Actividad: Escaneo con Nmap y Análisis de Tráfico con Wireshark

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

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:

• Número de paquetes: _____

• Observaciones: _____

3. Conclusión:

Describe en tus propias palabras el comportamiento de la red observado, relacionando los resultados de Nmap con el tráfico capturado.