
 <p>UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS</p>	Universidad Distrital FJDC	
	Ingeniería de Sistemas y Computación	
	Redes y Servicios	

Guía de Laboratorio Redes

Título del Experimento:

MAC Address Spoofing.

Objetivos:

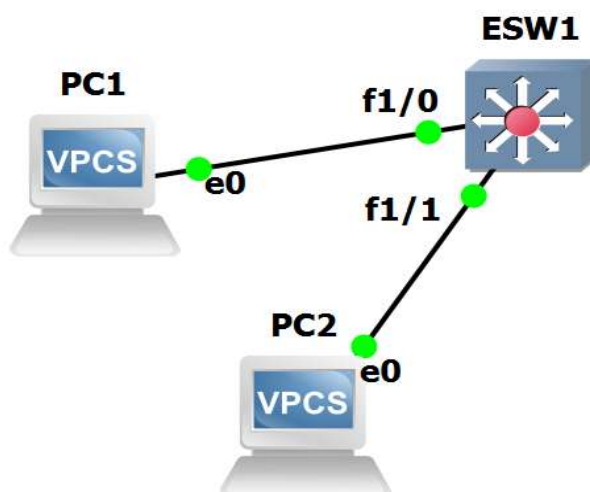
- Implementar un escenario de Hacking ético
- Implementar un red en GNS3 con equipos cisco y vulnerar el switch con Kali Linux.



Materiales:

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

Procedimiento:

1. Monte la topología descrita en GNS3 empleado un switch 2691



	Universidad Distrital FJDC	
	Ingeniería de Sistemas y Computación	
	Redes y Servicios	

2. Active el servicio de DHCP en el Switch:

```

ESW1# configure terminal
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
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-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-address 11.12.13.1 11.12.13.6
ESW1(config-if)#exit
ESW1#wr

```

3. Desde cada PC solicite DHCP

>ip dhcp

```

PC1> ip dhcp
DORA IP 11.12.13.7/28 GW 11.12.13.1



```

4. ARP en PCs

```

PC1> arp
00:50:79:66:68:01 11.12.13.8 expires in 73 seconds
PC1> █

```

 UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS	Universidad Distrital FJDC	
	Ingeniería de Sistemas y Computación	
	Redes y Servicios	

```
PC2> show ip

NAME       : PC2[1]
IP/MASK    : 0.0.0.0/0
GATEWAY    : 0.0.0.0
DNS        :
MAC        : 00:50:79:66:68:01
LPORT      : 20011
RHOST:PORT : 127.0.0.1:20012
MTU        : 1500
```

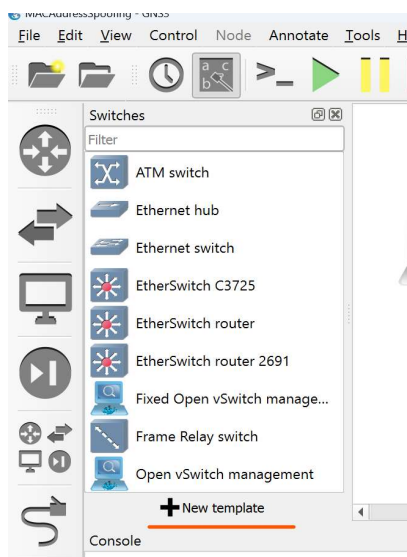
```
PC2> ip dhcp
DORA IP 11.12.13.9/28 GW 11.12.13.1
```



- Haga pruebas de conectividad y revise las tablas de direcciones físicas que se crean el switch:

```
ESW1#show mac-address-table vlan 1
Destination Address  Address Type  VLAN  Destination Port
-----
c001.0598.0000      Self         1     Vlan1
0a00.2700.0012      Dynamic      1     FastEthernet1/2
0800.275a.930b      Dynamic      1     FastEthernet1/2

ESW1#
```

- Conectar Kali: Se debe crear un nuevo template:



 UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS	Universidad Distrital FJDC	
	Ingeniería de Sistemas y Computación	
	Redes y Servicios	

New template

New template

Please select how you want to create a new template

- ☐ Install an appliance from the GNS3 server (recommended)
- ☐ Import an appliance file (.gns3a extension)
- ☒ Manually create a new template

