FACULTAD DE INGENIERÍA

TALLER 1

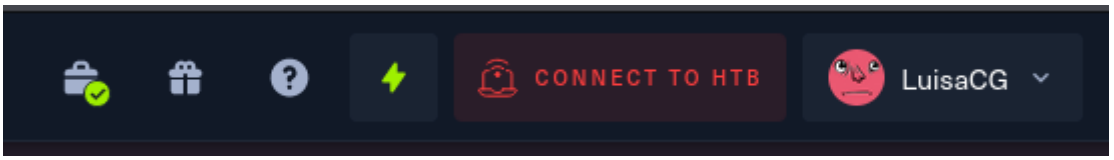
LUISA FERNANDA CELIS GONZÁLEZ

INGENIERÍA DE SOFTWARE

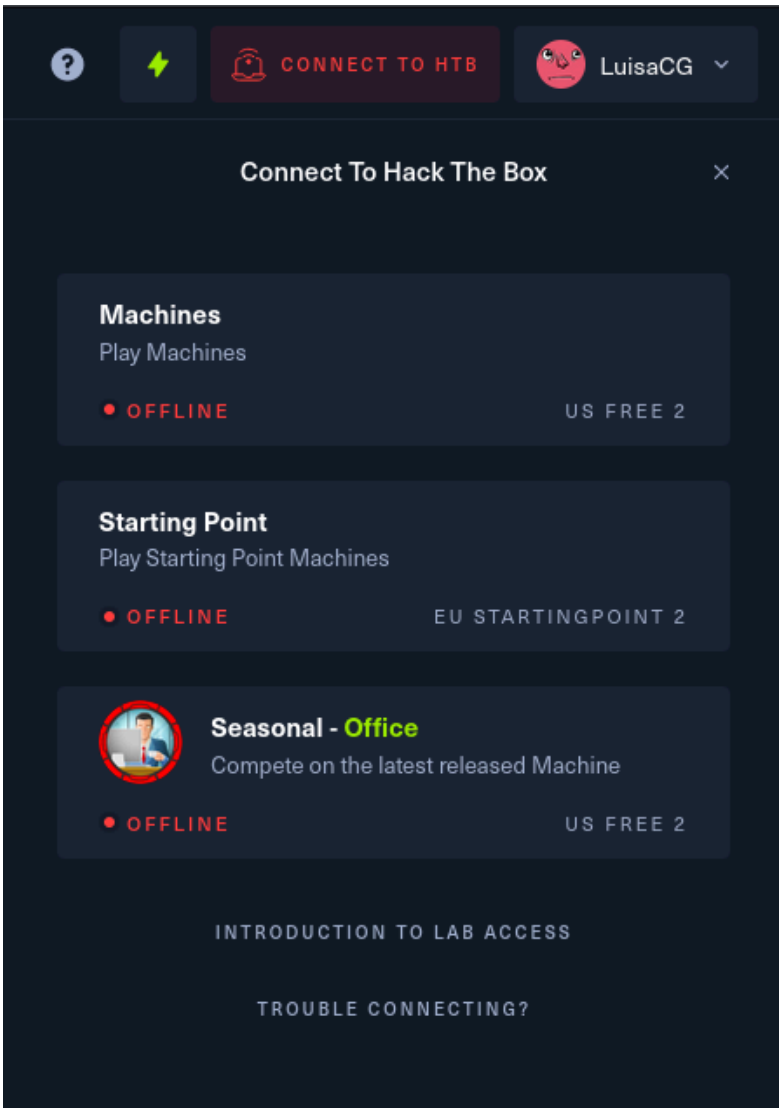
2024

Conexión a la VPN de Hack The Box

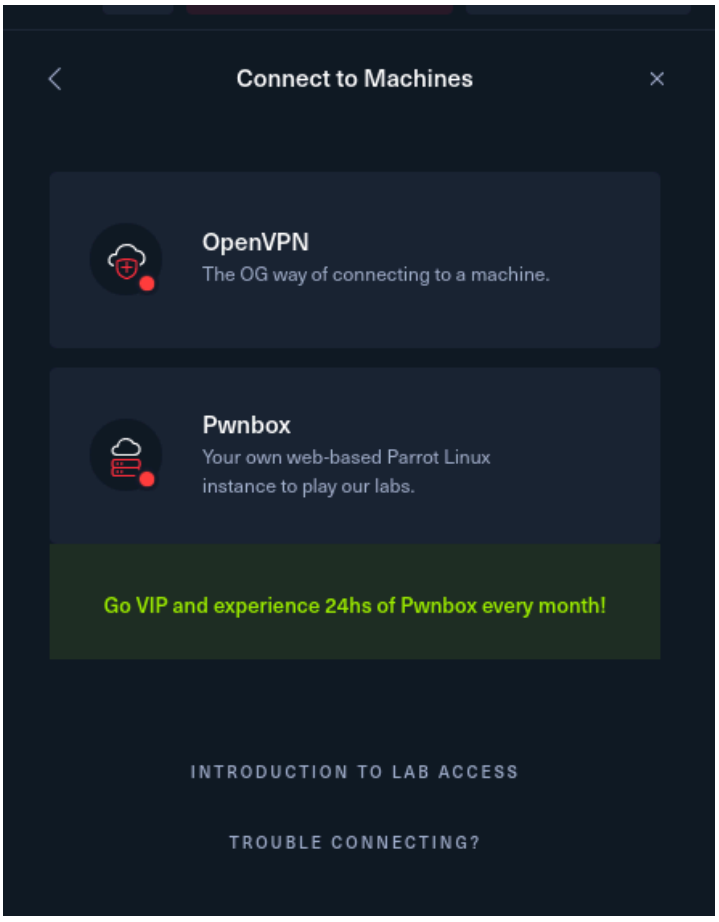
1. Para conectarnos a la VPN de Hack The Box, lo primero que debemos hacer es dirigirnos a la parte