



---

# ATAQUES

---

ING. MG. ANDREA SANCHEZ



ADMINISTRACIÓN DE REDES  
UNIVERSIDAD TÉCNICA DE AMBATO  
MUNIR CASTRO

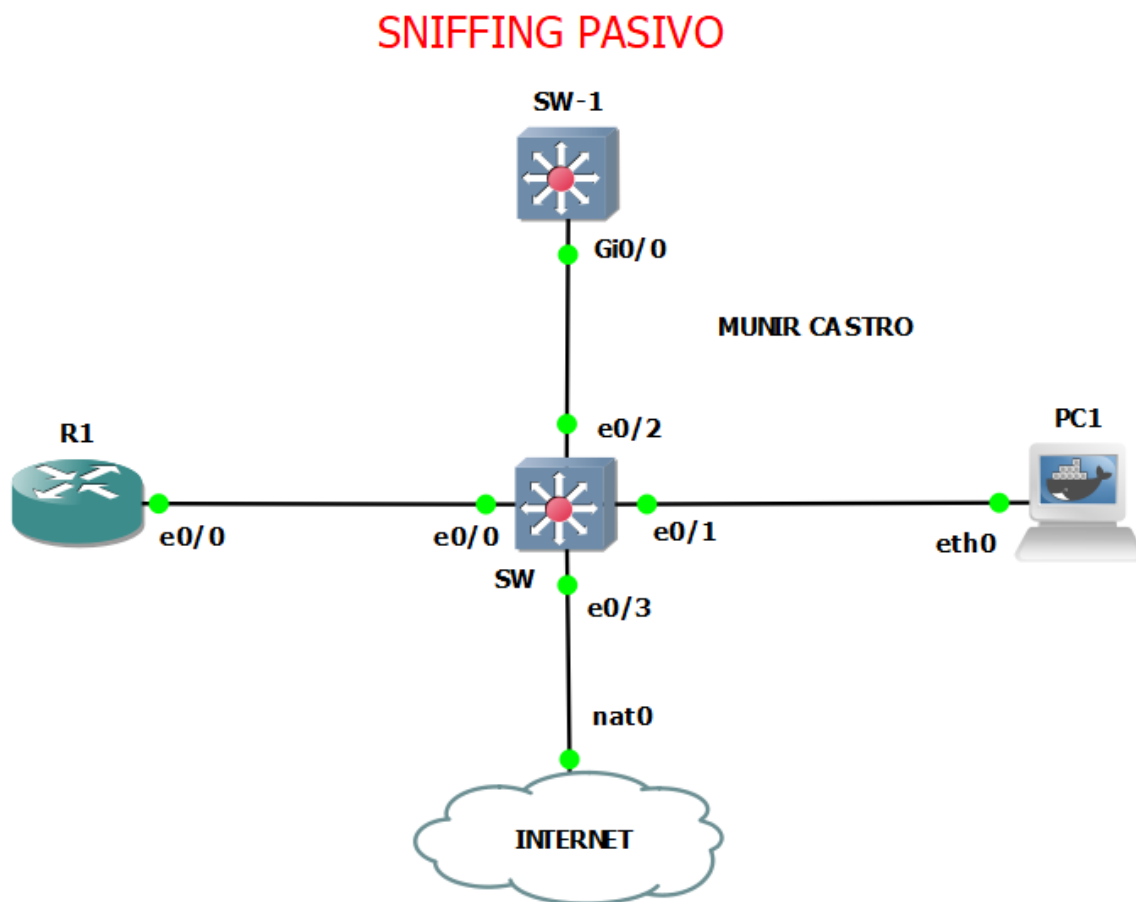
## Contenido

<b>SNIFFING PASIVO</b> .....	2
<b>Esquema:</b> .....	2
<b>Contramedidas:</b> .....	6
<b>VLAN VLAN-HOPPING</b> .....	8
<b>Esquema:</b> .....	8
<b>Contramedidas:</b> .....	13
<b>Ataque MiTM (hombre en la mitad)</b> .....	14
<b>Esquema:</b> .....	14
<b>Contramedidas:</b> .....	17

## SNIFFING PASIVO

El sniffing pasivo es una técnica utilizada en el campo de la seguridad informática y la administración de redes para capturar y analizar el tráfico de datos que circula por una red sin modificar su contenido ni interferir en su tránsito. Este método permite a un analista o a un atacante capturar datos que se envían y reciben en una red, como correos electrónicos, contraseñas, mensajes instantáneos y otra información sensible.

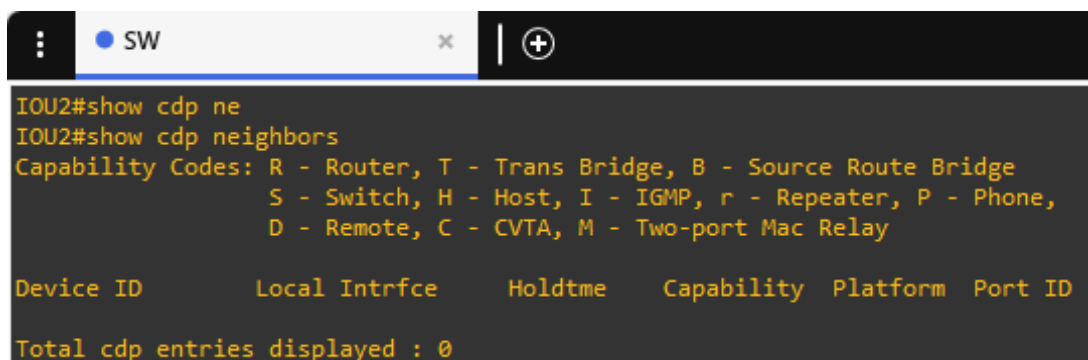
Esquema:



- Primero, una vez establecidas las conexiones correspondientes, se ingresa al SWITCH SW (IOU2) y se verifica con el siguiente comando **“show cdp neighbors”**. Este comando sirve para:
  1. **Verificar Conexiones Directas:** Permite comprobar qué dispositivos están conectados directamente al switch, proporcionando una lista detallada de los vecinos inmediatos.
  2. **Obtener Información de Dispositivos Vecinos:** Muestra información relevante sobre los dispositivos vecinos, como su

identificador (nombre del dispositivo), la interfaz local a la que están conectados, el tiempo de retención de la información (holdtime), las capacidades del dispositivo (como si es un switch, router, etc.), la plataforma (tipo de hardware) y la interfaz remota (port ID).

