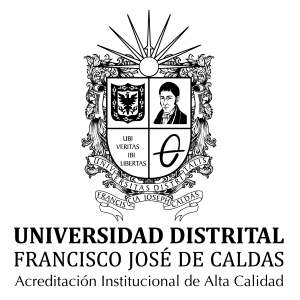
**UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS**



**AUDITORÍA DE SEGURIDAD WI-FI SIMULADA EN RED LOCAL**

**GRUPO DE TRABAJO GLUD**

**CIBERSEGURIDAD**

**CARLOS ANDRÉS ABELLA MAHECHA - 20201020112**

**FACULTAD DE INGENIERÍA**

**BOGOTÁ 2025**

[Objetivo general del proyecto 3](#_zak3y28gwv4m)

[Preparación del entorno de trabajo 3](#_dvyz4b3ew836)

[Simulación de punto de acceso abierto (sin cifrado) 4](#_wxh0p4wqbt2j)

[Captura de tráfico en red local 5](#_upcxheheeny2)

[Escaneo de servicios en el router de la red local 7](#_9eqj89qd24ka)

[Simulación de red WPA2 y análisis teórico del handshake 8](#_kjpnxa450ytz)

[Relación con un entorno universitario 10](#_f94ekd8bz5ws)

A continuación se describe el procedimiento realizado para llevar a cabo una simulación de auditoría Wi-Fi en un entorno controlado, utilizando como base una red local doméstica. Debido a limitaciones técnicas (falta de adaptador Wi-Fi USB en modo monitor), se optó por una estrategia teórico-práctica enfocada en los principios clave de reconocimiento pasivo, captura de tráfico y análisis de configuraciones WPA2.

# **Objetivo general del proyecto**

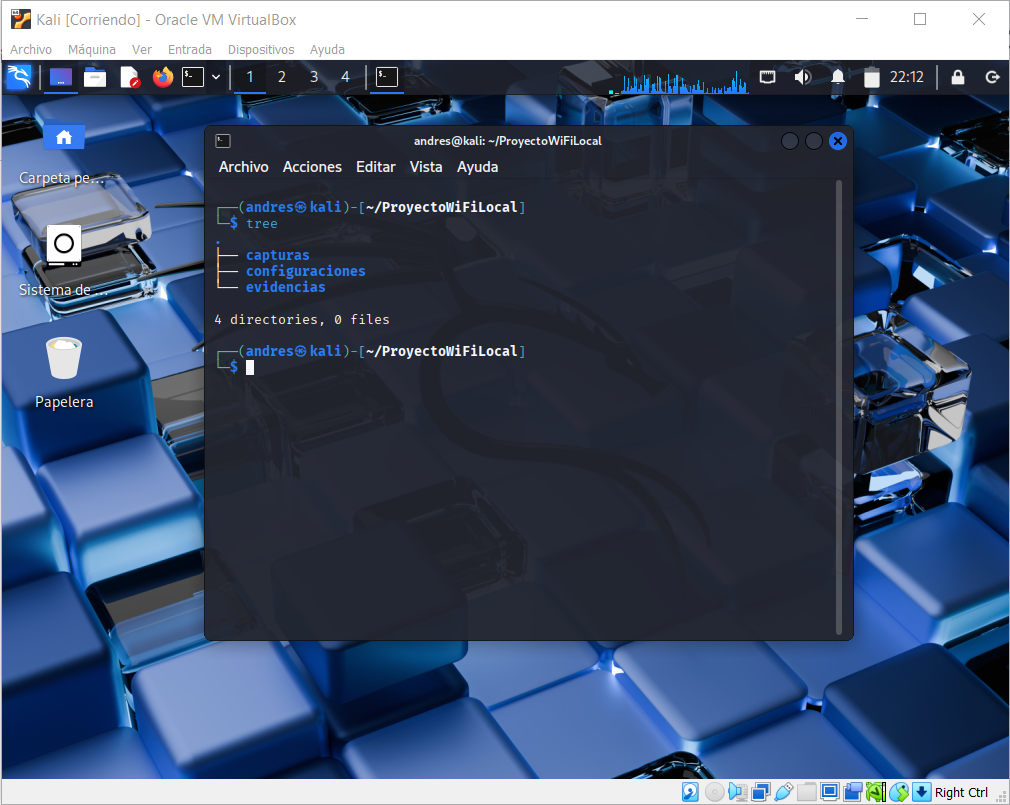
Analizar de forma introductoria la seguridad de una red Wi-Fi doméstica mediante técnicas básicas de captura de tráfico, escaneo de servicios y estudio del proceso de autenticación WPA2, simulando un ejercicio de auditoría ética.