superior derecha del navbar y dar clic en la opción “CONNECT TO HTB”



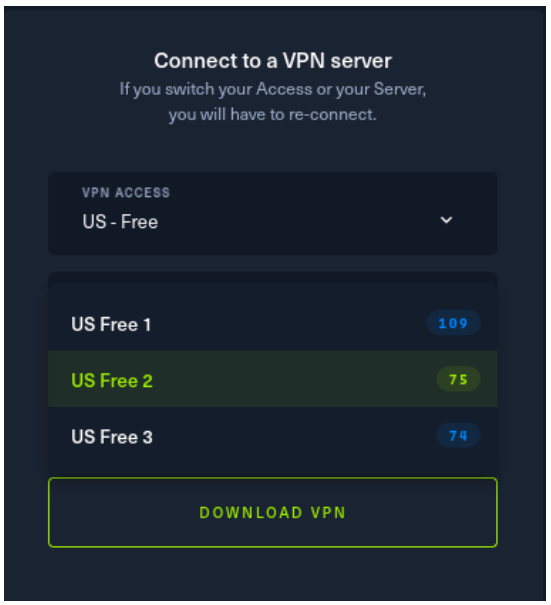
2. Seleccionamos el tipo de vpn a la que nos deseamos conectar o según las necesidad que tengamos.



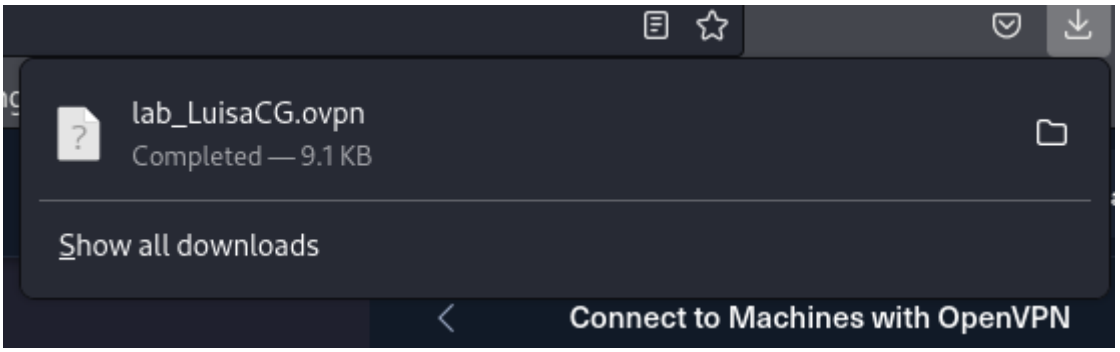
3. Después de elegir el tipo de vpn que deseamos vamos a dar clic en la opción de “OpenVPN”



