ESCANEO NMAP Y TSHARK (PCAP)

Perez Anota Omar Alejandro

UT CANCUN 22394061

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	Puerto de apache (xampp)
135	Msrpc	Microsoft Windows RPC	Desconozco su función
139	Netbios-ssn	MS Windows netbios-ssn	
7070	Ssl/realserver	Desconocido	Posible riesgo de ataques en este puerto.

2. Análisis en Wireshark:

- Filtro: http

• Número de paquetes: 18 paquetes

• Observaciones: Se observan paquetes con error 404 y 302.

- Filtro: dns

• Número de paquetes: 2

• Observaciones: _____

- Filtro: tcp.port == 22

- Número de paquetes: 4 paquetes
- Observaciones: Recibió intentos de conexión, pero fueron rechazados.

- Filtro: tcp.port == 80
- Número de paquetes: 105
- Observaciones: Probablemente esté abierto y respondiendo por el servidor apache ejecutándose con el servicio web.

- Filtro: Otro filtro:
- Número de paquetes: 2121

- Observaciones: Estos paquetes corresponden a paquetes SYN, es decir, intentos iniciales de establecer una conexión TCP (inicio del handshake). Un alto número de estos puede indicar intentos de conexión normales o, en exceso, intentos de escaneo o ataques tipo SYN.

3. Conclusión:

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

El funcionamiento de la red es como lo esperado. Un pc host escaneado que funge como servidor web, de base de datos y con los puertos comúnmente abiertos. A excepción del puerto 7070 que usa el servicio realserver y el que puede ser vulnerado, los demás protocolos y servicios están identificados. Algunos escaneos tendieron a fallar, pero el comportamiento fue lo normal.