FACULTAD DE INGENIERÍA

TALLER 1.1

CIBERSEGURIDAD

JOHAN SEBASTIAN GIRALDO HURTADO

LUISA FERNANDA PULIDO OROZCO

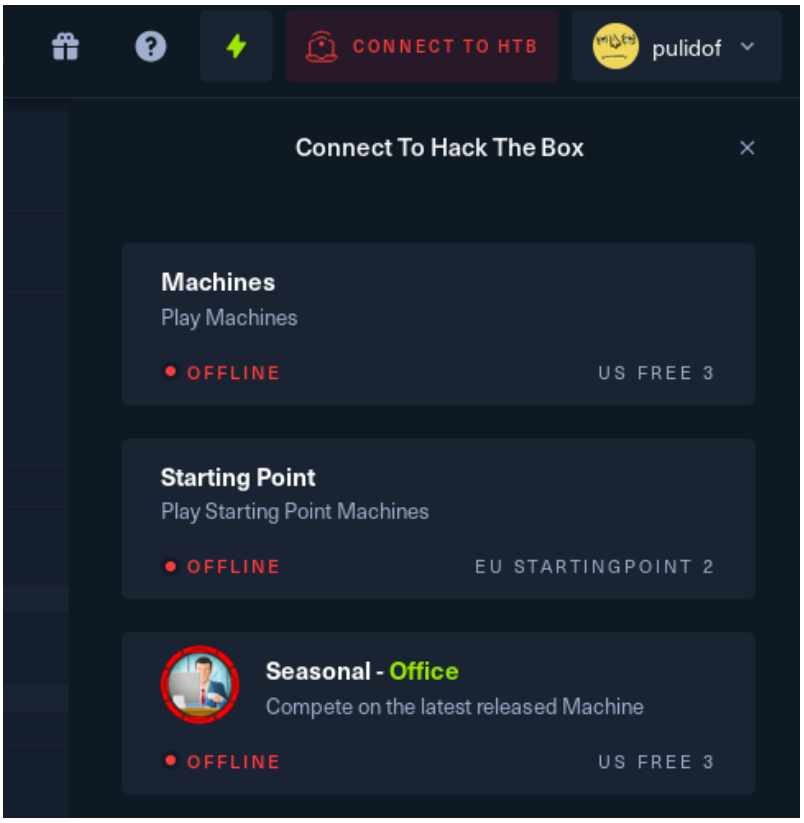
INGENIERÍA DE SOFTWARE

INFORME MAQUINAS HACK THE BOX

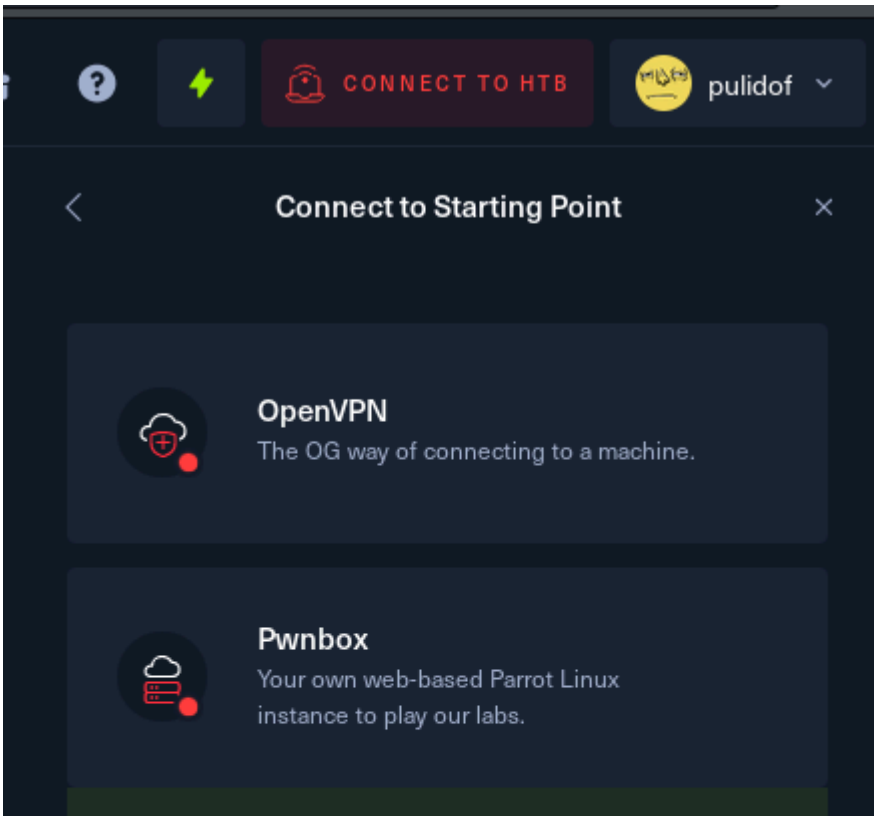
- Para poder hacer uso de las herramientas proporcionadas por hack the box y conectarnos a su vpn para las máquinas de prueba requerimos instalar **openvpn**

```
┌──(kali㉿kali)-[~/Downloads/tor-browser]
└─$ sudo apt-get install openvpn
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
openvpn is already the newest version (2.6.7-1).
openvpn set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 1190 not upgraded.
```

