CONMUTACIÓN: MAC ADDRESS SPOOFING

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

LUIS MIGUEL POLO 20182020158

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

INGENIERÍA DE SISTEMAS

TELEINFORMATICA I

ANDRES ALEXANDER FONSECA

2024-III

OBJETIVOS

- Implementar un escenario de Hacking ético
- Implementar una red en GNS3 con equipos cisco

MATERIALES

- Computador personal con acceso a internet
- GNS3 preferiblemente usando el servidor GNSVM, Kali Linux, IOS Cisco 2691, VirtualBox

PROCEDIMIENTO

Montaje de topología descrita en GNS3

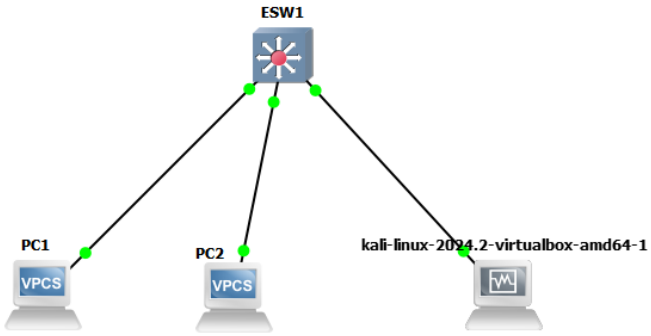

Figura 1. Topología asignada

Configuración DHCP Switch

```
ESW1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
ESW1(config)#interface vlan
ESW1(config)#interface vlan 1
ESW1(config-if)#ip add 11.12.13.2 255.255.255.240
ESW1(config-if)#no shutdown
ESW1(config-if)#exit
*Mar  1 00:04:59.099: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
*Mar  1 00:05:00.099: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
ESW1(config-if)#exit
ESW1(config)#serice dhcp
             ^
% Invalid input detected at '^' marker.

ESW1(config)#service dhcp
ESW1(config)#ip dhcp pool myPOOL
ESW1(dhcp-config)#network 11.12.13.0 255.255.255.240
ESW1(dhcp-config)#default-r
ESW1(dhcp-config)#default-router 11.12.13.1
ESW1(dhcp-config)#dns-server 8.8.8.4
ESW1(dhcp-config)#lease 0 7 20
ESW1(dhcp-config)#exit
ESW1(config)#ip dhcp excluded-
ESW1(config)#ip dhcp excluded-address 11.12.13.1 11.12.13.6
ESW1(config)#exit
ESW1#
*Mar  1 00:07:43.807: %SYS-5-CONFIG_I: Configured from console by console
ESW1#wr
```

Imagen 1. Configuración DHCP ESW1

Solicitud DCHP PC1

```
PC1> ip dhcp
DDDO
Can't find dhcp server

PC1> ip dhcp
DORA IP 11.12.13.7/28 GW 11.12.13.1
```

Imagen 2. Solicitud de dhcp PC1

```
PC1> show ip

NAME        : PC1[1]
IP/MASK     : 11.12.13.7/28
GATEWAY     : 11.12.13.1
DNS         : 8.8.8.4
DHCP SERVER : 11.12.13.2
DHCP LEASE  : 26358, 26400/13200/23100
MAC         : 00:50:79:66:68:00
LPORT       : 10012
RHOST:PORT  : 127.0.0.1:10013
MTU:        : 1500
```

Imagen 3. Verificación de IP asignada para PC1

Solicitud DCHP PC2

```
PC2> ip dhcp
DORA IP 11.12.13.8/28 GW 11.12.13.1

PC2> show ip

NAME        : PC2[1]
IP/MASK     : 11.12.13.8/28
GATEWAY     : 11.12.13.1
DNS         : 8.8.8.4
DHCP SERVER : 11.12.13.2
DHCP LEASE  : 26387, 26400/13200/23100
MAC         : 00:50:79:66:68:01
LPORT       : 10014
RHOST:PORT  : 127.0.0.1:10015
MTU:        : 1500
```

