
8. Sniffers
Julio Javier Iglesias Pérez
C|EH Julio Iglesias Pérez

Amenazas sniffing

- Colocando una tarjeta en la red en modo promiscuo un atacante puede capturar y analizar todo el tráfico de la red.
- Muchos puertos de las empresas están abiertos.
- Un packet sniffer solo puede capturar información de paquetes de una subred.
- Usualmente cualquier laptop puede conectarse a una red y obtener acceso a esta.

Wiretapping

Es el proceso de monitorear conversaciones telefónicas y de internet. Los atacantes conectan un dispositivo de escucha (hardware, software o una combinación de ambos) al circuito de información entre dos teléfonos o host en internet.

Wiretapping

- Un atacante puede robar información sensible "olfateando" una red. Passwords telnet, tráfico email, tráfico web, sesiones de chat, passwords ftp, configuración de routers, tráfico DNS, tráfico syslog, etc.

¿Cómo trabaja un sniffer?

- Coloca a la tarjeta NIC en modo promiscuo así puede escuchar todo el tráfico transmitido en su segmento.
- Puede leer constantemente toda la información que viaja por la red decodificando la información encapsulada en los paquetes de datos.

Tipos de sniffing

- Sniffing pasivo: Significa olfatear a través de un hub. En un hub el tráfico es enviado a todos los puertos.
- Passive sniffing no implica enviar paquetes, y monitorear el tráfico enviado por otros.
- Active sniffing implica enviar múltiples sondas de red para identificar APs.
- El uso de hubs está obsoleto hoy en día. Se usan switchs.

Tipos de sniffing

- Active sniffing: Cuando se realiza sniffing en una red switcheada se lo llama active sniffing.
- El olfateo activo se basa en inyectar paquetes (ARP) en una red.

Protocolos vulnerables al sniffing

- Telnet y Rlogin, HTTP, SMTP, NNTP, POP, FTP, IMAP.

- Es decir, datos enviados en texto claro

Protocolos vulnerables al sniffing

La capa donde trabaja el sniffer es en la de Data Link (enlace) del modelo OSI, por lo que no se adhieren a las mismas reglas como las aplicaciones y los servicios que residen en capas superiores.

Si alguna de las capas es hackeada, las comunicaciones están comprometidas sin que otras capas lo sepan.

Analizadores de protocolo de hardware

Es una pieza de equipo que captura las señales sin alterar el tráfico en un segmento de un cable.

Puede ser utilizado para monitorear el uso de una red e identificar tráfico de red malicioso generado por software un software de hacking instalado en la red.

Captura paquetes de datos y decodifica y analiza su contenido de acuerdo a ciertas reglas predeterminadas.

Algunos ejemplos de estos hardwares son: Agilent N2X N5540AS, Agilent E2960B, RADCOM PrismLite Protocol Analyzer, Flune Networks Optiview Network Analyzaer, etc.

Ataques MAC

MAC Flooding

1. Implica floodear el switch con numerosas solicitudes.
2. Los Swtiches tienen memoria limitada para mapear varias direcciones MAC a los puertos físicos en el switch.
3. MAC Flooding hace uso de esta limitación bombardeando el switch con direcciones MAC falsas hasta que el switch ya no pueda mantenerse.
4. Entonces el switch actúa como un hub difundiendo paquetes a todos los equipos en la red y los atacantes olfatean el tráfico fácilmente.

Ataques MAC

Direcciones MAC/Tabla CAM

Las tablas CAM (Content Addresable Memory) tienen tablas fijas. Almacenan información como direcciones MAC disponibles en puertos físicos con sus parámetros VLAN asociados.

Ataques MAC

¿Qué pasa cuando la tabla CAM está llena?

Tráfico de solicitudes ARP inundarán cada puerto en el switch. Básicamente esto cambia el switch a un hub. Este ataque también llenará las tablas CAM de switches adyacentes.

Ataques MAC

Herramienta macof: Es una herramienta Linux que es parte de la colección de dnsiff. Envía fuentes MAC al aleatorias y una dirección IP. Esta herramienta floodea el las tablas CAM del switch (131,000) por minuto enviado entradas MAC falsas.

Otras herramientas: Yersinia

¿Cómo defenderse de ataques MAC?

Configurando la seguridad de los puertos de los switch Cisco:

1. switchport port-security
2. switchport port-security maximum 1 vlan access
3. switchport port-security violation restrict
4. switchport port-security aging time 2
5. switchport port-security aging type inactivity
6. snmp-server enable traps port-security trap-rate 5

Nota: La seguridad del puerto limita los ataques flooding MAC y cierra el puerto y envía una trampa SNMP.