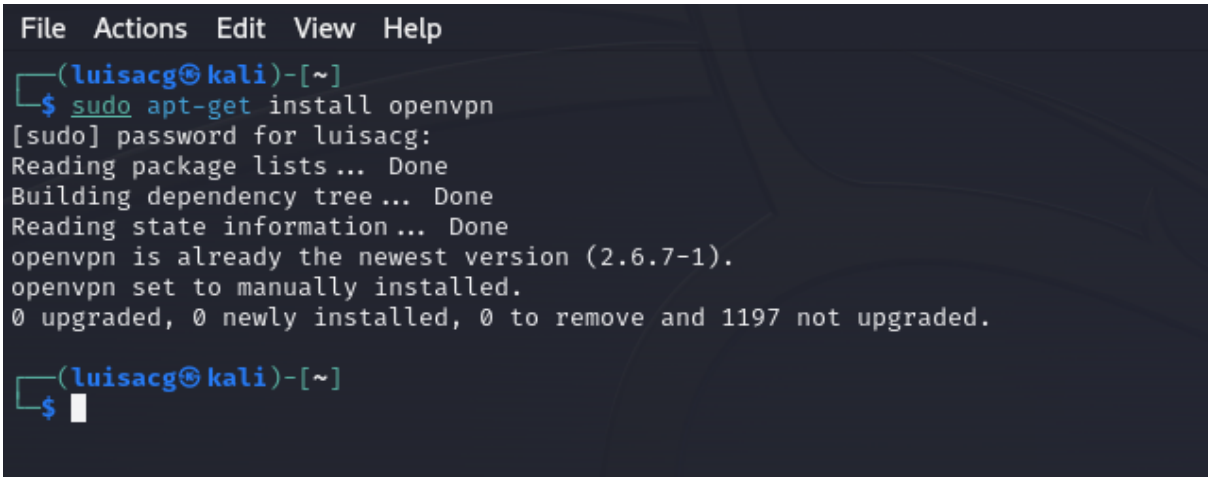
4. Realizamos la configuración básica y esencial de la vpn, es decir, seleccionamos el servidor al que nos deseamos conectar, preferiblemente, el que se encuentre más cerca a nuestra ubicación para lograr una mejor conexión.



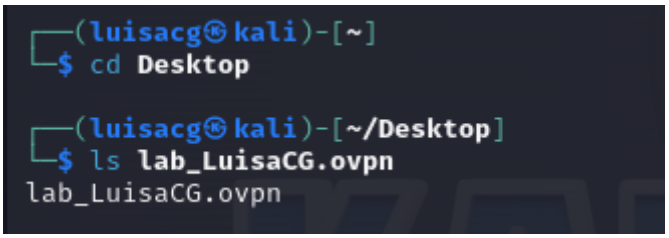
5. Después de elegir el servidor damos clic en descargar y esperamos unos segundos a que descargue nuestra vpn.



6. Ahora, para poder conectarnos a la vpn debemos abrir nuestra terminal de kali linux y realizar la siguiente instalación.