# **Preparación del entorno de trabajo**

Se creó una estructura organizada de carpetas en el sistema Kali Linux para almacenar los archivos de configuración, capturas de tráfico y evidencias gráficas del análisis.

Comando ejecutado:

mkdir -p ProyectoWiFiLocal/{configuraciones,capturas,evidencias}

   
Figura 1. Imagen de la terminal mostrando la estructura de carpetas con el comando tree.

# **Simulación de punto de acceso abierto (sin cifrado)**

Crea el archivo de configuración teórica:

nano configuraciones/hostapd\_open.conf

Pega:

interface=eth0

driver=nl80211

ssid=RedLocal\_Open

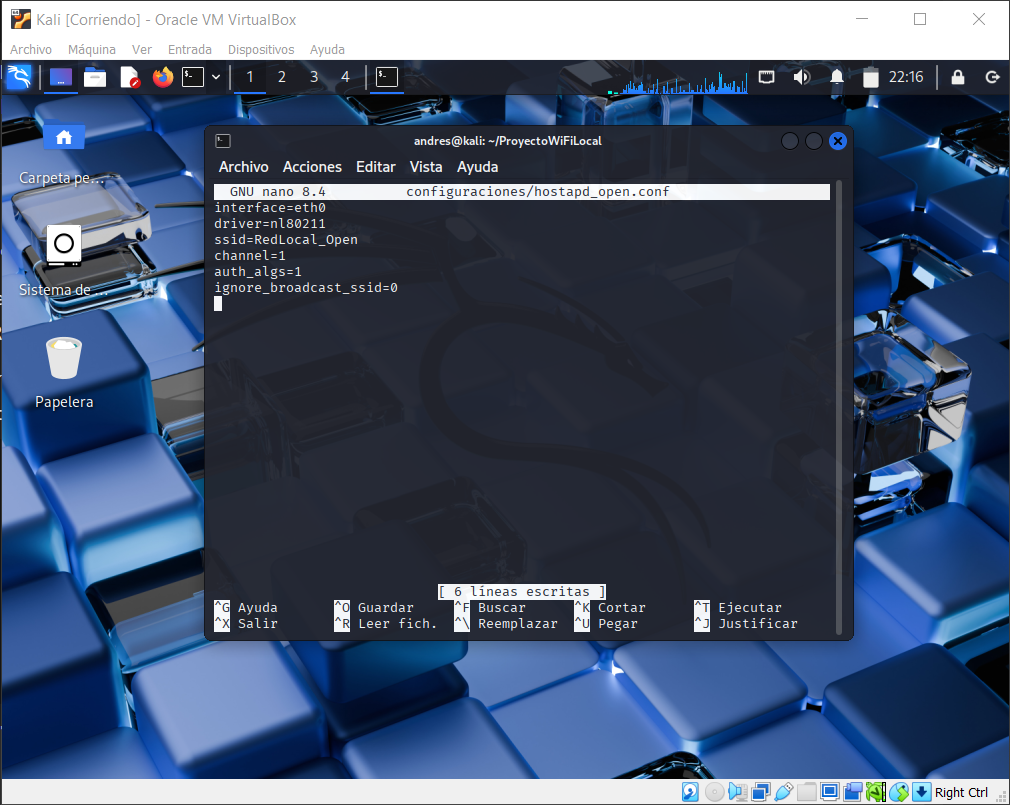
channel=1

auth\_algs=1

ignore\_broadcast\_ssid=0

Guarda (Ctrl+O) y sale (Ctrl+X).

Se creó un archivo de configuración de hostapd que simula una red inalámbrica abierta, llamada “RedLocal\_Open”, sin ningún mecanismo de autenticación ni cifrado.

  
Figura 2. Imagen del archivo hostapd\_open.conf abierto en terminal o editor nano.

# **Captura de tráfico en red local**

Se utilizó tcpdump para capturar tráfico de red generado manualmente mediante pings y una solicitud HTTP sin cifrado.

