“ATAQUES Y EVALUACIÓN DE VULNERABILIDADES – ATAQUES ACTIVOS”

Informe N°1

Laboratorio de Seguridad en Redes

Melanny Dávila
Ingeniería en Telecomunicaciones
Facultad de Eléctrica y Eléctronica
Quito, Ecuador
melanny.davila@epn.edu.ec

Alejandra Silva
Ingeniería en Telecomunicaciones
Facultad de Eléctrica y Eléctronica
Quito, Ecuador
alejandra.silva@epn.edu.ec

***Abstract*—Mediante el siguiente documento se presentará el desarrollo de la sesión de laboratorio de la materia Seguridad en Redes, con el fin de describir el ataque de hombre en el medio.**

***Index Terms*—Vulnerabilidad, ARP, KALI Linux, Metasploitable 2, ataque.**

I. Introducción

En el área de las seguridades se tiene dos tipos de ataques, pasivos y activos en este documento se hablara acerca de los activos que hace referencia a cambiar o modificar el flujo de datos o crear a su vez otro falso haciendo uso de la misma información que se recopilo como nombre de usuarios y contraseña. Este ataques se subdivide en:

- Hombre en Medio: Como su nombre lo dice se encuentra en la mitad entre dos elementos de la red.
- Envenenamiento ARP: Consiste en que la dirección IP que esta asociada a una dirección MAC inventada pertenece a una maquina real.
- Secuestro de sesión: Se hace uso mediante las cookies, lo que le permite robar y controlar la información cuando se encuentra en un sitio web.

II. Objetivos

- Implementar, en un entorno aislado y virtualizado, el ataque de “hombre en el medio” con el fin de evidenciar en la práctica sus consecuencias en una red.
- Analizar técnicamente los resultados de las distintas fases del ataque de “hombre en el medio”.

III. Cuestionario

A. Presente la configuración realizada en el laboratorio.

Para iniciar la práctica se configuraron las interfaces de red de todos los dispositivos que interactúan en la red que se va a analizar. Proceso que se explica a continuación:

Una vez que ambas máquinas virtuales se encontraban abiertas, se procedió a la configuración de los adaptadores de red con el fin de que tengan acceso a internet. Los adaptadores deben estar configurados de la siguiente manera:

- Primer adaptador: NAT
- Segundo adaptador: Host-only

Esto se presenta en la figura 1, donde dentro del recuadro rojo se presentan dichas configuraciones. Mientras, se realizó la configuración de las direcciones IP de las máquinas virtuales Kali y Metasploitable2.

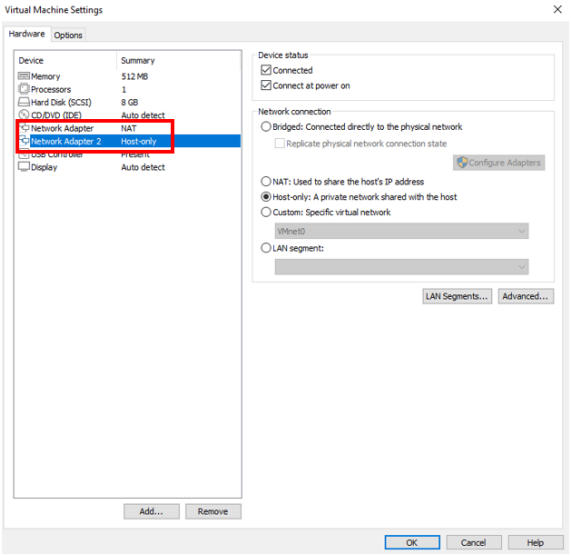


Fig. 1. Configuración de la máquina virtual

Posterior a eso, se configuró la dirección IP de la máquina física como se muestra en la figura 2.

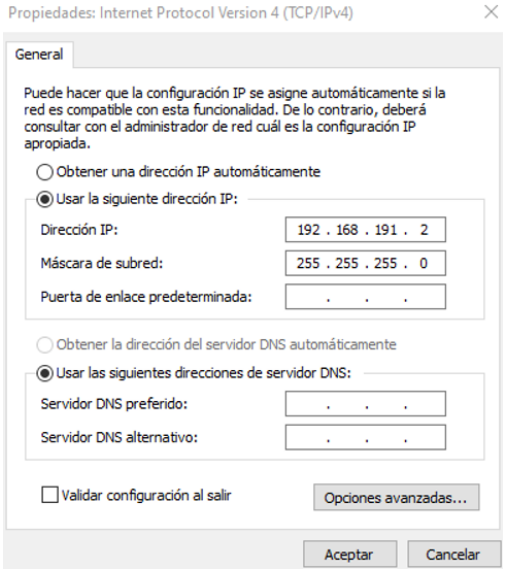


Fig. 2. Configuración de la dirección IP dentro de la máquina anfritrión

Luego, en metasploitable, se configuró la segunda tarjeta de red de la manera en la que se muestra en la figura 3.

