Escaneo y Enumeración de una red local con Nmap en Kali Linux

Introducción

En este proyecto, aprenderá a utilizar Nmap, una potente herramienta de escaneo de red, para descubrir dispositivos y servicios que se ejecutan en una red local. El escaneo y la enumeración de redes son habilidades críticas para hackers éticos, ya que ayudan a identificar posibles objetivos y vulnerabilidades dentro de una red. Al final de este proyecto, podrá realizar escaneos básicos de red, identificar puertos abiertos y recopilar información sobre los dispositivos de su red utilizando Kali Linux.

Pre-requisitos

- Comprención básica de los conceptos de redes (dirección IP, puertos, etc.).
- Familiaridad con el uso de la interfaz de línea de comandos (CLI).
- Kali Linux instalado en su máquina (ya sea de forma nativa, en una máquina virtual, o como una bota en vivo).

Configuración de laboratorio y herramientas

Herramitas

- **Kali Linux:** Distribuición Linux derivado de Debian diseñada para pruebas forenses digitales y de penetración.
- **Nmap** : Herramienta de exploración de redes y escáner de seguridad/porto (pre-instalado en Kali Linux).
- Una red local con múltiples dispositivos conectados (ordenadores, impresoras, dispositivos IoT, etc.).

Instalación

Nmap está preinstalado en Kali Linux. Puede verificar la instalación o actualizarlo usando el siguiente comando:

sudo apt-get update && sudo apt-get install nmap

Tareas

Tarea 1: Escane explora de red básica

Paso 1: Abra un terminal en su máquina Kali Linux. Paso 2: Ejecute un escaneo básico en su red local. Reemplaza 192.168.1.0/24 con el rango IP de su red.

nmap 192.168.1.0/24

Salida esperada: Una lista de dispositivos en su red, sus direcciones IP y los puertos abiertos.

Tarea 2: Escaneo de puertos específicos

Paso 1: Para escanear puertos específicos (por ejemplo, HTTP port 80), utilice la opción -p:

nmap -p 80 192.168.1.0/24

Salida esperada: Una lista de dispositivos con puerto 80 abierto.

Tarea 3: Detección de versión de servicio

Paso 1: Utilce la opción -sV para detectar la versión de los servicios que se ejecutan en puertos abiertos:

nmap -sV 192.168.1.0/24

Salida esperada: Una lista detallada de los puertos abiertos y los servicios que se ejecutan en ellos, incluyendo información de versión.

Tarea 4: Detección del sistema operativo

Paso 1: Utiliera la opción -O para detectar los sistemas operativos de los dispositivos en la red:

sudo nmap -O 192.168.1.0/24

Salida esperada: Los detalles del sistema operativo de los dispositivos de la red.

Tarea 5: Escanes agresivo

Paso 1: Realizar un escaneo agresivo usando la opción -A, que incluye detección de sistemas operativos, detección de versiones, escaneo de script y trazar ruta:

sudo nmap -A 192.168.1.0/24

Salida esperada: Información completa sobre los dispositivos de la red, incluyendo puertos abiertos, servicios, versiones, sistemas operativos y detalles de trazar rutas.

Recursos adicionales

Documentación oficial de la mapa Hoja de trampe de Nmap Curso de Nmap en línea sobre Udemy

Este proyecto le dará una base sólida en el uso de Nmap para el escaneo de red y la enumeración, habilidades esenciales para cualquier hacker ético.