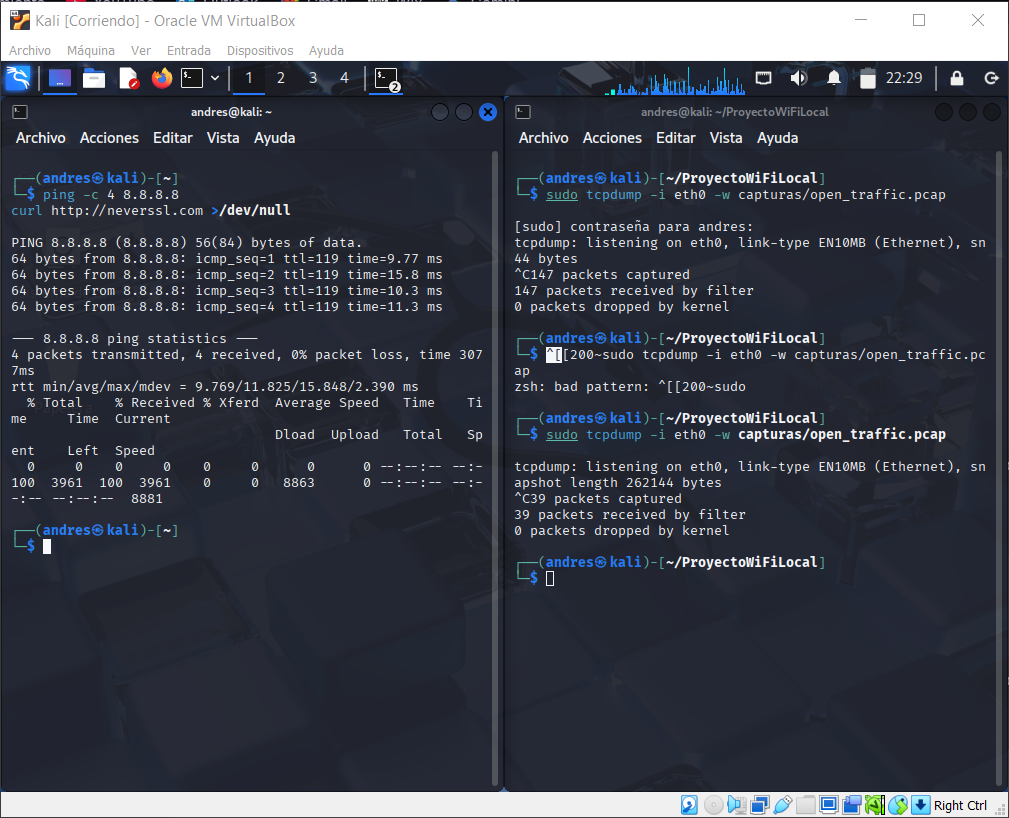
Comando para iniciar la captura:

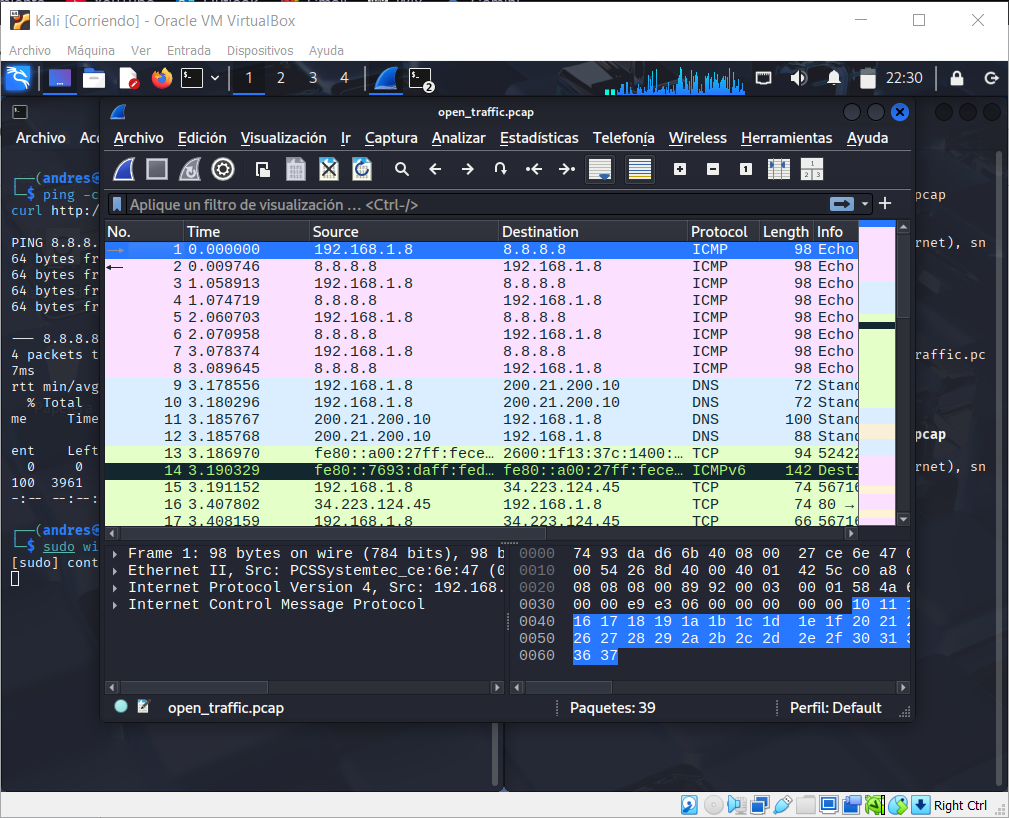
sudo tcpdump -i eth0 -w capturas/open\_traffic.pcap