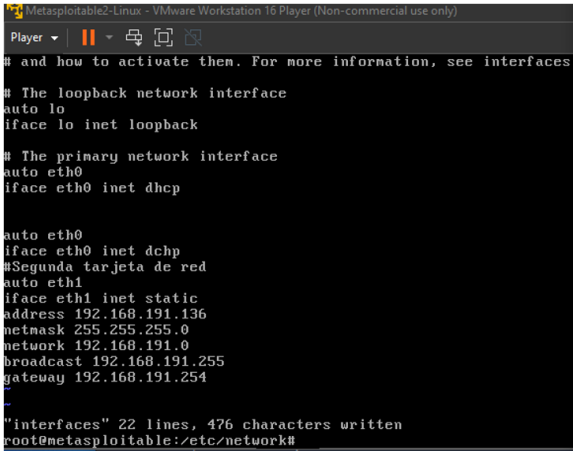


Fig. 3. Configuración de la dirección IP en Metasploitable dentro del archivo de configuración de interfaz de red

A continuación, se editó la interfaz de red de Kali y se reinicio el servicio de red del mismo.

Para poder recrear un escenario real se hace uso de un router que estará conectado al internet representado por la nube como se muestra en la figura 5. Este se configura de tal manera que se le asignan direcciones a las interfaces que usa como se muestra en la figura 6.
Para finalizar este primer proceso se verifica conectividad entre cada uno de los miembros como se puede observar en las figuras 7 y 8.

Para la segunda parte de la simulación de este escenario se procede a verificar las tablas ARP como se muestra en las figuras 9 y 10. Esto con el fin de verificar las direcciones MAC de cada uno de los miembros conectados, previo a la realización del ataque y así evidenciar la suplantanción de dirección MAC por parte del atacante.
Como primer paso a la realización del ataque se tiene que se vacía la tabla ARP del atacante y de la víctima como se muestra en las figuras 11 y 12.
Luego, empieza el ataque propiamente dicho con la inundación de mensajes ARP por parte del atacante. Esto se puede apreciar en la 13. Además, como una forma de verificación del ataque, se evidencian los mensajes ARP en wireshark mostrados en la figura 14.
Luego de dejar pasar un poco de tiempo para que el ataque surta efecto, se puede visualizar en la tabla ARP de la víctima que ahora el atacante es tomado como el default gateway. Mientras que, en la tabla ARP del router, el atacante es tomado con el host como se muestra en la figura 16.

B. Presentar las capturas de pantalla, con la debida explicación de los resultados mostrados.

Como se indicó previamente, para poder efectuar el ataque es importante que cada uno de los dispositivos esten conectados entre ellos.

Para cada uno de los casos se configura o dentro de la propia máquina anfitrión (interfaces de red virtuales), que se muestra en la figura 1 y 2, o con los archivos de configuración de red propios del sistema operativo como los que se muestran en la figura 3

En la figura 4 se verifica la configuración IP del interfaz de red de la máquina virtual a la vez que se ejecuta el comando "*networking restart*" para que se adopten todas las configuraciones realizadas.

