Arp spoofing-Teoría

Garza Ops

Don Bonk

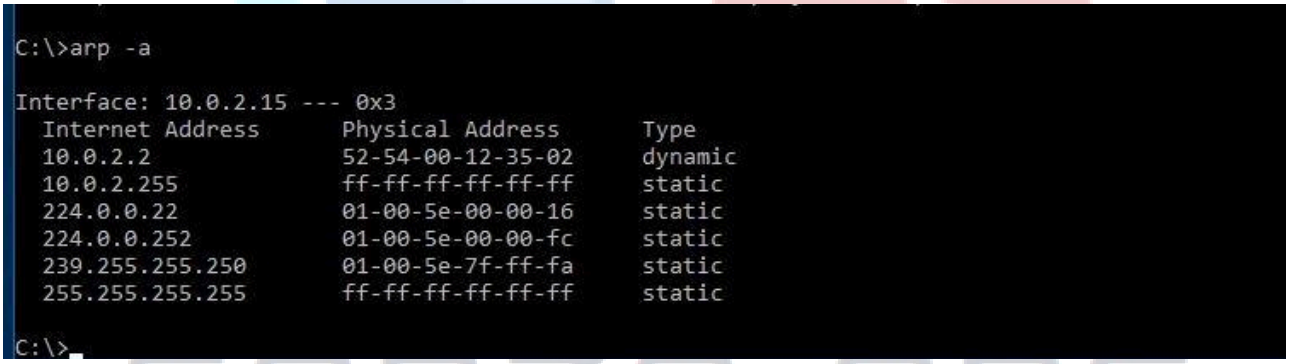
Juan Azuara (Kurko bein)

Maestro Jasson(TheGeneralisimo)

Juan Antonio(El Señor Stylers)

Que es el ARP spoofing (Envenenamiento ARP)

El Arp spoofing es un tipo de ciberataque que se realiza de manera local en la red (LAN) consiste en enviar paquetes ARP maliciosos a una puerta de enlace (GATEWAY) para cambiar la información en las tablas de direcciones IP o MAC.
Estos tipos de ataque pueden realizarse siempre y cuando el atacante tenga acceso a la red lan objetivo.
Primero definamos que es ARP. El ARP (Address Resolution Protocol) es un protocolo de comunicación utilizado en redes para asociar una dirección IP (Internet Protocol) con una dirección MAC (Media Access Control) en una red local (LAN). Su función principal es permitir que los dispositivos en una red encuentren la dirección física (MAC) de otro dispositivo a partir de su dirección IP, lo que es esencial para la transmisión de datos en redes Ethernet.
Esta información es guardada en una ARP table(tabla de ARP) y es en esta tabla donde se realizan las consultas para poder tener comunicación de los dispositivos en la red lan
A continuación se muestra un ejemplo de ARP table



Forma de ataque

El ataque de ARP Spoofing consiste en enviar mensajes ARP falsificados a la red para asociar la dirección MAC del atacante con la dirección IP de otro dispositivo (como un router o una computadora). Esto engaña a los dispositivos de la red para que envíen su tráfico al atacante en lugar de al destino legítimo.(Ettercap Team, s.f.)
Identificación de objetivos:

1. El atacante identifica dos dispositivos en la red: la víctima (por ejemplo, una computadora) y el gateway (por ejemplo, el router).
2. Envío de mensajes ARP falsificados:
   El atacante envía mensajes ARP falsificados a la víctima, diciendo: "La dirección MAC del gateway es [MAC del atacante]".
   Simultáneamente, envía mensajes ARP falsificados al gateway, diciendo: "La dirección MAC de la víctima es [MAC del atacante]".
3. Redirección del tráfico:
   La víctima y el gateway actualizan sus tablas ARP con la dirección MAC del atacante.
   Todo el tráfico entre la víctima y el gateway pasa por el atacante, quien puede interceptar, modificar o bloquear los datos.
   Interceptación o manipulación del tráfico:
4. El atacante puede capturar contraseñas, cookies, datos sensibles, o incluso inyectar código malicioso en el tráfico.

3. Ejemplo de un ataque ARP Spoofing:

Escenario:
Víctima: IP 192.168.1.10, MAC 00:11:22:33:44:55.
Gateway: IP 192.168.1.1, MAC AA:BB:CC:DD:EE:FF.
Atacante: IP 192.168.1.100, MAC 66:77:88:99:00:11.

Proceso:
El atacante envía un mensaje ARP a la víctima:
"La dirección MAC de 192.168.100.1 (gateway) es 66:77:88:99:00:11 (MAC del atacante)".
El atacante envía un mensaje ARP al gateway:
"La dirección MAC de 192.168.100.10 (víctima) es 66:77:88:99:00:11 (MAC del atacante)".
La víctima y el gateway actualizan sus tablas ARP con la dirección MAC del atacante.
El tráfico entre la víctima y el gateway pasa por el atacante, quien puede interceptarlo.