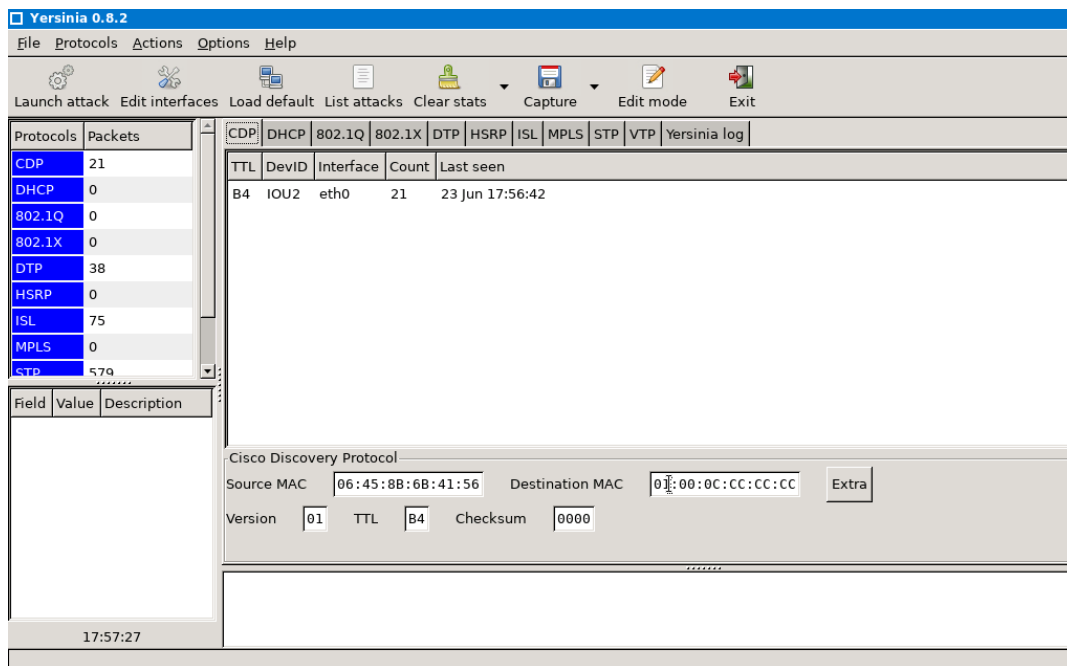
3. **Diagnosticar Problemas de Red:** Facilita la identificación de problemas de conectividad y configuración en la red. Al conocer qué dispositivos están conectados a qué interfaces, los administradores pueden localizar y resolver problemas de forma más eficiente.
4. **Mapear la Topología de la Red:** Ayuda a construir un mapa topológico de la red, lo cual es crucial para la gestión y planificación de la infraestructura de red. Saber cómo están interconectados los dispositivos permite una mejor administración y optimización de los recursos de red.



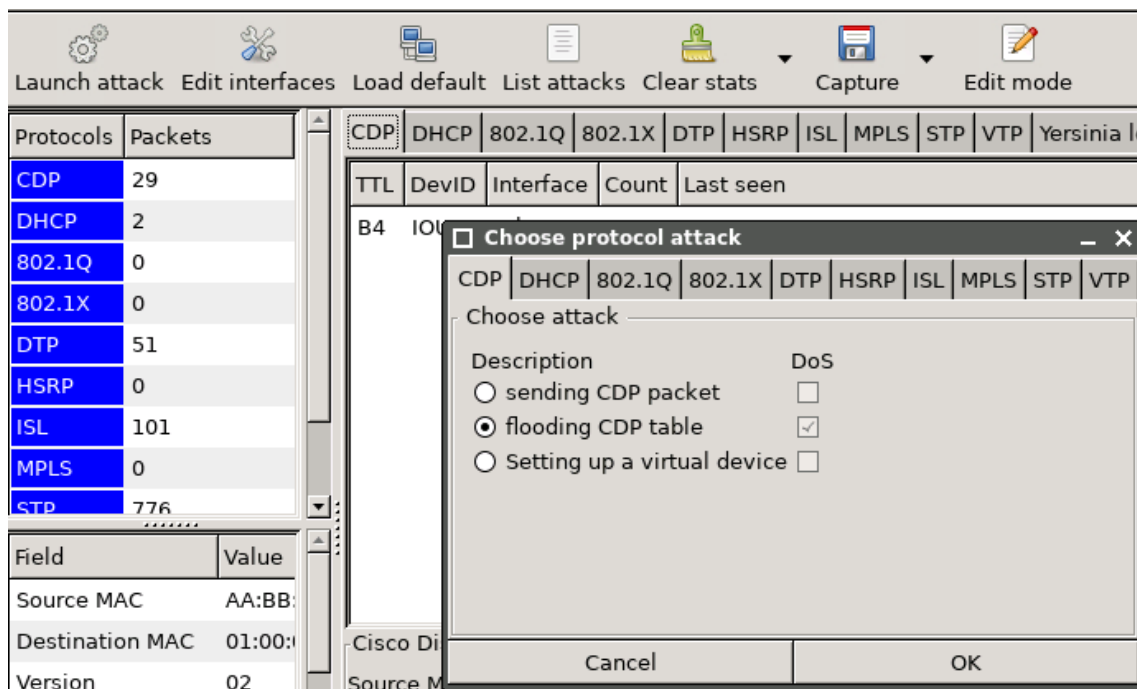
```
IOU2#show cdp ne
IOU2#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID          Local Intrfce   Holdtme    Capability Platform Port ID
Total cdp entries displayed : 0
```