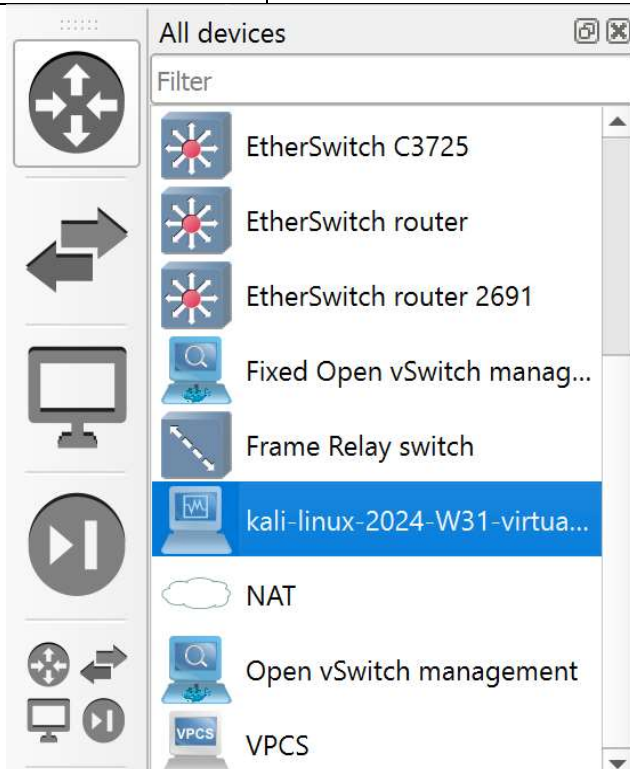
>Next > VirtualBox VMs

Preferences

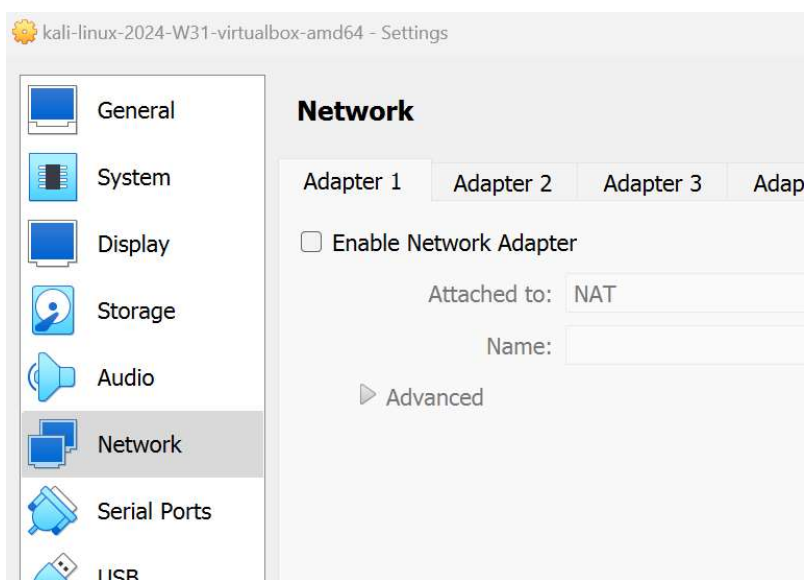
General
Server
GNS3 VM
Packet capture
Built-in
 Ethernet hubs
 Ethernet switches
 Cloud nodes
VPCS
 VPCS nodes
Dynamips
 IOS routers
IOS on UNIX
 IOU Devices
QEMU
 Qemu VMs
VirtualBox
 VirtualBox VMs
VMware



VirtualBox VM templates

Y carga la máquina de Kali si ya está elimínela y lo vuelve a realizar.