Prevención de ataque ARP spoofing

1. Usar ARP Static (Bindings Estáticos de ARP)
   Una de las formas más efectivas de prevenir el ARP Spoofing es configurar bindings estáticos de ARP en los dispositivos de la red. Esto implica asociar manualmente las direcciones IP con las direcciones MAC correspondientes en la tabla ARP de cada dispositivo.
   Cómo hacerlo:
   En Linux:
   sudo arp -s <IP> <MAC>

   Ejemplo:
   sudo arp -s 192.168.1.1 00:1a:2b:3c:4d:5e
   En Windows:
   arp -s <IP> <MAC>

   Ejemplo:
   arp -s 192.168.1.1 00-1a-2b-3c-4d-5e
   Ventajas:
   Evita que un atacante pueda envenenar la tabla ARP, ya que las entradas son fijas.
   Ideal para redes pequeñas o dispositivos críticos (como routers o servidores).
   Desventajas:
   No es escalable para redes grandes, ya que requiere configuración manual en cada dispositivo.
   Si cambian las direcciones MAC (por ejemplo, al reemplazar un dispositivo), la configuración debe actualizarse manualmente.

2. Implementar DHCP Snooping

El DHCP Snooping es una función de seguridad disponible en switches gestionables que ayuda a prevenir ataques de ARP Spoofing al validar y filtrar los mensajes DHCP en la red.

   Cómo funciona:
   El switch mantiene una tabla de direcciones IP y MAC asignadas legítimamente a través de DHCP.
   Bloquea los mensajes DHCP no autorizados o maliciosos.
   Ventajas:
   Previene ataques de suplantación de DHCP y ARP Spoofing.
   Escalable para redes grandes.
   Desventajas:
   Requiere switches gestionables con soporte para DHCP Snooping.
   Configuración más compleja.

3. Usar Detección de ARP Spoofing (ARPwatch)
   ARPwatch es una herramienta que monitorea la red en busca de cambios en las asociaciones IP-MAC y alerta sobre posibles intentos de ARP Spoofing.
   Cómo usarlo:
   Instala ARPwatch en Linux:
   sudo apt install arpwatch

   Inicia ARPwatch:
   sudo arpwatch -i <interfaz>

   Ejemplo:
   sudo arpwatch -i eth0
   Revisa los logs en /var/lib/arpwatch/arp.dat o en /var/log/syslog.

   Ventajas:
   Detecta cambios sospechosos en la tabla ARP.
   Fácil de implementar en redes pequeñas.
   Desventajas:
   No previene el ataque, solo lo detecta.
   Requiere supervisión manual de los logs.

4. Habilitar Dynamic ARP Inspection (DAI)
   Dynamic ARP Inspection (DAI) es una función de seguridad disponible en switches gestionables que valida los mensajes ARP en la red.
   Cómo funciona:
   El switch verifica que los mensajes ARP coincidan con la tabla de DHCP Snooping.
   Bloquea los mensajes ARP no válidos o maliciosos.
   Ventajas:
   Previene eficazmente el ARP Spoofing.
   Escalable para redes grandes.
   Desventajas:
   Requiere switches gestionables con soporte para DAI.
   Configuración más compleja.

5. Usar VLANs para Segmentar la Red
   La segmentación de la red mediante VLANs puede limitar el alcance de un ataque de ARP Spoofing.
   Cómo hacerlo:
   Divide la red en VLANs lógicas.
   Configura los switches para restringir el tráfico entre VLANs.
   Ventajas:
   Limita el impacto de un ataque a una sola VLAN.
   Mejora la seguridad y el rendimiento de la red.

Desventajas:
Requiere switches gestionables con soporte para VLANs.
Configuración más compleja.

6. Usar Protocolos de Seguridad como IPSec o HTTPS
   El uso de protocolos de seguridad como IPSec o HTTPS puede proteger el tráfico de red contra la interceptación, incluso si se produce un ARP Spoofing.
   Cómo funciona:
   IPSec: Encripta el tráfico IP entre dispositivos.
   HTTPS: Encripta el tráfico web entre el cliente y el servidor.
   Ventajas:
   Protege la confidencialidad e integridad de los datos.
   No depende de la prevención del ARP Spoofing.
   Desventajas:
   No previene el ARP Spoofing, solo mitiga sus efectos.
   Requiere configuración y soporte en los dispositivos.

Referencias

Ettercap Team. (s.f.). Ettercap User Manual. Recuperado el [26-02-2025], de https://www.ettercap-project.org/

Radware. (s.f.). Envenenamiento ARP (ARP Poisoning). Recuperado el [26-02-2025], de https://es.radware.com/security/ddos-knowledge-center/ddospedia/arp-poisoning/