Escuela de Ingenierías

Informe de Laboratorio – Seguridad de la información

(Practico)

[Taller #2]

Participantes

Datos del Estudiante	
Nombre	

Escuela de Ingenierías
Medellín, [2024.Octubre.16]

INFORME DE LABORATORIO: ESCANEO DE PUERTOS CON NMAP

Introducción

El escaneo de puertos es una técnica fundamental en la seguridad informática utilizada para descubrir servicios abiertos en una máquina y evaluar posibles vulnerabilidades. Nmap (Network Mapper) es una herramienta gratuita y de código abierto que permite realizar escaneos de red y detectar información sobre dispositivos y servicios en ejecución. En este laboratorio, exploraremos el uso de Nmap en entornos Windows y Linux para identificar puertos abiertos y entender su importancia en la seguridad.

Objetivos

- Comprender el concepto de escaneo de puertos y su importancia en ciberseguridad.
- Aprender a utilizar Nmap para realizar escaneos en sistemas Windows y Linux.
- Diferenciar los distintos tipos de escaneo que ofrece Nmap.
- Identificar puertos abiertos y servicios en ejecución.
- Aplicar medidas de seguridad para mitigar riesgos asociados a puertos expuestos.

Conceptos a Entender

3.1 Escaneo de Puertos El escaneo de puertos es una técnica utilizada para identificar qué puertos están abiertos en un sistema y qué servicios están corriendo en ellos. Los puertos abiertos pueden representar posibles puntos de ataque si no están protegidos adecuadamente.

3.2 Tipos de Escaneo en Nmap

- **Escaneo TCP Connect (-sT):** Realiza una conexión completa con el puerto de destino.
- **Escaneo SYN (-sS):** También llamado "escaneo sigiloso", envía paquetes SYN sin completar la conexión.
- **Escaneo UDP (-sU):** Explora puertos UDP abiertos.
- **Detección de sistema operativo (-O):** Intenta identificar el sistema operativo de un host.

Laboratorio Practico (Practica)

Punto 1: Instalación de Nmap

- En Linux, instala Nmap con el comando: sudo apt install nmap (Debian/Ubuntu) o sudo yum install nmap (CentOS/RHEL).
- En Windows, descarga e instala Nmap desde https://nmap.org/download.html.

Punto 2: Escaneo Básico de Puertos

- Abre una terminal o línea de comandos.
- Ejecuta nmap [IP_del_objetivo] para realizar un escaneo básico.
- Analiza los resultados y revisa qué puertos están abiertos.

Punto 3: Escaneo Avanzado

- Ejecuta un escaneo SYN con nmap -sS [IP_del_objetivo].
- Realiza un escaneo de sistema operativo con nmap -O [IP_del_objetivo].
- Usa nmap -sU [IP_del_objetivo] para explorar puertos UDP abiertos.

Punto 4: Escaneo de una Red Completa

- Ejecuta nmap -sP 192.168.1.0/24 para identificar dispositivos activos en una red local.
- Identifica posibles amenazas y servicios vulnerables (Esto mediante los CVS).

Punto 5: Medidas de Seguridad (Opcional)

- Utiliza firewalls para restringir el acceso a puertos innecesarios.
- Configura reglas de filtrado de tráfico en el firewall.
- Mantén actualizados los sistemas y los servicios en ejecución.