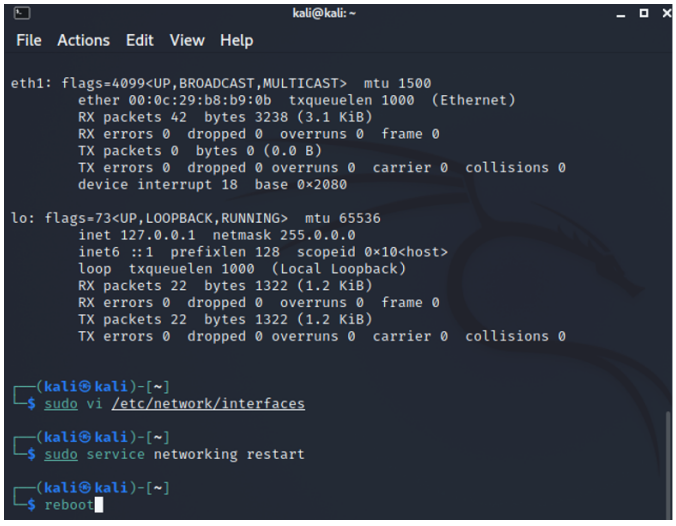


Fig. 4. Configuración de red en la máquina kali realizada y aplicada

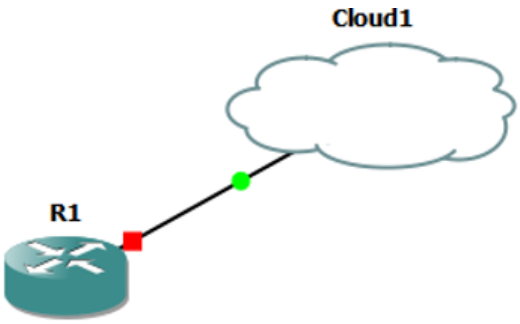


Fig. 5. Simulación de la conexión de internet con la red

En las figuras 6, 7 y 8 se pueden visualizar la configuración de las interfaces del router y las pruebas de conectividad entre los dispositivos de la red.

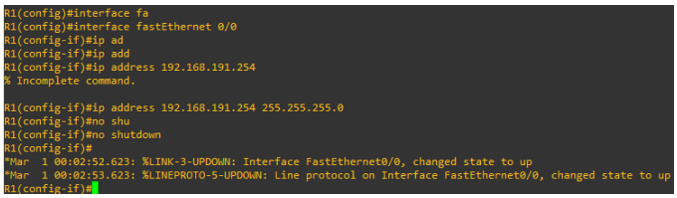


Fig. 6. Configuración de las interfaces del router

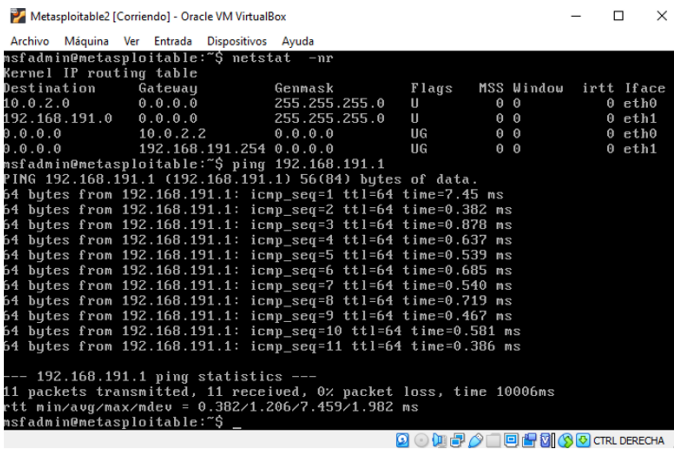


Fig. 7. Prueba de conectividad en la máquina metasploitable

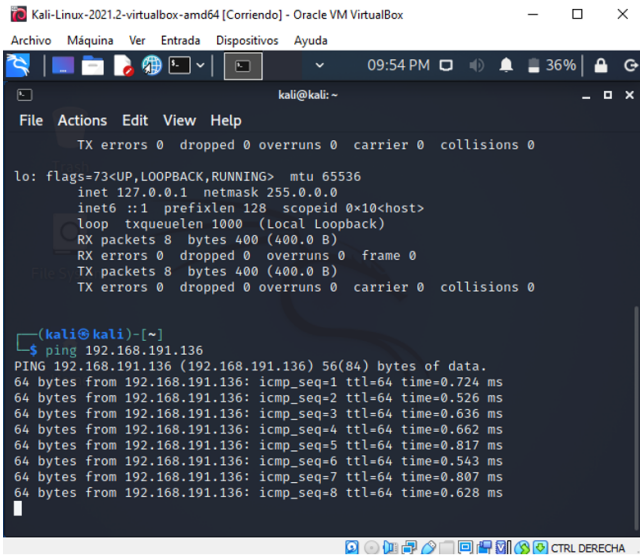


Fig. 8. Prueba de conectividad en la máquina kali

Para poder evidenciar los efectos del ataque sobre cada uno de los miembros que participan en él, se visualizan las tablas ARP de cada uno de ellos, esto por medio del comando "*arp -a*" para poder ver todo el contenido de las tablas. Esto se puede visualizar en las figuras 9 y 10.

