

Criptografía y Seguridad de la Información



Tema:

Laboratorio Hacking Ético

Curso:

C8 – 001

Integrantes:

Barrionuevo Sasig Michael Veyker

Celi Diaz Kevin Francisco

Lema Casa Dylan Antonio

Ninabanda Pambabay Jhonny Eduardo

Santamaria Romero Joan Santamaria

1. INTRODUCCIÓN

El presente proyecto final de la asignatura de Criptografía y Seguridad de la Información tiene como objetivo poner en práctica los conocimientos adquiridos sobre redes, seguridad y hacking ético. El laboratorio consistió en el diseño de una topología de red segmentada mediante VLANs, la configuración de dispositivos de red (Router, Switch y Access Point) y la ejecución controlada de pruebas de penetración utilizando la distribución Kali Linux.

A través de este informe se documenta el proceso de implementación de la red, la asignación de direcciones IP y la demostración de vulnerabilidades mediante ataques de denegación de servicio (DoS) y ataques a credenciales de red inalámbrica, así como el monitoreo de tráfico de red.

2. OBJETIVOS

2.1 Objetivo General

Diseñar e implementar una infraestructura de red segura y realizar pruebas de hacking ético para identificar vulnerabilidades y comprender los mecanismos de ataque y defensa en entornos de red.

2.2 Objetivos Específicos

1. Diseñar una topología de red que conecte 4 equipos distribuidos en 3 redes diferentes (VLANs) utilizando Router y Switch.
2. Configurar el direccionamiento IP y las VLANs para asegurar la conectividad y segmentación de la red.
3. Implementar herramientas de monitoreo de red para analizar el tráfico.
4. Ejecutar y documentar un ataque de denegación de servicio (DoS).
5. Realizar un ataque a las credenciales de una red WiFi y documentar el proceso.

3. MARCO TEÓRICO

3.1 Criptografía y Seguridad de la Información

La seguridad de la información se basa en la preservación de la confidencialidad, integridad y disponibilidad de los datos. La criptografía juega un papel fundamental al proveer mecanismos para cifrar la información y asegurar las comunicaciones. En este proyecto se analizan aspectos prácticos de la seguridad mediante la simulación de ataques que comprometen estos pilares.

3.2 Redes y VLANs

Una VLAN (Virtual LAN) es una tecnología de redes que permite crear redes lógicas independientes dentro de una misma red física. Esto mejora la seguridad y el rendimiento al reducir el dominio de difusión y permitir la segmentación del tráfico.

3.3 Hacking Ético

El hacking ético consiste en simular ataques a sistemas y redes con autorización, con el fin de encontrar vulnerabilidades antes de que sean explotadas por atacantes maliciosos. Herramientas como Kali Linux proporcionan un entorno robusto para realizar estas pruebas de penetración.

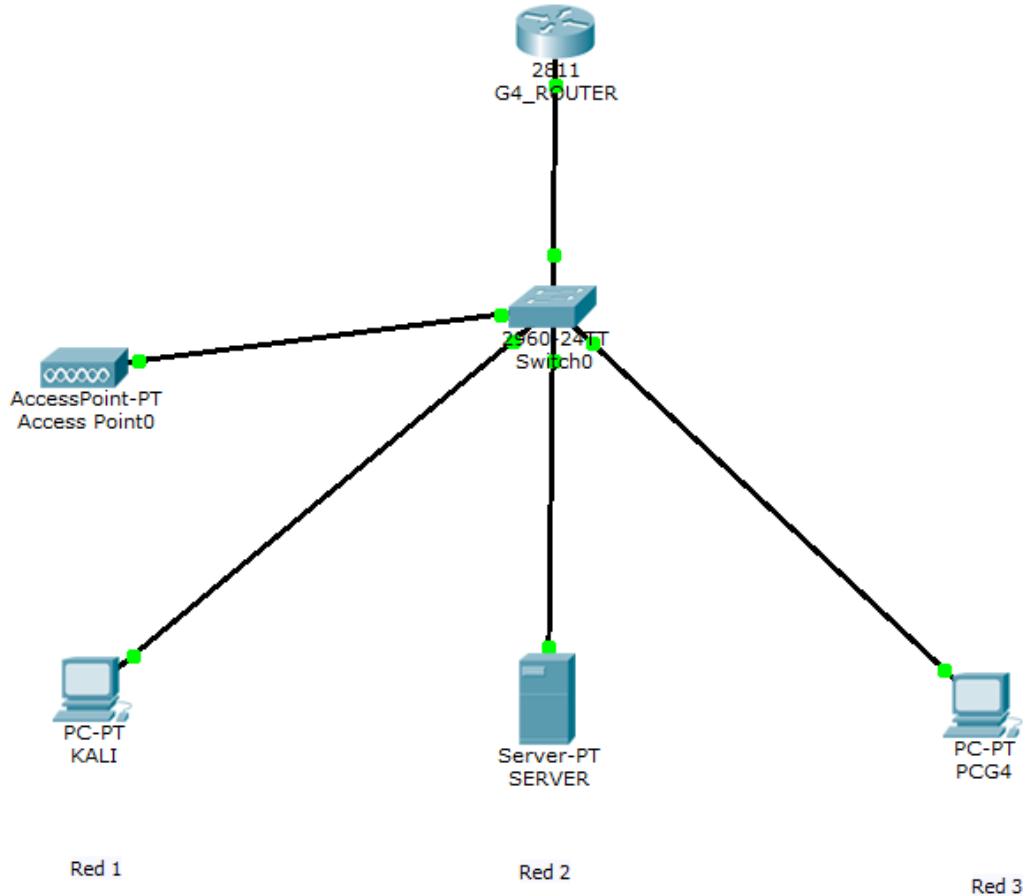
4. DESARROLLO DEL PROYECTO

4.1 Simulación en Packet Tracer

Esta sección documenta el diseño y configuración de la red en el entorno de simulación Cisco Packet Tracer.

4.1.1 *Diseño de la Topología*

La topología implementada en Cisco Packet Tracer conecta cuatro equipos distribuidos en tres redes diferentes (PCGX, SERVER, KALI y Access Point). Se utilizó un Router para el enrutamiento inter-VLAN y un Switch para la gestión de las conexiones.



Topología de Red implementada en Packet Tracer

4.1.2 Tabla de Direccionamiento IP

A continuación se detalla la asignación de direcciones IP para cada dispositivo y subred, cumpliendo con el requisito de utilizar el ID de grupo (4) en el esquema de direccionamiento (192.168.4X.0).

Dispositivo	Interfaz	Dirección IP	Máscara de Subred	Gateway Predeterminado	VLAN
G4_ROUTER	Fa0/0.41	192.168.41.1	255.255.255.0	N/A	41
G4_ROUTER	Fa0/0.42	192.168.42.1	255.255.255.0	N/A	42
G4_ROUTER	Fa0/0.43	192.168.43.1	255.255.255.0	N/A	43
KALI	Fa0	192.168.41.10*	255.255.255.0	192.168.41.1	41

SERVER	Fa0	192.168.42.10*	255.255.255.0	192.168.42.1	42
PCG4	Fa0	192.168.43.10*	255.255.255.0	192.168.43.1	43
Access Point	N/A	No aplica	No aplica	No aplica	41

Tabla de Direccionamiento IP

4.1.3 Justificación Técnica

La topología se diseñó implementando segmentación de red mediante VLANs para garantizar el aislamiento lógico del tráfico y mejorar la seguridad.

1. VLAN 41 (Red 1 - Gestión / KALI): Utilizada para la administración y pruebas de seguridad.
2. VLAN 42 (Red 2 - Servidores): Aísla los recursos críticos como el servidor.
3. VLAN 43 (Red 3 - Usuarios / PC): Red destinada a estaciones de trabajo generales.

Se implementó enrutamiento inter-VLAN utilizando la técnica Router-on-a-Stick en el dispositivo G4_ROUTER, permitiendo la comunicación controlada entre las subredes a través de subinterfaces con encapsulamiento dot1Q.

4.1.4 Configuración de Dispositivos (Simulación)

1. Router: Configuración de subinterfaces y verificación de la tabla de enrutamiento.

G4_ROUTER

Physical Config CLI

```
Press RETURN to get started!

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname G4_ROUTER
G4_ROUTER(config)#
G4_ROUTER(config)#! --- Seguridad ---
G4_ROUTER(config)#enable secret cisco
G4_ROUTER(config)#line console 0
G4_ROUTER(config-line)# password cisco
G4_ROUTER(config-line)# login
G4_ROUTER(config-line)#exit
G4_ROUTER(config)#
G4_ROUTER(config)#! --- Configuración de Interfaces (Router-on-a-Stick) ---
G4_ROUTER(config)#! Usamos f0/0 en lugar de g0/0/0
G4_ROUTER(config)#interface FastEthernet0/0.41
G4_ROUTER(config-subif)# encapsulation dot1q 41
G4_ROUTER(config-subif)# ip address 192.168.41.1 255.255.255.0
G4_ROUTER(config-subif)#
G4_ROUTER(config-subif)#interface FastEthernet0/0.42
G4_ROUTER(config-subif)# encapsulation dot1q 42
G4_ROUTER(config-subif)# ip address 192.168.42.1 255.255.255.0
G4_ROUTER(config-subif)#
G4_ROUTER(config-subif)#interface FastEthernet0/0.43
G4_ROUTER(config-subif)# encapsulation dot1q 43
G4_ROUTER(config-subif)# ip address 192.168.43.1 255.255.255.0
G4_ROUTER(config-subif)#
G4_ROUTER(config-subif)#! Encendemos la interfaz física principal
G4_ROUTER(config-subif)#interface FastEthernet0/0
G4_ROUTER(config-if)# no shutdown

G4_ROUTER(config-if)# exit
G4_ROUTER(config)#
G4_ROUTER(config)#! --- Servidor DHCP (Esto se mantiene igual) ---
G4_ROUTER(config)#ip dhcp excluded-address 192.168.41.1 192.168.41.9
G4_ROUTER(config)#ip dhcp excluded-address 192.168.42.1 192.168.42.9
G4_ROUTER(config)#ip dhcp excluded-address 192.168.43.1 192.168.43.9
G4_ROUTER(config)#
G4_ROUTER(config)#ip dhcp pool RED1
G4_ROUTER(dhcp-config)# network 192.168.41.0 255.255.255.0
G4_ROUTER(dhcp-config)# default-router 192.168.41.1
G4_ROUTER(dhcp-config)#
G4_ROUTER(dhcp-config)#ip dhcp pool RED2
G4_ROUTER(dhcp-config)# network 192.168.42.0 255.255.255.0
G4_ROUTER(dhcp-config)# default-router 192.168.42.1
G4_ROUTER(dhcp-config)#
G4_ROUTER(dhcp-config)#ip dhcp pool RED3
G4_ROUTER(dhcp-config)# network 192.168.43.0 255.255.255.0
G4_ROUTER(dhcp-config)# default-router 192.168.43.1
G4_ROUTER(dhcp-config)#
G4_ROUTER(dhcp-config)#do write
*LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

*LINK-5-CHANGED: Interface FastEthernet0/0.41, changed state to up
*LINK-5-CHANGED: Interface FastEthernet0/0.42, changed state to up
*LINK-5-CHANGED: Interface FastEthernet0/0.43, changed state to up
```