Tráfico generado durante la captura:

ping -c 4 8.8.8.8

curl http://neverssl.com >/dev/null

  
Figura 3. Imagen de la terminal con tcpdump en ejecución mostrando paquetes capturados.

  
Figura 4. Imagen de Wireshark abierta con open\_traffic.pcap, mostrando paquetes ICMP y tráfico HTTP.

# **Escaneo de servicios en el router de la red local**

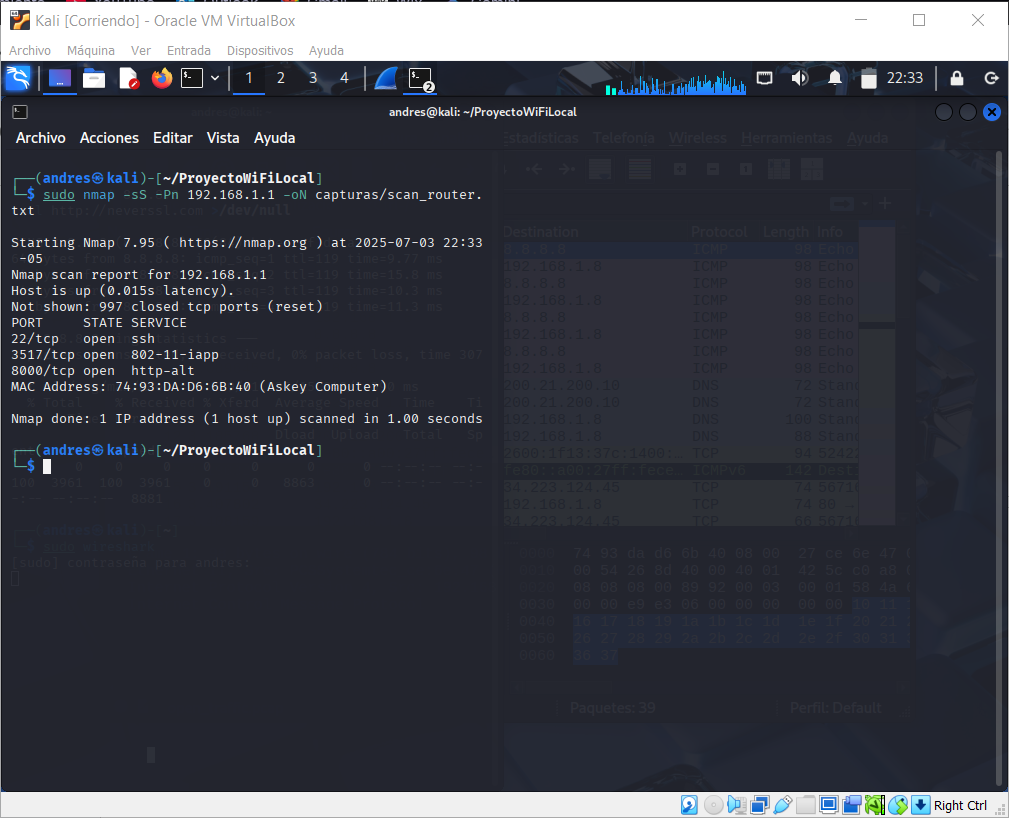
Se utilizó Nmap para identificar servicios activos en el gateway (router) de la red. Esto permite detectar posibles vectores de ataque internos, como puertos abiertos o servicios mal configurados.

