

Universidad Central del Ecuador

Facultad de Ingeniería

y ciencias Aplicadas

GRUPO 2:

John Andino

Anthony Cajamarca

Kevin Cruz

Diego Borja

Jami Mateo

Profesor:

Ing. Giovanny Moncayo

Materia:

Criptografía y seguridad de la información

Proyecto Final – Laboratorio de hacking ético.

1. Diseño y Configuración de la Red

Se implementó una red empresarial segmentada mediante el uso de subinterfaces en el Router (Router-on-a-Stick) y VLANs en el Switch para garantizar el aislamiento de tráfico.

Configuración de VLANs y Direcciónamiento

- **Segmentación:** Se configuraron VLANs específicas en el Switch (VLAN 21: KALI_ACCESS, VLAN 22: SERVER, VLAN 23: PCG2, VLAN 24: AP) para aislar el tráfico de cada departamento técnico.
- **Enrutamiento:** El Router actúa como Gateway predeterminado, gestionando las sub-interfaces FastEthernet0/0.21 a .24 con el esquema de direcciónamiento 192.168.2X.1.

Símbolo del sistema

```
Microsoft Windows [Versión 10.0.19045.3803]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\REDES>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Dirección IPv4. . . . . : 192.168.3.101
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . :

C:\Users\REDES>ipconfig

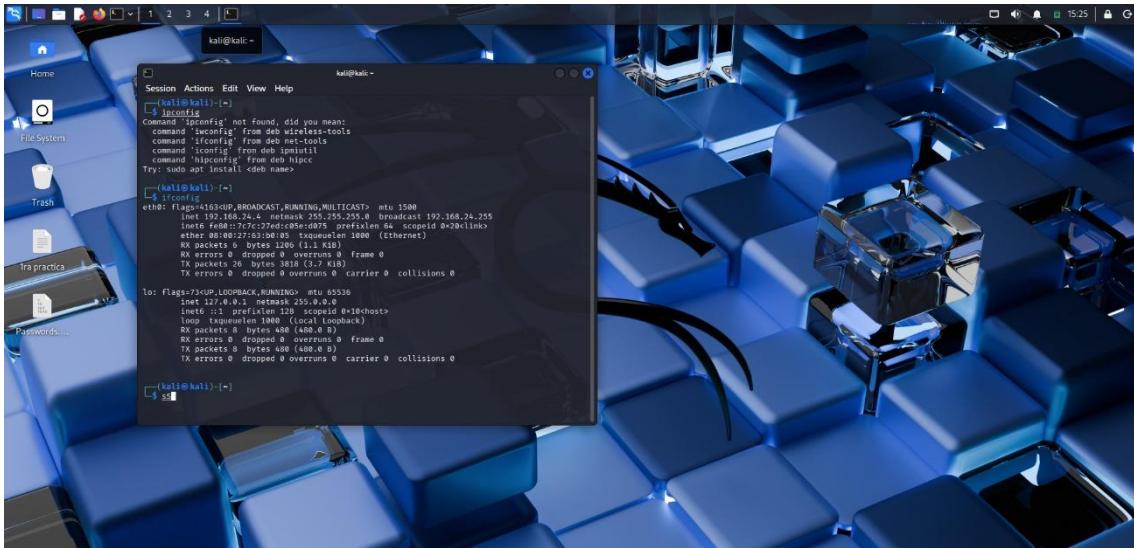
Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Dirección IPv4. . . . . : 192.168.23.2
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.23.1

C:\Users\REDES>
```

- **Equipos Finales:** Se verificó la conectividad en la **PCG2** (Red 3) con la IP 192.168.23.2 y en la máquina **Kali Linux** (Red 1) con la IP 192.168.24.4.



Configuración del Servidor de Monitorización (Ubuntu Server)

En la Red 2 (192.168.22.0/24), se desplegó un servidor **Ubuntu 24.04.3 LTS** como nodo central de servicios. Para asegurar la observabilidad del sistema, se implementó **Netdata** utilizando contenedores Docker.