Configuración de subinterfaces en el Router

```

G4_ROUTER>show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0     unassigned     YES unset  up           up
FastEthernet0/0.41   192.168.41.1  YES manual up        up
FastEthernet0/0.42   192.168.42.1  YES manual up        up
FastEthernet0/0.43   192.168.43.1  YES manual up        up
FastEthernet0/1      unassigned     YES unset  administratively down down
Vlan1               unassigned     YES unset  administratively down down
G4_ROUTER>

```

Verificación de la tabla de enrutamiento

2. Switch: Creación, asignación y verificación de VLANs.

Switch0

Physical Config CLI

```
Press RETURN to get started.

G4_SWITCH>enable
G4_SWITCH#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
G4_SWITCH(config)#hostname G4_SWITCH
G4_SWITCH(config)#
G4_SWITCH(config)#! --- Crear VLANs ---
G4_SWITCH(config)#vlan 41
G4_SWITCH(config-vlan)# name KALI
G4_SWITCH(config-vlan)#vlan 42
G4_SWITCH(config-vlan)# name SERVER
G4_SWITCH(config-vlan)#vlan 43
G4_SWITCH(config-vlan)# name PCGX
G4_SWITCH(config-vlan)#exit
G4_SWITCH(config)#
G4_SWITCH(config)#! --- Puerto Troncal ---
G4_SWITCH(config)#interface FastEthernet0/1
G4_SWITCH(config-if)# switchport mode trunk
G4_SWITCH(config-if)#exit
G4_SWITCH(config)#
G4_SWITCH(config)#! --- Puertos de Acceso ---
G4_SWITCH(config)#! Puerto 2 para el Access Point (VLAN 41)
G4_SWITCH(config)#interface FastEthernet0/2
G4_SWITCH(config-if)# switchport mode access
G4_SWITCH(config-if)# switchport access vlan 41
G4_SWITCH(config-if)#
G4_SWITCH(config-if)#! Puerto 3 para Server (VLAN 42)
G4_SWITCH(config-if)#interface FastEthernet0/3
G4_SWITCH(config-if)# switchport mode access
G4_SWITCH(config-if)# switchport access vlan 42
G4_SWITCH(config-if)#
G4_SWITCH(config-if)#! Puerto 4 para PCGX (VLAN 43)
G4_SWITCH(config-if)#interface FastEthernet0/4
G4_SWITCH(config-if)# switchport mode access
G4_SWITCH(config-if)# switchport access vlan 43
G4_SWITCH(config-if)#
G4_SWITCH(config-if)#! SOLO ESTO CAMBIA: Puerto 5 para conectar a KALI por cable
(VLAN 41)
G4_SWITCH(config-if)#interface FastEthernet0/5
G4_SWITCH(config-if)# switchport mode access
G4_SWITCH(config-if)# switchport access vlan 41
G4_SWITCH(config-if)#
G4_SWITCH(config-if)#do write
Building configuration...
[OK]
G4_SWITCH(config-if)#[
```

Creación y asignación de VLANs en el Switch

Switch0

Physical Config CLI

```
*LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up

G4_SWITCH#show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/1    unassigned      YES manual up       up
FastEthernet0/2    unassigned      YES manual up       up
FastEthernet0/3    unassigned      YES manual up       up
FastEthernet0/4    unassigned      YES manual up       up
FastEthernet0/5    unassigned      YES manual up       up
FastEthernet0/6    unassigned      YES manual down    down
FastEthernet0/7    unassigned      YES manual down    down
FastEthernet0/8    unassigned      YES manual down    down
FastEthernet0/9    unassigned      YES manual down    down
FastEthernet0/10   unassigned      YES manual down    down
FastEthernet0/11   unassigned      YES manual down    down
FastEthernet0/12   unassigned      YES manual down    down
FastEthernet0/13   unassigned      YES manual down    down
FastEthernet0/14   unassigned      YES manual down    down
FastEthernet0/15   unassigned      YES manual down    down
FastEthernet0/16   unassigned      YES manual down    down
FastEthernet0/17   unassigned      YES manual down    down
FastEthernet0/18   unassigned      YES manual down    down
FastEthernet0/19   unassigned      YES manual down    down
FastEthernet0/20   unassigned      YES manual down    down
FastEthernet0/21   unassigned      YES manual down    down
FastEthernet0/22   unassigned      YES manual down    down
FastEthernet0/23   unassigned      YES manual down    down
FastEthernet0/24   unassigned      YES manual down    down
GigabitEthernet1/1 unassigned      YES manual down    down
GigabitEthernet1/2 unassigned      YES manual down    down
Vlan1             unassigned      YES manual administratively down down
G4_SWITCH#
```

```

G4_SWITC# show interfaces trunk
Port      Mode       Encapsulation  Status        Native vlan
Fa0/1    on         802.1q        trunking     1

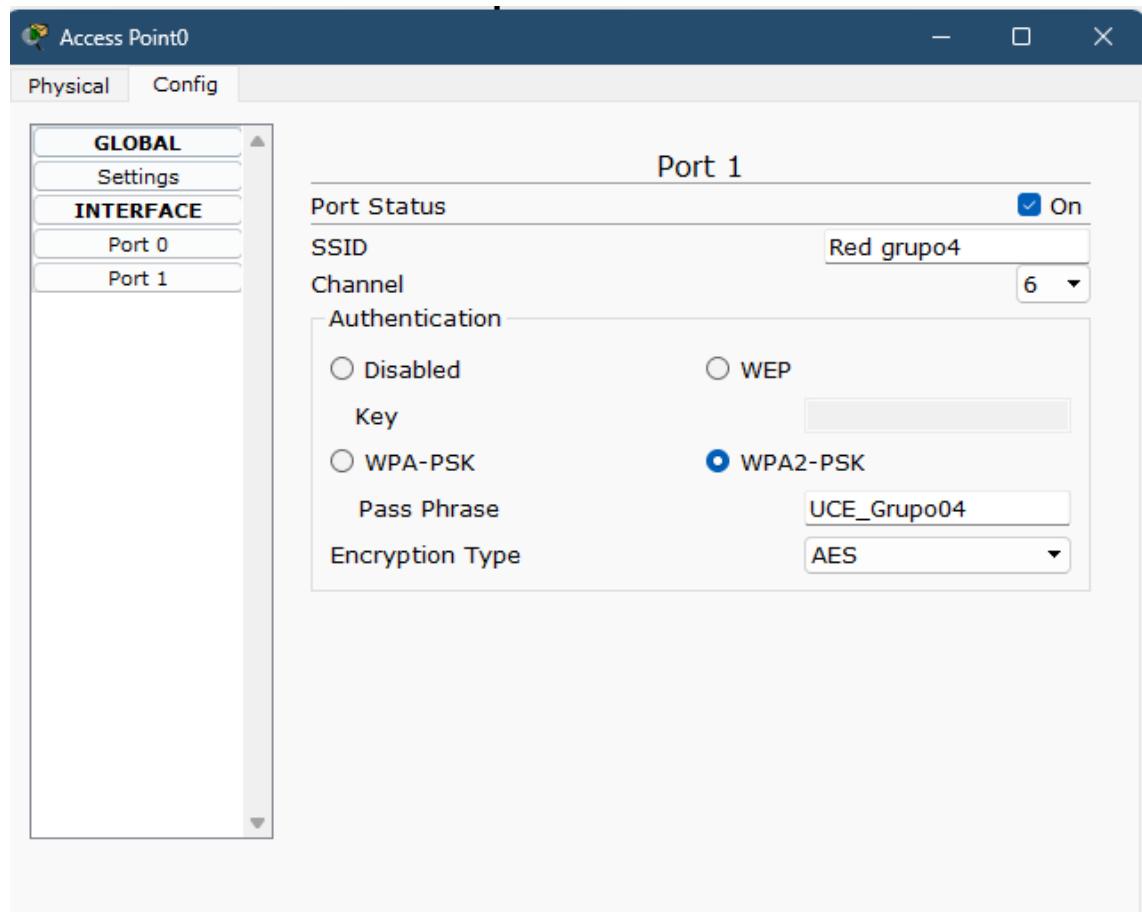
Port      Vlans allowed on trunk
Fa0/1    1-1005

Port      Vlans allowed and active in management domain
Fa0/1    1,41,42,43

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1    1,41,42,43
G4_SWITC#

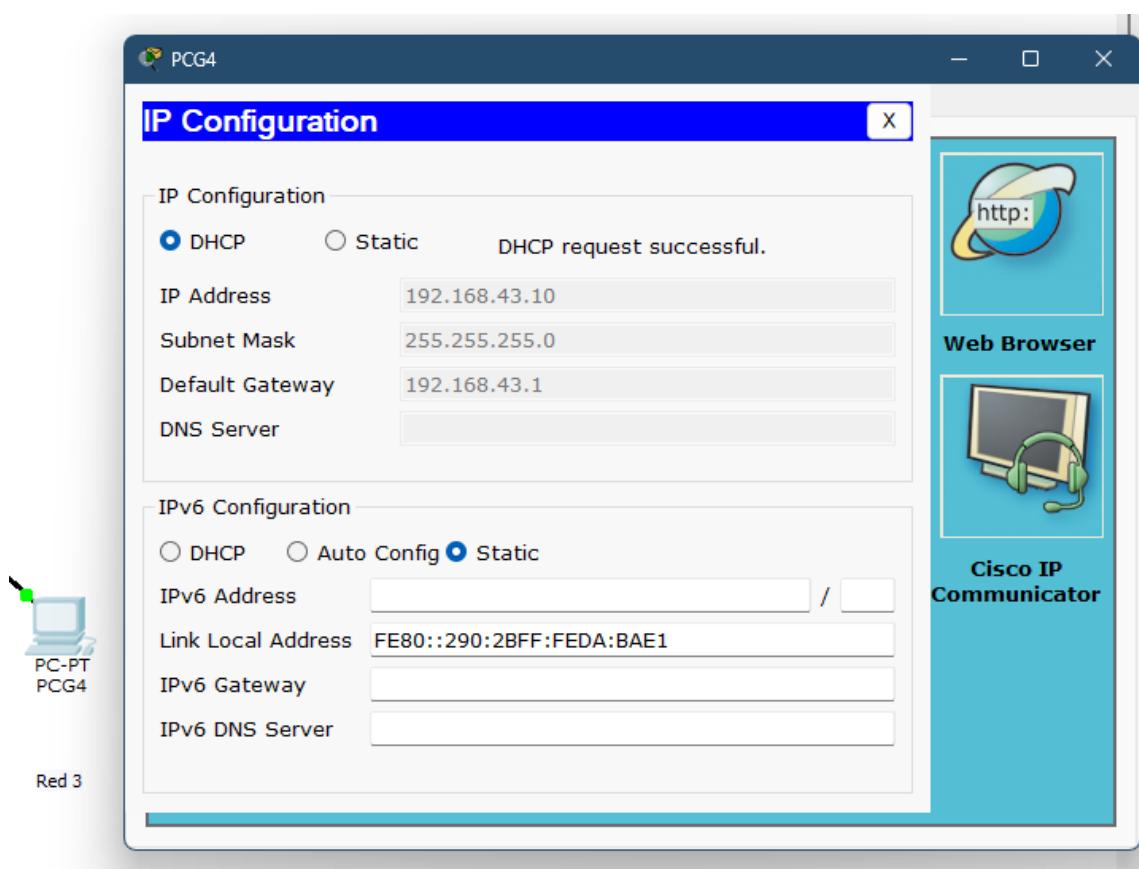
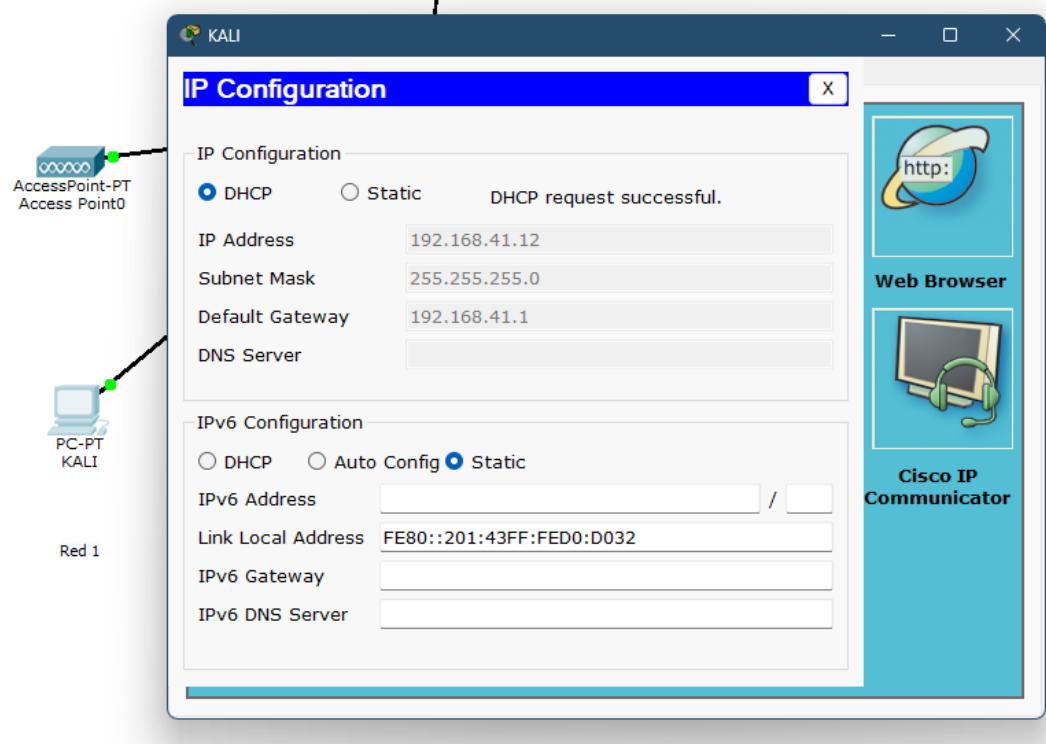
```