Imagen 4. Verificación de IP asignada para PC2

Solicitud ARP y pruebas de conectividad PC1, PC2 y Kali

```
PC1> ping 11.12.13.8
84 bytes from 11.12.13.8 icmp_seq=1 ttl=64 time=0.530 ms
84 bytes from 11.12.13.8 icmp_seq=2 ttl=64 time=0.409 ms
84 bytes from 11.12.13.8 icmp_seq=3 ttl=64 time=0.410 ms
84 bytes from 11.12.13.8 icmp_seq=4 ttl=64 time=0.395 ms
84 bytes from 11.12.13.8 icmp_seq=5 ttl=64 time=0.447 ms

PC1> ping 11.12.13.9
84 bytes from 11.12.13.9 icmp_seq=1 ttl=64 time=0.978 ms
84 bytes from 11.12.13.9 icmp_seq=2 ttl=64 time=1.524 ms
84 bytes from 11.12.13.9 icmp_seq=3 ttl=64 time=1.839 ms
84 bytes from 11.12.13.9 icmp_seq=4 ttl=64 time=2.050 ms
84 bytes from 11.12.13.9 icmp_seq=5 ttl=64 time=1.393 ms

PC1> arp

08:00:27:d2:26:79  11.12.13.9 expires in 118 seconds
00:50:79:66:68:01  11.12.13.8 expires in 89 seconds
```

Imagen 5. Ping de PC1 a PC2 y solicitud ARP

```
PC2> ping 11.12.13.7
84 bytes from 11.12.13.7 icmp_seq=1 ttl=64 time=0.397 ms
84 bytes from 11.12.13.7 icmp_seq=2 ttl=64 time=0.410 ms
84 bytes from 11.12.13.7 icmp_seq=3 ttl=64 time=0.418 ms
84 bytes from 11.12.13.7 icmp_seq=4 ttl=64 time=0.437 ms
84 bytes from 11.12.13.7 icmp_seq=5 ttl=64 time=0.448 ms
```

Imagen 6. Ping de PC2 a PC1

```
ESW1#show mac
ESW1#show mac-address-table vlan 1
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
c001.0d98.0000          Self          1     Vlan1
0050.7966.6801          Dynamic       1     FastEthernet1/1
0050.7966.6800          Dynamic       1     FastEthernet1/0
```

Imagen 7. Tabla de direcciones MAC en ESW1

MAC de kali (08:00:27:d2:26:79)