- **Despliegue de Netdata:** Se crearon volúmenes persistentes para asegurar la integridad de los datos y se ejecutó el contenedor con acceso al host para una monitorización completa del hardware y servicios.

```
sysadmin@host-grupo-02: ~ + 
Windows [Versión 10.0.26200.7623]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\darok>ssh sysadmin@192.168.100.50
sysadmin@192.168.100.50's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-90-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

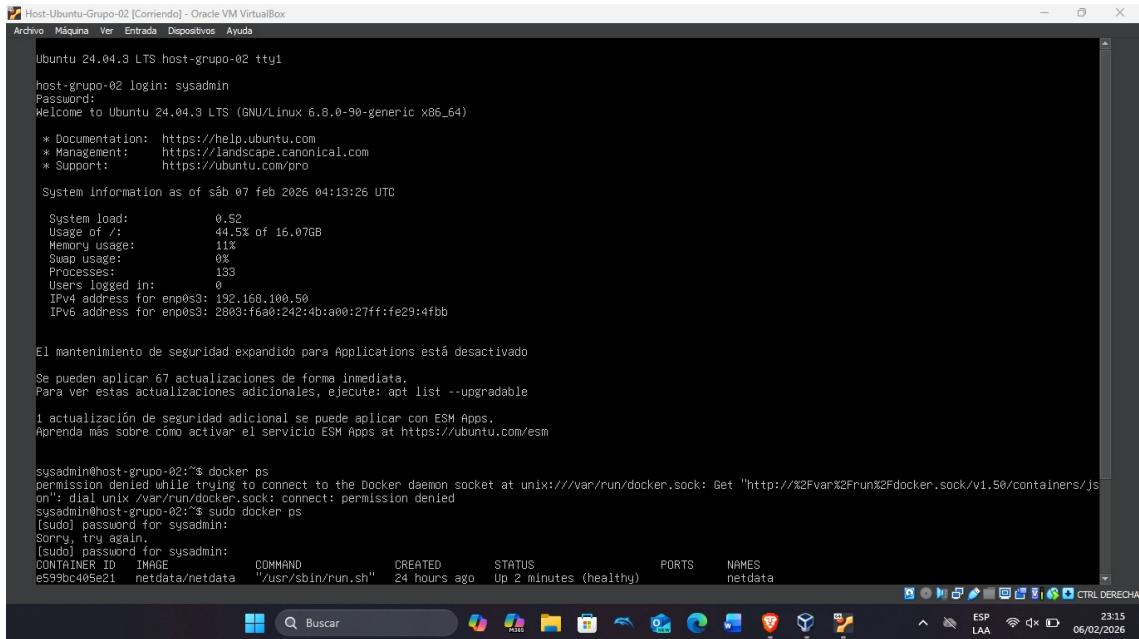
System information as of sáb 07 feb 2026 04:16:15 UTC

System load:          0.99
Usage of /:           44.5% of 16.07GB
Memory usage:         12%
Swap usage:           0%
Processes:            141
Users logged in:     1
IPv4 address for enp0s3: 192.168.100.50
IPv6 address for enp0s3: 2803:f6a0:242:4b:a00:27ff:fe29:4fbb

El mantenimiento de seguridad expandido para Applications está desactivado
Se pueden aplicar 67 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable
1 actualización de seguridad adicional se puede aplicar con ESM Apps.
Aprenda más sobre cómo activar el servicio ESM Apps at https://ubuntu.com/esm

Last login: Fri Feb  6 03:55:03 2026 from 192.168.100.7
sysadmin@host-grupo-02: ~
```

- **Verificación del Servicio:** Se confirmó el estado "Healthy" del contenedor mediante el comando sudo docker ps. El servicio quedó habilitado para iniciarse automáticamente con el sistema (systemctl enable netdata).



The screenshot shows a terminal window titled "Host-Ubuntu-Grupo-02 [Corriendo] - Oracle VM VirtualBox". The terminal displays the following text:

```
Ubuntu 24.04.3 LTS host-grupo-02 tty1
host-grupo-02 login: sysadmin
Password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-90-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information as of sáb 07 feb 2026 04:13:26 UTC

System load:      0.52
Usage of /:       44.5% of 16.07GB
Memory usage:    11%
Swap usage:      0%
Processes:        133
Users logged in: 0
IPv4 address for enp0s3: 192.168.100.50
IPv6 address for enp0s3: 2b03:f6a0:242:4b:a00:27ff:fe29:4fbb

El mantenimiento de seguridad expandido para Applications está desactivado
Se pueden aplicar 67 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

1 actualización de seguridad adicional se puede aplicar con ESM Apps.
Aprenda más sobre cómo activar el servicio ESM Apps en https://ubuntu.com/esm

sysadmin@host-grupo-02:~$ docker ps
permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: Get "http://<2>var<2>run<2>fdocker.sock/v1.50/containers/<3>on": dial unix /var/run/docker.sock: connect: permission denied
sysadmin@host-grupo-02:~$ sudo docker ps
[sudo] password for sysadmin:
Sorry, try again.
[sudo] password for sysadmin:
CONTAINER ID   IMAGE          COMMAND           CREATED          STATUS          PORTS          NAMES
e599bc405e21   netdata/netdata "usr/sbin/run.sh"  24 hours ago   Up 2 minutes (healthy)   netdata
```