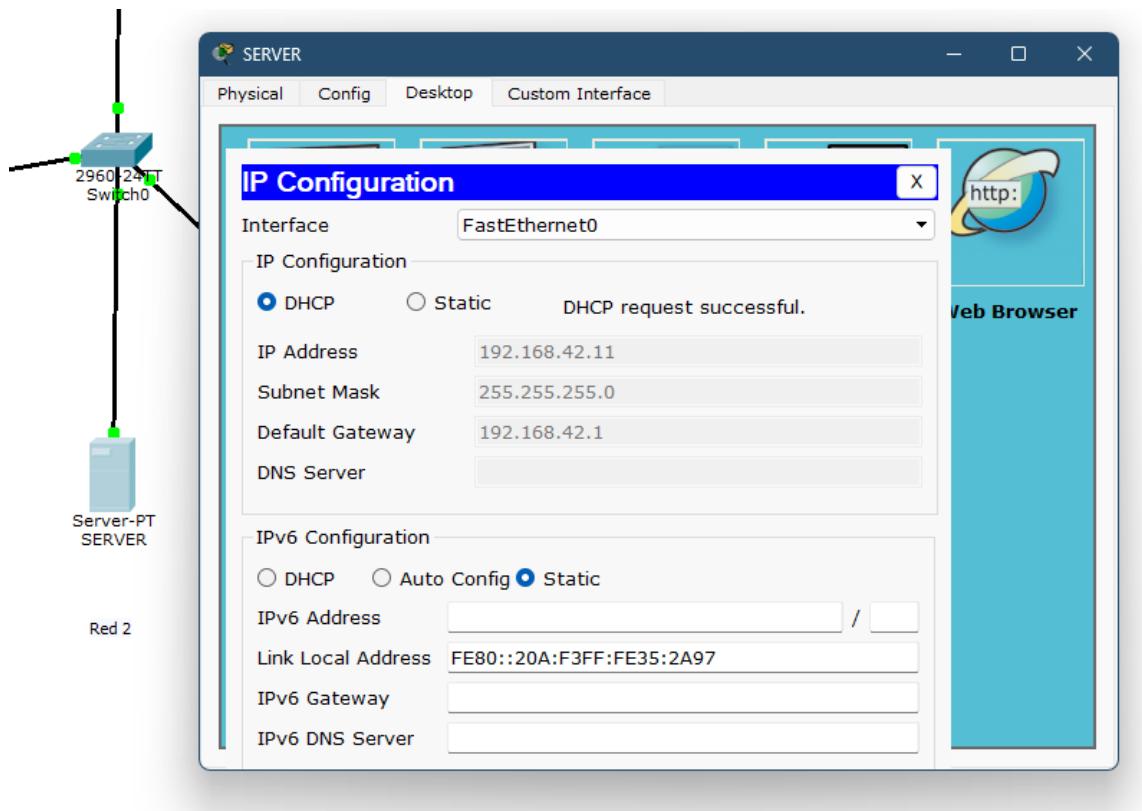
3. Access Point: Configuración de red inalámbrica.



4.1.5 Validación de Servicios y Conectividad

Se verificó la correcta asignación de direcciones IP mediante DHCP y la conectividad entre los dispositivos usando pruebas de ping entre Kali, Server y PC.





Verificación de conectividad (Pruebas de ping)

De KALI hacia SERVER

The screenshot shows a Kali Linux desktop environment. At the top, there is a menu bar with tabs: Physical, Config, Desktop, and Custom Interface. Below the menu bar is a toolbar with several icons. A main window titled "Command Prompt" is open, displaying a terminal session. The terminal output is as follows:

```
PC>clear
Invalid Command.

PC>cls
Invalid Command.

PC>clear
Invalid Command.

PC>cls
Invalid Command.

PC>ping 192.168.42.11

Pinging 192.168.42.11 with 32 bytes of data:

Reply from 192.168.42.11: bytes=32 time=13ms TTL=127
Reply from 192.168.42.11: bytes=32 time=14ms TTL=127
Reply from 192.168.42.11: bytes=32 time=10ms TTL=127
Reply from 192.168.42.11: bytes=32 time=8ms TTL=127

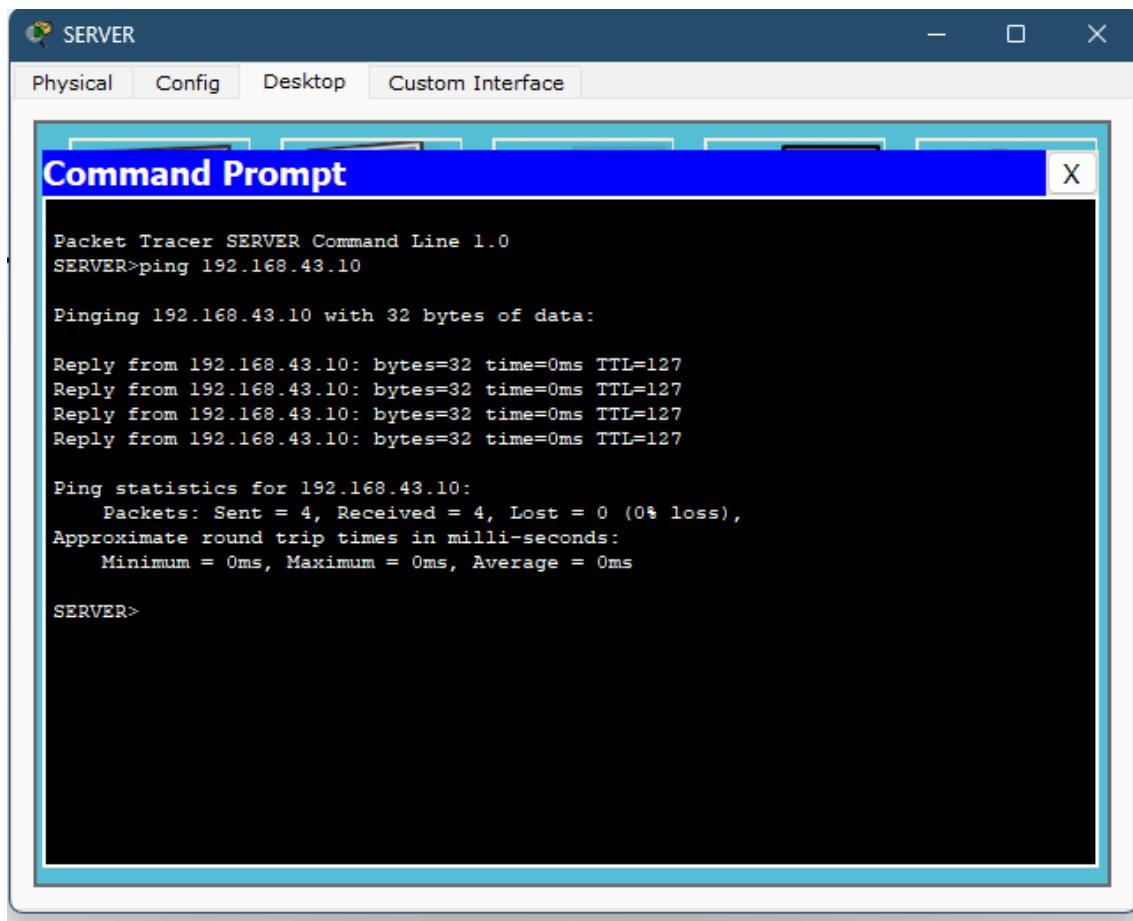
Ping statistics for 192.168.42.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 14ms, Average = 11ms
```