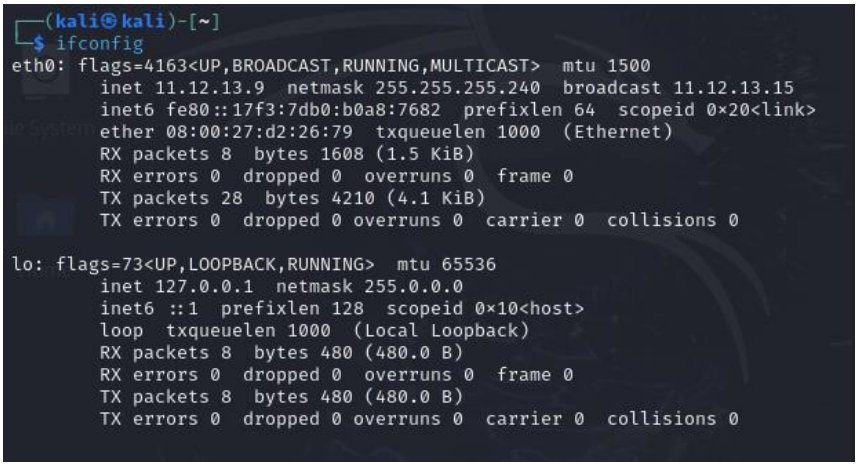

Imagen 8. Verificación de DHCP en Kali

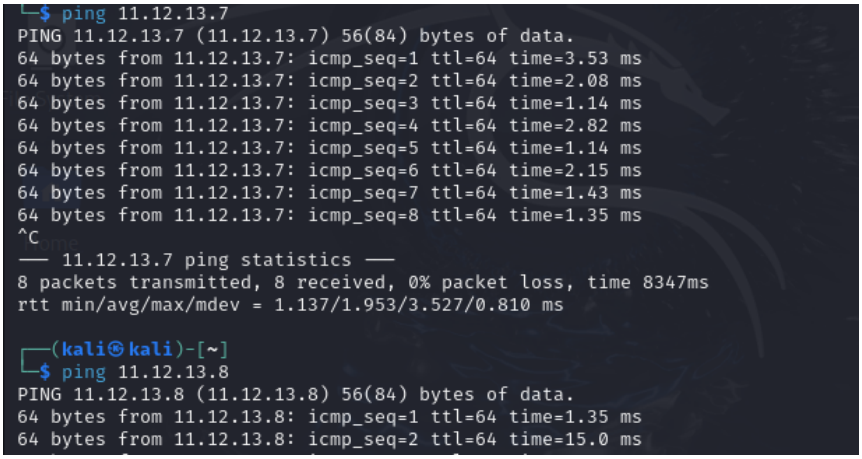

Imagen 9. Ping a PC1 y PC2 desde Kali

Ping a Kali desde PC1 y captura de tráfico con Wireshark

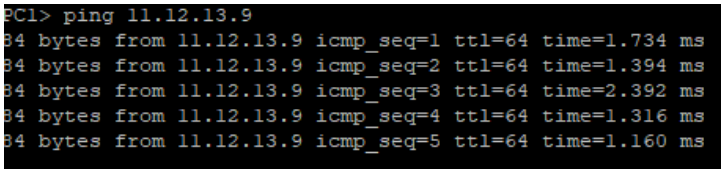

Imagen 10. Ping a Kali desde PC1

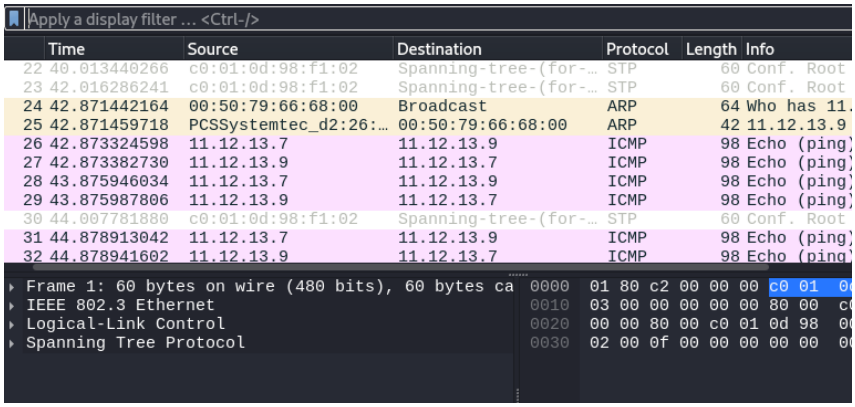

Imagen 11. Captura de tráfico con Wireshark de ping de PC1 a Kali

Suplantación MAC de PC2 en Kali

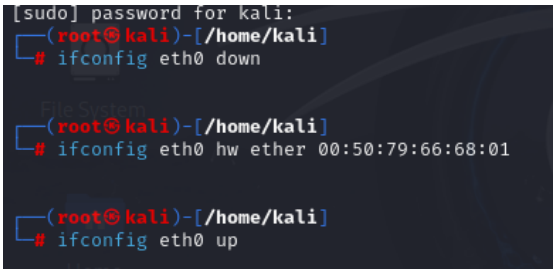

Imagen 12. Cambio de MAC de Kali

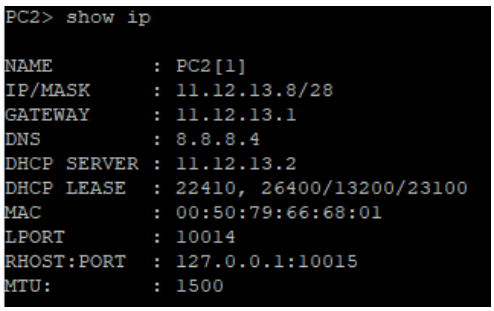

Imagen 13. Visualización IP de PC2

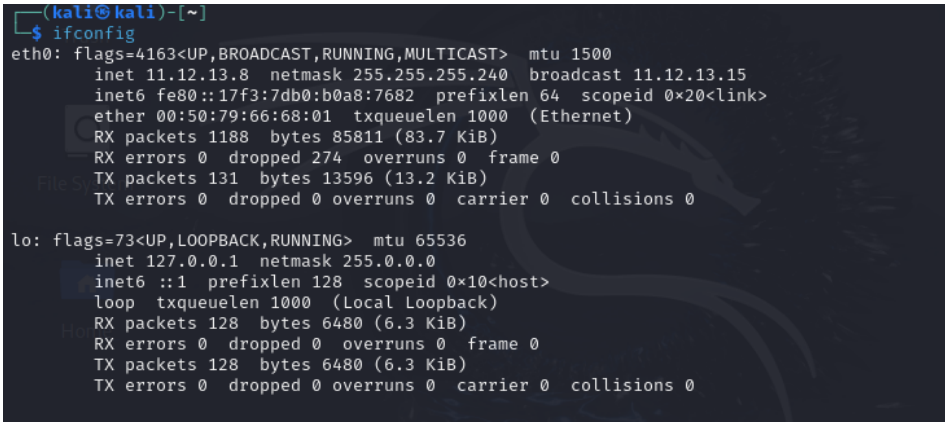

Imagen 14. Visualización IP de Kali (Se puede observar que es la misma que PC2)

Ping de PC1 a PC2 y captura de tráfico con Wireshark

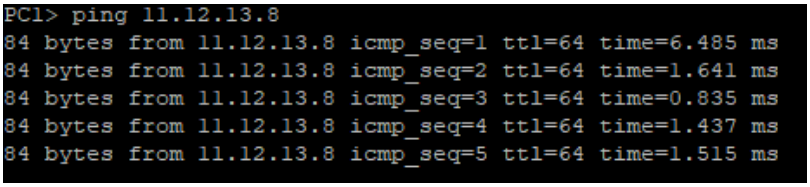

Imagen 15. Ping de PC1 a PC2