1.1. Configuración de Conmutación (Switching)

Se configuró un Switch multicapa con las siguientes VLANs según el archivo de configuración Switch G2.txt:

- **VLAN 21 (KALI_ACCESS):** Puerto Fa0/1 para la estación de auditoría.
- **VLAN 22 (SERVER):** Puerto Fa0/2 destinado a servicios centrales.
- **VLAN 23 (PCG2):** Puerto Fa0/3 para usuarios finales.
- **VLAN 24 (AP):** Puerto Fa0/4 para el punto de acceso inalámbrico. Se habilitó **Spanning-Tree Portfast** en los puertos de acceso para optimizar el tiempo de convergencia.

COM8 - Tera Term VT

Archivo Editar Configuracion Control Ventana Ayuda

```

1004 fddinet-default      act/unsup
1005 tmet-default        act/unsup
Grupo2#enable
Grupo2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Grupo2(config)#hostname Grupo2
Grupo2(config)#$ que el switch se congele si escribes mal un comando
Grupo2(config)#no ip domain-lookup
Grupo2(config)#
Grupo2(config)##! 2. Crear las VLANs (Alineadas con tu Grupo/ IPs)
Grupo2(config)##vlan 21
Grupo2(config)#name KALI_ACCESS
Grupo2(config)#exit
Grupo2(config)#
Grupo2(config)##vlan 22
Grupo2(config)#name SERVER
Grupo2(config)#exit
Grupo2(config)#
Grupo2(config)##vlan 23
Grupo2(config)#name POG2
Grupo2(config)#exit
Grupo2(config)#
Grupo2(config)##vlan 24
Grupo2(config)#name AP
Grupo2(config)#exit
Grupo2(config)#
Grupo2(config)#exit
Grupo2#end
#Mon 00:33:01.489: %SYS-5-CONFIG_I: Configured from console by console
Grupo2#end
translating "end"
% Unknown command or computer name, or unable to find computer address
Grupo2#write memory
Building configuration...
[OK]
Grupo2#show vlan brief
VLAN Name          Status    Ports
-----  

1   default         active    Gi0/1, Gi0/2
10  TELEFONIA_CISCO active    Fa0/13, Fa0/14, Fa0/15, Fa0/16
20  COMPUTADORAS   active    Fa0/5, Fa0/6
21  KALI_ACCESS     active    Fa0/1
22  SERVER          active    Fa0/2
23  POG2            active    Fa0/3
24  AP               active    Fa0/4
30  CAMARAS         active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
40  ASTERISK        active    Fa0/11, Fa0/12
                               Fa0/19, Fa0/20, Fa0/21, Fa0/22
                               Fa0/23
99  NATIVA          active
1002 fddinet-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 tmet-default    act/unsup