De PCG4 hacia KALI

The screenshot shows a software interface titled "PCG4" with tabs for "Physical", "Config", "Desktop", and "Custom Interface". A "Command Prompt" window is open, displaying the results of a ping test between two hosts. The output is as follows:

```
Pinging 192.168.41.12 with 32 bytes of data:  
Reply from 192.168.41.12: bytes=32 time=6ms TTL=127  
Reply from 192.168.41.12: bytes=32 time=0ms TTL=127  
Reply from 192.168.41.12: bytes=32 time=0ms TTL=127  
Reply from 192.168.41.12: bytes=32 time=0ms TTL=127  
  
Ping statistics for 192.168.41.12:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 6ms, Average = 1ms  
  
PC>ping 192.168.41.12  
  
Pinging 192.168.41.12 with 32 bytes of data:  
Reply from 192.168.41.12: bytes=32 time=0ms TTL=127  
  
Ping statistics for 192.168.41.12:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 0ms, Average = 0ms  
  
PC>
```

De SERVER hacia PCG4



4.2 Práctica Real en Laboratorio

Esta sección documenta la implementación y pruebas realizadas en el entorno de laboratorio utilizando hardware real y Kali Linux.

4.2.1 Configuración de Dispositivos (Entorno Real)

Router Real: Configuración de subinterfaces y verificación.

Configuración del Router G4 (Router-on-a-Stick) en el Rack del laboratorio

Para hacer la configuración hay que tener en cuenta el formateo del dispositivo:

- f) Apagar el dispositivo
- f) Conectar el cable de consola Router y la PC
- f) En el Router quitar la memoria y volver a conectar
- f) Prender el router
- f) Revisar mediante TeraTerm si se formateo correctamente
- f) YA SE REALIZO UN ARCHIVO DE CONFIGURACION PARA PEGAR EN MODO ADMINISTRADOR

1. Acceso y configuración básica

Se accede al modo privilegiado, se entra a configuración global y se asigna un nombre al router para su correcta identificación en la red.

```
enable  
configure terminal  
hostname G4_ROUTER
```

2. Configuración de seguridad

Se establece una contraseña para el modo privilegiado y se protege el acceso por consola.

```
enable secret cisco  
line console 0  
password cisco  
login  
exit
```

3. Configuración de interfaces (Router-on-a-Stick)

Se configura la interfaz **FastEthernet0/0** con subinterfaces para permitir el enrutamiento entre VLANs usando encapsulación **802.1Q**.

```
interface FastEthernet0/0.41  
encapsulation dot1q 41  
ip address 192.168.41.1 255.255.255.0
```

```
interface FastEthernet0/0.42
encapsulation dot1q 42
ip address 192.168.42.1 255.255.255.0
```

```
interface FastEthernet0/0.43
encapsulation dot1q 43
ip address 192.168.43.1 255.255.255.0
```

Activación de la interfaz física principal

```
interface FastEthernet0/0
no shutdown
exit
```

Subinterfaz	VLAN	Dirección IP
F0/0.41	41	192.168.41.1
F0/0.42	42	192.168.42.1
F0/0.43	43	192.168.43.1

4. Configuración del servidor DHCP

Se reservan direcciones IP para uso estático y se crean pools DHCP para cada red VLAN.

Direcciones excluidas

```
ip dhcp excluded-address 192.168.41.1 192.168.41.9
ip dhcp excluded-address 192.168.42.1 192.168.42.9
ip dhcp excluded-address 192.168.43.1 192.168.43.9
```

Pools DHCP

```
ip dhcp pool RED1
network 192.168.41.0 255.255.255.0
default-router 192.168.41.1
```

```
ip dhcp pool RED2
network 192.168.42.0 255.255.255.0
default-router 192.168.42.1
```

```
ip dhcp pool RED3
network 192.168.43.0 255.255.255.0
default-router 192.168.43.1
```

5. Guardar la configuración

Se guarda la configuración para evitar la pérdida de datos tras un reinicio.

```
do write
// este usar en caso de error de sintaxis al final

write memory
```

6. Verificación de configuración

```
COM12 - Tera Term VT
Archivo Editar Configuracion Control Ventana Ayuda
Router(config)#hostname G4_ROUTER
G4_ROUTER(config)#
G4_ROUTER(config)#! --- Seguridad ---
G4_ROUTER(config)#enable secret cisco
G4_ROUTER(config)#line console 0
G4_ROUTER(config-line)# password cisco
G4_ROUTER(config-line)# login
G4_ROUTER(config-line)#exit
G4_ROUTER(config)#
G4_ROUTER(config)#! --- Configuraci3n de Interfaces (Router-on-a-Stick) ---
G4_ROUTER(config)#! Usamos f0/0 en lugar de g0/0/0
G4_ROUTER(config)#interface FastEthernet0/0.41
G4_ROUTER(config-subif)# encapsulation dot1q 41
G4_ROUTER(config-subif)# ip address 192.168.41.1 255.255.255.0
G4_ROUTER(config-subif)#
G4_ROUTER(config-subif)#interface FastEthernet0/0.42
G4_ROUTER(config-subif)# encapsulation dot1q 42
G4_ROUTER(config-subif)# ip address 192.168.42.1 255.255.255.0
G4_ROUTER(config-subif)#
G4_ROUTER(config-subif)#interface FastEthernet0/0.43
G4_ROUTER(config-subif)# encapsulation dot1q 43
G4_ROUTER(config-subif)# ip address 192.168.43.1 255.255.255.0
G4_ROUTER(config-subif)#
G4_ROUTER(config-subif)#! Encendemos la interfaz f0-sica principal
G4_ROUTER(config-subif)#interface FastEthernet0/0
G4_ROUTER(config-if)# no shutdown
G4_ROUTER(config-if)# exit
G4_ROUTER(config)#! --- Servidor DHCP (Esto se mantiene igual) ---
G4_ROUTER(config)#ip dhcp excluded-address 192.168.41.1 192.168.41.9
G4_ROUTER(config)#ip dhcp excluded-address 192.168.42.1 192.168.42.9
G4_ROUTER(config)#ip dhcp excluded-address 192.168.43.1 192.168.43.9
G4_ROUTER(config)#
G4_ROUTER(config)#ip dhcp pool RED1
G4_ROUTER(dhcp-config)# network 192.168.41.0 255.255.255.0
G4_ROUTER(dhcp-config)# default-router 192.168.41.1
G4_ROUTER(dhcp-config)#
G4_ROUTER(dhcp-config)#ip dhcp pool RED2
G4_ROUTER(dhcp-config)# network 192.168.42.0 255.255.255.0
G4_ROUTER(dhcp-config)# default-router 192.168.42.1
G4_ROUTER(dhcp-config)#
G4_ROUTER(dhcp-config)#ip dhcp pool RED3
G4_ROUTER(dhcp-config)# network 192.168.43.0 255.255.255.0
G4_ROUTER(dhcp-config)# default-router 192.168.43.1
```

7. Configuraciones verificadas

```
COM12 - Tera Term VT
Archivo Editar Configuracion Control Ventana Ayuda
G4_ROUTER con0 is now available

Press RETURN to get started.

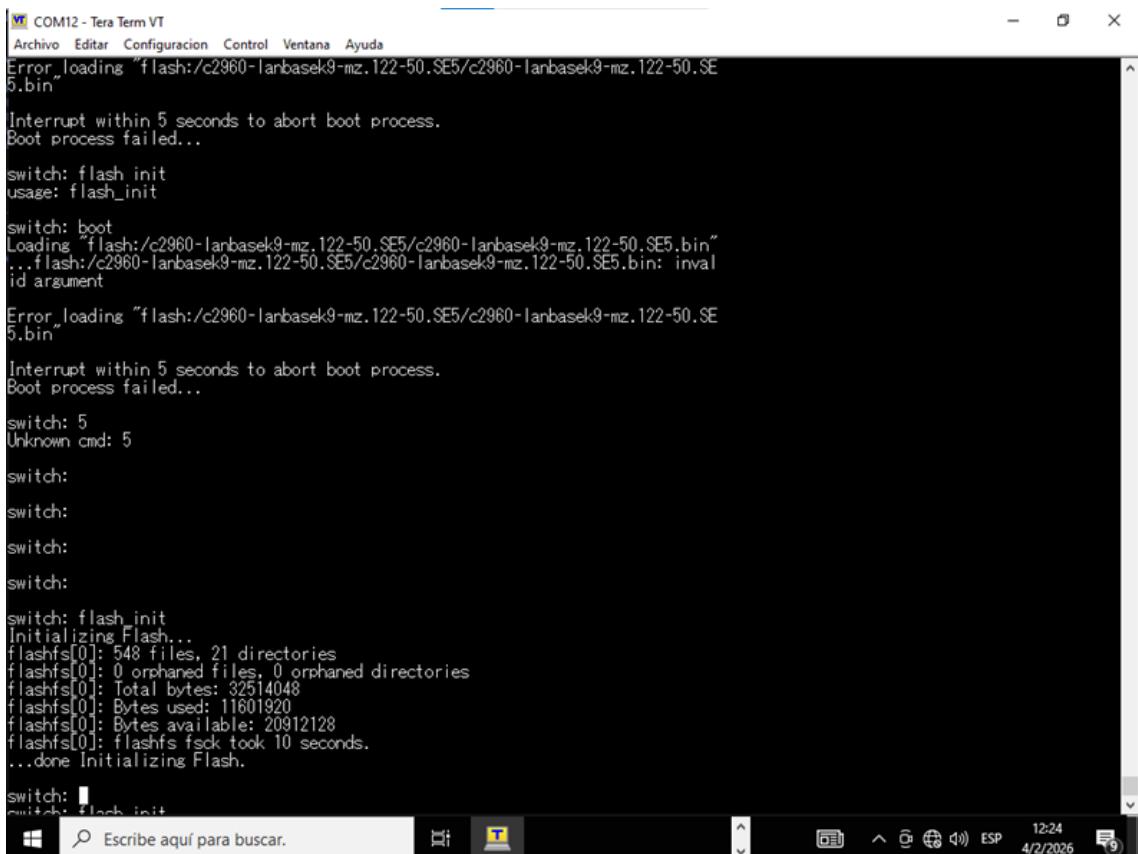
User Access Verification

Password:
G4_ROUTER>show ip interface brief
Interface          IP-Address      OK? Method Status        Protocol
FastEthernet0/0     unassigned      YES unset  up           down
FastEthernet0/0.41   192.168.41.1   YES manual up           down
FastEthernet0/0.42   192.168.42.1   YES manual up           down
FastEthernet0/0.43   192.168.43.1   YES manual up           down
FastEthernet0/1     unassigned      YES unset  administratively down
Serial0/1/0         unassigned      YES unset  administratively down
Serial0/1/1         unassigned      YES unset  administratively down
G4_ROUTER>
```