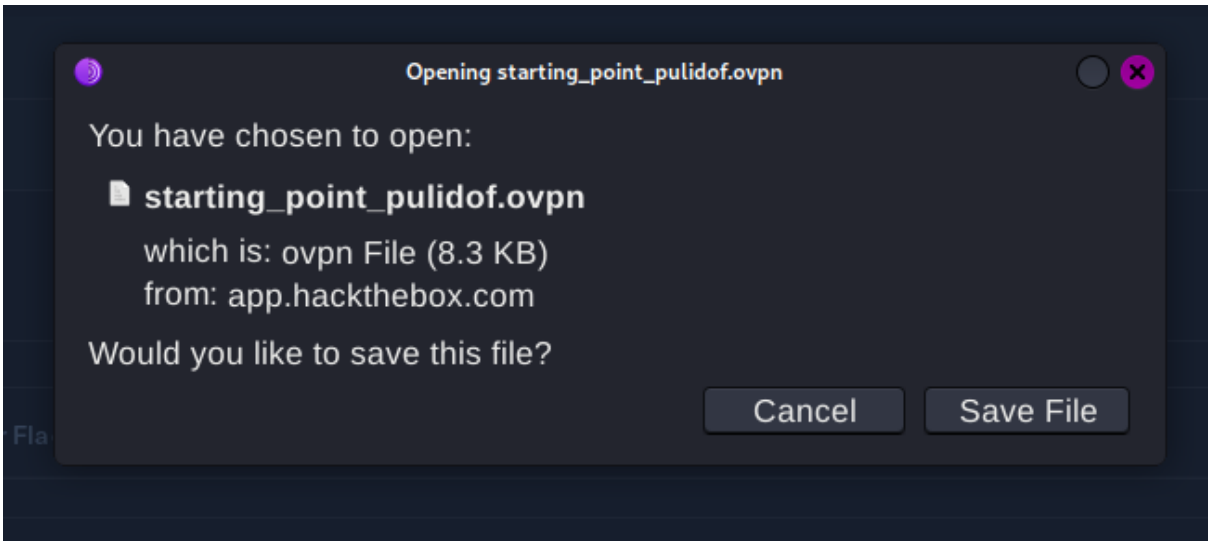
- Una vez accedemos a nuestra cuenta de hack the box, al lado izquierdo de nuestro nombre de usuario y foto de perfil, encontraremos el botón "**CONNECT TO HTB**", cuando demos click en él, se desplegará un menú donde elegiremos la opción "Starting Point".