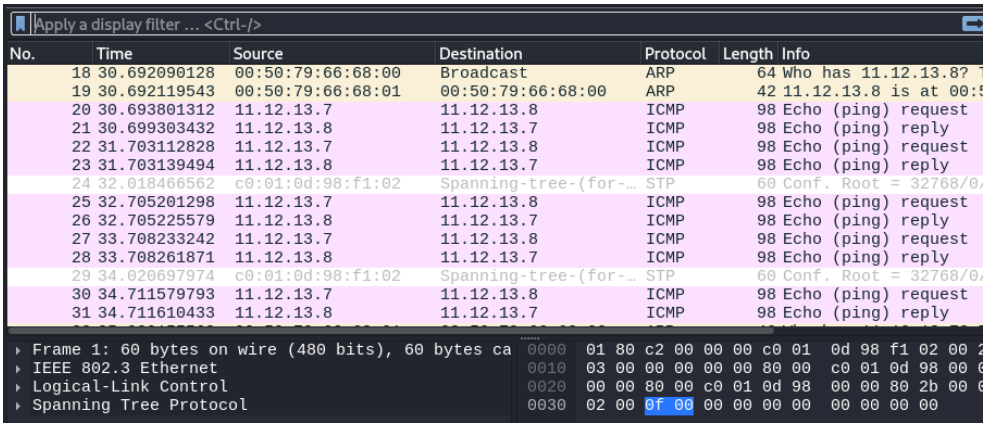

Imagen 16. Visualización tráfico de ping de PC1 a PC2

En las tablas de switch se muestra que PC2 **(f1/1)** fue movido al puerto de Kali **(f1/2).**

En la parte superior se observa la configuración original y en la parte inferior el cambio realizado.

```
ESW1#show mac-address-table vlan 1
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
c001.0d98.0000          Self          1    Vlan1
0050.7966.6801          Dynamic       1    FastEthernet1/1
0050.7966.6800          Dynamic       1    FastEthernet1/0

ESW1#show mac
ESW1#show mac-address-table vlan 1
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
c001.0d98.0000          Self          1    Vlan1
0050.7966.6800          Dynamic       1    FastEthernet1/0
0050.7966.6801          Dynamic       1    FastEthernet1/2
```