Configuración del Switch G4 en el Rack de laboratorio

Para hacer la configuración hay que tener en cuenta el formateo del dispositivo:

- f) Presionar el botón de al frente y desconectar y volver a conectar
- f) En la PC conectar el cable de consola con el Switch
- f) Mediante TeraTerm conectar hacer la conexión
- f) Mantener presionado esperar que la terminal de señales



```
COM12 - Tera Term VT
Archivo Editar Configuracion Control Ventana Ayuda
Error loading "flash:/c2960-lanbasek9-mz.122-50.SE5/c2960-lanbasek9-mz.122-50.SE5.bin"
Interrupt within 5 seconds to abort boot process.
Boot process failed...
switch: flash init
usage: flash_init
switch: boot
Loading "flash:/c2960-lanbasek9-mz.122-50.SE5/c2960-lanbasek9-mz.122-50.SE5.bin"
...flash:/c2960-lanbasek9-mz.122-50.SE5/c2960-lanbasek9-mz.122-50.SE5.bin: invalid argument
Error loading "flash:/c2960-lanbasek9-mz.122-50.SE5/c2960-lanbasek9-mz.122-50.SE5.bin"
Interrupt within 5 seconds to abort boot process.
Boot process failed...
switch: 5
Unknown cmd: 5
switch:
switch:
switch:
switch:
switch: flash_init
Initializing Flash...
flashfs[0]: 548 files, 21 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 32514048
flashfs[0]: Bytes used: 11601920
flashfs[0]: Bytes available: 20912128
flashfs[0]: flashfs fsck took 10 seconds.
...done Initializing Flash.

switch: [REDACTED]
switch: flash init
Windows Escribe aquí para buscar. 12:24 4/2/2026
```

- f) En terminal seguir los siguientes comandos cuando salga el modo de recuperación para eliminar configuraciones anteriores:
 - a. flash_init, esperar que cargue
 - b. dir flash:
 - c. verificamos los archivos config.text y vlan.dat para eliminarlos
 - d. delete flash:config.text
 - e. delete flash:vlan.dat
 - f. boot
- f) Ahora esperar a que termine de lanzar y entrar al modo administrador y configurar:
 - a. ya se realizo un archivo para solo pegar

```

COM12 - Tera Term VT
Archivo Editar Configuracion Control Ventana Ayuda
Motherboard revision number : A0
Model number : WS-C2960-24TC-L
System serial number : FCQ1533Z5FL
Top Assembly Part Number : 800-32796-01
Top Assembly Revision Number : H0
Version ID : V09
CLEI Code Number : COM3K00BRE
Hardware Board Revision Number : 0x0A

Switch Ports Model SW Version SW Image
----- -----
* 1 26 WS-C2960-24TC-L 12.2(50)SE5 C2960-LANBASEK9-M

Press RETURN to get started!

*Mar 1 00:00:31.541: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
*Mar 1 00:00:32.698: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for type vlan
*Mar 1 00:00:53.678: %SYS-5-RESTART: System restarted --
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(50)SE5, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Tue 28-Sep-10 13:44 by prod_rel_team

--- System Configuration Dialog ---

Enable secret warning
-----
In order to access the device manager, an enable secret is required
If you enter the initial configuration dialog, you will be prompted for the enable secret
If you choose not to enter the intial configuration dialog, or if you exit setup without setting the enable secret,
please set an enable secret using the following CLI in configuration mode:
enable secret 0 <cleartext password>
-----
Would you like to enter the initial configuration dialog? [yes/no]: n
Switch>enable
Switch#

```

1. Acceso al modo de configuración

Se habilita el modo privilegiado y se accede al modo de configuración global del switch.

Además, se asigna un nombre al dispositivo para su identificación en la red.

```

enable
configure terminal
hostname G4_SWITCH

```

2. Creación de VLANs

Se crean tres VLANs para segmentar la red, cada una asociada a un tipo de dispositivo específico.

```

vlan 41
name KALI
vlan 42
name SERVER
vlan 43
name PCGX

```

```
exit
```

VLAN	Nombre	Uso
41	KALI	Equipos Kali Linux y Access Point
42	SERVER	Servidor
43	PCGX	Computadora PCGX

3. Configuración del puerto troncal

El puerto **FastEthernet0/1** se configura en modo troncal para transportar el tráfico de todas las VLANs hacia otro dispositivo de red (por ejemplo, otro switch o un router).

```
interface FastEthernet0/1
switchport mode trunk
exit
```

4. Configuración de puertos de acceso

Cada puerto de acceso se asigna a una VLAN específica según el dispositivo conectado.

Asignación de puertos:

- **FastEthernet0/2** → Access Point (VLAN 41)
- **FastEthernet0/3** → Servidor (VLAN 42)
- **FastEthernet0/4** → PCGX (VLAN 43)
- **FastEthernet0/5** → Kali Linux por cable (VLAN 41)

```
interface FastEthernet0/2
switchport mode access
switchport access vlan 41
```

```
interface FastEthernet0/3
switchport mode access
switchport access vlan 42
```

```
interface FastEthernet0/4
```

```
switchport mode access
```

```
switchport access vlan 43
```

```
interface FastEthernet0/5
```

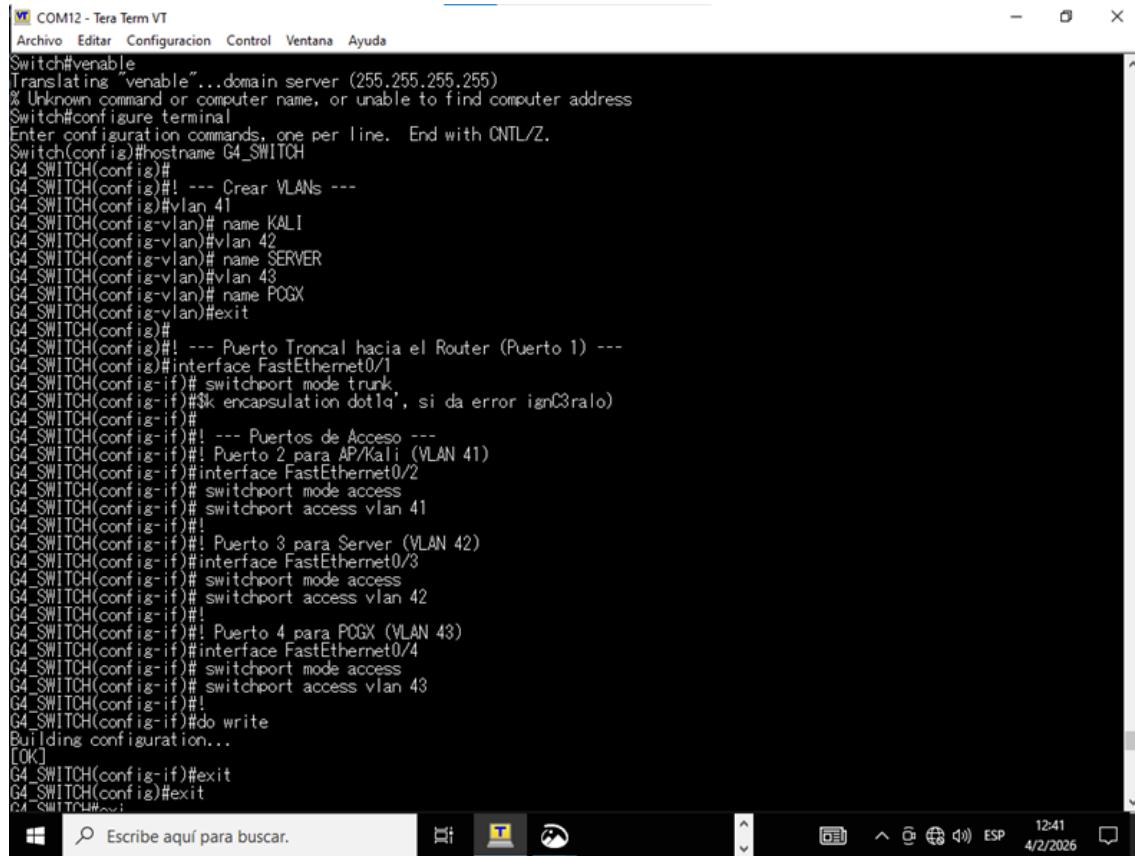
```
switchport mode access
```

```
switchport access vlan 41
```

5. Guardar la configuración

Se guarda la configuración actual en la memoria del dispositivo para que no se pierda al reiniciar.

```
do write
```



```
Switch#enable
Translating "enable" ...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname G4_SWITCH
G4_SWITCH(config)#
G4_SWITCH(config)#! --- Crear VLANs ---
G4_SWITCH(config)#vlan 41
G4_SWITCH(config-vlan)# name KALI
G4_SWITCH(config-vlan)#vlan 42
G4_SWITCH(config-vlan)# name SERVER
G4_SWITCH(config-vlan)#vlan 43
G4_SWITCH(config-vlan)# name POGX
G4_SWITCH(config-vlan)#exit
G4_SWITCH(config)#
G4_SWITCH(config)#! --- Puerto Troncal hacia el Router (Puerto 1) ---
G4_SWITCH(config)#interface FastEthernet0/1
G4_SWITCH(config-if)# switchport mode trunk
G4_SWITCH(config-if)#$k encapsulation dot1q, si da error ignC3ralo
G4_SWITCH(config-if)#
G4_SWITCH(config-if)#! --- Puertos de Acceso ---
G4_SWITCH(config-if)#! Puerto 2 para AP/Kali (VLAN 41)
G4_SWITCH(config-if)#interface FastEthernet0/2
G4_SWITCH(config-if)# switchport mode access
G4_SWITCH(config-if)# switchport access vlan 41
G4_SWITCH(config-if)#
G4_SWITCH(config-if)#! Puerto 3 para Server (VLAN 42)
G4_SWITCH(config-if)#interface FastEthernet0/3
G4_SWITCH(config-if)# switchport mode access
G4_SWITCH(config-if)# switchport access vlan 42
G4_SWITCH(config-if)#
G4_SWITCH(config-if)#! Puerto 4 para POGX (VLAN 43)
G4_SWITCH(config-if)#interface FastEthernet0/4
G4_SWITCH(config-if)# switchport mode access
G4_SWITCH(config-if)# switchport access vlan 43
G4_SWITCH(config-if)#
G4_SWITCH(config-if)#do write
Building configuration...
[OK]
G4_SWITCH(config-if)#exit
G4_SWITCH(config)#exit
G4_SWITCH#~:
```

6. Ya levantado las redes

COM12 - Tera Term VT

Archivo Editar Configuracion Control Ventana Ayuda

G4_SWITCH con0 is now available

Press RETURN to get started.