```

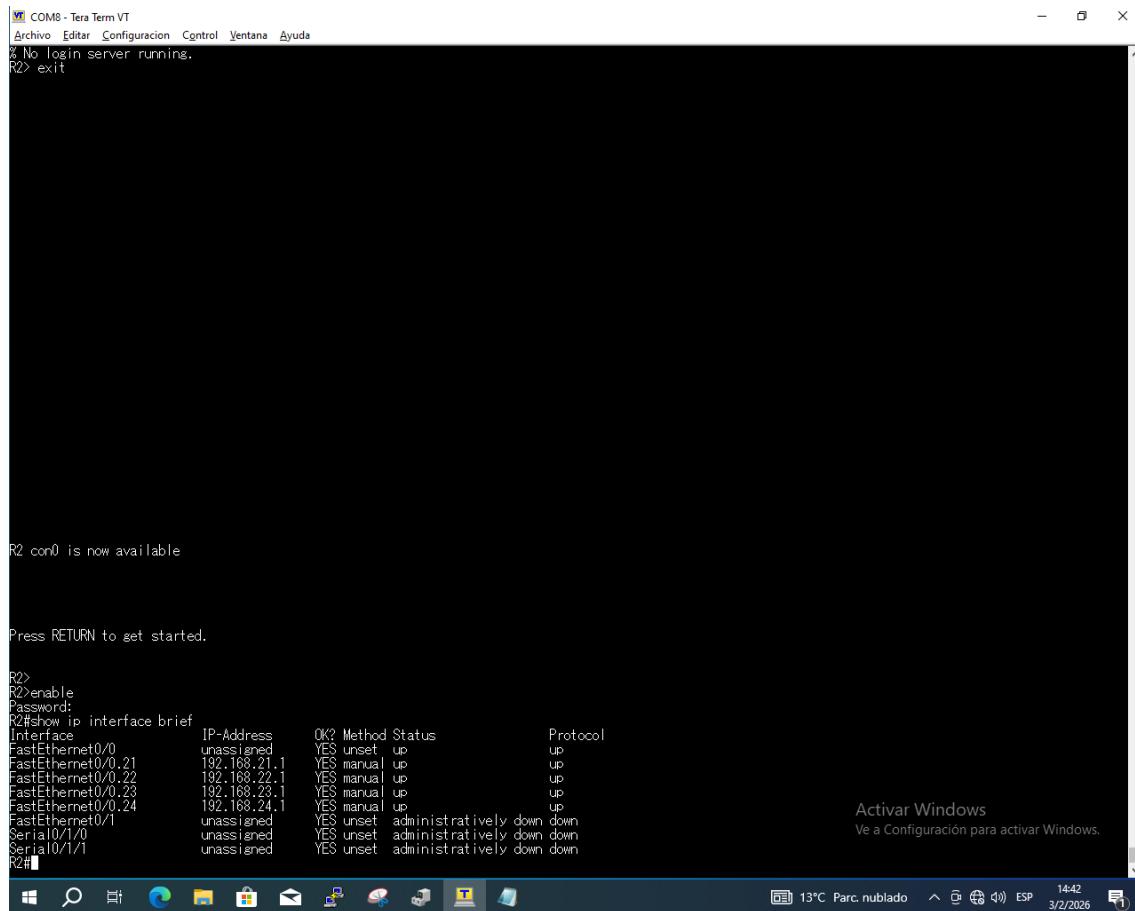
Activar Windows
Ve a la Configuración para activar Windows.

Windows taskbar icons: Start, Search, Task View, File Explorer, Mail, Photos, Videos, Taskbar settings, Taskbar search, Taskbar preview, Taskbar pinned items, Taskbar status bar showing: 13°C Parc. nublado, 14:40, ESP, 3/2/2026.

1.2. Configuración de Enrutamiento y DHCP

El Router central (R2) gestiona el tráfico inter-VLAN mediante subinterfaces FastEthernet0/0.X con encapsulación **dot1Q**. Además, se configuraron pools DHCP para cada segmento:

- **Red 1 (Kali):** 192.168.21.0/24
- **Red 2 (Server):** 192.168.22.0/24
- **Red 3 (PCG2):** 192.168.23.0/24 (Gateway: 192.168.23.1).



```
COM8 - Tera Term VT
Archivo Editar Configuracion Control Ventana Ayuda
% No login server running.
R2> exit

R2 con0 is now available

Press RETURN to get started.

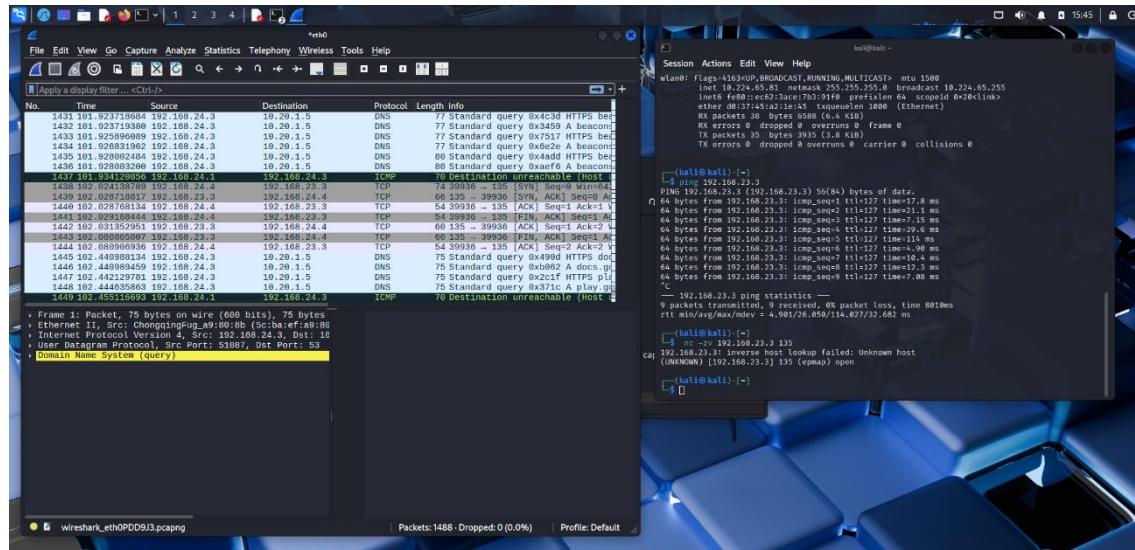
R2>
R2>enable
Password:
R2#show ip interface brief
Interface          IP-Address      OK? Method Status        Protocol
FastEthernet0/0    unassigned      YES unset  up           up
FastEthernet0/0.21 192.168.21.1   YES manual up           up
FastEthernet0/0.22 192.168.22.1   YES manual up           up
FastEthernet0/0.23 192.168.23.1   YES manual up           up
FastEthernet0/0.24 192.168.24.1   YES manual up           up
FastEthernet0/1    unassigned      YES unset  administratively down down
Serial0/0/0        unassigned      YES unset  administratively down down
Serial0/0/1        unassigned      YES unset  administratively down down
R2#
```

