**EJERCICIOS NMAP**

**Prerrequisitos**

**Descargar la imagen de máquina virtual Metasploitable2:**

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

**Seguir la guía de instalación de Metasploitable2:**

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

**En VirtualBox, entrar en "Configuración-Red" de Metasploitable2 y asignarle una red NAT**

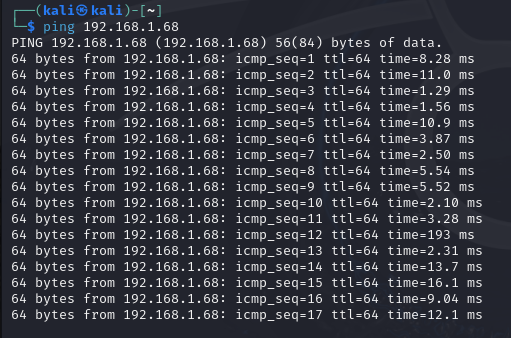
**Entrar en las máquinas virtuales y comprobar:**

**Dirección IP de Kali Linux**

**Dirección IP de Metasploitable2**

**Credenciales: msfadmin/msfadmin**

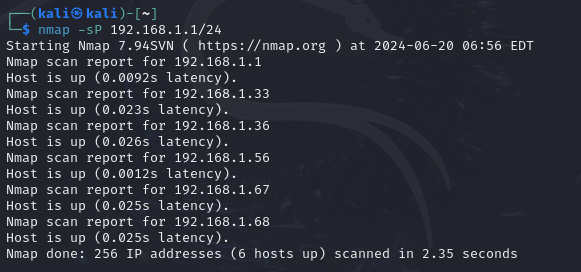
**Hacer un ping para comprobar la conectividad entre ellas**

****

**Ejercicio 1**

**Descubre los equipos conectados a la red NAT 10.0.2.X/255.255.255.0 o /24**

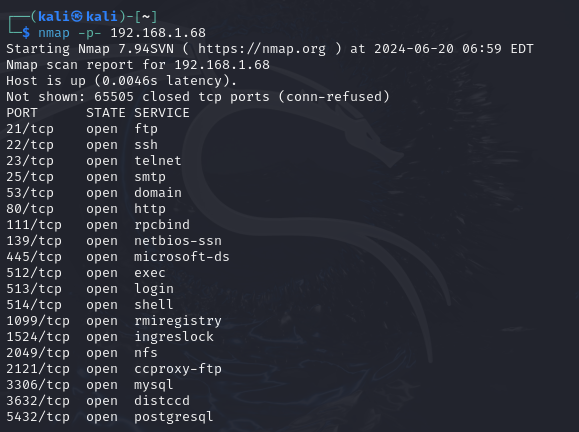
**Comprobar que la IP de la máquina Metasploitable2 aparece**

****

El IP de Mestasploitable2 es 192.168.1.68

**Ejercicio 2**

**Escanear los puertos de la máquina Metasploitable2**



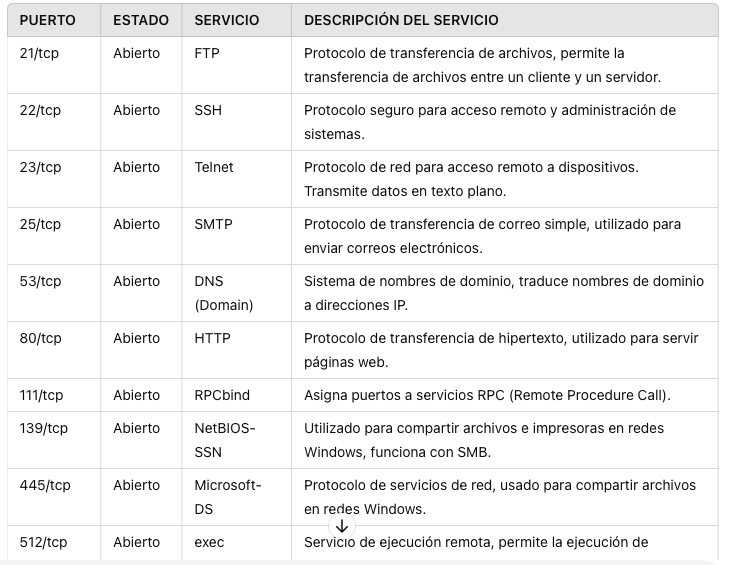
**Ejercicio 3**

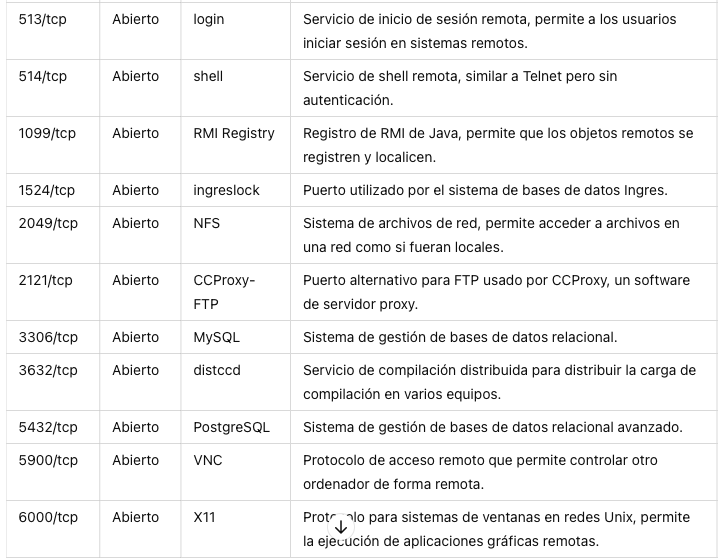
**Realizar un esquema de la siguiente forma:**