G4_SWITCH>show ip interface brief

% Invalid input detected at '***' marker.

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	unassigned	YES	unset	up	down
FastEthernet0/1	unassigned	YES	unset	down	down
FastEthernet0/2	unassigned	YES	unset	down	down
FastEthernet0/3	unassigned	YES	unset	down	down
FastEthernet0/4	unassigned	YES	unset	down	down
FastEthernet0/5	unassigned	YES	unset	down	down
FastEthernet0/6	unassigned	YES	unset	down	down
FastEthernet0/7	unassigned	YES	unset	down	down
FastEthernet0/8	unassigned	YES	unset	down	down
FastEthernet0/9	unassigned	YES	unset	down	down
FastEthernet0/10	unassigned	YES	unset	down	down
FastEthernet0/11	unassigned	YES	unset	down	down
FastEthernet0/12	unassigned	YES	unset	down	down
FastEthernet0/13	unassigned	YES	unset	down	down
FastEthernet0/14	unassigned	YES	unset	down	down
FastEthernet0/15	unassigned	YES	unset	down	down
FastEthernet0/16	unassigned	YES	unset	down	down
FastEthernet0/17	unassigned	YES	unset	down	down
FastEthernet0/18	unassigned	YES	unset	down	down
FastEthernet0/19	unassigned	YES	unset	down	down
FastEthernet0/20	unassigned	YES	unset	down	down
FastEthernet0/21	unassigned	YES	unset	down	down
--More--					
FastEthernet0/20	unassigned	YES	unset	down	down

Escribe aquí para buscar. 12:42 4/2/2026

Informe Técnico: Explotación de Redes

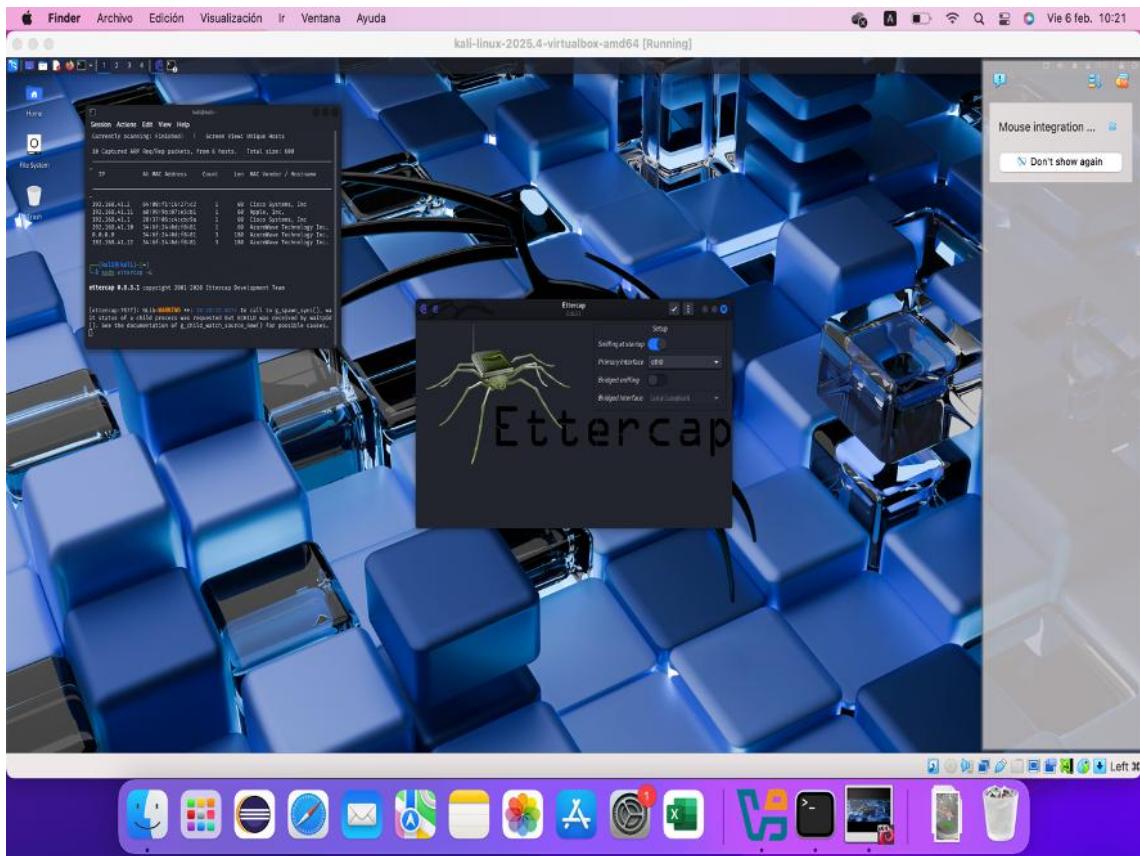
Herramienta de Trabajo: Kali Linux 2025.4 (Entorno Virtualizado)

Objetivo: Evaluar la resiliencia de una infraestructura LAN compuesta por tres subredes (Gestión, Servicios y Clientes).

1. Monitoreo y Reconocimiento de Red

Herramientas: Netdiscover y Ettercap (Modo Gráfico)

- **Fundamento Teórico:** El monitoreo en Capa 2 (Enlace de Datos) permite identificar dispositivos mediante el protocolo ARP (Address Resolution Protocol) antes de iniciar cualquier fase de explotación.
- **Resultados Obtenidos:** En la captura de pantalla se evidencia la detección de 6 hosts activos, incluyendo dispositivos de fabricantes como **Cisco Systems**, **Apple** y **AzureWave**.
- **Análisis:** Esta fase es crítica porque permite al auditor seleccionar objetivos específicos (como el **Server** o el **PCGX**) basándose en la dirección MAC y el fabricante.
- **Objetivo:** Identificar los nodos activos en las tres redes interconectadas.
- **Procedimiento:** Se utilizó netdiscover para realizar un escaneo basado en peticiones ARP. Esto permite obtener la dirección IP, la dirección MAC y el fabricante de los dispositivos en la red 192.168.41.0/24.
- **Comando ejecutado:** Bash `sudo netdiscover -r`
- **Explicación técnica:** Al trabajar en Capa 2, este comando es altamente efectivo para detectar equipos incluso si tienen un firewall que bloquea el protocolo ICMP (ping). En la práctica, se logró visualizar dispositivos **Cisco**(Router),**Apple** y **AzureWave** (PCGX/Server).