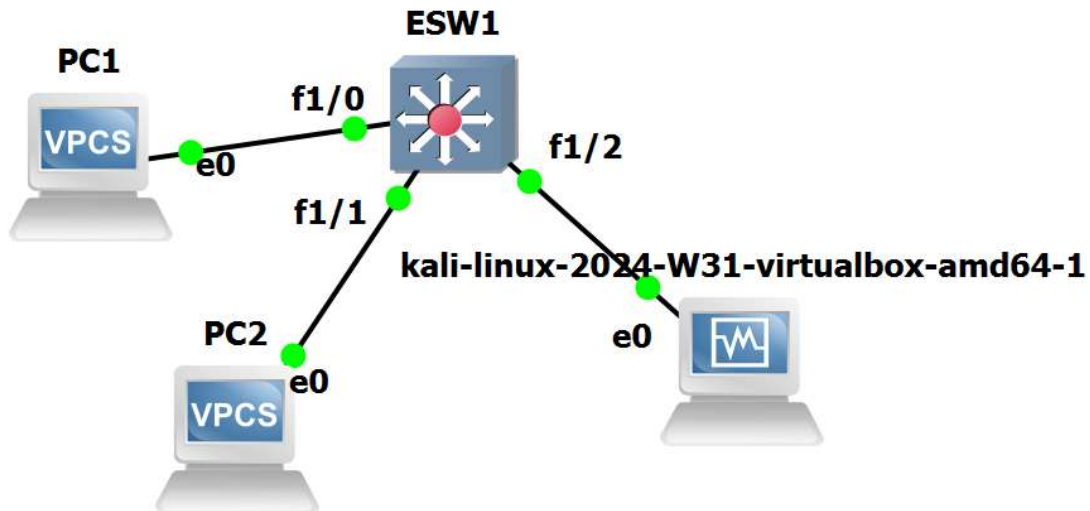


7. Para conectar Kali con GNS3 debe deshabilitar la tarjeta en la configuración de la maquina virtual.



	Universidad Distrital FJDC	
	Ingeniería de Sistemas y Computación	
	Redes y Servicios	

8. Inserte al Pc Kali a la topología y conéctelo



9. Active todos los dispositivos en GNS3 y automáticamente la máquina virtual de Kali se inicia:

Y desde un termina Kali: corrobore que recibió dirección por DHCP y haga ping a uno de los PC.

```

kali@kali: ~
File Actions Edit View Help
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 11.12.13.8 netmask 255.255.255.240 broadcast 11.12.13.15
    inet6 fe80::3e76:f07d:8b60:752b prefixlen 64 scopeid 0<link>
    ether 08:00:27:54:e1:f8 txqueuelen 1000 (Ethernet)
    RX packets 10 bytes 2292 (2.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 21 bytes 3040 (2.9 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 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 19 bytes 1129 (1.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 19 bytes 1129 (1.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$ ping 11.12.13.7
PING 11.12.13.7 (11.12.13.7) 56(84) bytes of data:
64 bytes from 11.12.13.7: icmp_seq=1 ttl=64 time=3.24 ms
64 bytes from 11.12.13.7: icmp_seq=2 ttl=64 time=1.49 ms
64 bytes from 11.12.13.7: icmp_seq=3 ttl=64 time=4.41 ms
64 bytes from 11.12.13.7: icmp_seq=4 ttl=64 time=1.79 ms
64 bytes from 11.12.13.7: icmp_seq=5 ttl=64 time=2.30 ms
  
```


10. Vuelva a revisar las tablas de direcciones física en el switch: ya debe aparecer la MAC de Kali.

```
ESW1#show mac-address-table vlan 1
Destination Address  Address Type  VLAN  Destination Port
-----
c001.0598.0000      Self         1      Vlan1
0050.7966.6800      Dynamic      1      FastEthernet1/0
0050.7966.6801      Dynamic      1      FastEthernet1/1
0800.2754.e1f8      Dynamic      1      FastEthernet1/2
ESW1#
```

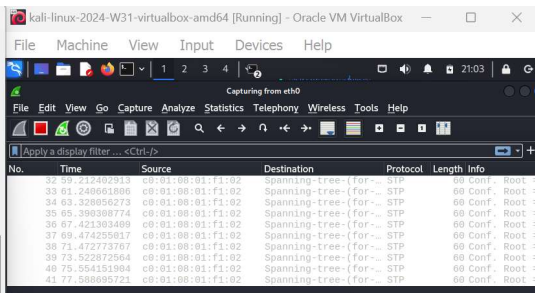
11. Antes de empezar el proceso de hacking ético, se corrobora que el Kali solo recibe tráfico cuando va hacia el:

