Práctica 3: Escaneo Y Descubrimiento de Red con Nmap

Alumnos: _____ Calificación: _____

Enrique Morales Aguilar[a]

[a] *Profesor de Facultad de Ciencias de la Computación - FCC Cub. CC01-108*

Resumen—Esta práctica introduce al estudiante en el uso de Nmap (Network Mapper), una herramienta fundamental para el descubrimiento de hosts activos y servicios en una red. Se realizarán escaneos básicos para identificar dispositivos, puertos abiertos y versiones de servicios, desarrollando habilidades esenciales de reconocimiento de red.

Objetivo

- Familiarizarse con los comandos básicos de Nmap.
- Identificar hosts activos en una red local.
- Descubrir puertos abiertos y servicios en ejecución.
- Interpretar los resultados del escaneo para mapear la topología de red.

Requisitos

- Instalar una distribución de Kali Linux o en su defecto la herrameinta Nmap (https://nmap.org/download.html)

Introducción

Nmap es una herramienta de código abierto utilizada para exploración de redes y auditorías de seguridad. Permite a los administradores de red descubrir qué dispositivos están conectados, qué puertos están abiertos y qué servicios están en ejecución. En esta práctica, utilizaremos diferentes tipos de escaneos *ping sweep, TCP connect scan, SYN scan* para realizar un inventario completo de una red de prueba.

El reconocimiento de red es la primera fase en cualquier evaluación de seguridad y es fundamental para la administración efectiva de redes. Los comandos básicos incluyen:

- **nmap -sn 192.168.1.0/24** (descubrimiento de hosts).
- **nmap -sV 192.168.1.1** (detección de versiones de servicios).
- **nmap -p- 192.168.1.1** (escaneo de todos los puertos).

Resolución Esperada

1. Verificar instalación de Nmap.
2. Identificar interfaz de red.
3. Escaneo Ping (descubrir host activos)
4. Escaneo de puertos de manera generalizada y específica.
5. Tipos de escaneo.
6. Detectar versiones de servicios.
7. Detección del Sistema Operativo.
8. Uso de scripts NSE (Nmap Scripting Engine).
9. Escaneo múltiple de hosts.
10. Detectar hosts ocultos.
11. Control de la velocidad de escaneo.
12. Escaneo sigiloso.
13. Análisis de resultados.
14. Guardar resultados y escaneos completos

Observaciones

- Asegúrate de realizar los escaneos únicamente en redes de prueba o en entornos autorizados.
- Los escaneos SYN **(-sS)** requieren privilegios de root. El tiempo de escaneo varía según el rango de IPs y puertos seleccionados.
- Documenta todos los hosts y servicios descubiertos para referencia futura.
- Algunos firewalls pueden bloquear o detectar escaneos activos.

Entregable

El alumno debe entregar su reporte y un archivo de texto. El archivo de texto deberá ser hecho con nano, en el cual deberá incluir:

1. Hosts descubiertos: Número total, IPs, MACs.
2. Servicios por host: Enlistar los puertos abiertos y los servicios.
3. Sistemas operativos detectados.
4. ¿Cuáles son las versiones de servicios y software identificados?
5. Posibles vulnerabilidades.

Preguntas de Ayuda

- ¿Cuántos hosts activos encontraste en tu red?
- ¿Qué puertos están abiertos con más frecuencia?
- ¿Detectaste algún servicio desactualizado?
- ¿Hubo diferencias entre escaneo TCP y SYN?
- ¿Qué hosts no responden a ping pero tienen puertos abiertos?
- ¿Identificaste algún riesgo de seguridad evidente?