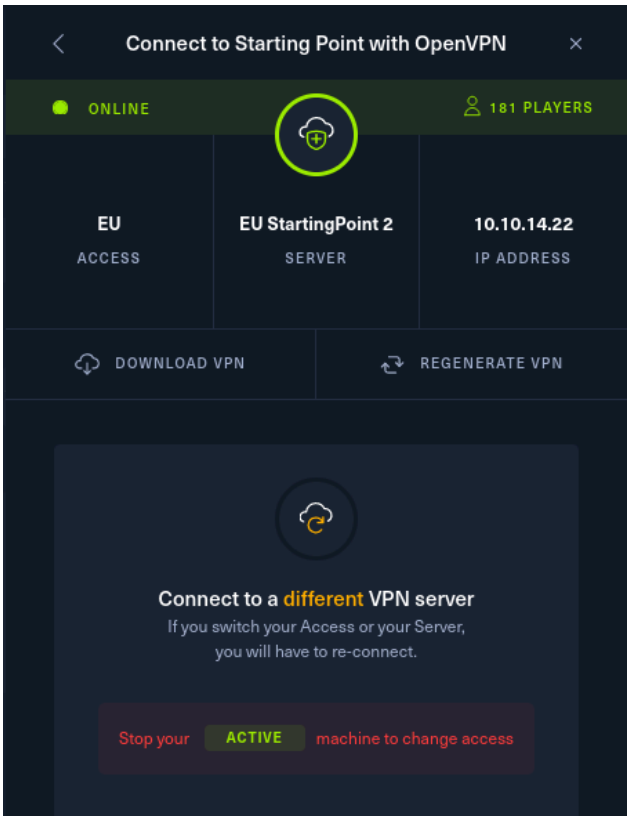
7. Después de que se haya instalado nos vamos a dirigir al directorio donde guardamos nuestra vpn.



8. Para poder conectarnos a la vpn vamos a hacer uso de la instalación que realizamos en el paso 6 y vamos a ejecutar el siguiente comando.

```
┌──(luisacg㉿kali)-[~/Desktop]
└─$ sudo openvpn lab_LuisaCG.ovpn
2024-02-20 23:15:31 WARNING: Compression for receiving enabled. Compression has been used in the past to break encr
yption. Sent packets are not compressed unless "allow-compression yes" is also set.
2024-02-20 23:15:31 Note: --data-cipher-fallback with cipher 'AES-128-CBC' disables data channel offload.
2024-02-20 23:15:31 OpenVPN 2.6.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AE
AD] [DCO]
2024-02-20 23:15:31 library versions: OpenSSL 3.0.11 19 Sep 2023, LZO 2.10
2024-02-20 23:15:31 DCO version: N/A
2024-02-20 23:15:31 TCP/UDP: Preserving recently used remote address: [AF_INET]173.208.98.30:1337
2024-02-20 23:15:31 Socket Buffers: R=[212992→212992] S=[212992→212992]
2024-02-20 23:15:31 UDPv4 link local: (not bound)
2024-02-20 23:15:31 UDPv4 link remote: [AF_INET]173.208.98.30:1337
2024-02-20 23:15:31 TLS: Initial packet from [AF_INET]173.208.98.30:1337, sid=78e565c8 14dc2da0
2024-02-20 23:15:31 VERIFY OK: depth=1, C=UK, ST=City, L=London, O=HackTheBox, CN=HackTheBox CA, name=htb, emailAdd
ress=info@hackthebox.eu
2024-02-20 23:15:31 VERIFY KU OK
2024-02-20 23:15:31 Validating certificate extended key usage
2024-02-20 23:15:31 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authenticati
on
2024-02-20 23:15:31 VERIFY EKU OK
2024-02-20 23:15:31 VERIFY OK: depth=0, C=UK, ST=City, L=London, O=HackTheBox, CN=htb, name=htb, emailAddress=info@
hackthebox.eu
2024-02-20 23:15:31 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 2048 bits RS
A, signature: RSA-SHA1, peer temporary key: 253 bits X25519
2024-02-20 23:15:31 [htb] Peer Connection Initiated with [AF_INET]173.208.98.30:1337
2024-02-20 23:15:31 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_src=1
2024-02-20 23:15:31 TLS: tls_multi_process: initial untrusted session promoted to trusted
2024-02-20 23:15:33 SENT CONTROL [htb]: 'PUSH_REQUEST' (status=1)
2024-02-20 23:15:33 PUSH: Received control message: 'PUSH_REPLY,route 10.10.10.0 255.255.254.0,route 10.129.0.0 255
.255.0.0,route-ipv6 dead:beef::/64,explicit-exit-notify,tun-ipv6,route-gateway 10.10.14.1,topology subnet,ping 10,p
ing-restart 120,ifconfig-ipv6 dead:beef:2::1022/64 dead:beef:2::1,ifconfig 10.10.14.36 255.255.254.0,peer-id 42,cip
her AES-256-CBC'
2024-02-20 23:15:33 OPTIONS IMPORT: --ifconfig/up options modified
2024-02-20 23:15:33 OPTIONS IMPORT: route options modified
2024-02-20 23:15:33 OPTIONS IMPORT: route-related options modified
2024-02-20 23:15:33 net_route_v4_best_gw query: dst 0.0.0.0
2024-02-20 23:15:33 net_route_v4_best_gw result: via 192.168.161.2 dev eth0
```

