EJERCICIOS ESCÁNER DE RED NMAP

Prerrequisitos

Kali Linux

Metasploitable2

Creación del laboratorio

Descarga la imagen de máquina virtual de Metasploitable2:

https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

Sigue esta guía de instalación para crear la máquina virtual Metasploitable2:

https://www.hacking-tutorial.com/tips-and-trick/install-metasploitable-on-virtual-box/

Utiliza la siguiente configuración para las máquinas virtuales Metasploitable2 y Kali Linux:

Configuración > Red > Adaptador 1 > Red NAT > NatNetwork > Aceptar

Enciende las máquinas virtuales, Metasploitable2 y Kali Linux, y comprueba:

Dirección IP de Kali Linux

Dirección IP de Metasploitable2

Haz ping para comprobar la conectividad entre ellas

En caso de obtener resultado negativo, revisa todos los pasos comenzando de nuevo desde el principio. En caso de obtener resultado positivo, realiza los siguientes ejercicios

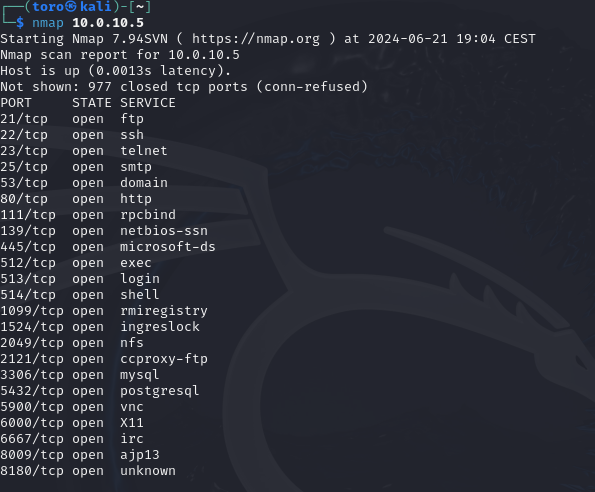
Ejercicio 1 - Nmap

Descubre los equipos conectados a la Red NAT 10.0.2.X-255 o 10.0.2.X/24

Comprueba que la IP de la máquina Metasploitable2 aparece

Ejercicio 2 - Nmap

Escanea los puertos de la máquina Metasploitable2



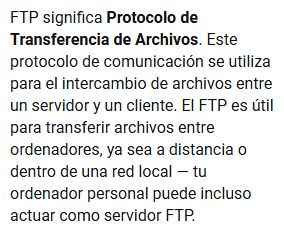
Ejercicio 3 - Nmap

Realiza un esquema de la siguiente forma:

PUERTO - ESTADO - SERVICIO - QUE HACE ESTE SERVICIO para todos los puertos del equipo

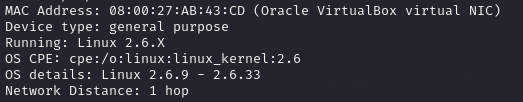
Busca información de los puertos y servicios según el resultado de Nmap en Google

Pd: por cuestión de tiempo no ha sido posible hacer todas las busquedas en google, asi que pongo la primera y las siguiente iran con el mismo metodo!



Ejercicio 4 - Nmap

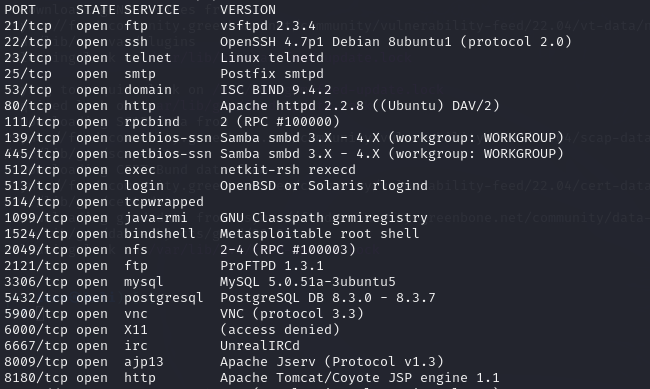
¿Qué versión de sistema operativo utiliza?



Ejercicio 5 - Nmap

Completa el esquema del ejercicio 3 con la versión de los servicios desplegados.

PUERTO - ESTADO - SERVICIO - VERSION DEL SERVICIO



Ejercicio 6 - Nmap, Http, Netcat y Telnet

Comprueba manualmente la versión de dos de los servicios levantados utilizando nc, telnet y navegador web



