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
80	HTTP	Apache httpd 2.4.58 ((win64) OpenSSL/3.1.3 PHP/8.2.12)	Sitio web corriendo sobre Apache en Windows con soporte para PHP.
135	msrpc	Microsoft Windows RPC	Servicio RPC típico de sistemas Windows.
139	netbios-ssn	Microsoft Windows netbios-ssn	Comunicación NetBIOS, puede indicar recurso compartido o red local Windows.
443	ssl/http	Apache httpd 2.4.58 + PHP 8.2.12	Sitio web seguro (HTTPS) con PHP,mismo que en puerto 80 pero cifrado.

445	microsoft-ds	No detectada claramente	Puerto SMB de Windows, probable uso para compartir archivos.
3306	mysql	MariaDB 5.5.5-10.4.32	

2. Análisis en Wireshark:

- Filtro: http

• Número de paquetes: 0

• Observaciones: de seguro el antivirus esta bloqueando

- Filtro: dns

• Número de paquetes: 0

• Observaciones: no tuvo consultas por eso no detecto paquetees

- Filtro: tcp.port == 22

• Número de paquetes: 0

• Observaciones: SSH bloqueada seguramente

- Filtro: tcp.port == 80

• Número de paquetes: 0

• Observaciones: web no encendida

- Filtro: Otro filtro: tcp.flags.reset == 1

• Número de paquetes: 1

• Observaciones: es una conexión rechazada

3. Conclusión:

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

Tuvimos pocos resultados por el tema de que es local el escaneo y solo se lo hizo a mi ip nos mostro que teníamos varios puertos abiertos los cuales cargaban servicios como HTTP hasta Mysql