Activar Windows
Ve a Configuración para activar Windows.

2. Auditoría de Seguridad y Herramientas de Explotación

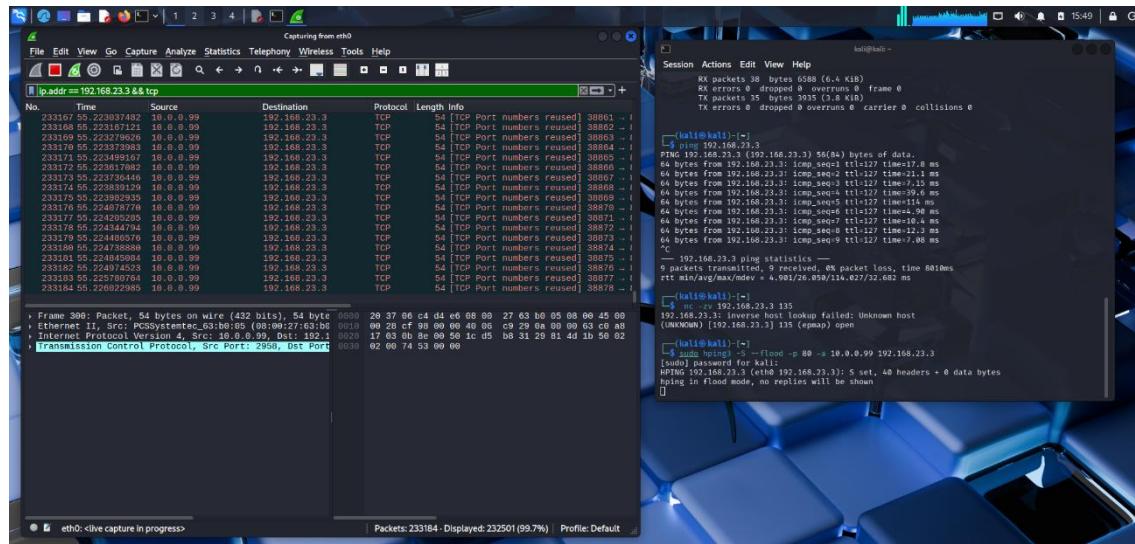
2.1. Monitoreo de Red (Wireshark)

Utilizando **Wireshark** en el host Kali (192.168.24.4), se realizó un análisis del tráfico de red. Se detectaron paquetes de resolución de nombres (DNS) y tráfico ICMP (ping) entre las redes. Como se observa en las capturas, se analizó el flujo de datos hacia la IP 192.168.23.2, confirmando la visibilidad entre segmentos tras el enrutamiento.