Ataques DHCP

Ataque DHCP Starvation

El atacante manda difusión de discovery request para todo el ámbito DHCP e intenta concesionar todas las direcciones DHCP disponibles en el ámbito. Este es un ataque DoS utilizando concesiones DHCP.

Herramienta de ataque DHCP Starvation: Globbler

Ataques DHCP

Ataque Rogue DHCP

El atacante un servidor DHCP rogue (pillo) en la red para proveer direcciones a los usuarios.

¿Cómo defenderse contra los ataques de DHCP Starvation y Rogue?

Habilitar seguridad del puerto para defenderse contra el ataque starvation.

Comandos del IOS switch

switchport port-security

switchport port-security maximum 1

switchport port-security violation restrict

switchport port-security aging time 2

switchport port-security aging type inactivity

Habilitar DHCP snooping (espionaje) para defenderse contra los ataques rogue.

Comandos IOS switch

```
ip dhcp snooping vlan 4,104
no ip dhpc snooping information option
ip dhcp snooping
```

Ataques ARP Poisoning.

¿Qué es ARP (Address Resolution Protocol)?

Es un protocolo para mapear una dirección IP a una dirección física. El protocolo ARP difunde los equipos de red para encontrar sus direcciones MAC. Cuando un equipo necesita comunicarse con otro, busca la tabla ARP. Si la dirección MAC no se encuentra en la tabla, la ARP es difundida por la red. Todos los equipos compararán en la red su dirección IP y su dirección MAC. Si alguno identifica con su dirección, el equipo responderá y este se almacenará en la tabla ARP y la comunicación se dará.

Ataque ARP Spoofing

Los paquetes ARP pueden ser falsificados para enviar datos al equipo del atacante. ARP Spoofing implica construir un número largo de solicitudes ARP falsificados y responde paquetes para sobrecargar un switch. Los atacantes floodean la caché ARP de un equipo con entradas falsas también conocidas como poisoning. El switch se establece a "forwarding mode" luego de que la tabla ARP es floodeada con respuestas ARP falsas y los atacantes pueden olfatear todos los paquetes de la red.

¿Cómo trabaja el ARP Spoofing?

Cuando un usuario A inicia una sesión con un usuario B en el mismo dominio de difusión en capa2, una solicitud ARP es difundida utilizando el IP del usuario B y el usuario A espera a que el usuario B responda con la máscara de subred.

1. Hola 10.1.1.1 estas ahí??
2. Si, aquí estoy y mi máscara es 1:2:3:4:5:6

Un usuario malicioso escucha a escondidas en la no protegida capa2 y puede responder al usuario A spoofeando la MAC del usuario B.

3. NO, aquí estoy 10.1.1.1 y mi máscara es 9:8:7:6:5:4

Amenazas del ARP Poisoning

- Ataque DoS.
- Intercepción de datos.
- VoIP Call tapping.
- Robo de contraseñas.
- Manipulación de datos.

Todo lo que pase en texto claro será interceptado.

Herramientas para ARP Poisoning: Cain&Abel, WinArpAttacker, Ufasoft Snif.

¿Cómo defenderse contra ARP Poisoning?

- Utilizar la DHCP Snooping Binding Table y la inspección dinámica ARP.
- Revisar la MAC y la IP para ver que el ARP de la interfaz está en la unión.

Configurando DHCP Snooping y Inspección ARP dinámica en switches Cisco

```
ip dhcp snooping
ip dhcp snooping vlan 10
show ip dhcp snooping

show ip dhcp snooping binding

ip arp inspection vlan 10
^Z
show ip arp inspection
```

MAC Spoofing/Duplicando

Este ataque es realizado cuando se olfatea una rec por direcciones MAC de los clientes que activamente están asociados a un puerto del switch y re utilizan otras una de esas direcciones.

Escuchando el tráfico de la red, un usuario malicioso puede interceptar una MAC address legítima de otro usuario para recibir todo el tráfico destinado para ese usuario.

Esta técnica funciona en Wireless AP con el MAC filtering habilitado.

Amenazas de ataques Spoofing

MAC Spoofing

- Si la MAC es utilizada para acceder a la red un atacante puede obtener acceso a la red.
- Un atacante puede asumir la identidad de alguien en la red.

Amenazas de ataques Spoofing

- IP Spoofing
  - Ping de la muerte.
  - ICMP unreachable storm.
  - SYN flood.
  - IPs de confianza pueden ser spoofeados.

Herramentas MAC Spoofing: SMAC

¿Cómo defenderse contra MAC Spoofing?