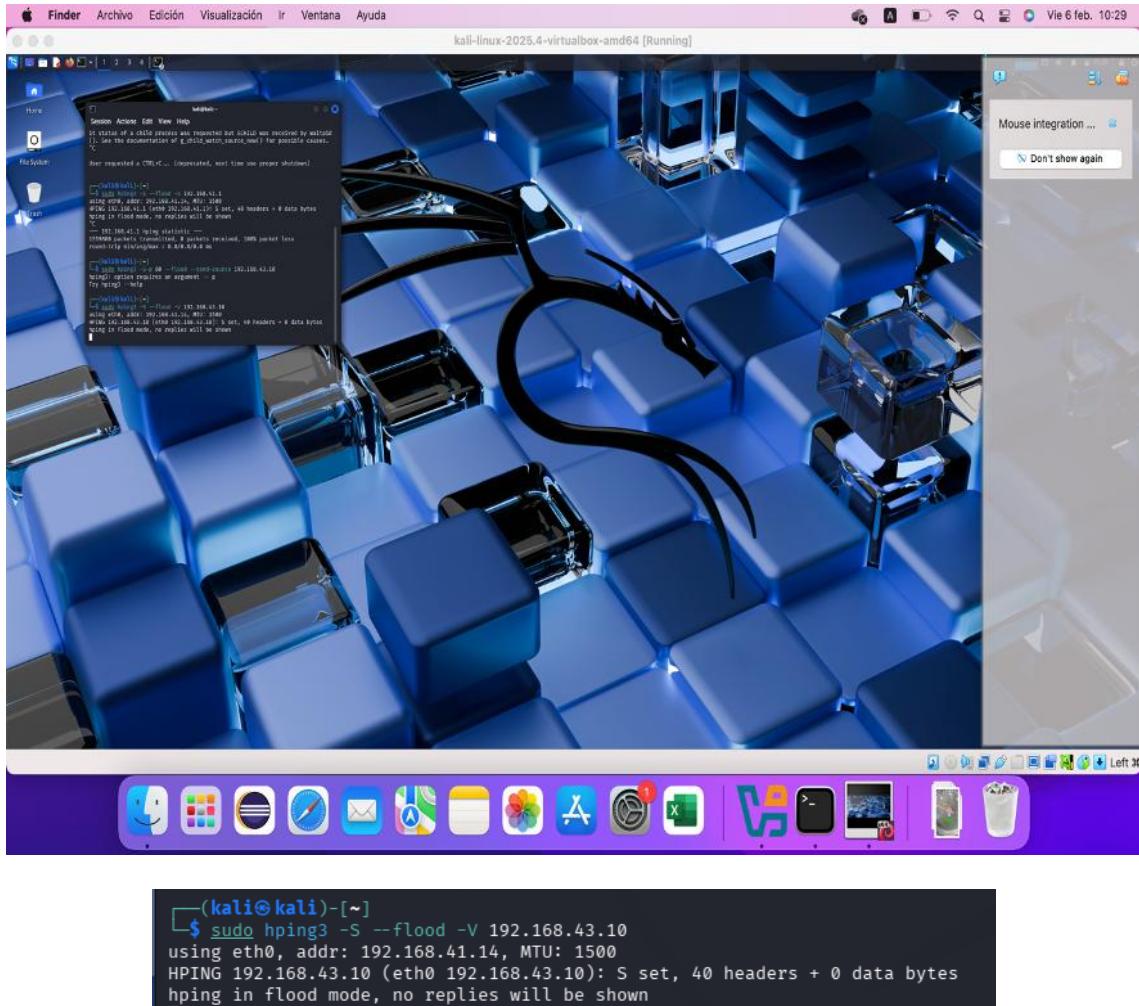


2. Denegación de Servicio (DoS) por Inundación

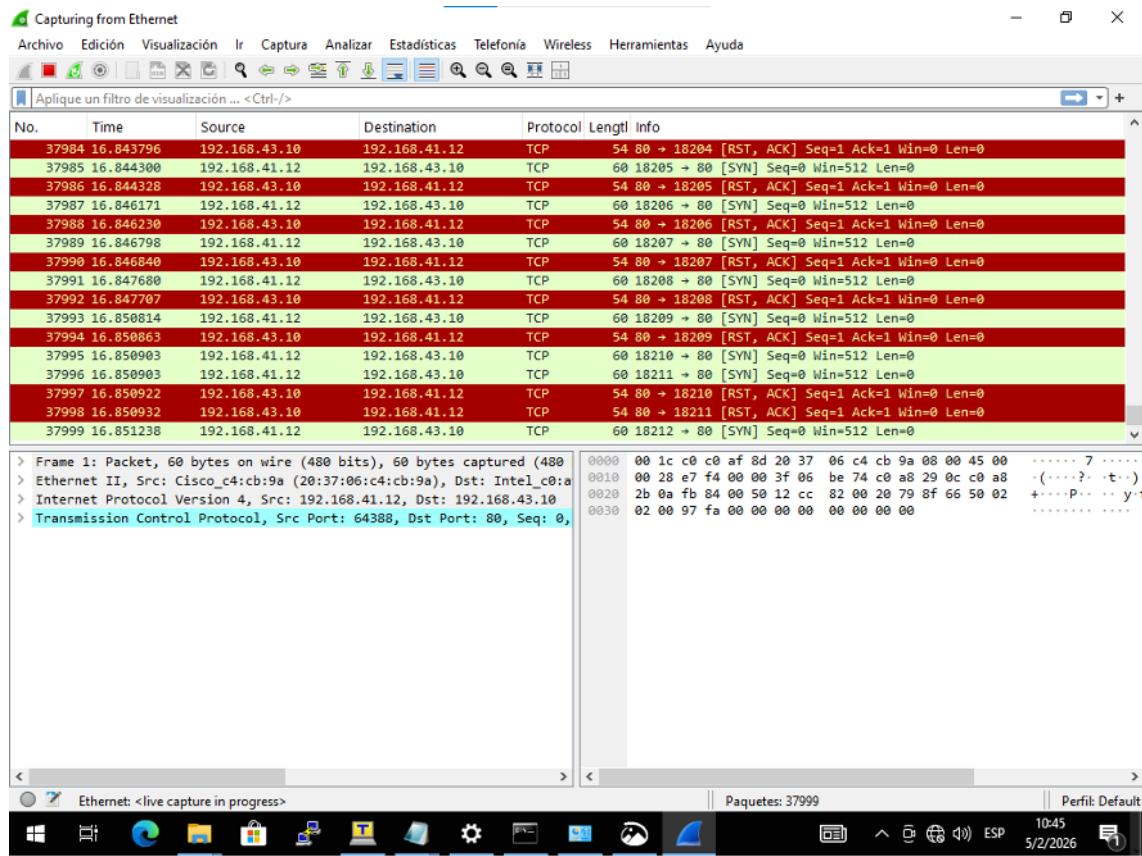
Herramienta: hping3

- **Fundamento Teórico:** El ataque TCP SYN Flood aprovecha el "apretón de manos" de tres vías (Three-way Handshake) de TCP. El atacante envía paquetes SYN pero nunca responde al SYN-ACK del servidor, dejando conexiones "medio abiertas" que agotan la memoria RAM.
- **Impacto:** Al usar `--flood`, el sistema envía paquetes a la máxima capacidad del hardware. La opción `--rand-source` dificulta la mitigación por parte de firewalls, ya que el tráfico parece provenir de múltiples direcciones aleatorias.
- **Objetivo:** Evaluar la capacidad del Router/Access Point para manejar tráfico masivo.
- **Procedimiento:** Utilizando hping3, se lanzó una inundación de paquetes con la bandera SYN activa hacia la dirección IP del objetivo.
- **Comando ejecutado:** Bash `sudo hping3 -S --flood --rand-source 192.168.41.1`
- **Explicación técnica:** El parámetro `--flood` envía paquetes sin esperar respuesta, saturando el ancho de banda. La opción `--rand-source` falsifica la IP de

origen en cada paquete, lo que provoca que el router agote su tabla de conexiones intentando gestionar miles de peticiones de "clientes" que no existen.



- **Resultado Obtenido:** Mediante la herramienta Wireshark vimos que nuestro ataque se realizó con éxito.

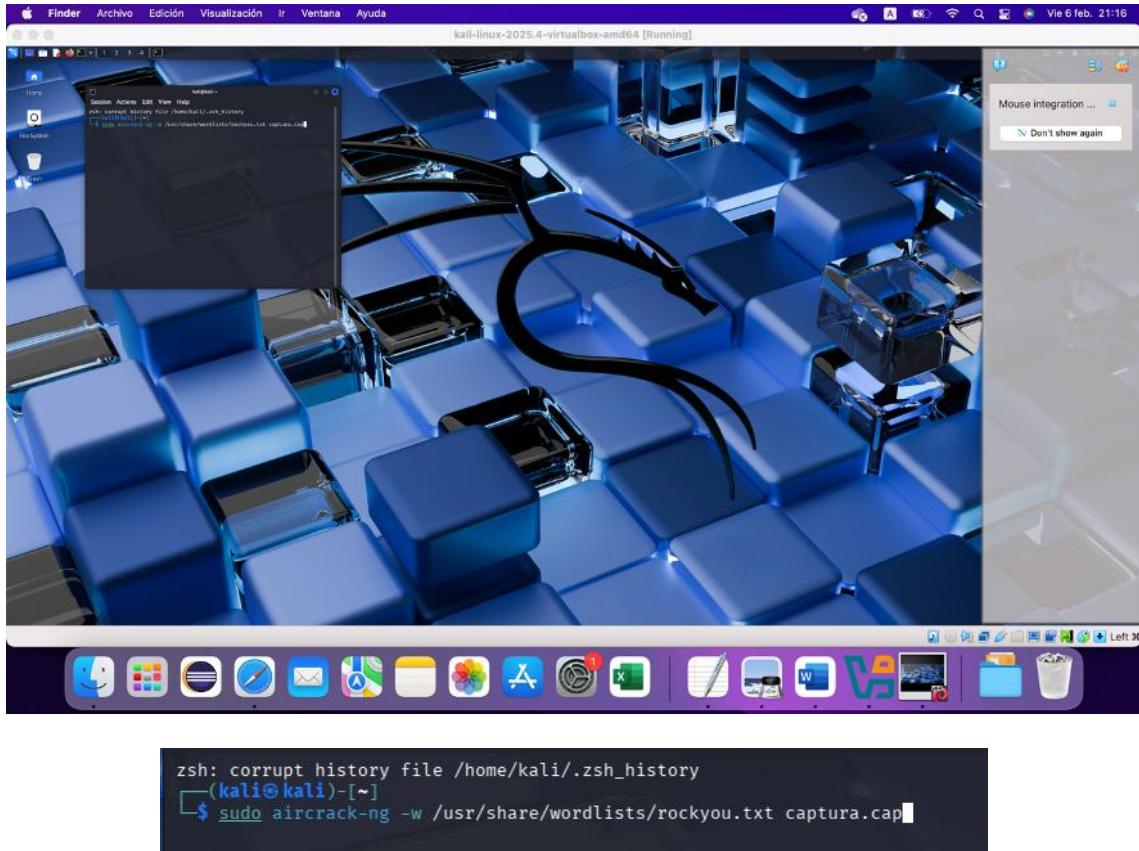


3. Ataque a Credenciales Wi-Fi (Cracking Offline)

Herramienta: Suite Aircrack-ng

- **Fundamento Teórico:** La seguridad WPA/WPA2 se basa en un intercambio de 4 pasos (4-way handshake). Si un atacante captura este intercambio, puede intentar descifrar la clave mediante fuerza bruta fuera de la red (offline), sin riesgo de ser bloqueado por el Access Point.
- **Justificación:** Se seleccionó esta técnica por su eficacia en redes con contraseñas débiles y por su naturaleza indetectable durante la fase de cracking.
- **Objetivo:** Recuperar la clave de acceso del Access Point mediante el análisis de un apretón de manos (handshake).
- **Procedimiento:** Una vez capturado el tráfico de autenticación en un archivo .cap, se procedió al descifrado mediante un ataque de diccionario.
- **Comando ejecutado:** Bash `sudo aircrack-ng -w /usr/share/wordlists/rockyou.txt captura.cap`

- **Explicación técnica:** Aircrack-ng toma cada palabra del diccionario `rockyou.txt`, genera un hash con el nombre de la red (SSID) y lo compara con el capturado en el archivo. Si coinciden, se revela la contraseña. Este proceso es **offline**, por lo que el router no puede detectar ni bloquear los intentos.