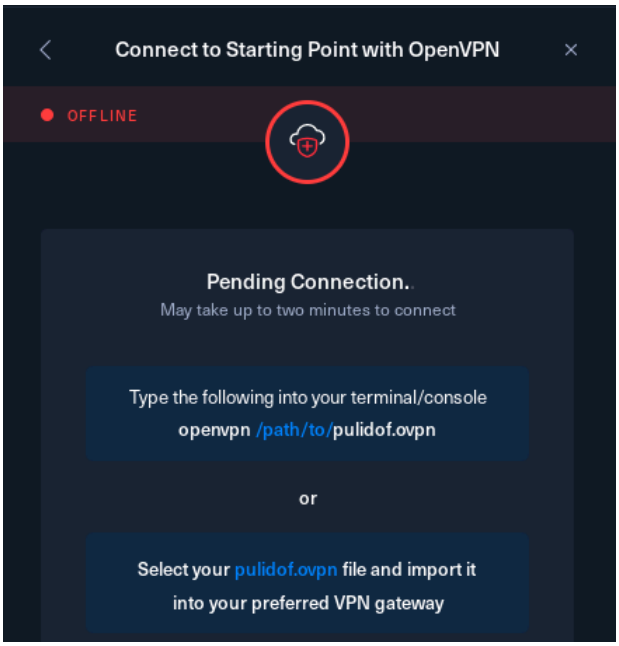
- Después de lo anterior realizado, nos mostrará el siguiente menú, donde seleccionaremos la opción de “**OpenVPN**”



- Se inicializará la descarga del siguiente archivo en nuestro dispositivo que debemos usar para nuestra conexión al vpn



- En el primer instante podemos observar el estado actual de nuestra conexión al vpn y es correcto porque aún no iniciamos el proceso de conexión.

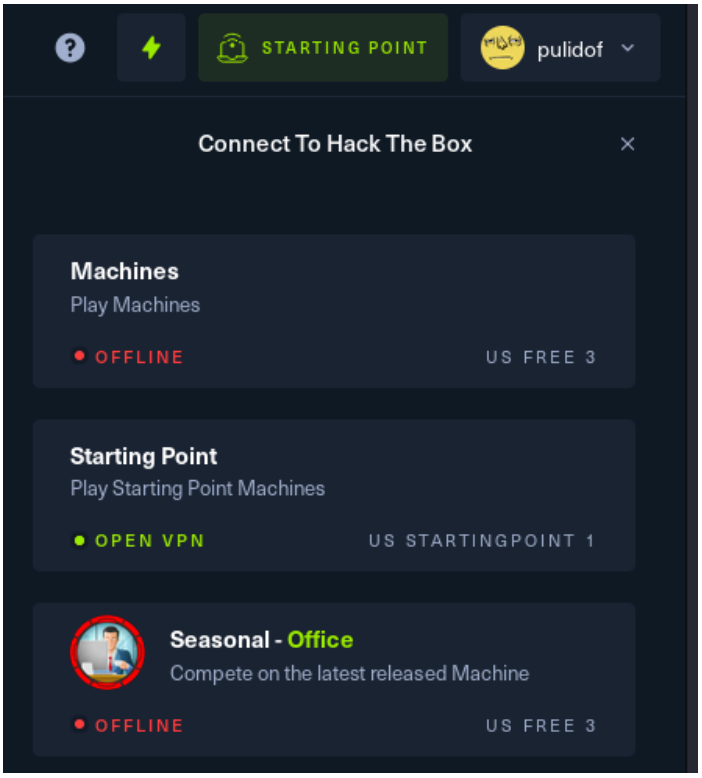


- Nos dirigimos a una terminal a la dirección del archivo que descargamos hace un momento y con el comando de openvpn inicializamos la conexión al vpn