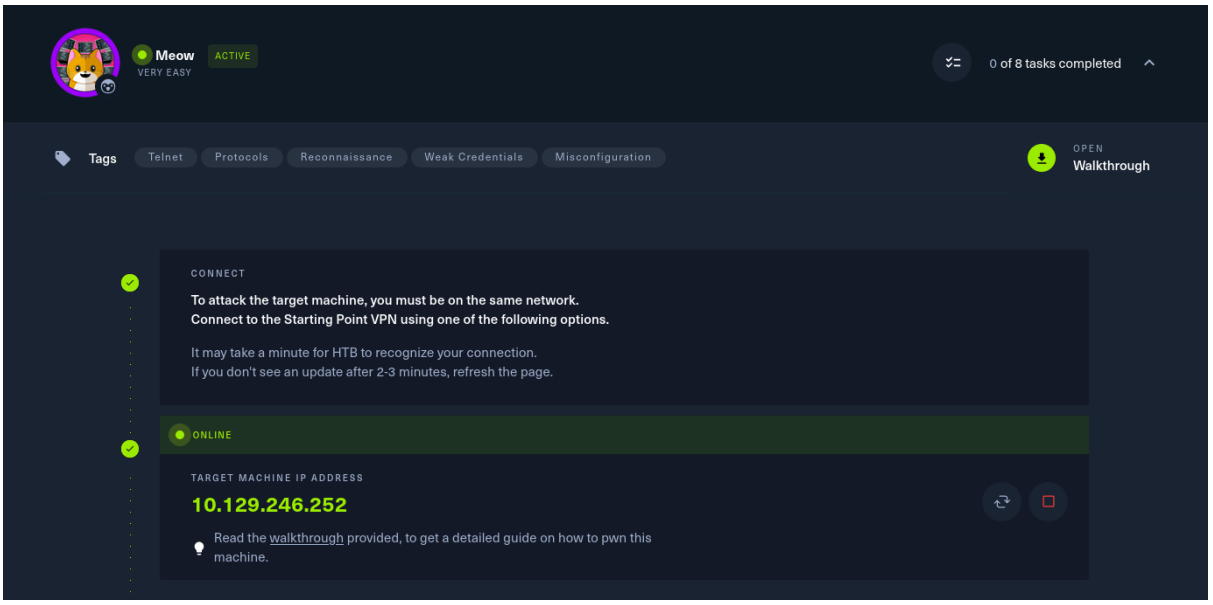
9. Listo, ya estamos conectados a nuestra vpn, para confirmarlo podemos entrar en el sitio web de Hack The Box y dirigirnos al menú donde la descargamos.