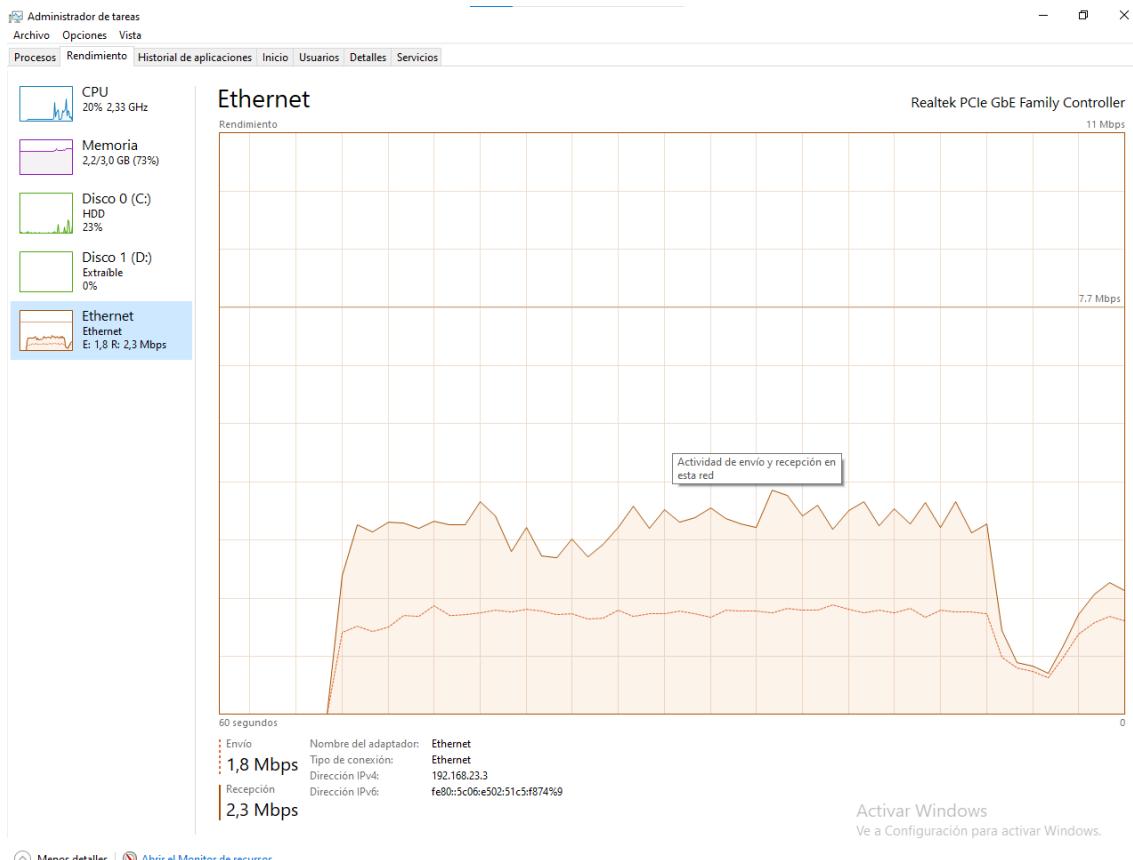


2.2. Ataque de Denegación de Servicio (DoS - hping3)

Se ejecutó una prueba de estrés mediante un ataque de inundación SYN hacia la PCG2 (192.168.23.3).