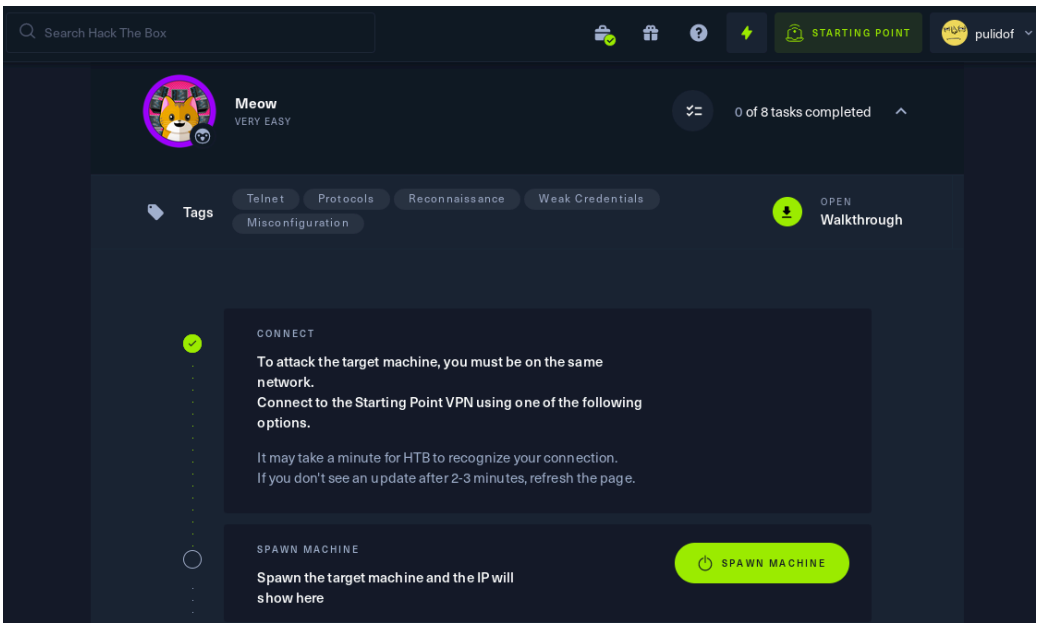
```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls
starting_point_pulidof.ovpn

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo openvpn starting_point_pulidof.ovpn
```

```
2024-02-21 20:43:55 net_route_v6_best_gw result: via fe80::c289:abff:fee8:237
a dev eth0
2024-02-21 20:43:55 ROUTE6_GATEWAY fe80::c289:abff:fee8:237a IFACE=eth0
2024-02-21 20:43:55 TUN/TAP device tun0 opened
2024-02-21 20:43:55 net_iface_mtu_set: mtu 1500 for tun0
2024-02-21 20:43:55 net_iface_up: set tun0 up
2024-02-21 20:43:55 net_addr_v4_add: 10.10.14.48/23 dev tun0
2024-02-21 20:43:55 net_iface_mtu_set: mtu 1500 for tun0
2024-02-21 20:43:55 net_iface_up: set tun0 up
2024-02-21 20:43:55 net_addr_v6_add: dead:beef:2::102e/64 dev tun0
2024-02-21 20:43:55 net_route_v4_add: 10.10.10.0/23 via 10.10.14.1 dev [NULL]
 table 0 metric -1
2024-02-21 20:43:55 net_route_v4_add: 10.129.0.0/16 via 10.10.14.1 dev [NULL]
 table 0 metric -1
2024-02-21 20:43:55 add_route_ipv6(dead:beef::/64 → dead:beef:2::1 metric -1
) dev tun0
2024-02-21 20:43:55 net_route_v6_add: dead:beef::/64 via :: dev tun0 table 0
metric -1
2024-02-21 20:43:55 Initialization Sequence Completed
2024-02-21 20:43:55 Data Channel: cipher 'AES-256-CBC', auth 'SHA256', peer-i
d: 52, compression: 'lzo'
2024-02-21 20:43:55 Timers: ping 10, ping-restart 120
2024-02-21 20:43:55 Protocol options: explicit-exit-notify 1, protocol-flags
cc-exit tls-ekm dyn-tls-crypt
```