PC1 hace ping a PC2 y en Wireshark corriendo en Kali no se recibe nada:

```
192.168.56.101 - PuTTY
84 bytes from 11.12.13.8 icmp_seq=5 ttl=64 time=1.422 ms

PC1> ping 11.12.13.9
84 bytes from 11.12.13.9 icmp_seq=1 ttl=64 time=0.149 ms
84 bytes from 11.12.13.9 icmp_seq=2 ttl=64 time=0.189 ms
84 bytes from 11.12.13.9 icmp_seq=3 ttl=64 time=0.179 ms
84 bytes from 11.12.13.9 icmp_seq=4 ttl=64 time=0.174 ms
84 bytes from 11.12.13.9 icmp_seq=5 ttl=64 time=0.160 ms

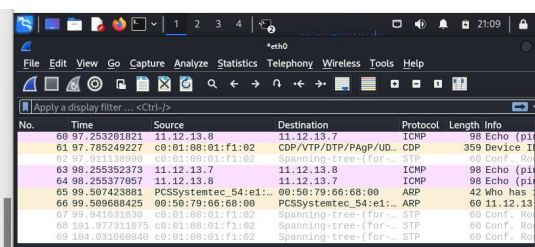
PC1> ping 11.12.13.9
84 bytes from 11.12.13.9 icmp_seq=1 ttl=64 time=0.159 ms
84 bytes from 11.12.13.9 icmp_seq=2 ttl=64 time=0.122 ms
84 bytes from 11.12.13.9 icmp_seq=3 ttl=64 time=0.146 ms
84 bytes from 11.12.13.9 icmp_seq=4 ttl=64 time=0.159 ms
84 bytes from 11.12.13.9 icmp_seq=5 ttl=64 time=0.370 ms
```



PC1 hace ping a Kali y se empieza a capturar tráfico en Wireshark

```
PC1> ping 11.12.13.9
84 bytes from 11.12.13.9 icmp_seq=1 ttl=64 time=0.159 ms
84 bytes from 11.12.13.9 icmp_seq=2 ttl=64 time=0.122 ms
84 bytes from 11.12.13.9 icmp_seq=3 ttl=64 time=0.146 ms
84 bytes from 11.12.13.9 icmp_seq=4 ttl=64 time=0.159 ms
84 bytes from 11.12.13.9 icmp_seq=5 ttl=64 time=0.370 ms

PC1> ping 11.12.13.8
84 bytes from 11.12.13.8 icmp_seq=1 ttl=64 time=1.149 ms
84 bytes from 11.12.13.8 icmp_seq=2 ttl=64 time=1.650 ms
84 bytes from 11.12.13.8 icmp_seq=3 ttl=64 time=1.259 ms
84 bytes from 11.12.13.8 icmp_seq=4 ttl=64 time=1.976 ms
84 bytes from 11.12.13.8 icmp_seq=5 ttl=64 time=1.473 ms
```



12. Para este ataque se cambia la MAC de Kali, logrando que el switch sea engañado:

#sudo su

#sudo ifconfig eth0 down

Se va a suplantar PC2 por lo cual se usa su MAC:

MAC : 00:50:79:66:68:01

```
#sudo ifconfig eth0 hw ether 00:50:79:66:68:01
```

```
#sudo ifconfig eth0 up
```

```
(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 00:50:79:66:68:01

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

13. Capture tráfico haciendo ping entre PC1 y PC2:

El switch le da la misma IP de PC2 a Kali por tener la misma MAC

```
PC2> show ip
NAME       : PC2[1]
IP/MASK    : 11.12.13.9/28
GATEWAY    : 11.12.13.1
DNS        : 8.8.8.4
DHCP SERVER: 11.12.13.2
DHCP LEASE : 23792, 26400/13200/23100
MAC        : 00:50:79:66:68:01
LPORT     : 20011
RHOST:PORT : 127.0.0.1:20012
MTU       : 1500

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::3e76:f87d:8b60:752b prefixlen 64 scopeid 0<20<link>
ether 00:50:79:66:68:01 txqueuelen 1000 (Ethernet)
RX packets 134 bytes 14313 (13.9 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 85 bytes 9086 (8.7 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 0<10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 79 bytes 4129 (4.0 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 79 bytes 4129 (4.0 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

PC1 hace ping a PC2 y Kali puede capturar el tráfico:

```
84 bytes from 11.12.13.9 icmp_seq=5 ttl=64 time=0.370 ms
PC1> ping 11.12.13.8
84 bytes from 11.12.13.8 icmp_seq=1 ttl=64 time=1.149 ms
84 bytes from 11.12.13.8 icmp_seq=2 ttl=64 time=1.650 ms
84 bytes from 11.12.13.8 icmp_seq=3 ttl=64 time=1.259 ms
84 bytes from 11.12.13.8 icmp_seq=4 ttl=64 time=1.976 ms
84 bytes from 11.12.13.8 icmp_seq=5 ttl=64 time=1.473 ms
PC1> ping 11.12.13.9
84 bytes from 11.12.13.9 icmp_seq=1 ttl=64 time=1.562 ms
84 bytes from 11.12.13.9 icmp_seq=2 ttl=64 time=1.654 ms
84 bytes from 11.12.13.9 icmp_seq=3 ttl=64 time=1.660 ms
84 bytes from 11.12.13.9 icmp_seq=4 ttl=64 time=1.332 ms
84 bytes from 11.12.13.9 icmp_seq=5 ttl=64 time=1.247 ms
```