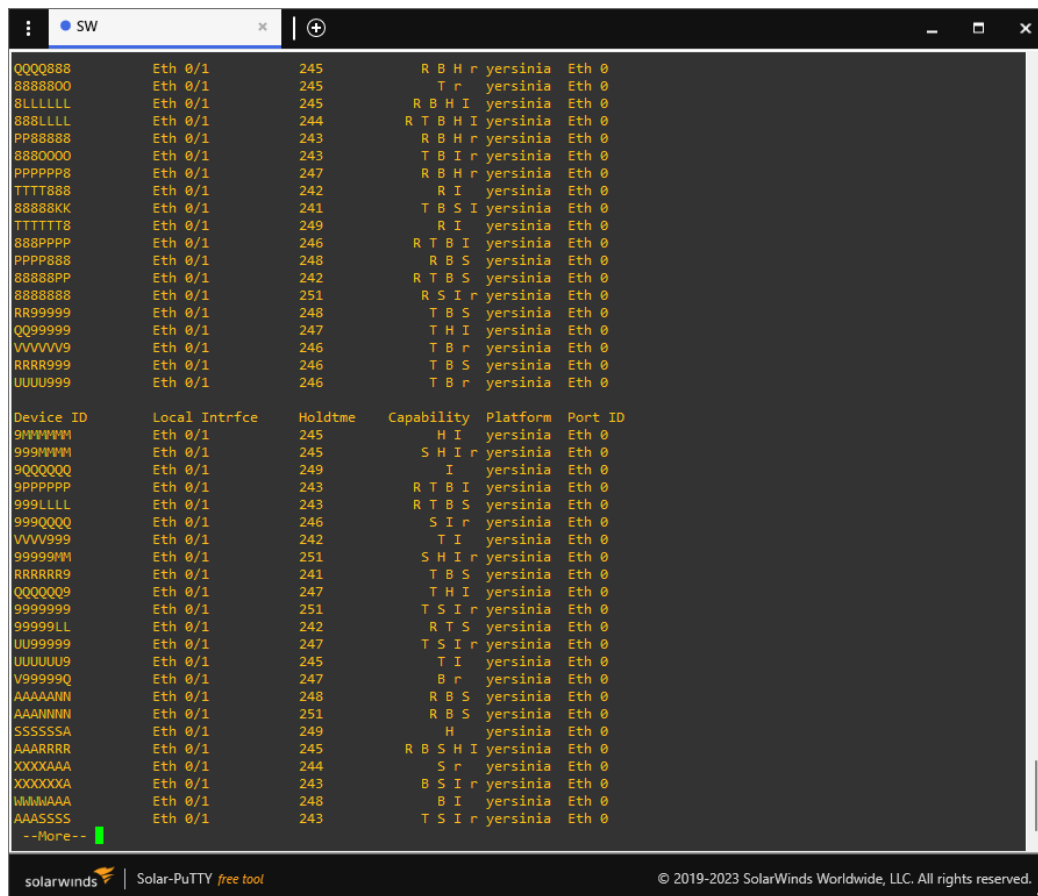
- Segundo, se edita la configuración del equipo atacante en su “edit config” descomentando las líneas “**auto eth0 & iface eth0 inet dhcp**”, realizado esta configuración, se debe abrir ahora la PC, dentro de la misma se debe actualizar sus librerías mediante el comando “**apt-get update -y**” realizado esto, se procede a instalar WIRESHARK & YERSINIA, utilizando el comando “**apt-get install wireshark yersinia -y**”.
- Tercero, una vez instalado YERSINIA & WIRESHARK, se utiliza el comando “**yersinia -G**” para abrir la aplicación y realizar el ataque.



- Cuarto, dentro de la aplicación Yersinia, se inicia el ataque seleccionando la opción **"Launch Attack"**. Esto despliega un menú de opciones, donde se elige **"CDP"** y luego **"flooding cdp table"**. Este ataque tiene como objetivo inundar la tabla CDP del switch con mensajes falsos, lo que puede interrumpir la función normal del protocolo CDP y degradar el rendimiento del dispositivo de red. Esta técnica es útil para pruebas de penetración y para evaluar la robustez de la infraestructura de red frente a este tipo de ataques.



- Se inicia el ataque y se verifica en el switch SW (IOU 2) para confirmar que el ataque se ha llevado a cabo correctamente. Este paso es crucial para asegurar que la inyección de mensajes falsos en la tabla CDP del switch se está realizando como se esperaba. La verificación incluye la observación de cualquier interrupción en la función normal del protocolo CDP y la degradación del rendimiento del dispositivo de red. Esta validación no solo garantiza la efectividad del ataque, sino que también proporciona información valiosa sobre la capacidad del switch para manejar y mitigar tales ataques.