Utilizar la DHCP Snooping Binding Table, Inspección ARP dinámica e IP Source Guard.

```
sh ip dhcp snooping binding
```

DNS Poisoning

Técnicas DNS Poisoning

1. DNS Poisoning es una técnica que engaña un servidor DNS dentro de uno creíble que fue recibido de la información de autenticación cuando realmente no lo hizo.
2. Lo que hace es sustituir una dirección de un proveedor de internet falso en nivel DNS.

El objetivo es resolver nombres de host en otras direcciones IP, generalmente para enviar por ejemplo a sitios web falsos.

Servidor Proxy DNS Poisoning

El atacante envía un troyano a un equipo y cambia sus opciones de Proxy Server en el navegador para que apunte a otro IP.

DNS Cache Poisoning

Cambia los registros DNS por falsos.

¿Cómo Defenderse contra DNS Spoofing?

1. Resolver todas las consultas DNS al servidor DNS.
2. Bloquear consultas DNS que vayan a servidores externos
3. Implementar DNSSEC
4. Configurar resolución DNS para que use un nuevo puerto de origen disponible para cada consulta de salida.
5. Configurar el firewall para restringir DNS lookup externo.
6. Restringir servicio DNS recursivo, parcial o total a los usuarios autorizados.
7. Utilizar limitación de velocidad

Mostrando filtros en Wireshark

Estos filtros son utilizados para cambiar la vista de los paquetes capturados

Ejemplo: Se teclea el protocolo en el filter box: arp, http, tcp, udp, dns, etc.

tcp.port==23

ip.addr==192.168.1.100 machine

ip addr==192.168.1.100 && tcp.port==23

ip.addr==10.0.0.1 or ip.addr==10.0.0.4

Herramientas Sniffing

Herramienta Wireshark

1. Es un paquete gratuito. Utiliza Winpcap para capturar paquetes, así que solo puede capturar paquetes en redes soportadas por Winpcap.
2. Captura tráfico de redes vivas desde Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, redes FDDI.
3. Los archivos pueden ser editados vía línea de comandos.

Filtros de Wireshark adicionales

1. Mostrar todos los TCP resets: tcp.flags.reset==1
2. Mostrar todos las solicitudes HTTP gets: http.request
3. Mostrar todos los paquetes TCP que contengan la palabra "traffic" tcp contains traffic
4. Filtro para valores HEX 0x33 0x27 a cualquier offset: udp contains 33:27:58
5. Muestra todas las retransmisiones en el trazo: tcp.analysis.retransmission

Herramientas

- Herramientas Sniffing: CACE Pilot, Tcpdump/Windump
- Herramientas discovery: NetworkView, the Dude Sniffer
- Herramienta Password Sniffing: Ace
- Herramientas Packet Sniffing: Capsa Network Analyzer.

Herramientas

- OmniPeek Network Analyzer: Utiliza Google Map para capturar la locación de una IP pública de los paquetes capturados
- Network Packet Analyzer: Observer
- Session Capture Sniffer: NetWitness
- Email Message Sniffer: Big-Mother
- TCP/IP Packet Crafter: Packet Builder

¿Cómo un atacante hackea una red utilizando Sniffers?

1. Un atacante conecta su laptop a un puerto del swtich.
2. Ejecuta discovery tools para aprender acerca de la topología de la red.
3. Identifica el equipo de la víctima para realizar tu ataque.
4. Envenena (poison) el equipo de la víctima utilizando técnicas ARP spoofing.
5. El tráfico destinado para la víctima es re direccionado al usuario.
6. El hacker extrae passwords y datos sensibles del tráfico redirigido.

Contramedidas

¿Cómo defenderse contra Sniffing?

- Restringir el acceso físico a la red, asegurando que no se puede instalar packet sniffers.
- Utilizar encriptación para proteger información confidencial.
- Permanentemente agregar la dirección MAC de la puerta de enlace a la caché ARP.

Contramedidas

- Utilizar direcciones estáticas y tablas ARP estáticas para prevenir a los atacantes agregar entradas ARP spoofeadas.
- Apagar el network identification broadcasts y si es posible restringir la red a usuarios autorizados para proteger la red de ser descubierta por herramientas sniffing.
- Utilizar IPv6 en vez de IPv4.
- Utilizar sesiones cifradas como SSH en vez de Telnet, Secure Copy (SCP) en vez de FTP, SSL para mails, etc. para proteger la red inalámbrica contra ataques sniffing.

Técnicas de prevención Sniffing.