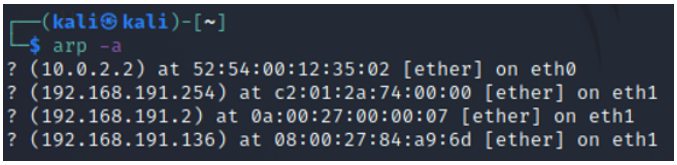


Fig. 9. Tabla ARP de la máquina kali

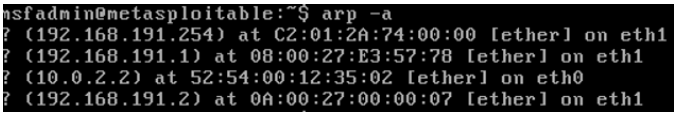


Fig. 10. Tabla ARP de la máquina metasploitable

El primer paso para realizar el ataque es el limpiar las tablas ARP de todos los miembros que intervienen en la red. Esto, para los sistemas operativos linux se realiza con el comando "*ip -s -s neigh flush all*" con permisos de admininstrador (root), esto se evidencia en las figuras 11 y 12.

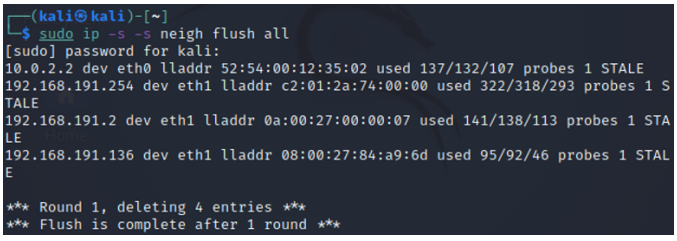
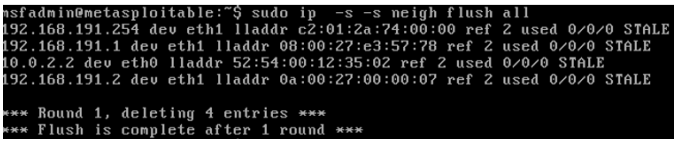


Fig. 11. Limpieza de la tabla ARP de la máquina kali



```
msfadmin@metasploitable:~$ sudo ip  -s -s neigh flush all
192.168.191.254 dev eth1 lladdr c2:01:2a:74:00:00 ref 2 used 0/0/0 STALE
192.168.191.1 dev eth1 lladdr 08:00:27:e3:57:78 ref 2 used 0/0/0 STALE
10.0.2.2 dev eth0 lladdr 52:54:00:12:35:02 ref 2 used 0/0/0 STALE
192.168.191.2 dev eth1 lladdr 0a:00:27:00:00:07 ref 2 used 0/0/0 STALE

*** Round 1, deleting 4 entries ***
*** Flush is complete after 1 round ***
```

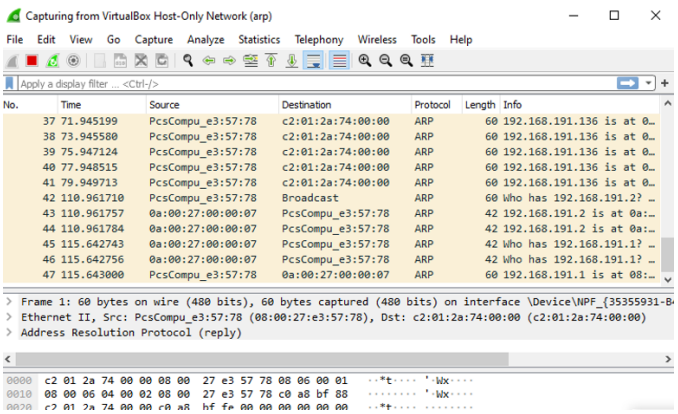
Fig. 12. Limpieza de la tabla ARP de la máquina metasploitable

Luego, para realizar el ataque, se usa el comando "*-i eth1 -t [ip] -r [ip]*" donde se colocan las direcciones IP del host auténtico de la red y la IP del default gateway respectivamente. Esto se evidencia la figura 13. Hay que destacar que no se debe detener este comando hasta que se haya terminado el ataque, ya que de lo contrario las tablas ARP se actualizarán a como estaban antes.

```
┌──(kali㉿kali)-[~]
└─$ sudo arpspoof -i eth1 -t 192.168.191.136 -r 192.168.191.254              1 ✕
8:0:27:e3:57:78 8:0:27:84:a9:6d 0806 42: arp reply 192.168.191.254 is-at 8:0:
27:e3:57:78
8:0:27:e3:57:78 c2:1:2a:74:0:0 0806 42: arp reply 192.168.191.136 is-at 8:0:2
7:e3:57:78
8:0:27:e3:57:78 8:0:27:84:a9:6d 0806 42: arp reply 192.168.191.254 is-at 8:0:
27:e3:57:78
8:0:27:e3:57:78 c2:1:2a:74:0:0 0806 42: arp reply 192.168.191.136 is-at 8:0:2
7:e3:57:78
8:0:27:e3:57:78 8:0:27:84:a9:6d 0806 42: arp reply 192.168.191.254 is-at 8:0:
27:e3:57:78
8:0:27:e3:57:78 c2:1:2a:74:0:0 0806 42: arp reply 192.168.191.136 is-at 8:0:2
7:e3:57:78
8:0:27:e3:57:78 8:0:27:84:a9:6d 0806 42: arp reply 192.168.191.254 is-at 8:0:
27:e3:57:78
8:0:27:e3:57:78 c2:1:2a:74:0:0 0806 42: arp reply 192.168.191.136 is-at 8:0:2
7:e3:57:78
```