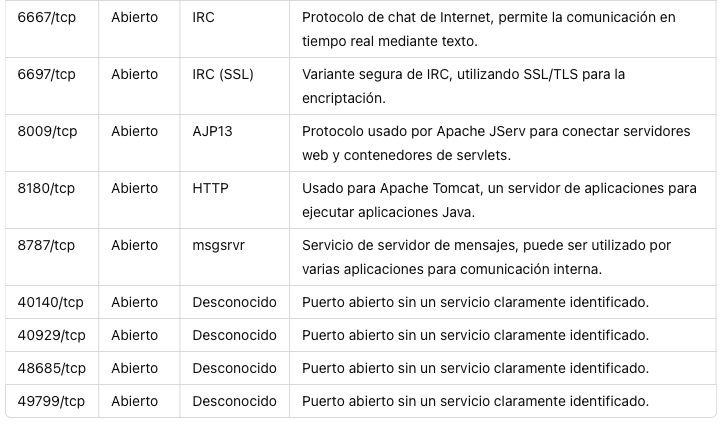
**PUERTO - ESTADO - SERVICIO - QUE HACE ESTE SERVICIO para todos los puertos del equipo**

**Buscar información de los puertos y servicios según el resultado de Nmap en Google.**

**NOTA: El objetivo es entender qué servicios están levantados en la máquina y para qué sirven.**







**Ejercicio 4**

**¿Qué versión de SO utiliza?**

****

****

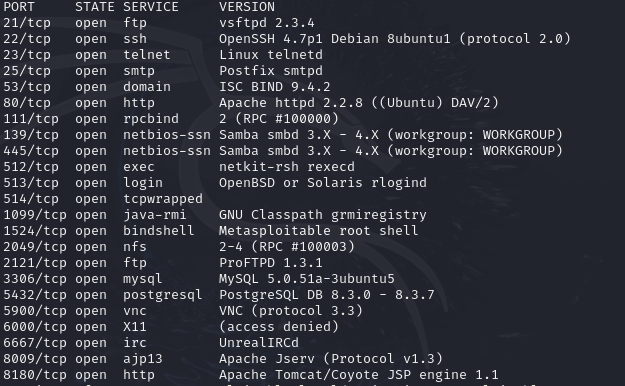
Linux 2.6.9 -2.6.33

**Ejercicio 5**

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

**PUERTO - ESTADO - SERVICIO - VERSION DEL SERVICIO**

****



**Ejercicio 6**

**Comprueba manualmente la versión de dos de los servicios levantados utilizando nc, telnet o navegador web.**

**NOTA: Se puede establecer una conexión con el puerto del servicio de manera manual, utilizando diferentes herramientas como netcat o telnet**

**(independientemente del cliente) o con clientes propios (navegador web, cliente ssh). De esta manera contrastamos de manera manual las hay versiones**

**detectadas por Nmap.**

****

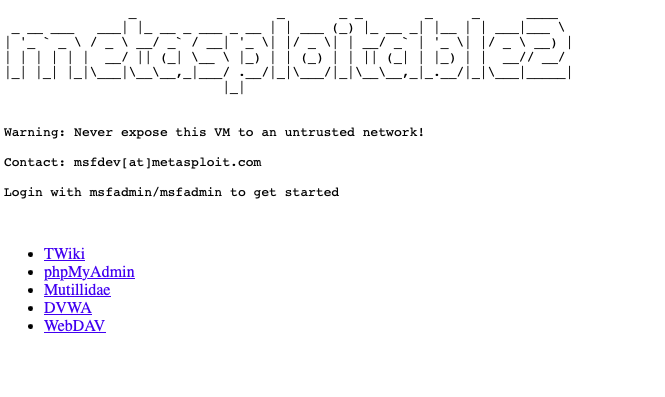
(puerto 21): Pude obtener la versión del servicio (vsFTPd 2.3.4) sin necesidad de autenticación adicional, lo cual es común en muchos servidores FTP que muestran la información de versión al conectar.

Al intentar entrar con nc desde la terminal al puerto 80 del IP de metasploit me da la siguiente respuesta:

****

Esta respuesta indica que el servidor HTTP en el puerto 80 está solicitando credenciales de inicio de sesión (USER Y PASS) para poder interactuar más profundamente con el servidor.

Si lo intento buscando la ip en internet:



Al buscarlo en internet me da el user y la contraseña: msfadmin

**Ejercicio 7**

**Utiliza un script NSE para extraer más información de un servicio en concreto.**