Para mitigar un ataque de inundación de la tabla CDP en un switch, se deben desactivar CDP en puertos no necesarios, configurar listas de control de acceso para restringir el tráfico a dispositivos autorizados, usar sistemas de monitoreo para detectar comportamientos anómalos,

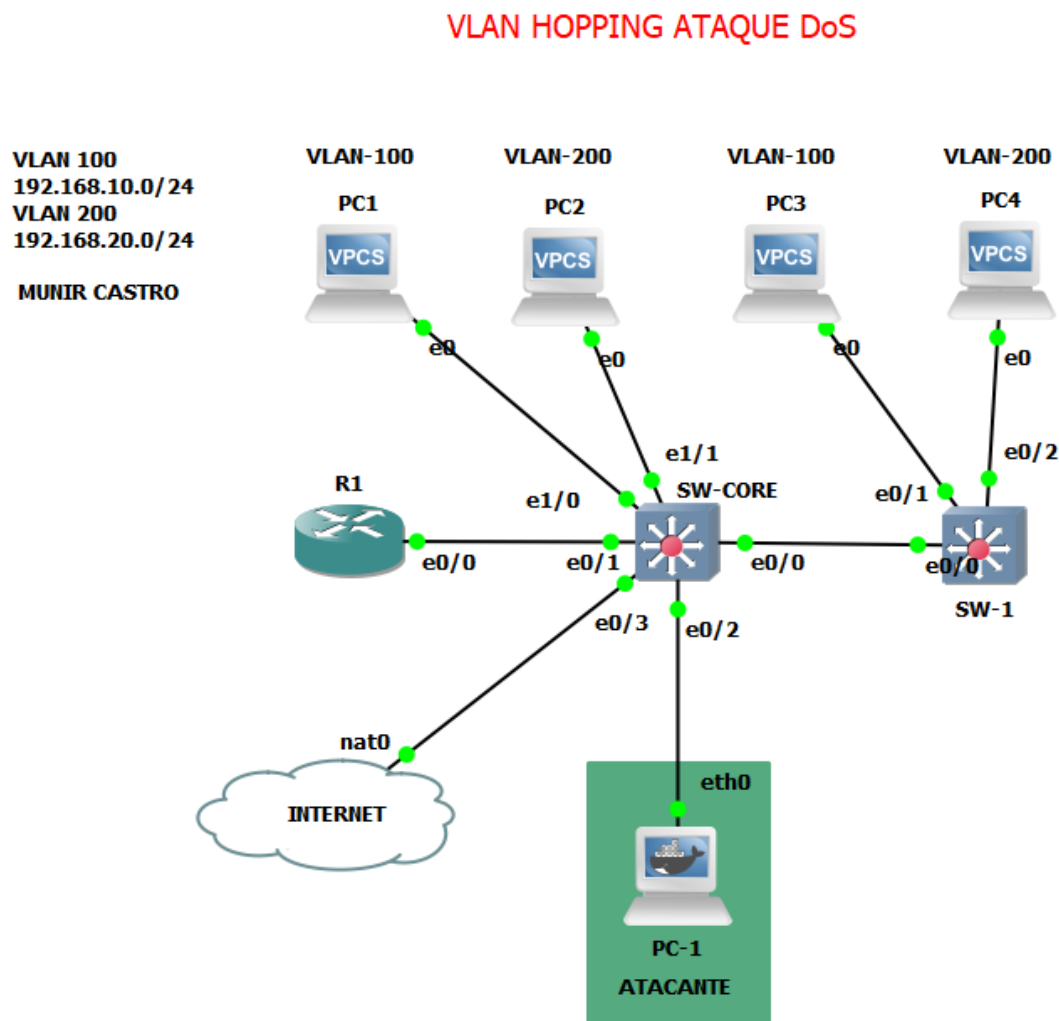
aplicar límites de tasa para el tráfico CDP, segmentar la red mediante VLANs y mantener los dispositivos actualizados con los últimos parches de seguridad.



## VLAN VLAN-HOPPING

Las VLANs (Redes de Área Local Virtuales) son una tecnología que permite segmentar una red física en múltiples redes lógicas, mejorando la seguridad y eficiencia del tráfico de red. Sin embargo, las VLANs no están exentas de vulnerabilidades. Una de las técnicas de ataque más conocidas es el VLAN Hopping, donde un atacante explota configuraciones incorrectas de la red para saltar de una VLAN a otra, accediendo a segmentos de red que deberían estar aislados. Esto puede comprometer la seguridad y permitir el acceso no autorizado a recursos sensibles.

Esquema:



- Primero, se crean y asignan VLANs específicas a cada uno de los switches, garantizando que cada segmento de red tenga su propia VLAN dedicada. Además, se configura cada una de las interfaces de los switches conectados a los dispositivos para que pertenezcan a la VLAN correspondiente. Esta configuración incluye la asignación de puertos de acceso a las VLANs designadas, lo cual asegura que cada dispositivo solo pueda comunicarse dentro de su propio segmento de red.

- El comando **switchport trunk encapsulation dot1q** se utiliza en dispositivos Cisco para especificar el tipo de encapsulación de trunk que se utilizará en un puerto de switch configurado como trunk. Permite que el puerto trunk transporte tráfico de múltiples VLANs entre switches, routers y otros dispositivos de red que estén configurados para usar VLANs..
  - **SW-CORE**

```
SW-CORE#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Et0/1, Et0/2, Et0/3, Et1/2 Et1/3, Et2/0, Et2/1, Et2/2 Et2/3, Et3/0, Et3/1, Et3/2 Et3/3
100	p1	active	Et1/0
200	p2	active	Et1/1
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

```
SW-CORE#
```

```

SW-CORE
SW-1

interface Ethernet0/0
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet1/0
  switchport access vlan 100
  switchport mode access
!
interface Ethernet1/1
  switchport access vlan 200
  switchport mode access
!

```

- **SW-1**

```
SW-1#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Et0/3, Et1/0, Et1/1, Et1/2 Et1/3, Et2/0, Et2/1, Et2/2 Et2/3, Et3/0, Et3/1, Et3/2 Et3/3
100	p1	active	Et0/1
200	p2	active	Et0/2
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