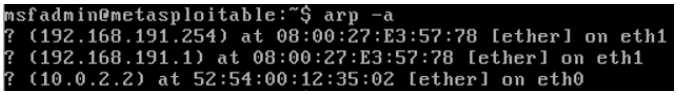
Fig. 13. Realización del envenenamiento ARP

Finalmente, se evidencia tanto la inundación ARP con la captura de paquetes de wireshark que se muestra en la figura 14. Como el cambio de direcciones MAC del host y el default gateway en las tablas ARP de cada uno de los miembros de la red, que se muestran en las figuras 15, 16 y 28. Consecuencias todas del envenenamiento ARP y muestras del éxito del ataque.



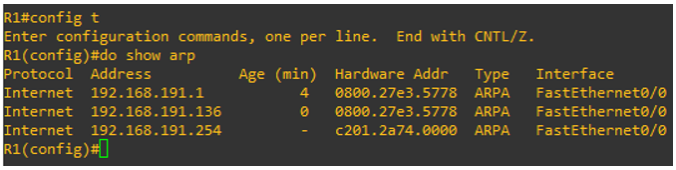
```
No.     Time        Source              Destination         Protocol Length Info
     37 71.945199   PcsCompu_e3:57:78   c2:01:2a:74:00:00   ARP          60 192.168.191.136 is at 0…
     38 73.945580   PcsCompu_e3:57:78   c2:01:2a:74:00:00   ARP          60 192.168.191.136 is at 0…
     39 75.947124   PcsCompu_e3:57:78   c2:01:2a:74:00:00   ARP          60 192.168.191.136 is at 0…
     40 77.948515   PcsCompu_e3:57:78   c2:01:2a:74:00:00   ARP          60 192.168.191.136 is at 0…
     41 79.949713   PcsCompu_e3:57:78   c2:01:2a:74:00:00   ARP          60 192.168.191.136 is at 0…
     42 110.961710  PcsCompu_e3:57:78   Broadcast           ARP          60 Who has 192.168.191.2? …
     43 110.961757  0a:00:27:00:00:07   PcsCompu_e3:57:78   ARP          42 192.168.191.2 is at 0a:…
     44 110.961784  0a:00:27:00:00:07   PcsCompu_e3:57:78   ARP          42 192.168.191.2 is at 0a:…
     45 115.642743  0a:00:27:00:00:07   PcsCompu_e3:57:78   ARP          42 Who has 192.168.191.1? …
     46 115.642756  0a:00:27:00:00:07   PcsCompu_e3:57:78   ARP          42 Who has 192.168.191.1? …
     47 115.643000  PcsCompu_e3:57:78   0a:00:27:00:00:07   ARP          60 192.168.191.1 is at 08:…

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{35355931-B
> Ethernet II, Src: PcsCompu_e3:57:78 (08:00:27:e3:57:78), Dst: c2:01:2a:74:00:00 (c2:01:2a:74:00:00)
> Address Resolution Protocol (reply)

0000  c2 01 2a 74 00 00 08 00  27 e3 57 78 08 06 00 01   ··*t···· '·Wx····
0010  08 00 06 04 00 02 08 00  27 e3 57 78 c0 a8 bf 88   ········ '·Wx····
0020  c2 01 2a 74 00 00 c0 a8  bf fe 00 00 00 00 00 00   ··*t···· ········
```