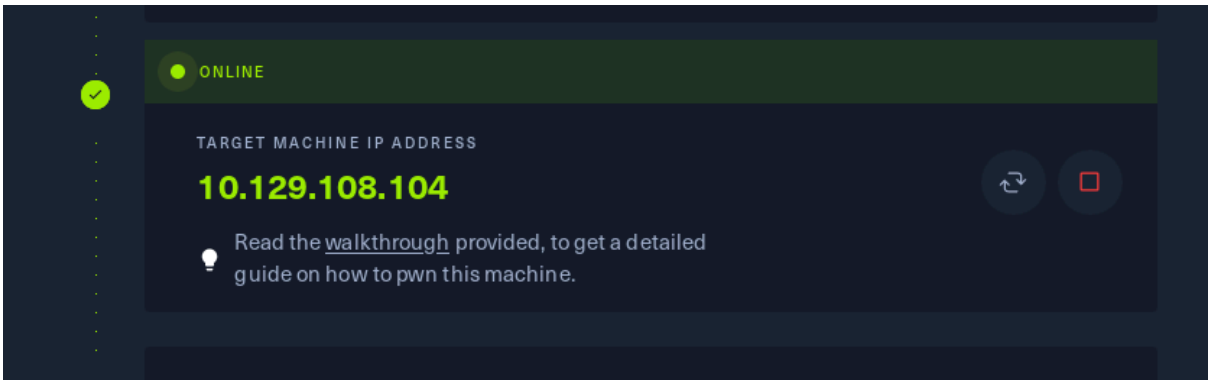
- Después de haber realizado de manera correcta los pasos anteriores ya tendremos una conexión a la vpn para conectarnos seguidamente a las máquinas virtuales de práctica de HTB.



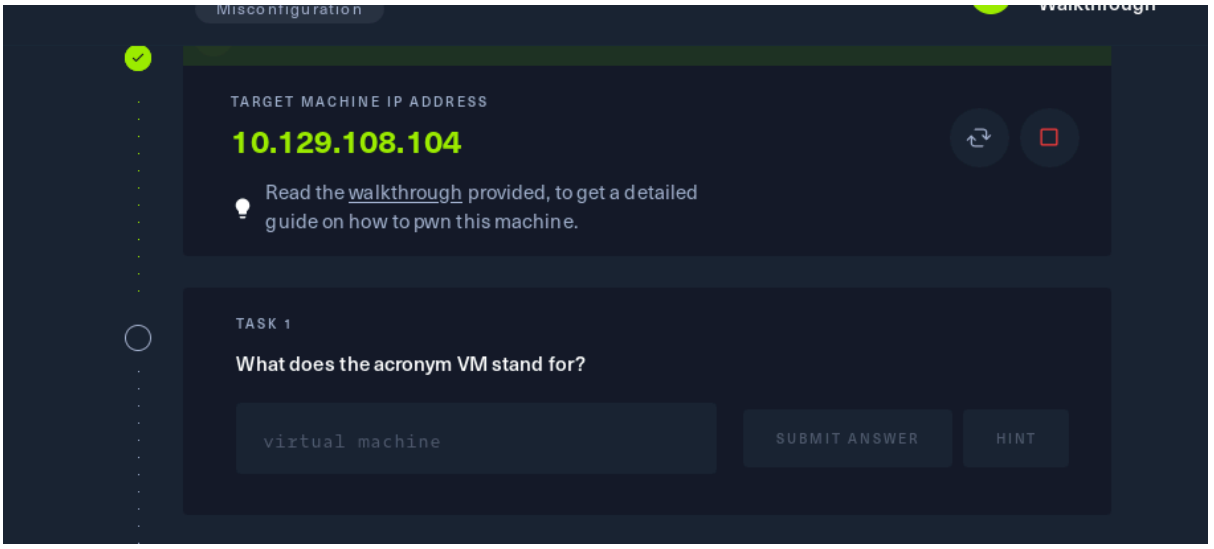
- Elegimos la máquina a la que vamos a iniciar el ataque, en esta ocasión como tenemos el VPN Starter point, es la MV que vamos a usar