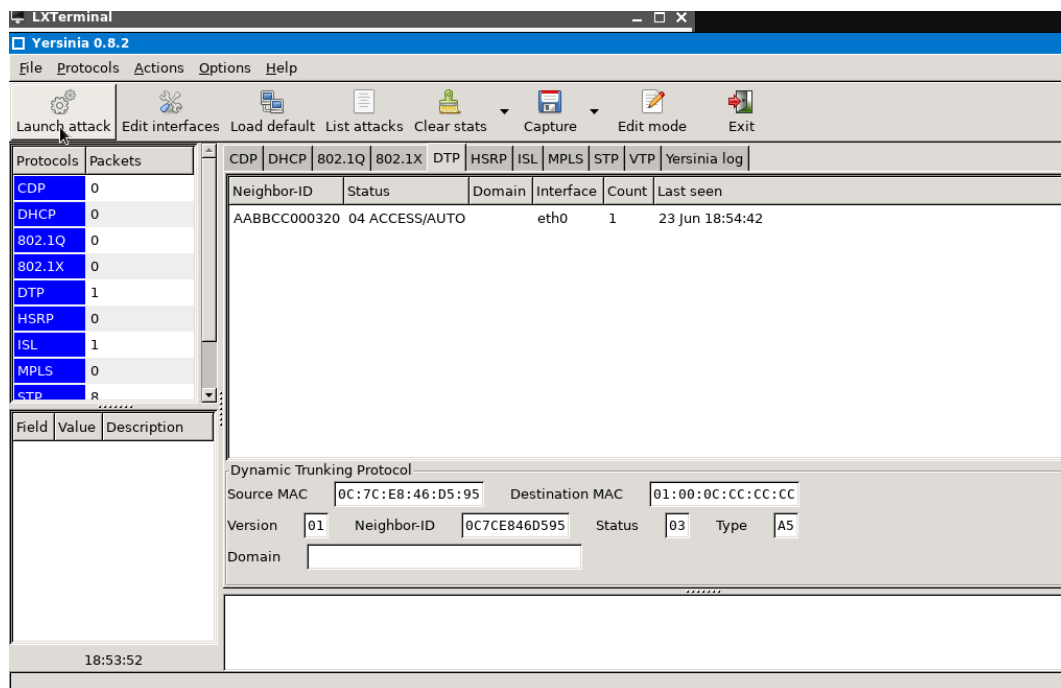
```
SW-1#
```

```

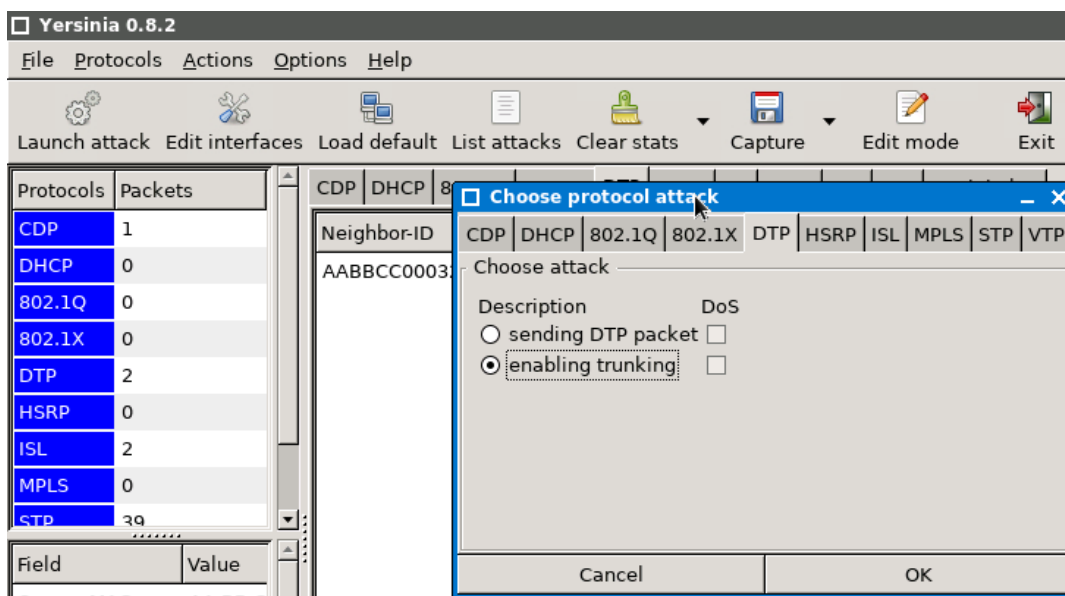
!
!
!
interface Ethernet0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Ethernet0/1
 switchport access vlan 100
 switchport mode access
!
interface Ethernet0/2
 switchport access vlan 200
 switchport mode access
!

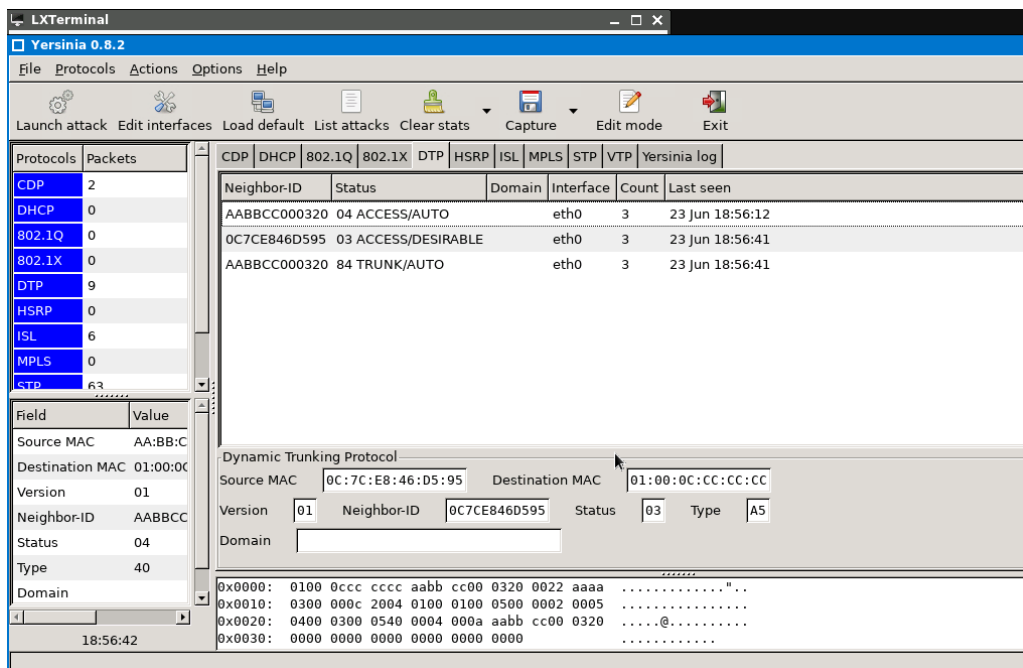
```