Fig. 14. Paquetes obtenidos en Wireshark



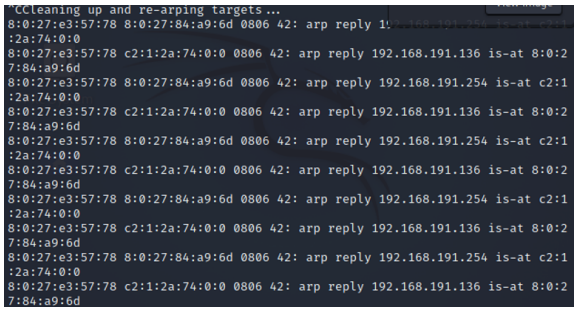
```
msfadmin@metasploitable:~$ arp -a
? (192.168.191.254) at 08:00:27:E3:57:78 [ether] on eth1
? (192.168.191.1) at 08:00:27:E3:57:78 [ether] on eth1
? (10.0.2.2) at 52:54:00:12:35:02 [ether] on eth0
```

Fig. 15. Configuración de la dirección IP



```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#do show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.191.1           4   0800.27e3.5778  ARPA   FastEthernet0/0
Internet  192.168.191.136         0   0800.27e3.5778  ARPA   FastEthernet0/0
Internet  192.168.191.254         -   c201.2a74.0000  ARPA   FastEthernet0/0
R1(config)#
```

Fig. 16. Configuración de la dirección IP

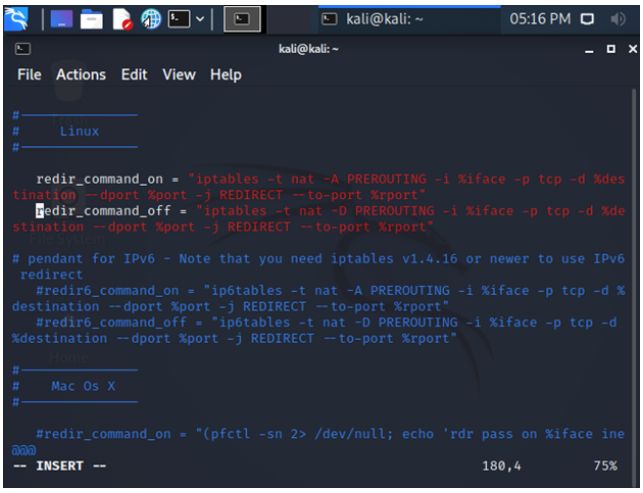


```
^CCleaning up and re-arping targets...
8:0:27:e3:57:78 8:0:27:84:a9:6d 0806 42: arp reply 192.168.191.254 is-at c2:1
:2a:74:0:0
8:0:27:e3:57:78 c2:1:2a:74:0:0 0806 42: arp reply 192.168.191.136 is-at 8:0:2
7:84:a9:6d
8:0:27:e3:57:78 8:0:27:84:a9:6d 0806 42: arp reply 192.168.191.254 is-at c2:1
:2a:74:0:0
8:0:27:e3:57:78 c2:1:2a:74:0:0 0806 42: arp reply 192.168.191.136 is-at 8:0:2
7:84:a9:6d
8:0:27:e3:57:78 8:0:27:84:a9:6d 0806 42: arp reply 192.168.191.254 is-at c2:1
:2a:74:0:0
8:0:27:e3:57:78 c2:1:2a:74:0:0 0806 42: arp reply 192.168.191.136 is-at 8:0:2
7:84:a9:6d
8:0:27:e3:57:78 8:0:27:84:a9:6d 0806 42: arp reply 192.168.191.254 is-at c2:1
:2a:74:0:0
8:0:27:e3:57:78 c2:1:2a:74:0:0 0806 42: arp reply 192.168.191.136 is-at 8:0:2
7:84:a9:6d
8:0:27:e3:57:78 8:0:27:84:a9:6d 0806 42: arp reply 192.168.191.254 is-at c2:1
:2a:74:0:0
8:0:27:e3:57:78 c2:1:2a:74:0:0 0806 42: arp reply 192.168.191.136 is-at 8:0:2
7:84:a9:6d
```

Fig. 17. Configuración de la dirección IP

C. Implemente el ataque de envenenamiento ARP usando la interfaz gráfica de Ettercap, disponible en Kali Linux (Applications/09-Sniffing and Spoofing/ettercap-graphical). Incluya capturas de pantalla y comentarios breves.

Para implementar el ataque con ese interfaz se debe modificar 4 líneas de código como se indica en al figura a continuación y me de permiso para escanear los hosts que se tiene [1].



```
#————————————
#      Linux
#————————————

   redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp -d %des
tination --dport %port -j REDIRECT --to-port %rport"
   redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp -d %de
stination --dport %port -j REDIRECT --to-port %rport"

# pendant for IPv6 - Note that you need iptables v1.4.16 or newer to use IPv6
 redirect
   #redir6_command_on = "ip6tables -t nat -A PREROUTING -i %iface -p tcp -d %
destination --dport %port -j REDIRECT --to-port %rport"
   #redir6_command_off = "ip6tables -t nat -D PREROUTING -i %iface -p tcp -d
%destination --dport %port -j REDIRECT --to-port %rport"

#————————————
#    Mac Os X
#————————————

   #redir_command_on = "(pfctl -sn 2> /dev/null; echo 'rdr pass on %iface ine
@@@
-- INSERT --                                                180,4         75%
```

Fig. 18. Cambio de archivo de configuración.