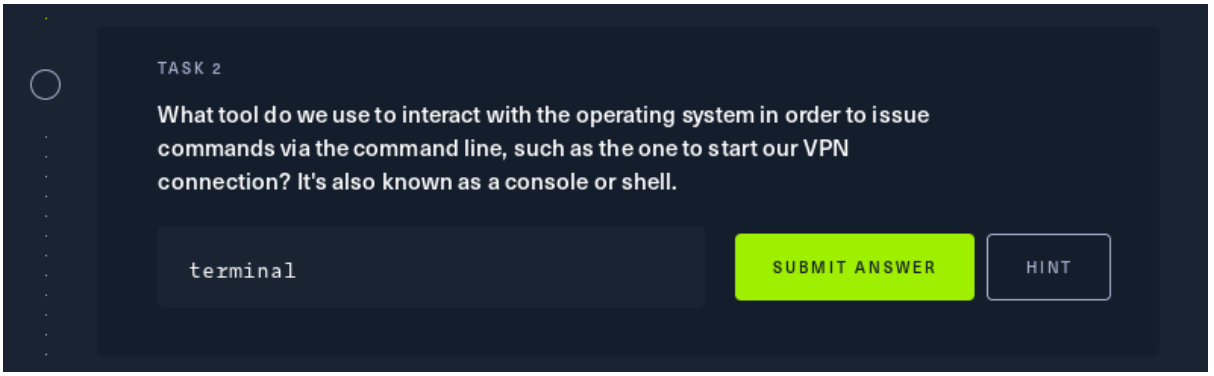


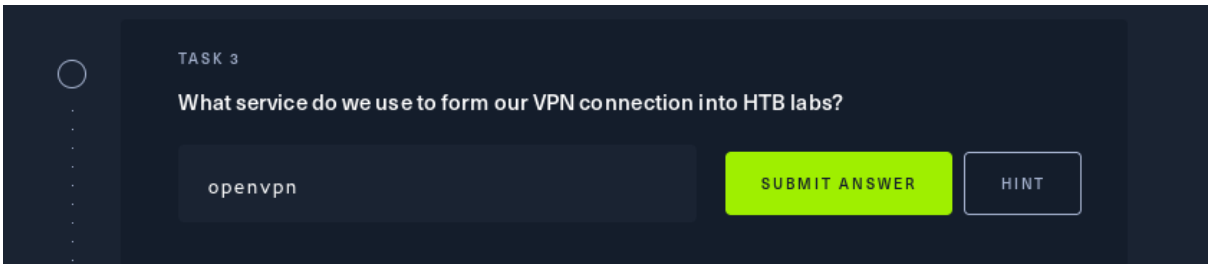
- Spawneamos la maquina y podremos ver los datos de está para poder realizar diferentes acciones sobre ella.



- Tendremos una serie de preguntas por resolver para ir descubriendo cosas de la maquina