- Segundo, se edita la configuración del equipo atacante en su “edit config” descomentando las líneas “**auto eth0 & iface eth0 inet dhcp**”, realizado esta configuración, se debe abrir ahora la PC, dentro de la misma se debe actualizar sus librerías mediante el comando “**apt-get update -y**” realizado esto, se procede a instalar WIRESHARK & YERSINIA, utilizando el comando “**apt-get install wireshark yersinia -y**”.
- Tercero, una vez instalado YERSINIA & WIRESHARK, se utiliza el comando “**yersinia -G**” para abrir la aplicación y realizar el ataque.



- Cuarto, dentro de la aplicación Yersinia, se inicia el ataque seleccionando la opción **"Launch Attack"**. Esto despliega un menú de opciones, donde se elige **"DTP"** y luego **"enabling trunking"**. Este ataque tiene como objetivo inundar la tabla de asignación de puertos dinámicos (DTP) del switch con mensajes falsos, lo que puede llevar a la activación del trunking en puertos no autorizados y comprometer la seguridad de la red al permitir el acceso no autorizado a múltiples VLANs.





- Tras iniciar el ataque, se procede a verificar en el switch SW-CORE para confirmar su éxito. La inspección revela la habilitación de puertos trunk, lo que facilita al atacante establecer conexiones entre diversas VLAN. Esta vulnerabilidad compromete la seguridad de la red al permitir el acceso no autorizado a segmentos de red que deberían estar aislados.

```
SW-CORE#show interfaces trunk

Port      Mode      Encapsulation  Status        Native vlan
Et0/0     on        802.1q         trunking      1
Et0/2     auto      n-802.1q       trunking      1

Port      Vlans allowed on trunk
Et0/0     1-4094
Et0/2     1-4094

Port      Vlans allowed and active in management domain
Et0/0     1,100,200
Et0/2     1,100,200

Port      Vlans in spanning tree forwarding state and not pruned
Et0/0     1,100,200
Et0/2     1,100,200
SW-CORE#
```

**Yersinia 0.8.2**

File Protocols Actions Options Help

Launch attack Edit interfaces Load default List attacks Clear stats Capture Edit mode Exit

Protocols	Packets
CDP	4
DHCP	0
802.1Q	0
802.1X	0
DTP	16
HSRP	0
ISL	6
MPLS	0
STP	125

Neighbor-ID	Status	Domain	Interface	Count	Last seen
AABBCC000320	04 ACCESS/AUTO		eth0	3	23 Jun 18:56:12
0C7CE846D595	03 ACCESS/DESIRABLE		eth0	3	23 Jun 18:56:41
AABBCC000320	84 TRUNK/AUTO		eth0	7	23 Jun 18:58:42
0C7CE846D595	83 TRUNK/DESIRABLE		eth0	4	23 Jun 18:58:44

Field Value

Source MAC AA:BB:C

Destination MAC 01:00:0C

Version 01

Neighbor-ID AABBCC

Status 04

Type 40

Domain

Dynamic Trunking Protocol

Source MAC 0C:7C:E8:46:D5:95 Destination MAC 01:00:0C:CC:CC:CC

Version 01 Neighbor-ID 0C7CE846D595 Status 03 Type A5

Domain

0x0000: 0100 0ccc cccc aabb cc00 0320 0022 aaaa .....  
 0x0010: 0300 000c 2004 0100 0100 0500 0002 0005 .....  
 0x0020: 0400 0300 0540 0004 000a aabb cc00 0320 .....@.....  
 0x0030: 0000 0000 0000 0000 0000 0000 .....  
 18:58:44