Imagen 17. Visualización de cambios en la tabla de direcciones MAC en ESW1

Restauración configuración original Kali (08:00:27:d2:26:79)

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# sudo ifconfig eth0 down

┌──(root㉿kali)-[/home/kali]
└─# sudo ifconfig eth0 hw ether 08:00:27:d2:26:79

┌──(root㉿kali)-[/home/kali]
└─# sudo ifconfig eth0 up
```

Imagen 18. Restauración de MAC de Kali

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 11.12.13.9  netmask 255.255.255.240  broadcast 11.12.13.15
        inet6 fe80::17f3:7db0:b0a8:7682  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:d2:26:79  txqueuelen 1000  (Ethernet)
        RX packets 2209  bytes 158295 (154.5 KiB)
        RX errors 0  dropped 494  overruns 0  frame 0
        TX packets 183  bytes 18500 (18.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 268  bytes 13480 (13.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 268  bytes 13480 (13.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Imagen 19. Visualización de MAC e IP de Kali

```
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
c001.0d98.0000           Self         1    Vlan1
0050.7966.6800           Dynamic      1    FastEthernet1/0
0050.7966.6801           Dynamic      1    FastEthernet1/1
0800.27d2.2679           Dynamic      1    FastEthernet1/2
```

Imagen 20. Revisión de tabla de direcciones físicas en ESW1

Analicé el tráfico capturado, desde el punto de vista de capa 2. Recuerde documentarse en las características del protocolo para identificar qué se esta portando y ¿Por qué?

No.	Time	Source	Destination	Protocol	Length	Info
21	28.872560436	11.12.13.7	11.12.13.9	ICMP	98	Echo (ping) request
22	28.872603517	11.12.13.9	11.12.13.7	ICMP	98	Echo (ping) reply
23	29.877238061	11.12.13.7	11.12.13.9	ICMP	98	Echo (ping) request
24	29.877268824	11.12.13.9	11.12.13.7	ICMP	98	Echo (ping) reply
25	30.018164541	c0:01:0d:98:f1:02	Spanning-tree-(for-…	STP	60	Conf. Root = 32768/0/
26	30.881310080	11.12.13.7	11.12.13.9	ICMP	98	Echo (ping) request
27	30.881333641	11.12.13.9	11.12.13.7	ICMP	98	Echo (ping) reply

Imagen 21. Captura de Ping de PC1 a Kali en Wireshark

Esta captura nos muestra un intercambio de información entre dos dispositivos en una red local, identificados por las direcciones IP 11.12.13.7 (PC1) y 11.12.13.9 (Kali). Los paquetes corresponden a un tipo de solicitud conocido como "ping" (protocolo ICMP), que se utiliza para verificar la conectividad entre dispositivos.