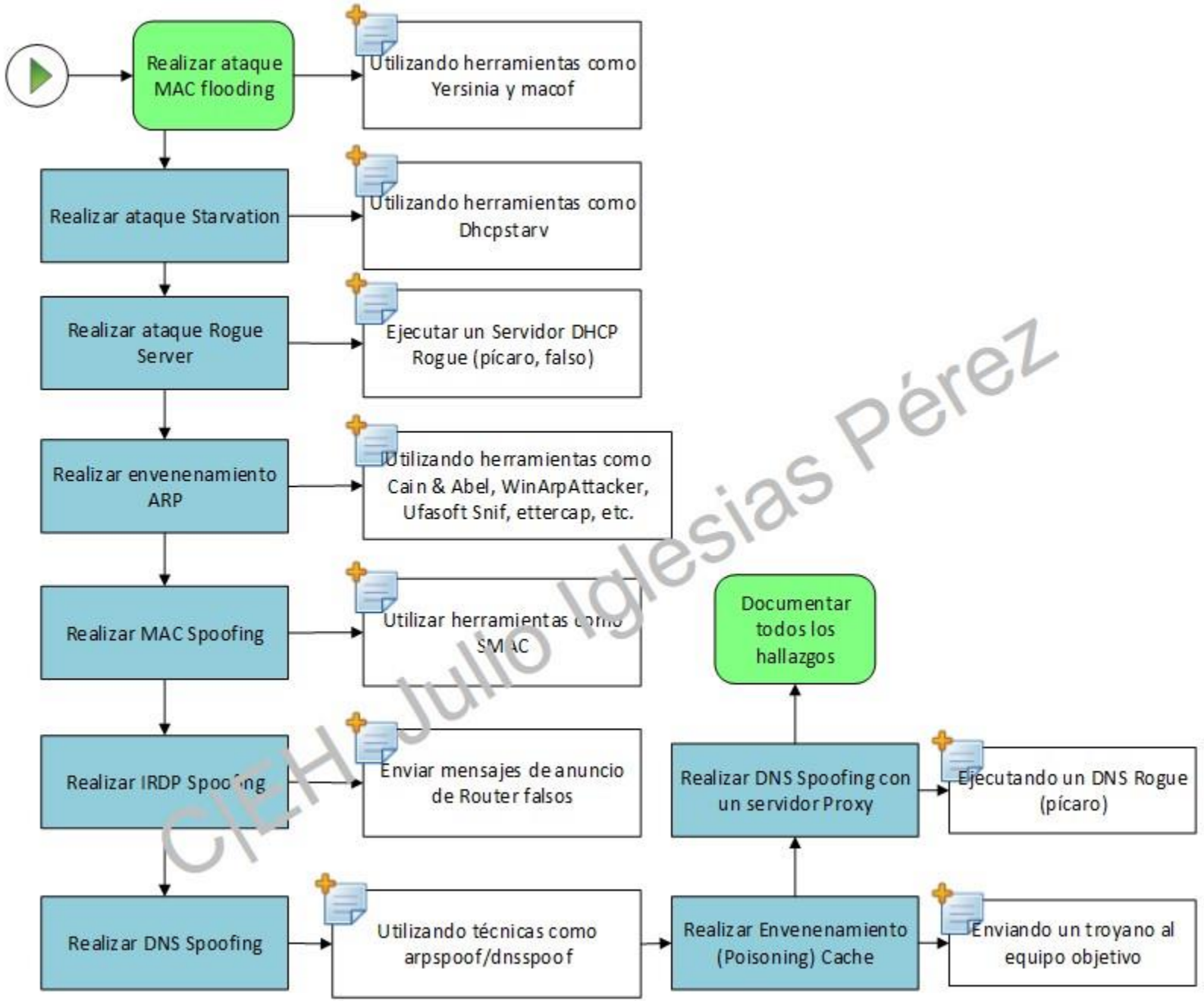
- Utilizar PGP y S/MIME.
- Utilizar VPNs.
- Utilizar SSH.
- Utilizar IPSec.
- Utilizar One-time Passwords (OTP).
- Utilizar protocolo SSL/TLS.

¿Cómo detectar sniffing?

- Debe revisar qué equipos están corriendo en modo promiscuo.
- Ejecutar IDS y notificar si las direcciones MAC de algunos equipos ha sido cambiada (como por ej. la MAC del router).
- Ejecutar herramientas de red como HP Performance Insight para monitorear la red buscando paquetes extraños.

Herramientas de detección de modo promiscuo: PromqryUI, PromiScan, etc.


Test de Intrusión con Sniffers
C|EH
Julio Iglesias Suárez




¡Muchas Gracias!
C|EH Julio Iglesias Perez