TASK 4

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

ping

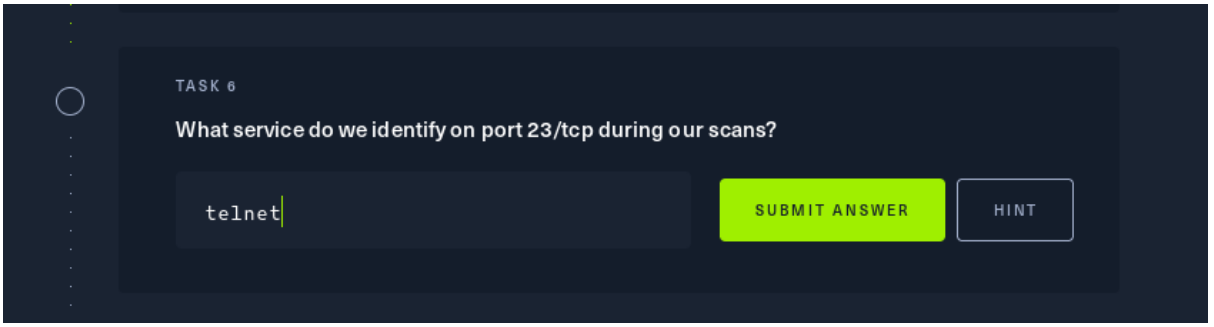
SUBMIT ANSWER HINT

- Hacemos ping a la maquina para saber si puede recibir paquetes

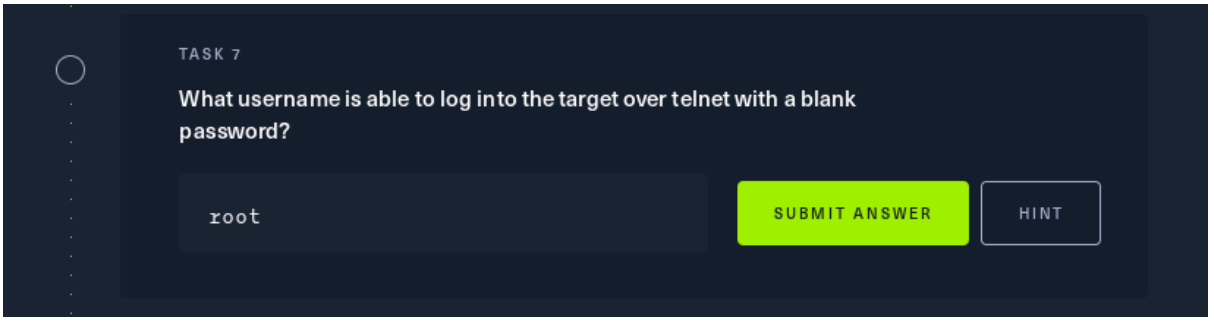
```
┌──(kali㉿kali)-[~]
└─$ ping 10.129.108.104
PING 10.129.108.104 (10.129.108.104) 56(84) bytes of data.
64 bytes from 10.129.108.104: icmp_seq=1 ttl=63 time=180 ms
64 bytes from 10.129.108.104: icmp_seq=2 ttl=63 time=138 ms
64 bytes from 10.129.108.104: icmp_seq=3 ttl=63 time=161 ms
64 bytes from 10.129.108.104: icmp_seq=4 ttl=63 time=184 ms
64 bytes from 10.129.108.104: icmp_seq=5 ttl=63 time=114 ms
64 bytes from 10.129.108.104: icmp_seq=6 ttl=63 time=231 ms
64 bytes from 10.129.108.104: icmp_seq=7 ttl=63 time=1562 ms
64 bytes from 10.129.108.104: icmp_seq=8 ttl=63 time=530 ms
64 bytes from 10.129.108.104: icmp_seq=9 ttl=63 time=109 ms
64 bytes from 10.129.108.104: icmp_seq=10 ttl=63 time=186 ms
64 bytes from 10.129.108.104: icmp_seq=11 ttl=63 time=1446 ms
64 bytes from 10.129.108.104: icmp_seq=12 ttl=63 time=419 ms
64 bytes from 10.129.108.104: icmp_seq=13 ttl=63 time=112 ms
^C
--- 10.129.108.104 ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 12071ms
rtt min/avg/max/mdev = 108.716/413.138/1561.757/480.651 ms, pipe 2
```

- Podemos fijarnos que despues de usar la herramienta nmap el puerto 23 pertenece el tcp con servicio telnet

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 10.129.108.104
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-27 17:24 EST
Nmap scan report for 10.129.108.104
Host is up (0.12s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
23/tcp open  telnet

