

# Actividad: Escaneo con Nmap y Análisis de Tráfico con Wireshark

**JAMIN ALBERTO BOLAINA BURGOS IRIYC-91**

## Objetivo

Ejecutar un script que realice un escaneo de puertos con Nmap y capture tráfico de red con Tshark. Analizar los resultados de Nmap y el archivo de captura en Wireshark, aplicando filtros específicos, para describir el comportamiento de la red y los servicios detectados.

## Requisitos

- Entorno Linux con Nmap y Tshark instalados. - Script 'scan\_and\_capture.sh' con permisos de ejecución. Wireshark para abrir y analizar la captura. - Acceso a la terminal de comandos.

## Instrucciones de Ejecución

1. Copia el script 'scan\_and\_capture.sh' en tu directorio de trabajo. 2. Concede permisos de ejecución: `chmod +x scan_and_capture.sh` 3. Ejecuta el script indicando objetivo y duración (s), por ejemplo: `./scan_and_capture.sh 192.168.1.100 60` 4. Se generarán los archivos: - `nmap_results.txt` - `capture.pcap` 5. Abre 'nmap\_results.txt' y extrae los datos solicitados. 6. Abre 'capture.pcap' en Wireshark y aplica los filtros indicados.

## Campos para Completar

1. Resultados de Nmap:

Puerto	Servicio	Versión	Comentario
80	httpd		Protocolo abierto
22	Tcp.port		Protocolo abierto

2. Análisis en Wireshark:

- Filtro: http

• Número de paquetes: \_\_\_\_\_

• Observaciones: \_\_\_\_\_

- Filtro: dns

• Número de paquetes: \_\_\_\_\_

• Observaciones: \_\_\_\_\_

- Filtro: tcp.port == 22

• Número de paquetes: \_\_\_\_\_

• Observaciones: \_\_\_\_\_

- Filtro: tcp.port == 80

• Número de paquetes: \_\_\_\_\_

• Observaciones: \_\_\_\_\_

- Filtro: Otro filtro:icmp

• Número de paquetes: \_\_\_\_\_ 200 \_\_\_\_\_

• Observaciones: son paquetes de echo y reply que se usan para ping solo estafico que se genero

### 3. Conclusión:

Básicamente es un laboratorio que hace un escaneo de nuestro trafico en el cual nos arroja nuestro trafico en la red nuestra protocolos como httpd y icmp en mi caso por alguna razón no me arrojó nada en el .pcap pero si me dijo de otros como el icmp que fue realmente el ping.