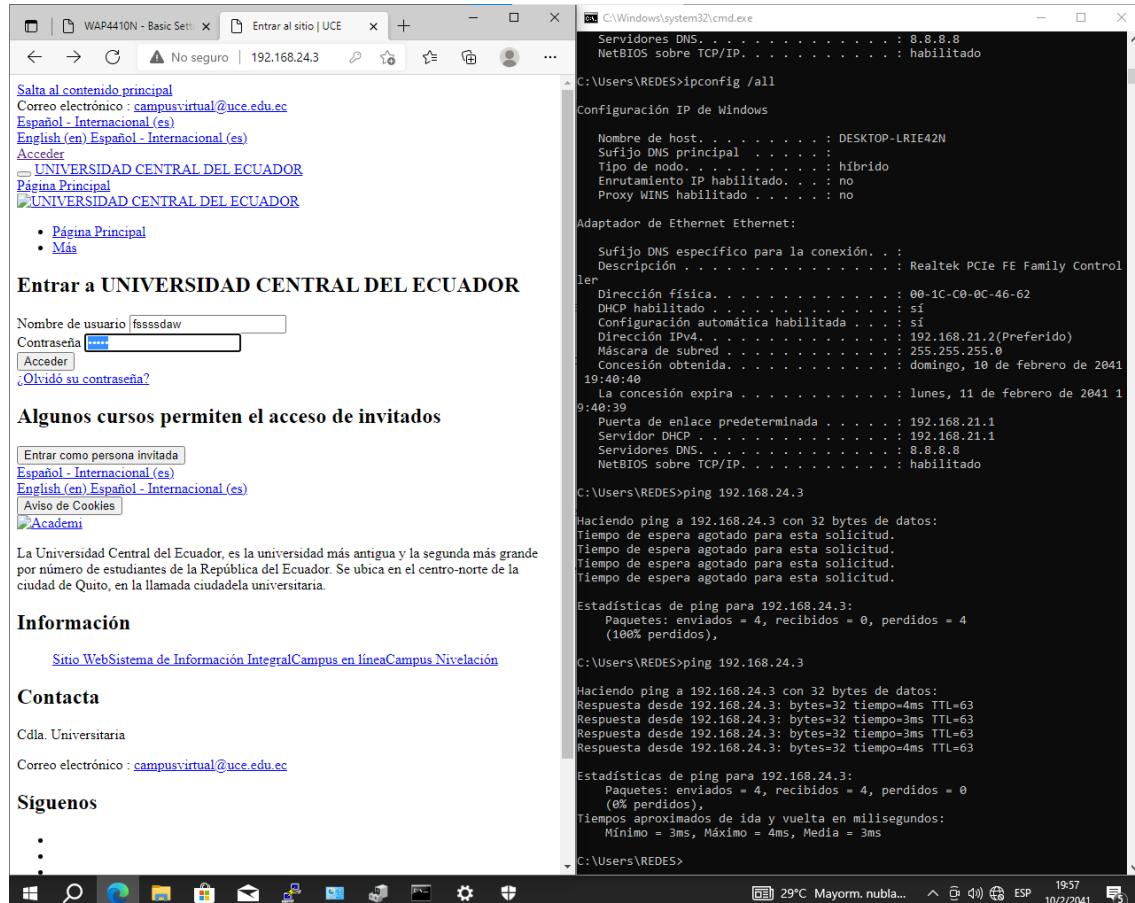


- **Comando:** sudo hping3 -S --flood -p 80 -a 10.0.0.99 192.168.23.3.
- **Resultado:** El monitor de recursos de la víctima mostró una recepción constante de **2.3 Mbps** de tráfico, lo que representa una saturación de la pila TCP del equipo objetivo bajo un escenario de inundación.

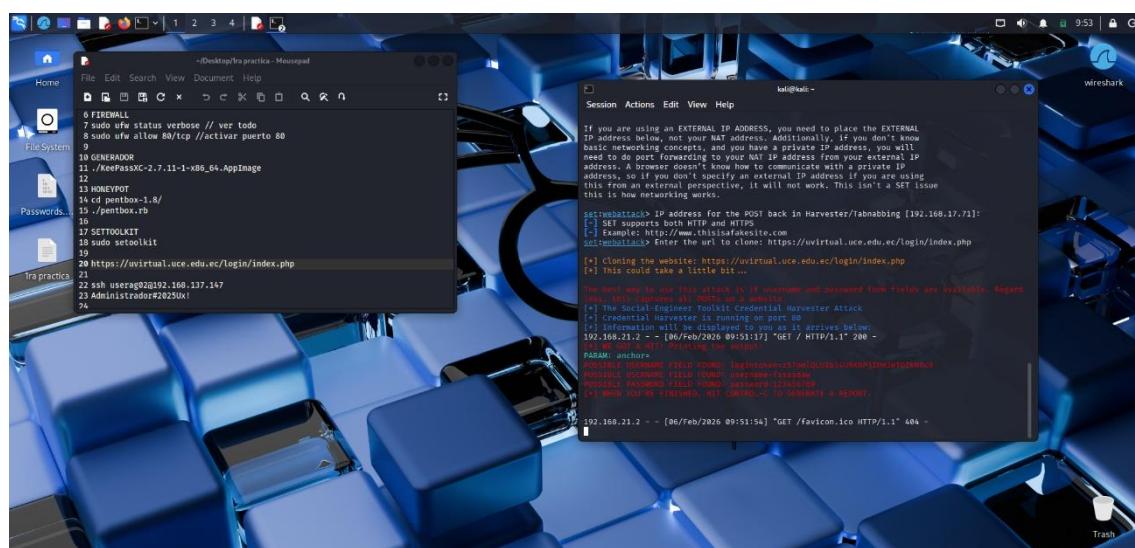


2.3. Ataque a Credenciales (SET - Social Engineering Toolkit)

Se realizó un ataque de **Credential Harvesting** clonando el portal de acceso de la **Universidad Central del Ecuador (UCE)**.



