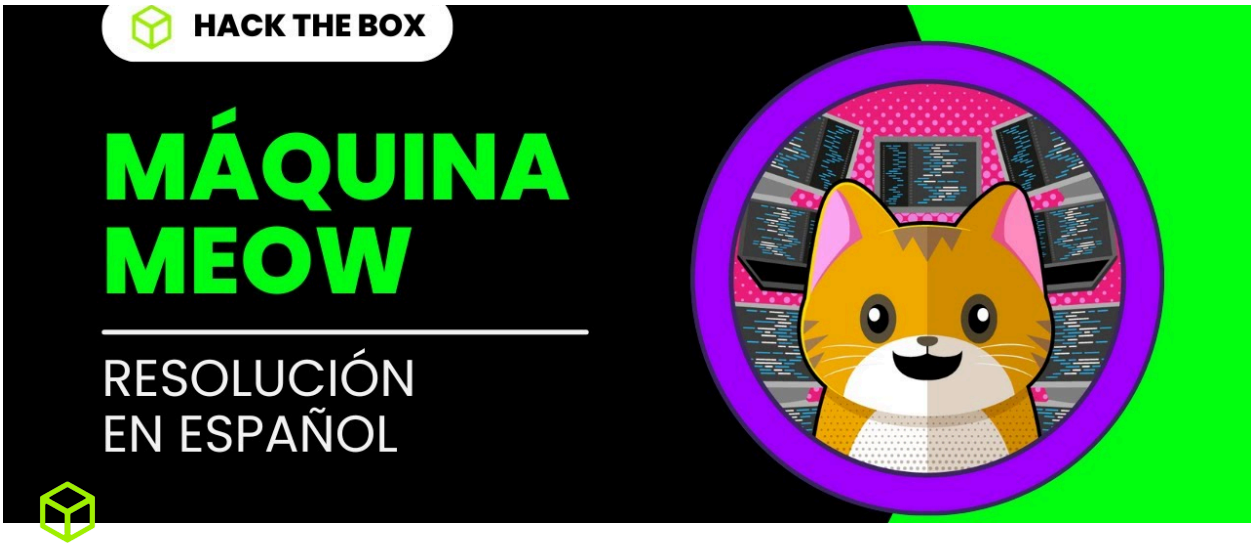


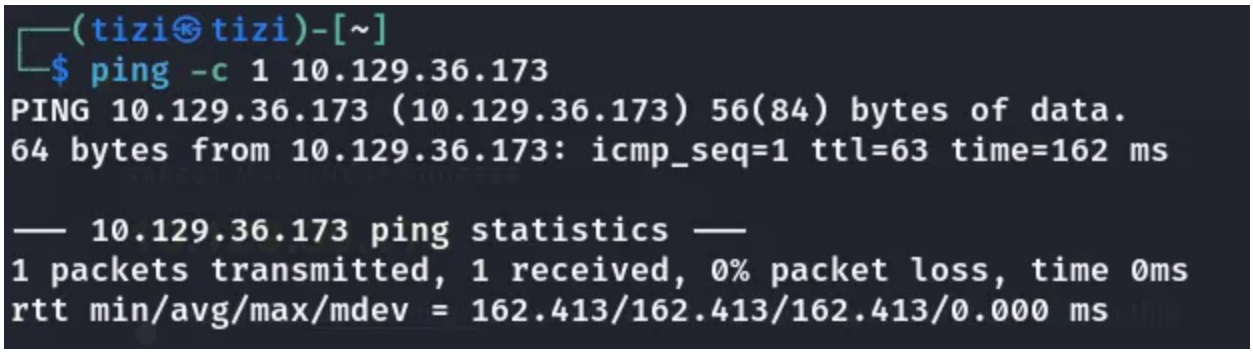
Hack the Box — Máquina Meow

Máquina Meow

- **Perfil**: Red Team - Pentesting
- **Sección**: Starting Point
- **Dificultad**: Muy fácil

Comenzaremos con lo básico: prender el equipo víctima, para ello tocamos el botón de “Spawn Machine” y esperaremos unos segundos hasta que esté prendida.

Una vez culminado el proceso, se nos desvelará la **dirección IP** de la máquina a la cual debemos vulnerar. Para corroborar que tenemos conexión con ella, le realizamos un **ping**, el cual es el envío de un paquete de datos y así podremos observar si llegó y fue respondido.



Los parámetros que hemos colocado nos permiten agilizar el proceso al enviar tan solo un paquete, el cual fue recibido con éxito. De esta manera, confirmamos que tenemos conexión con el equipo a atacar.

A continuación, vamos a responder las preguntas básicas de las cuales no es necesario hacer el proceso de penetración.

Task 1:

> What does the acronym VM stand for? (¿Qué significa el acrónimo VM?)
>
> ***Virtual Machine*** *(máquina virtual)*

Como ya sabemos, requerimos de una máquina virtual para hacer todo este proceso con OpenVPN. **Virtual Machine** traducido a español significa Máquina Virtual.