Luego se debe dirigir a las aplicaciones que tiene la maquina virtual Kali y escoger ettercap-graphical como se indica.

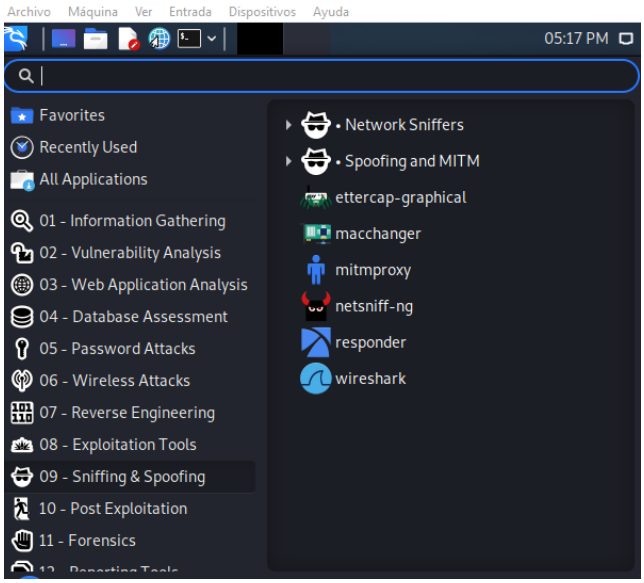


Fig. 19. Abrir la interfaz.

Antes de realizar cualquier escaneo se debe escoger la opción en modo Promiscuo y selección el visto para iniciar el interfaz.

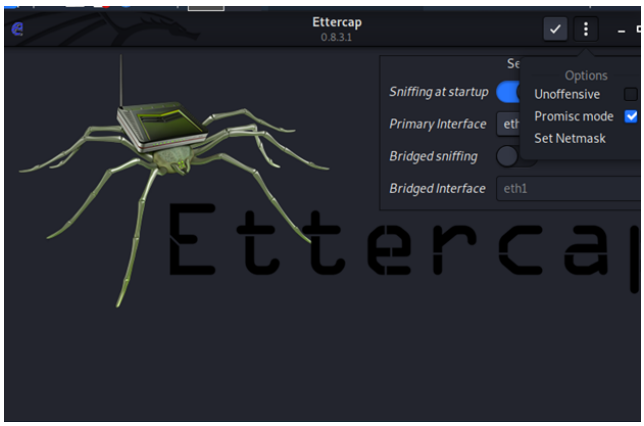


Fig. 20. Configuración de la Interfaz.

Una vez inicializada la interfaz se debe dirigir a la opción Hosts y seleccionar host list como se indica a continuación.

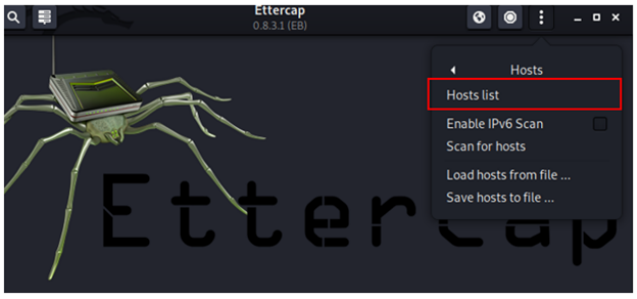


Fig. 21. Visualización de Hosts.

Se desplegara al lista de Host en la que se debe seleccionar primera la del Metasploitable y seleccionar la opción Add Target 1 tal como se indica.

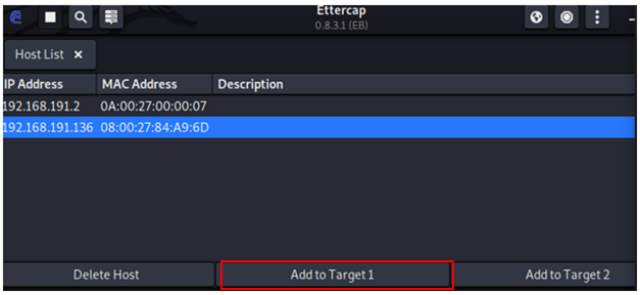


Fig. 22. Añadir víctima.