```
▸ Frame 21: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) o
▾ Ethernet II, Src: 00:50:79:66:68:00 (00:50:79:66:68:00), Dst: PCSSyst
  ▸ Destination: PCSSystemtec_d2:26:79 (08:00:27:d2:26:79)
  ▸ Source: 00:50:79:66:68:00 (00:50:79:66:68:00)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 11.12.13.7, Dst: 11.12.13.9
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x94e6 (38118)
  ▸ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0xb59b [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 11.12.13.7
    Destination Address: 11.12.13.9
```

Imagen 22. Desglose Trama de paquete 21

Wireshark nos proporciona un desglose detallado del paquete capturado en la red, mostrando tanto la capa de enlace como la de red.

Capa Ethernet II:

- Dirección MAC de origen: 00:50:79:66:68:00 (PC1)

- Dirección MAC de destino: 00:50:79:66:26:79 (Kali)

- Tipo: IPv4 (0x0800), indicando que el siguiente protocolo es IPv4.

Capa de red (IPv4):

- Versión: IPv4.

- Dirección IP de origen: 11.12.13.7 (PC1)

- Dirección IP de destino: 11.12.13.9 (Kali)

- Longitud total del paquete: 84 bytes.

- Identificación: 0x94e6 (38118).

- Time to Live (TTL): 64, lo que indica el número de saltos que le quedan al paquete antes de ser descartado.

- Protocolo: ICMP (1), lo que confirma que este paquete es un mensaje de control de red.

Análisis y Discusión:

- Analice cómo un atacante podría combinar la suplantación de la dirección MAC con un ataque de ARP spoofing para maximizar el impacto en una red local. Describa el flujo completo del ataque y sus posibles consecuencias.

  Rta: Un atacante puede combinar la suplantación de la dirección MAC con un ataque de ARP spoofing para maximizar el impacto en una red local, afectando la integridad, confidencialidad y disponibilidad de la red.

  Flujo completo del ataque

  - Reconocimiento de la red: El atacante comienza realizando un escaneo de la red local para identificar dispositivos y obtener información sobre las direcciones IP y las correspondientes direcciones MAC de los hosts importantes, como el router o gateway, servidores críticos, y otros dispositivos clave.

  - Suplantación de la dirección MAC: El atacante cambia su dirección MAC para coincidir con la dirección MAC de un dispositivo legítimo en la red, como el

router o un servidor clave. Este paso es crucial para evitar ser detectado por algunos mecanismos de seguridad, como filtros de dirección MAC en switches o firewalls que podrían permitir tráfico solo desde direcciones MAC específicas.

- ARP Spoofing (envenenamiento ARP): ARP (Address Resolution Protocol) es un protocolo que vincula direcciones IP con direcciones MAC en una red local. El atacante explota la falta de autenticación en ARP mediante el envío de respuestas ARP falsas a los dispositivos en la red. Esto provoca que ambos dispositivos actualicen sus tablas ARP con la información falsa, redirigiendo el tráfico hacia el atacante.

- Intercepción y manipulación del tráfico: Ahora, el atacante se encuentra en una posición de Man-in-the-Middle (MitM), donde todo el tráfico entre el router y la víctima pasa por el dispositivo del atacante. Herramientas como Ettercap, Cain & Abel, o Bettercap permiten ejecutar ARP spoofing y capturar el tráfico de manera sencilla.

- Mantenimiento del ataque: El atacante debe seguir enviando respuestas ARP falsas de manera continua para evitar que las tablas ARP en los dispositivos se actualicen con la información correcta. Los intervalos de actualización de ARP son cortos (aproximadamente cada 30 segundos), por lo que es necesario mantener el flujo de mensajes maliciosos.

Posibles consecuencias del ataque

- Intercepción de datos sensibles: Si el tráfico no está cifrado (como en redes HTTP), el atacante puede obtener credenciales, correos electrónicos, conversaciones, y cualquier tipo de información sensible que pase entre la víctima y otros dispositivos en la red.

- Modificación de datos: El atacante puede manipular los paquetes interceptados para modificar el contenido de las comunicaciones. Esto puede incluir redirigir a los usuarios a sitios web maliciosos o modificar archivos descargados para incluir malware.

- Destrucción o interrupción del servicio (Denial of Service, DoS): El atacante puede dejar de reenviar los paquetes, causando una interrupción del servicio para la víctima o incluso para toda la red, si logra realizar ARP spoofing en múltiples dispositivos a la vez, incluyendo el router.

- Acceso no autorizado: Con la suplantación de la dirección MAC y ARP spoofing, el atacante puede hacerse pasar por dispositivos autorizados y acceder a recursos de red que normalmente estarían restringidos, como servidores internos o redes privadas.