Averigua la IP de tu gateway (router):  
  
ip route | grep default

Resultado: default via 192.168.1.1 dev eth0 proto dhcp src 192.168.1.8 metric 100

Escanea puertos con nmap:

sudo nmap -sS -Pn 192.168.1.1 -oN capturas/scan\_router.txt

Figura 5. Imagen de la terminal mostrando el resultado del escaneo Nmap, con listado de puertos abiertos.

# **Simulación de red WPA2 y análisis teórico del handshake**

Se redactó un archivo de configuración para una red WPA2-PSK con contraseña débil, para analizar la importancia del handshake en la autenticación del cliente.

Archivo: configuraciones/hostapd\_wpa2.conf

interface=eth0

driver=nl80211

ssid=RedLocal\_WPA2

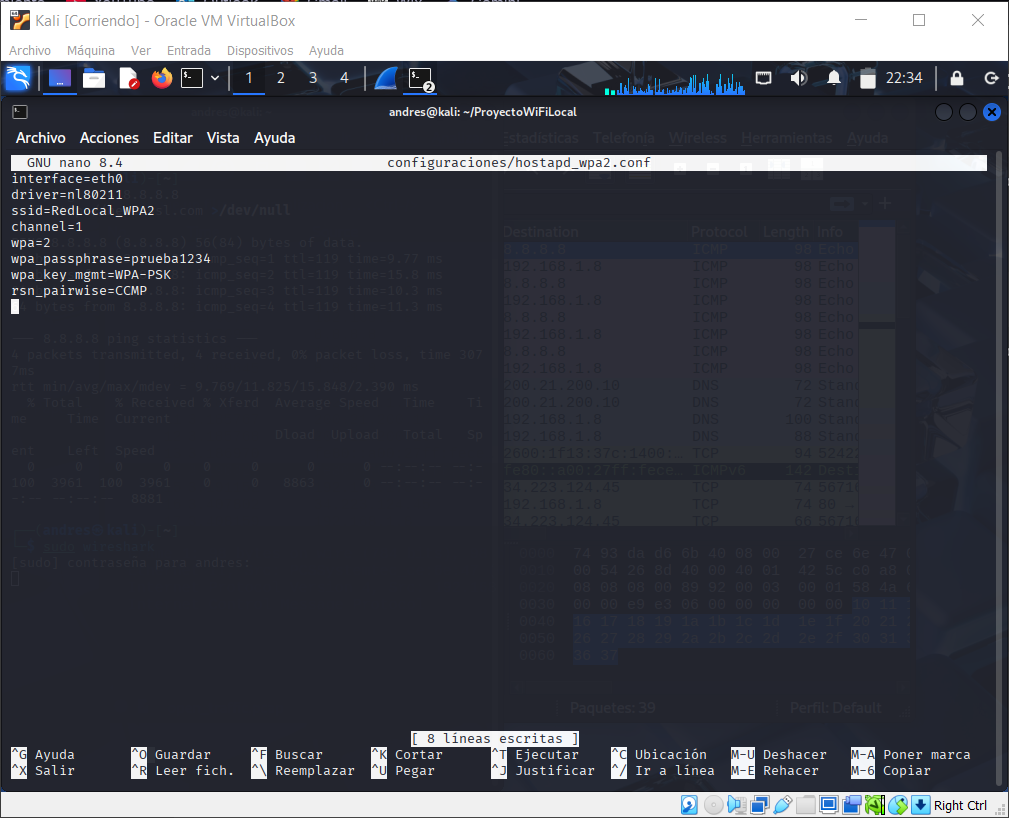
channel=1

wpa=2

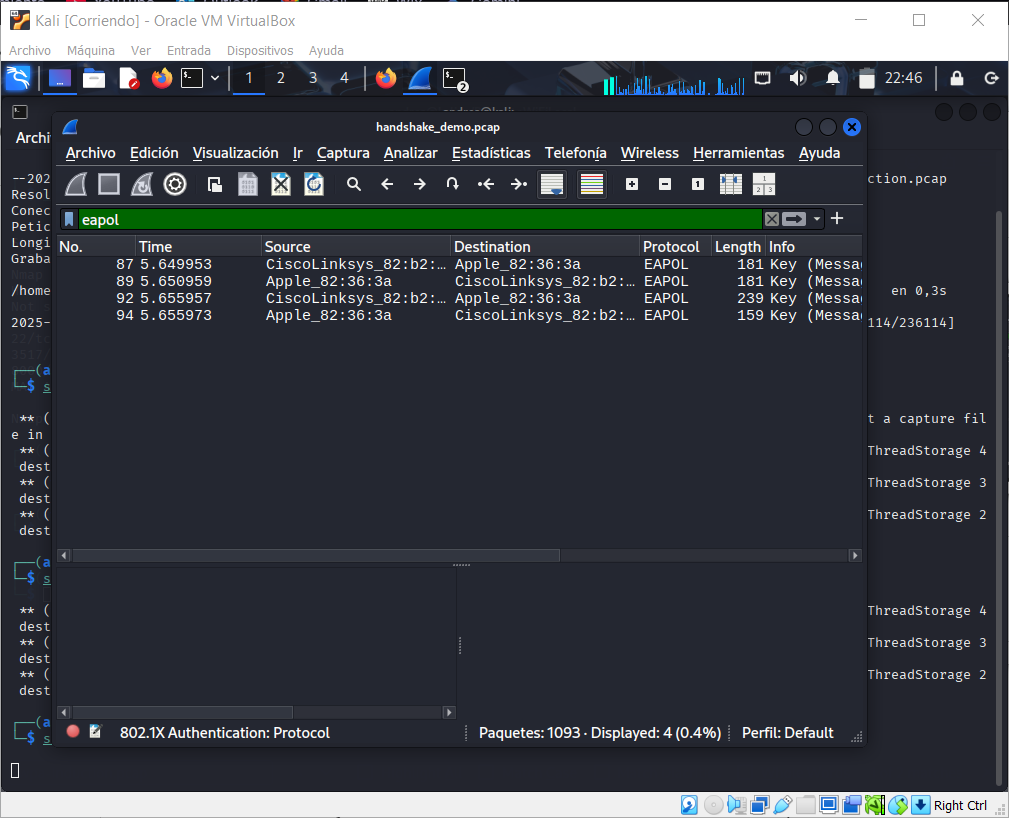
wpa\_passphrase=prueba1234

wpa\_key\_mgmt=WPA-PSK

rsn\_pairwise=CCMP

  
Figura 6. Imagen del archivo hostapd\_wpa2.conf en el editor.

Dado que no se pudo capturar un handshake real, se analizó un archivo de ejemplo oficial (handshake\_demo.cap) descargado de una fuente confiable. Se utilizó Wireshark para aplicar el filtro eapol y observar las 4 tramas del 4-way handshake.

  
Figura 7. Imagen de Wireshark con el filtro “eapol” aplicado, mostrando las 4 tramas del handshake.

Este análisis demuestra cómo un atacante podría capturar este intercambio y realizar un ataque offline con herramientas como aircrack-ng, usando diccionarios de contraseñas.

# **Relación con un entorno universitario**

Todo lo realizado en esta red local se puede extrapolar a una red universitaria:

* En redes abiertas, el tráfico podría ser capturado como en el paso 3.
* Servicios expuestos podrían detectarse con Nmap como en el paso 4.
* En redes WPA2, un atacante podría capturar el handshake y usar herramientas como aircrack-ng si la contraseña es predecible.

Este proyecto demuestra que incluso con recursos limitados y en un entorno doméstico, es posible aplicar conocimientos fundamentales de auditoría Wi-Fi, comprendiendo las principales amenazas y técnicas utilizadas en la ciberseguridad de redes inalámbricas.

Las técnicas y observaciones realizadas en la red local son extrapolables a un entorno universitario. En una red abierta del campus, sería posible capturar tráfico sin cifrar de múltiples dispositivos. Un escaneo de red permitiría identificar servicios expuestos en servidores internos o impresoras en red. Además, en redes protegidas con WPA2-PSK, capturar el handshake permitiría intentar romper la clave compartida usando ataques de diccionario si esta es débil.