Task 2:

> What tool do we use to interact with the operating system in order to issue commands via the command line, such as the one to start our VPN connection? It’s also known as a console or shell.
>
> ***Terminal*** *(terminal)*

La **terminal** es el lugar donde el usuario puede interactuar con el sistema operativo e introducir los comandos referidos a lo que la persona desea ejecutar. Todos los sistemas operativos cuentan con una y Linux no es la excepción.

Task 3:

> What service do we use to form our VPN connection into HTB labs?
>
> ***OpenVPN***

OpenVPN es una servicio de código abierto utilizado por Hack the Box para establecer una conexión con cifrado extremo a extremo y de forma segura, para que así actores maliciosos no interfieran en el proceso.

Task 4:

> What tool do we use to test our connection to the target with an ICMP echo request?
>
> ***Ping***

Como mencionamos, con el comando **ping** podemos mandar un paquete con información hacia cualquier dirección para así ver si lo está recibiendo con éxito.

Task 5:

> What is the name of the most common tool for finding open ports on a target?
>
> ***Nmap***

Nmap es una herramienta de código abierto con una alta popularidad en el hacking diseñada para el escaneo de puertos, pudiendo detectar qué servicios

están corriendo en dichos puertos, así como también visualizar si están abiertos, cerrados o filtrados. Es una parte obligatoria del proceso de penetración.

Vamos a realizar un **escaneo nmap** hacia la máquina víctima para descubrir qué servicios están en funcionamiento.

```
┌──(tizi㉿tizi)-[~/Downloads]
└─$ nmap -sV -T4 10.129.57.27
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-30 14:31 -03
```

Si ya tenemos Kali Linux o la versión security de Parrot, esta herramienta debe estar instalada.

Utilizamos **nmap** para ejecutar el comando y le sumamos también el parámetro **-sV -T4** para visualizar la versión de los servicios en los puertos y agilizar el escaneo respectivamente. Al costado irá la **dirección IP** a escanear.

```
┌──(tizi㉿tizi)-[~/Downloads]
└─$ nmap -sV -T4 10.129.57.27
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-30 14:31 -03
Nmap scan report for 10.129.57.27
Host is up (0.23s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
23/tcp open  telnet  Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

El escaneo arrojó que el **puerto 23** está abierto, en el que corre el servicio de **Telnet**.

Task 6:

> What service do we identify on port 23/tcp during our scans?
>
> ***Telnet***

Telnet (*TErminaL NETwork*) es un tipo de protocolo que permite la conexión con otro equipo a través de una interfaz creando sesiones remotas. Hay que tener en

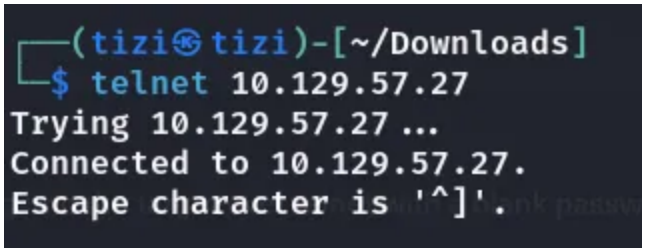
cuenta que **este protocolo es extremadamente vulnerable e inseguro**, pues no cuenta con ningún tipo de encriptación.

Task 7:

> What username is able to log into the target over telnet with a blank password?
>
> *Root*

Root es el usuario con máximos privilegios en cualquier sistema basado en Unix.

Vamos a proceder con la vulneración, entrando hacia el servicio Telnet de la máquina víctima.



Una vez ingresado el comando, esperamos unos segundos y se nos pedirá que ingresemos un usuario y contraseña. El usuario es **root** y la contraseña la **dejamos en blanco** pues justamente queremos ingresar con ese usuario, el cual en este caso no requiere de una credencial. Tras ello, estaremos dentro para ejecutar comandos y ver que se aloja en el equipo.

Una vez dentro, listamos el contenido con el comando **ls** y observaremos un archivo de nombre **flag.txt**. Este nombre, siempre y en todo momento que nos encontremos en la plataforma, hará alusión a que allí se aloja la contraseña que debemos colocar en el sitio web para validar que hemos completado exitosamente el trabajo.

Ese archivo podemos leerlo con el comando **cat** y se nos mostrará por pantalla la **flag**, que es una combinación extensa de números y letras.

Una vez copiada y pegada la flag en HTB, habremos completado con éxito esta máquina.

Por ser la primera, resultará realmente sencilla, pero este es el primer paso de un camino extenso donde cada vez aumentará el nivel de dificultad.

RESOLUCIÓN EN VIDEO:

https://www.youtube.com/watch?v=Eg5NvTQm-Ic&t=46s