- Exposición de la red a ataques avanzados: El acceso a los datos y al control del tráfico puede servir como puerta de entrada a ataques más avanzados, como la escalada de privilegios, movimiento lateral dentro de la red, o incluso la instalación de un backdoor para persistencia.

- Alteración del enrutamiento de red: Un atacante podría redirigir el tráfico hacia otros hosts o hacia dispositivos controlados externamente, permitiendo ataques remotos o el desvío de tráfico fuera de la red local, exponiendo los datos a entidades externas.

- En un entorno con autenticación basada en 802.1X, explicar cómo este tipo de autenticación podría dificultar un ataque de suplantación de MAC y qué otras medidas podrían ser necesarias para reforzar la seguridad de la red.

  Rta: La autenticación basada en 802.1X proporciona un mecanismo sólido para evitar ataques de suplantación de direcciones MAC al requerir una autenticación antes de que un dispositivo pueda acceder a la red. Este estándar funciona como un protocolo de control de acceso a nivel de puerto para las redes conmutadas, y garantiza que solo los dispositivos autorizados pueden conectarse a la red, incluso si un atacante intenta suplantar una dirección MAC.

- Durante un ejercicio de hacking ético, ¿La suplantación de MAC afecta el tráfico como se esperaba? Identifique y discuta al menos tres posibles razones técnicas o de configuración de la red que podrían estar impidiendo el éxito del ataque.

  Rta: Durante un ejercicio de hacking ético, la suplantación de MAC puede no afectar el tráfico como se espera debido a varias razones técnicas o de configuración de la red. En primer lugar, las redes pueden estar implementando filtrado de direcciones MAC, lo que evita que una dirección no autorizada acceda a la red o genere tráfico. En segundo lugar, las VLAN (redes locales virtuales) o segmentación de red pueden estar configuradas para aislar el tráfico entre diferentes segmentos, dificultando la manipulación directa del tráfico. Finalmente, algunas redes implementan medidas de seguridad adicionales como el port security en los switches, que restringe la cantidad de direcciones MAC permitidas por puerto, impidiendo que la suplantación tenga éxito.

- En una red segmentada con VLANs, evalúe cómo un atacante podría aprovechar la suplantación de MAC para intentar saltar de una VLAN a otra. Detalle los desafíos técnicos y los métodos que podrían utilizarse para realizar este tipo de ataque.

  Rta: En una red segmentada con VLANs, un atacante podría intentar saltar de una VLAN a otra utilizando la suplantación de MAC para evadir las restricciones de segmentación. Para lograr esto, el atacante podría intentar manipular las tablas de

conmutación de los switches mediante la suplantación de la dirección MAC para que los paquetes se dirijan a una VLAN diferente.

Los desafíos técnicos incluyen la necesidad de conocimientos específicos sobre la configuración de VLANs y switches, así como la dificultad de obtener acceso a puertos de switch que permitan el tráfico entre VLANs. Además, los switches modernos suelen implementar mecanismos de seguridad como el Dynamic ARP Inspection o el VLAN Access Control List (VACL), que dificultan este tipo de ataques al validar y restringir el tráfico de acuerdo con las políticas de seguridad configuradas. Para superar estos desafíos, el atacante podría intentar técnicas avanzadas como el VLAN hopping, donde envía tramas etiquetadas con VLANs distintas para acceder a segmentos no autorizados.

- Considerando un entorno de red con monitoreo avanzado y detección de anomalías, analice cómo un atacante podría disfrazar la suplantación de una dirección MAC para evitar ser detectado. Discuta las técnicas de evasión que podrían ser empleadas y su efectividad.

  Rta: En un entorno de red con monitoreo avanzado y detección de anomalías, un atacante podría emplear varias técnicas para disfrazar la suplantación de una dirección MAC y evitar la detección.

  Una estrategia efectiva podría ser la modificación dinámica de la dirección MAC, cambiándola periódicamente para evitar que las herramientas de monitoreo identifiquen patrones inusuales. Además, el atacante podría utilizar técnicas de MAC address spoofing en combinación con tráfico cifrado para ocultar el origen real de los paquetes. Otra técnica sería la imitación de tráfico legítimo y la sincronización con el comportamiento de red normal, para no generar anomalías notables.

  También podrían utilizarse herramientas para fragmentar los paquetes o manipular los intervalos de envío, haciendo más difícil para los sistemas de detección identificar comportamientos sospechosos. La efectividad de estas técnicas depende de la sofisticación del sistema de monitoreo y la capacidad de la red para identificar patrones y anomalías en tiempo real.