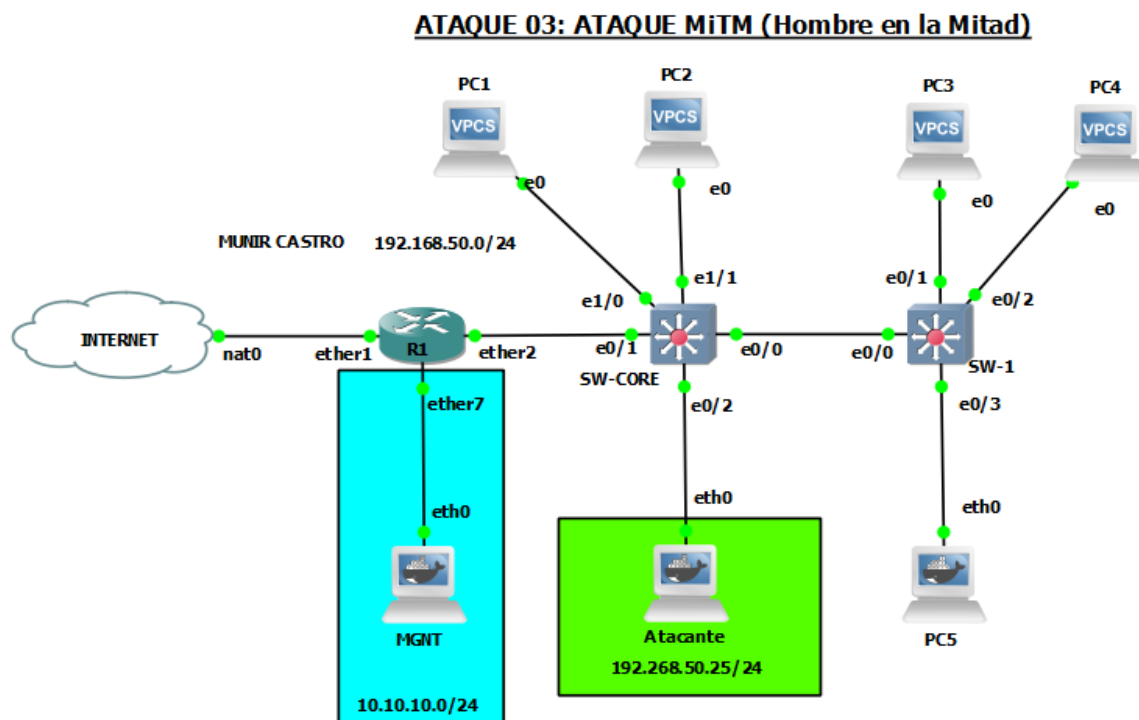
## Contramiedidas:

Para mitigar el ataque VLAN Hopping, es esencial desactivar DTP en puertos no utilizados mediante el comando `switchport nonegotiate`, asignar puertos no utilizados a una VLAN específica que no se use en otros lugares, habilitar la autenticación en puertos de acceso y trunking, aplicar listas de control de acceso (ACLs) para restringir el tráfico no autorizado entre VLANs, y utilizar PVLANS (Private VLANs) para un aislamiento adicional. Estas medidas combinadas aumentan la seguridad de la red y previenen el acceso no autorizado entre diferentes VLANs.

## Ataque MiTM (hombre en la mitad)

El Ataque de Hombre en el Medio (MiTM, por sus siglas en inglés "Man-in-the-Middle") es una técnica de ciberataque donde un atacante intercepta y manipula la comunicación entre dos partes, sin que ninguna de ellas sea consciente de la presencia del atacante. En este escenario, el atacante puede leer, modificar e incluso insertar mensajes en la comunicación, lo que le permite robar información confidencial, como contraseñas, datos bancarios o credenciales de inicio de sesión.

### Esquema:



- **SW-CORE**

Se configura el servicio DHCP dentro del SW-CORE con el propósito de proporcionar direcciones IP dinámicas a los dispositivos de la red, lo que simplifica la gestión de direcciones IP y facilita la conectividad de los dispositivos sin necesidad de configuraciones manuales. Asimismo, se establece la VLAN 1 y se le asigna una dirección IP con el fin de organizar y segmentar el tráfico de red en subredes virtuales, lo que mejora la eficiencia y la seguridad de la red al permitir la comunicación entre dispositivos dentro de la misma VLAN.

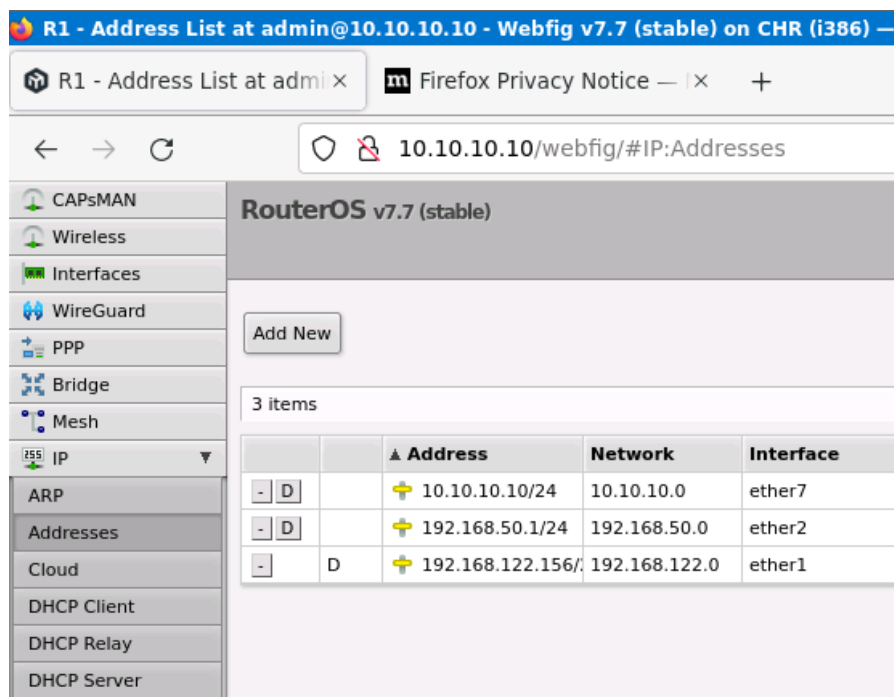
```

!
no ip icmp rate-limit unreachable
!
ip dhcp excluded-address 192.168.50.1 192.168.50.19
!
ip dhcp pool LAN-1
network 192.168.50.0 255.255.255.0
default-router 192.168.50.1
dns-server 1.1.1.1
!
!

interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
ip address 192.168.50.2 255.255.255.0
!
ip forward-protocol nd
!
!