- **Proceso:** Se configuró un servidor fraudulento en Kali. Al acceder la víctima, la herramienta SET interceptó en tiempo real el usuario (issssdaw) y la contraseña ingresada, demostrando la eficacia de los ataques de ingeniería social en redes locales.



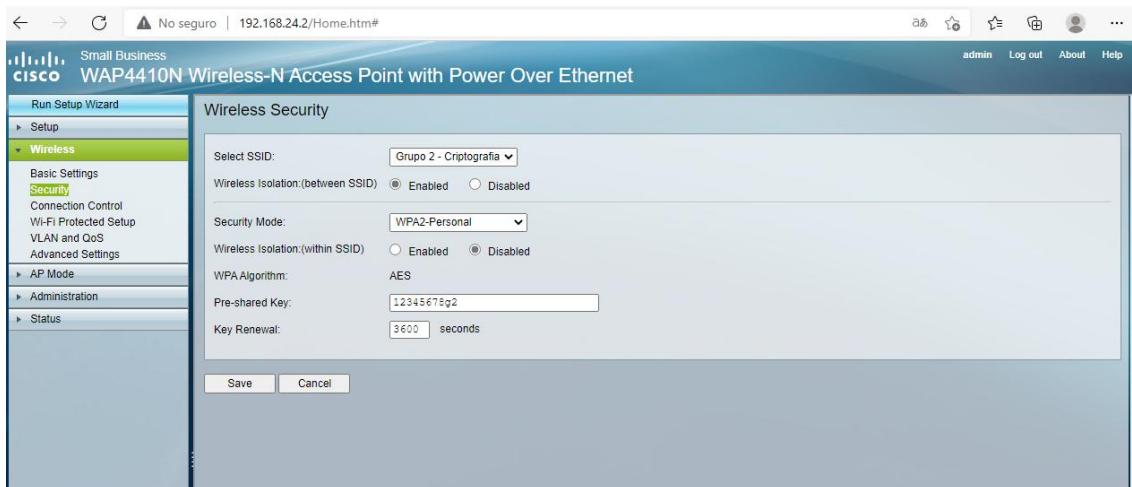
2.4. Actividad Opcional: Escaneo con Netcat (nc)

Como actividad adicional, se utilizó **Netcat** para verificar la disponibilidad de puertos críticos en la Red 3. El escaneo al puerto 135 (RPC) devolvió un estado **open**, permitiendo identificar posibles vectores de entrada para ataques de ejecución remota de código.

3. Configuración del Access Point (Wireless)

Se configuró un equipo Cisco WAP4410N con los siguientes parámetros de seguridad:

- **SSID:** Grupo 2 - Criptografia.
- **Seguridad:** WPA2-Personal (AES).
- **Clave:** 12345678g2.



4. Bibliografía

[1] Cisco Systems, "Cisco IOS IP Configuration Guide, Release 15.x," 2024. [En línea]. Disponible en: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr/config_guide/15-mt/iad-15-mt-cg-book.html

[2] Kali Linux Documentation, "Social-Engineer Toolkit (SET) Usage," 2024. [En línea]. Disponible en: <https://www.kali.org/tools/set/>

[3] Docker Documentation, "Run a container: Docker run reference," 2024. [En línea]. Disponible en: <https://docs.docker.com/engine/reference/run/>

[4] Netdata Inc., "Deploy Netdata with Docker," 2025. [En línea]. Disponible en: <https://learn.netdata.cloud/docs/installing/docker>

[5] G. Lyon, "Nmap Network Scanning," Insecure.org, 2024. [En línea]. Disponible en: <https://nmap.org/book/man.html>

[6] Wireshark Foundation, "Wireshark User's Guide," 2024. [En línea]. Disponible en: https://www.wireshark.org/docs/wsug_html_chunked/

[7] Canonical Ltd., "Ubuntu Server Guide: Introduction to Ubuntu Server," 2024. [En línea]. Disponible en: <https://ubuntu.com/server/docs>

[9] Linux Foundation, "Standard Linux Command Line Administration," 2024. [En línea]. Disponible en: <https://docs.kernel.org/>