Nmap done: 1 IP address (1 host up) scanned in 2.57 seconds
```



- Respondemos la pregunta pero debemos tener un acceso para acceder a la bandera y dejar marcada como hecha la maquina



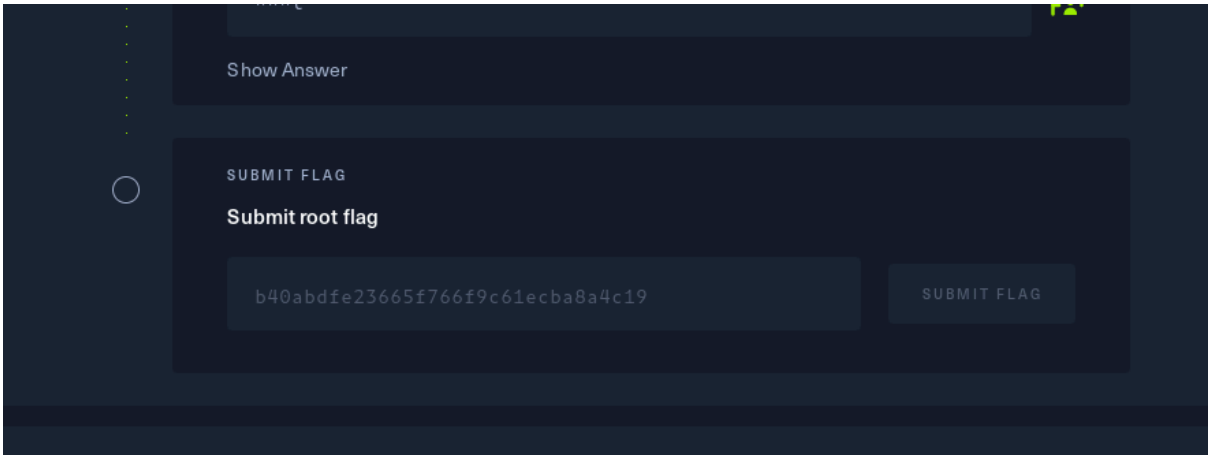
- Nos conectamos al servicio telnet para obtener la bandera

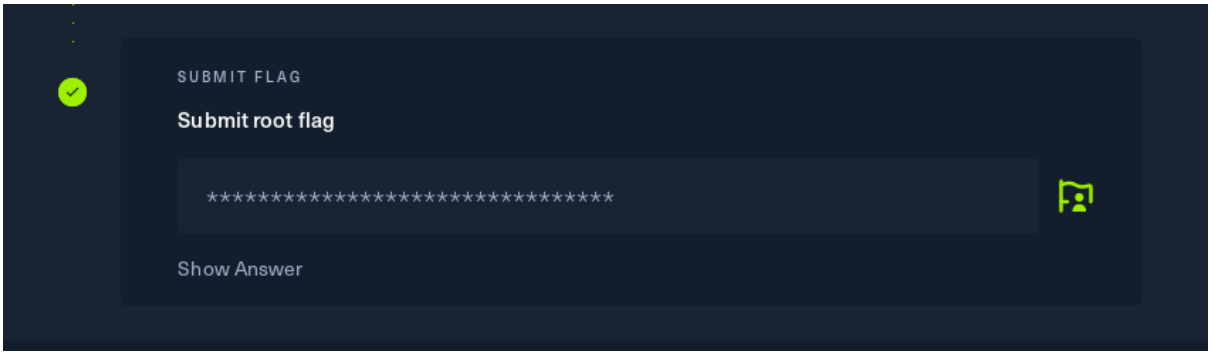
```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ telnet 10.129.108.104
Trying 10.129.108.104 ...
Connected to 10.129.108.104.
Escape character is '^]'.

Hack the Box

Meow login: root
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-77-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue 27 Feb 2024 10:31:05 PM UTC

  System load:           0.11
  Usage of /:            41.7% of 7.75GB
  Memory usage:          4%
  Swap usage:            0%
  Processes:             135
  Users logged in:       0
  IPv4 address for eth0: 10.129.108.104
  IPv6 address for eth0: dead:beef::250:56ff:feb0:8861

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

75 updates can be applied immediately.
```

- Cuando ya entremos a la maquina podremos hacer un ls para obtener la bandera y pegarla en HTB

```
The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon Sep  6 15:15:23 UTC 2021 from 10.10.14.18 on pts/0
root@Meow:~# ls
flag.txt  snap
root@Meow:~# cat flag.txt
b40abdfe23665f766f9c61ecba8a4c19
root@Meow:~#
```

- Asi terminamos la maquina de Meow


Show Answer
SUBMIT FLAG
Submit root flag
b40abdfe23665f766f9c61ecba8a4c19
SUBMIT FLAG


SUBMIT FLAG
Submit root flag
****
Show Answer