```

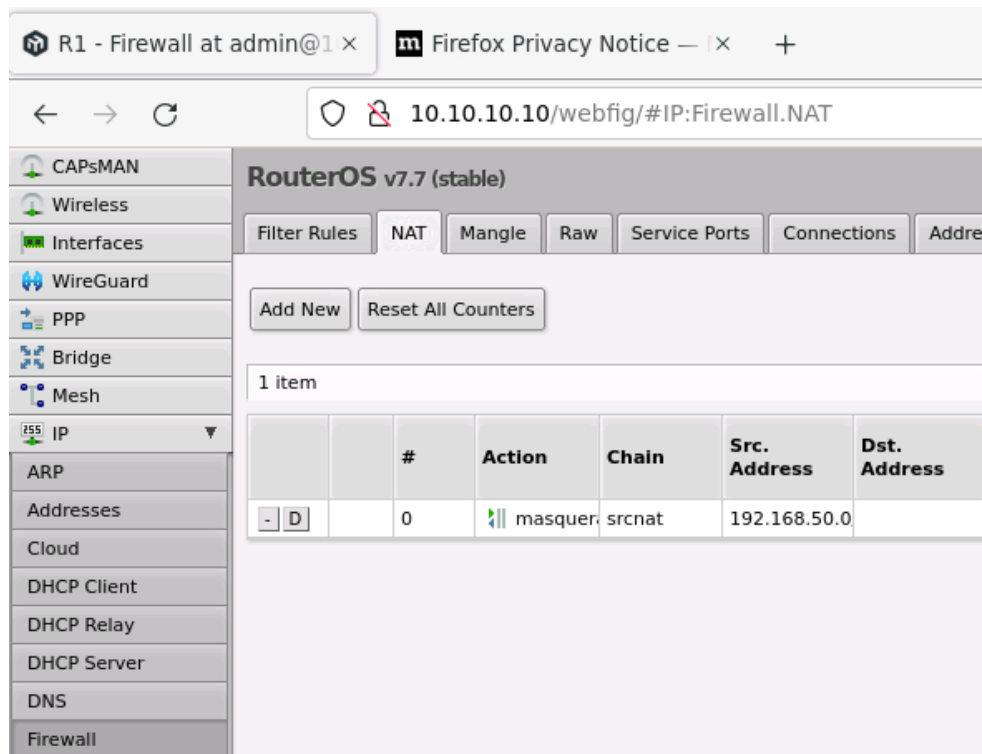
- **Addresses**



- **Firewall**

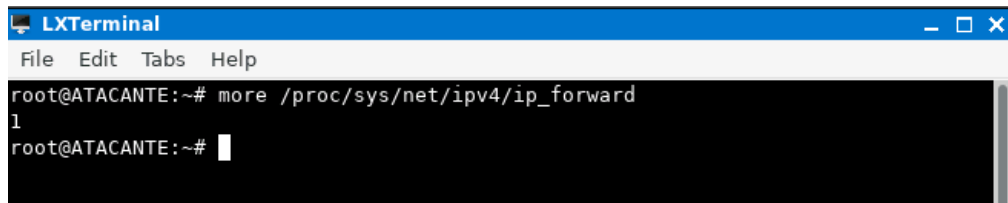
En la configuración del firewall, se establece la regla NAT **action masquerade** con destino a la IP 192.168.50.0/24. Esta regla tiene como función principal enmascarar las direcciones IP de origen de los paquetes que provienen de la red 192.168.50.0/24, reemplazándolas por la dirección IP pública del dispositivo de salida.



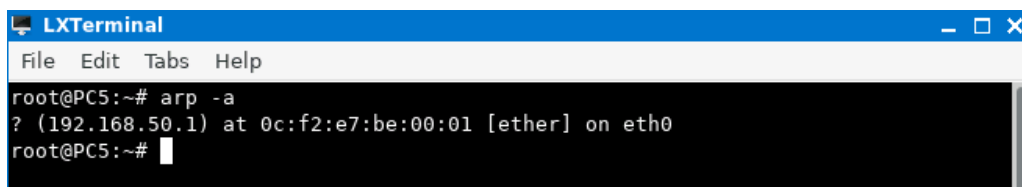


- **Atacante**

El comando **more /proc/sys/net/ipv4/ip\_forward** se utiliza para ver el contenido del archivo "ip\_forward" en el sistema de archivos /proc, que controla el reenvío de paquetes IP (IP forwarding) en sistemas Linux.



- **PC5**



- **Mikrotik**

```
[admin@R1] > ip arp print
Flags: D, P - PUBLISHED; C - COMPLETE
Columns: ADDRESS, MAC-ADDRESS, INTERFACE
#   ADDRESS      MAC-ADDRESS     INTERFACE
0 DC 192.168.50.25  0E:61:BF:5D:04:E5 ether2
1 D  192.168.50.20  8E:01:89:8A:71:77 ether2
2 DC 192.168.122.1  52:54:00:75:42:AF ether1
3 D  192.168.50.23  EA:44:51:67:5F:51 ether2
4 DC 192.168.50.24  46:A2:0E:09:D8:54 ether2
5 DC 192.168.50.21  CA:53:7B:04:85:9A ether2
```

### **Contramedidas:**

Para contrarrestar un ataque de Hombre en el Medio (MiTM), es crucial implementar varias contramedidas. Estas incluyen el uso de protocolos seguros como HTTPS en lugar de HTTP para la comunicación web, la autenticación mutua mediante certificados digitales, el uso de redes privadas virtuales (VPN) para cifrar el tráfico entre puntos finales y la segmentación de la red para reducir la superficie de ataque.