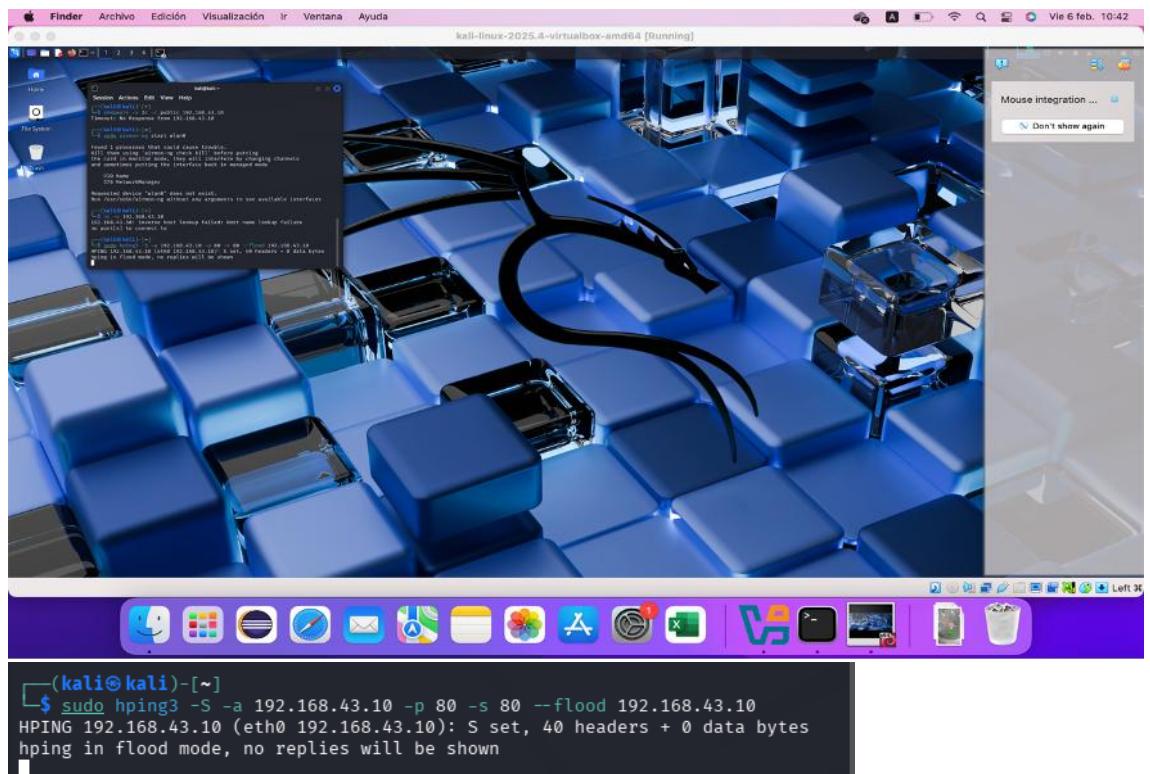


4. Actividad Opcional: Land Attack (Paquete Suicida)

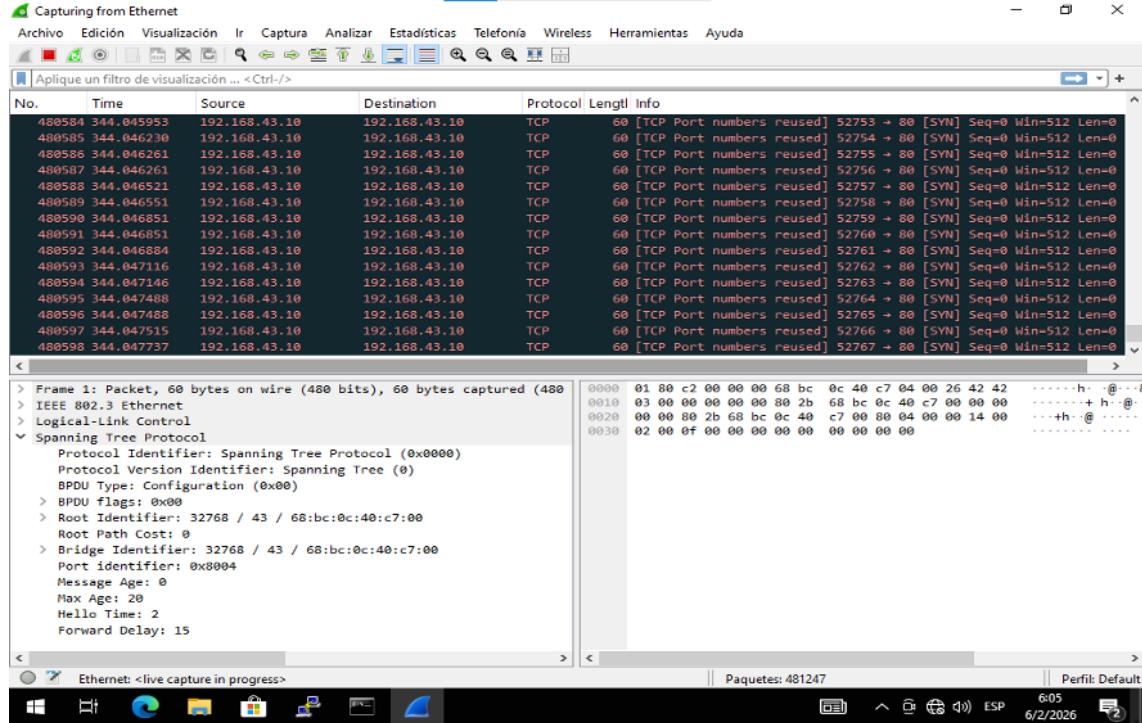
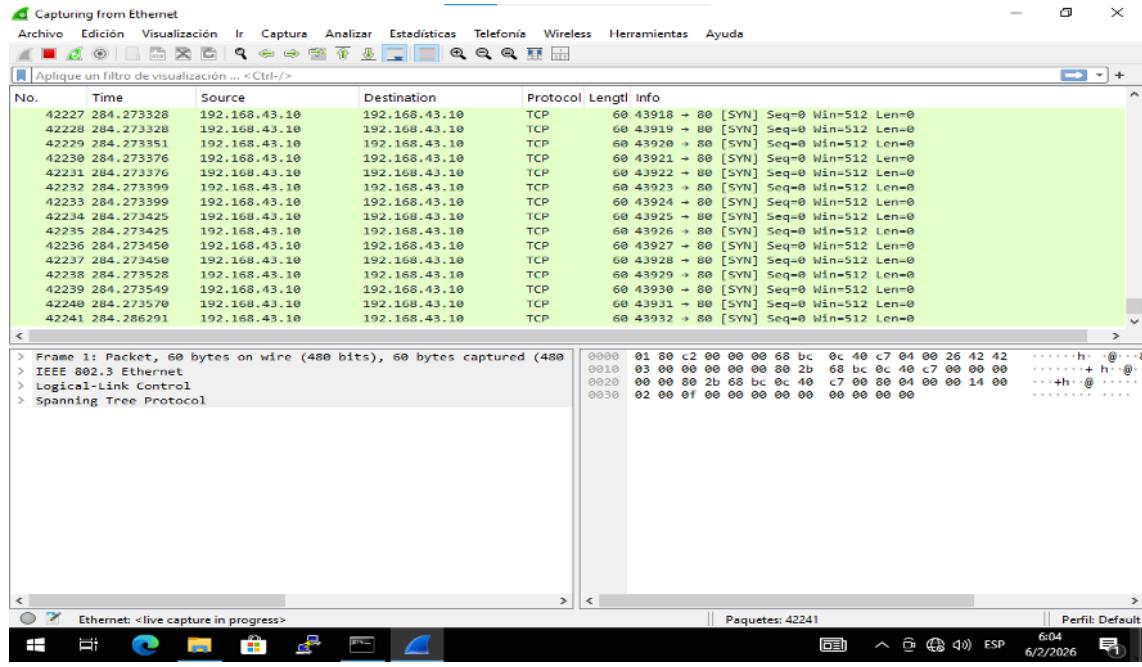
Herramienta: hping3 (Manipulación de cabeceras)

- **Fundamento Teórico:** El **Land Attack** es un tipo de DoS que consiste en enviar un paquete TCP SYN falsificado donde la **IP de origen y el puerto** son idénticos a la **IP y puerto de destino**.
- **Mecánica de Fallo:** El dispositivo víctima (en este caso el Router o el Server) recibe el paquete e intenta responderse a sí mismo de forma infinita. Esto genera un bucle de procesamiento que satura el CPU del sistema operativo, provocando un congelamiento total o reinicio del hardware.
- **Objetivo:** Comprobar la vulnerabilidad de la pila de protocolos ante paquetes malformados.

- **Procedimiento:** Se configuró hping3 para enviar un paquete donde la IP de origen y destino son idénticas (192.168.43.10), dirigidas al puerto 80.
- **Comando ejecutado:** Bash `sudo hping3 -S -a 192.168.43.10 -p 80 -s 80 --flood 192.168.43.10`
- **Explicación técnica:** Este ataque engaña al sistema operativo de la víctima (Router o Server). Al recibir el paquete, el sistema intenta responderse a sí mismo en un bucle infinito. Esto genera una condición de **carrera crítica en el CPU**, causando que el equipo deje de procesar tráfico legítimo y se bloquee.



- **Resultado Obtenido:** Mediante la herramienta Wireshark vimos que nuestro ataque se realizó con éxito.



5. CONCLUSIONES

1. La implementación de VLANs permitió segmentar la red de manera efectiva, aislando el tráfico de los diferentes departamentos o grupos definidos en la topología (Red 1, Red 2, Red 3).
2. El uso de herramientas de hacking ético en un entorno controlado permitió comprender las vulnerabilidades inherentes a los protocolos de red y la importancia de implementar medidas de seguridad robustas.
3. Los ataques de DoS y a redes inalámbricas demostraron la facilidad con la que servicios no protegidos pueden ser interrumpidos o comprometidos, resaltando la necesidad de monitoreo constante y configuración segura de dispositivos.

6. BIBLIOGRAFÍA

[1] G. Lyon, Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning, Insecure.com, 2023. [En línea]. Disponible en: <https://nmap.org/book/> [2] A. Salvatore, Hping3 Manual, 2023. [En línea]. Disponible en: <http://www.hping.org/manpage.html> [3] Aircrack-ng Team, Aircrack-ng Documentation, 2023. [En línea]. Disponible en: <https://www.aircrack-ng.org/documentation.html> [4] C. Sullo, Nikto Web Scanner, 2023. [En línea]. Disponible en: <https://cirt.net/Nikto2> [5] Rapid7, Metasploit Framework Documentation, 2023. [En línea]. Disponible en: <https://docs.rapid7.com/metasploit/> [6] Openwall, John the Ripper Documentation, 2023. [En línea]. Disponible en: <https://www.openwall.com/john/doc/> [7] OWASP Foundation, OWASP Testing Guide v4.0, 2023. [En línea]. Disponible en: <https://owasp.org/www-project-web-security-testing-guide/> [8] NIST, Special Publication 800-115: Technical Guide to Information Security Testing and Assessment, National Institute of Standards and Technology, 2023. [9] Kali Linux Documentation, Kali Linux Tools, 2023. [En línea]. Disponible en: <https://www.kali.org/tools/> [10] Kali Linux Team, Nmap - Kali Linux Tools, 2023. [En línea]. Disponible en: <https://www.kali.org/tools/nmap/> [11] Kali Linux Team, Hydra - Kali Linux Tools, 2023. [En línea]. Disponible en: <https://www.kali.org/tools/hydra/> [12] Kali Linux Team, John the Ripper - Kali Linux Tools, 2023. [En línea]. Disponible en: <https://www.kali.org/tools/john/> [13] Kali Linux Team, Metasploit Framework - Kali Linux Tools, 2023. [En línea]. Disponible en: <https://www.kali.org/tools/metasploit-framework/> [14] Cisco Networking Academy, Lab Downloads - Networking Academy, 2023. [En línea]. Disponible en: <https://www.netacad.com/resources/lab-downloads?courseLang=en-US> [15] Cisco Systems, VLAN Configuration Guide, 2023. [En línea]. Disponible en: <https://www.cisco.com/c/en/us/support/docs/lan-switching/vlan/10000-vlansconfigure.html>