Lo mismo sera en el siguiente paso pero se debe escoger la IP del Host-only tal como se indica y seleccionar Add Target 2.

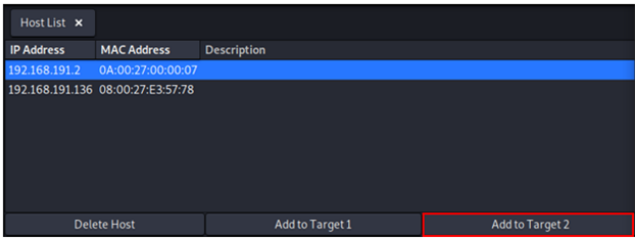


Fig. 23. Selección de la 2 víctima.

Ahora se procede a dar click en el icono MITM menú que se presenta en la siguiente figura.

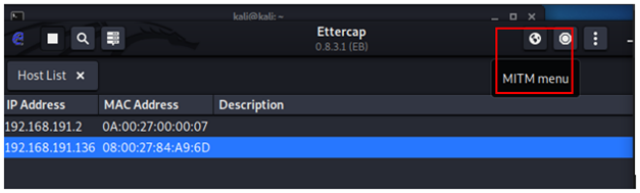


Fig. 24. MITM Menú.

Posteriormente, se debe seleccionar la opción de ARP poisoning.

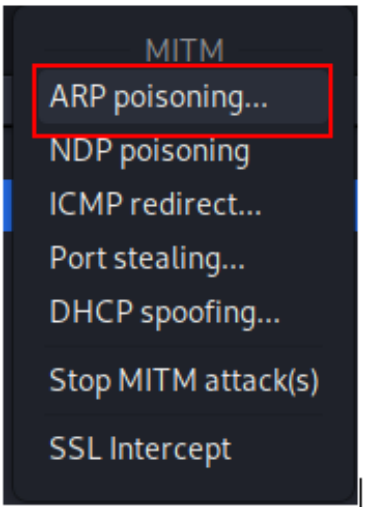


Fig. 25. ARP Poisoning.

Después de esto se despliega una pantalla que permite que se detecte que la opción de Sniff remote connection este habilitada y finalmente se da click en OK.

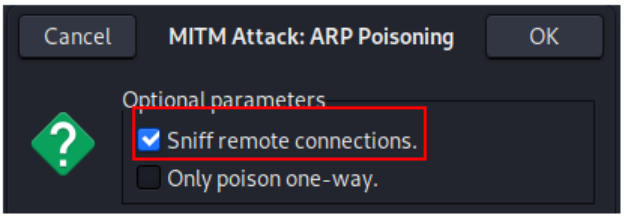


Fig. 26. Verificación de Sniff Connection.

Ahora casi por finalizar se da click en el icono de reproducir que se encuentra en la esquina superior izquierda de play para relizar los cambios.

Fig. 27. Play a la Configuración.

Finalmente, podemos observar que desde un cmd de la computadora física se observa que las direcciones MAC son las mismas que de la maquina virtual Kali [1].

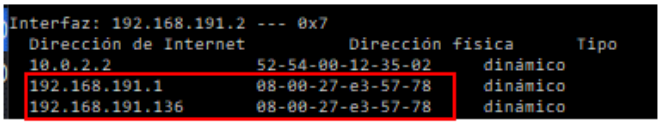


Fig. 28. Visualización de la MAC igual.

D. Conclusiones

- A través del uso del sistema operativo Kali Linux se puede profundizar los conocimientos de aplicaciones que permiten implementar seguridad de redes.
- Con el uso de Metasploitable2 se pudo implementar una prueba básica de penetración de seguridad con el fin de poder analizar vulnerabilidades del protocolo ARP.
- Mediante la visualización de la tabla arp de la maquina víctima se puede visualizar que el ataque se realizo con éxito ya que se observa que la dirección MAC de la maquina víctima es al misma que la MAC de la maquina que esta atacando, haciendo exitoso el ataque ARP.

E. Recomendaciones

- Es importante conocer los comandos básicos y herramientas que permitirán llevar acabo la administración de la seguridad de redes.
- Se debe verificar que la máquina virtual pueda acceder a internet mediante un adaptador puente.
- Verificar el uso correcto del adaptador Host Only para poder realizar el objetivo de la practica que son los dos diferentes tipos de ataques.

REFERENCES

[1] "Uso de Kali Linux ettercap". https://programmerclick.com/article/8802549131/ (accedido jun. 17, 2021).