No.	Time	Source	Destination	Protocol	Length	Info
20	20.805170940	11.12.13.9	11.12.13.7	ICMP	98	Echo (pi...
21	21.589116350	00:01:08:01:f1:02	CDP/VTP/OT...	CDP	359	Device I...
22	21.807877500	11.12.13.7	11.12.13.9	ICMP	98	Echo (pi...
23	21.807900263	11.12.13.9	11.12.13.7	ICMP	98	Echo (pi...
24	22.197710800	00:01:08:01:f1:02	Spanning-tree (for...	STP	68	Conf. Ro...
25	22.808997906	11.12.13.7	11.12.13.9	ICMP	98	Echo (pi...
26	22.809026470	11.12.13.9	11.12.13.7	ICMP	98	Echo (pi...
27	24.861626051	00:50:79:66:68:01	00:50:79:66:68:00	ARP	42	Who has ...
28	24.866448056	00:50:79:66:68:00	00:50:79:66:68:01	ARP	60	11.12.13...
29	24.235210979	00:01:08:01:f1:02	Spanning-tree (for...	STP	68	Conf. Ro...

PC2 hace ping a PC1 y Kali también puede capturar esa interacción

```
PC2> ping 11.12.13.7
84 bytes from 11.12.13.7 icmp_seq=1 ttl=64 time=1.095 ms
84 bytes from 11.12.13.7 icmp_seq=2 ttl=64 time=0.157 ms
```

No.	Time	Source	Destination	Protocol	Length	Info
46	87.530578889	00:01:08:01:f1:02	Spanning-tree (for...	STP	68	Conf. Ro...
47	88.854933542	11.12.13.9	11.12.13.7	ICMP	98	Echo (pi...
48	89.553843384	00:01:08:01:f1:02	Spanning-tree (for...	STP	68	Conf. Ro...
49	90.808140486	00:01:08:01:f1:02	CDP/VTP/OT...	CDP	359	Device I...
50	91.519392942	00:01:08:01:f1:02	Spanning-tree (for...	STP	68	Conf. Ro...
51	93.561849247	00:01:08:01:f1:02	Spanning-tree (for...	STP	68	Conf. Ro...

Y en las tablas del switch: muestra que PC2 sea movido al puerto de Kali.

 UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS	Universidad Distrital FJDC		
	Ingeniería de Sistemas y Computación		
	Redes y Servicios		

```
ESW1#show mac-address-table vlan 1
Destination Address  Address Type  VLAN  Destination Port
-----
c001.0598.0000      Self         1     Vlan1
0050.7966.6801      Dynamic      1     FastEthernet1/2
```

13. Restaure la MAC de Kali a su valor por defecto:

```
# sudo ifconfig eth0 down
```

```
#sudo ifconfig eth0 hw ether 08:00:27:54:e1:f8
```

```
#sudo ifconfig eth0 up
```

```
#ifconfig
```

```
(root@kali)-[/home/kali]
# sudo ifconfig eth0 down

(root@kali)-[/home/kali]
# sudo ifconfig eth0 hw ether 08:00:27:54:e1:f8

(root@kali)-[/home/kali]
# sudo ifconfig eth0 up



(root@kali)-[/home/kali]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 11.12.13.8 netmask 255.255.255.240 broadcast 11.12.13.15
    inet6 fe80::3e76:f07d:8b60:752b prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:54:e1:f8 txqueuelen 1000 (Ethernet)
    RX packets 408 bytes 34716 (33.9 KiB)
```

La IP ahora es otra vez 11.12.13.8

Y en la tabla del switch ahora muestra que Kali está en el puerto que antes estaba PC2

```
ESW1#show mac-address-table vlan 1
Destination Address  Address Type  VLAN  Destination Port
-----
c001.0598.0000      Self         1     Vlan1
0800.2754.e1f8      Dynamic      1     FastEthernet1/2
```

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

	Universidad Distrital FJDC	
	Ingeniería de Sistemas y Computación	
	Redes y Servicios	

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.
- 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.
- 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.
- 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.
- 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.

Resultados:

- Realice un informe en .pdf donde documenta sus resultados y responde las preguntas.