque (Laboratorio Seguro):

Requisitos:

- Kali Linux (para simular el ataque).
- Un servidor DNS local.

Pasos:

1. Configura un servidor DNS en una red local.
2. Usa herramientas como dnsspoof o ettercap para manipular respuestas DNS.
3. Observa cómo las consultas legítimas son redirigidas a direcciones IP maliciosas.

Advertencia: Solo realizar estas simulaciones en entornos controlados y con permisos adecuados.

5. Ataques VLAN

5. Ataques VLAN

Los ataques a VLAN (Virtual Local Area Network) son amenazas que explotan vulnerabilidades en redes que utilizan segmentación virtual para separar el tráfico de datos. Aunque las VLANs mejoran la seguridad y la eficiencia de la red, pueden ser objeto de diversas técnicas de ataque si no están configuradas adecuadamente.

Tipos de Ataques VLAN

1. VLAN Hopping

Descripción: Este ataque permite a un atacante enviar tráfico de una VLAN a otra, eludiendo las restricciones de segmentación.

Métodos Comunes:

Switch Spoofing:

- El atacante configura su dispositivo para comportarse como un switch.
- Envía tramas etiquetadas como si fuera un dispositivo legítimo, ganando acceso a múltiples VLANs.

5. Ataques VLAN

Double Tagging:

- El atacante envía paquetes con dos etiquetas VLAN (802.1Q).
- El primer switch elimina la etiqueta externa y reenvía el paquete a una VLAN no autorizada.

Prevención:

- Deshabilitar los puertos trunk en los switches, excepto donde sea estrictamente necesario.
- Configurar las VLAN nativas en puertos trunk a una VLAN no utilizada.
- Habilitar mecanismos de seguridad en el switch, como DTP (Dynamic Trunking Protocol) deshabilitado.

5. Ataques VLAN

2. Ataques de ARP Spoofing en VLANs

Descripción:

Un atacante utiliza ARP Spoofing para interceptar o redirigir tráfico dentro de una VLAN específica.

Impacto: Permite realizar ataques como Man-in-the-Middle (MITM).

Prevención:

- Implementar seguridad en las tablas ARP con Dynamic ARP Inspection (DAI).
- Utilizar switches administrados con funciones avanzadas de seguridad.

3. Ataques de Flooding de MAC

Descripción: El atacante satura la tabla de direcciones MAC de un switch, forzándolo a actuar como un hub y enviar tráfico a todos los puertos.
Impacto: Exposición de tráfico de VLAN a dispositivos no autorizados.
Prevención:

1. Habilitar Port Security en los switches para limitar el número de direcciones MAC por puerto.
2. Monitorear tráfico para identificar patrones anómalos.

5. Ataques VLAN

4. VLAN Bypass

Descripción: Un atacante utiliza vulnerabilidades en la configuración de VLANs para superar las restricciones de segmentación.

Métodos:

- Configuración incorrecta de puertos.
- Uso de VLAN predeterminadas.

Prevención:

- Revisar y auditar las configuraciones de VLAN regularmente.
- Asegurarse de que las VLAN predeterminadas no se utilicen para tráfico crítico

5. Ataques VLAN

5. Inter-VLAN Routing Exploitation

Descripción: Un atacante aprovecha errores en la configuración de rutas entre VLANs para acceder a redes restringidas.

Prevención:

- Implementar reglas estrictas de firewall para controlar el tráfico inter-VLAN.
- Usar Access Control Lists (ACLs) para definir políticas de acceso.

Medidas de Protección General para VLANs

1. **Configurar VLANs Nativas:** Asignar la VLAN nativa de los puertos trunk a una VLAN no utilizada.
2. **Habilitar Port Security:** Limitar el número de direcciones MAC permitidas por puerto y bloquear dispositivos no autorizados.
3. **Deshabilitar DTP (Dynamic Trunking Protocol):** Configurar manualmente los puertos trunk en lugar de permitir la negociación automática.
4. **Separación de Tráfico Crítico:** Colocar sistemas críticos (servidores, dispositivos de seguridad) en VLANs separadas y protegidas.
5. **Habilitar 802.1X:** Autenticar dispositivos que se conectan a la red para garantizar acceso autorizado.
6. **Monitorizar la Red:** Usar herramientas de análisis para detectar tráfico anómalo y posibles ataques.
7. **Implementar DAI y DHCP Snooping:** Proteger contra ataques como ARP Spoofing y asignaciones maliciosas de direcciones IP

Ejemplo Práctico: VLAN Hopping (Double Tagging)

Simulación Controlada:

- **Requisitos:**
  - Un switch administrado.
  - Dos dispositivos configurados en diferentes VLANs.
- **Pasos:**
  - Configura el switch con VLANs separadas para cada dispositivo.
  - En el dispositivo atacante, utiliza herramientas como Scapy para crear paquetes etiquetados con dos VLANs.
  - Observa cómo el switch procesa las etiquetas y reenvía el tráfico.
- **Contramedidas:**
  - Implementa las prácticas recomendadas descritas arriba.