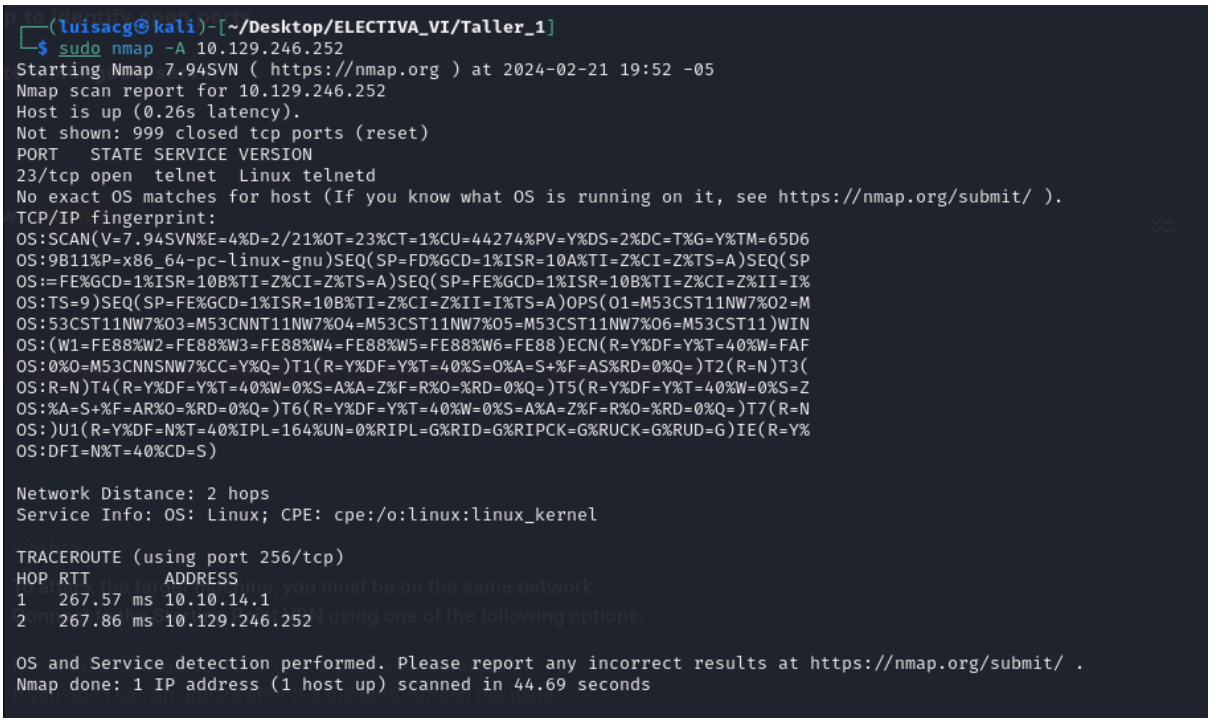
Conectándonos a las máquinas de Hack The Box

Máquina Meow

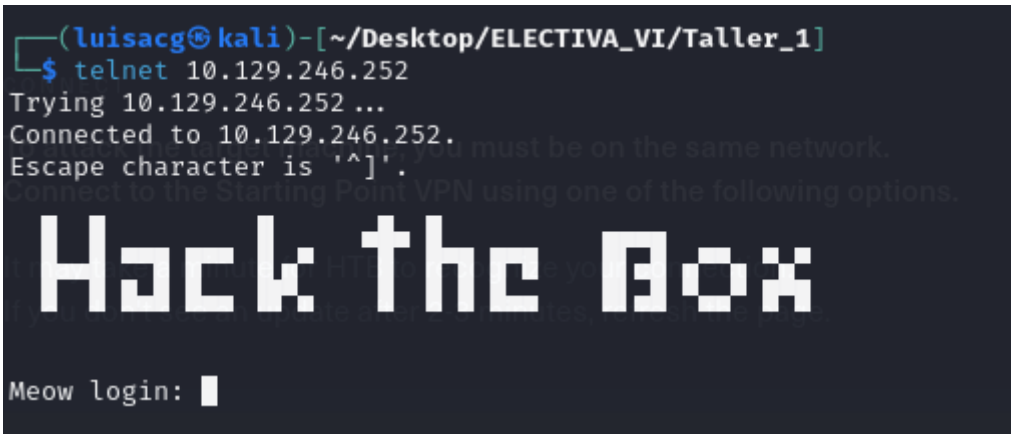
1. Lo primero que debemos hacer para entrar en la máquina seleccionada es generar la ip a la cual le aplicaremos la función de nmap.



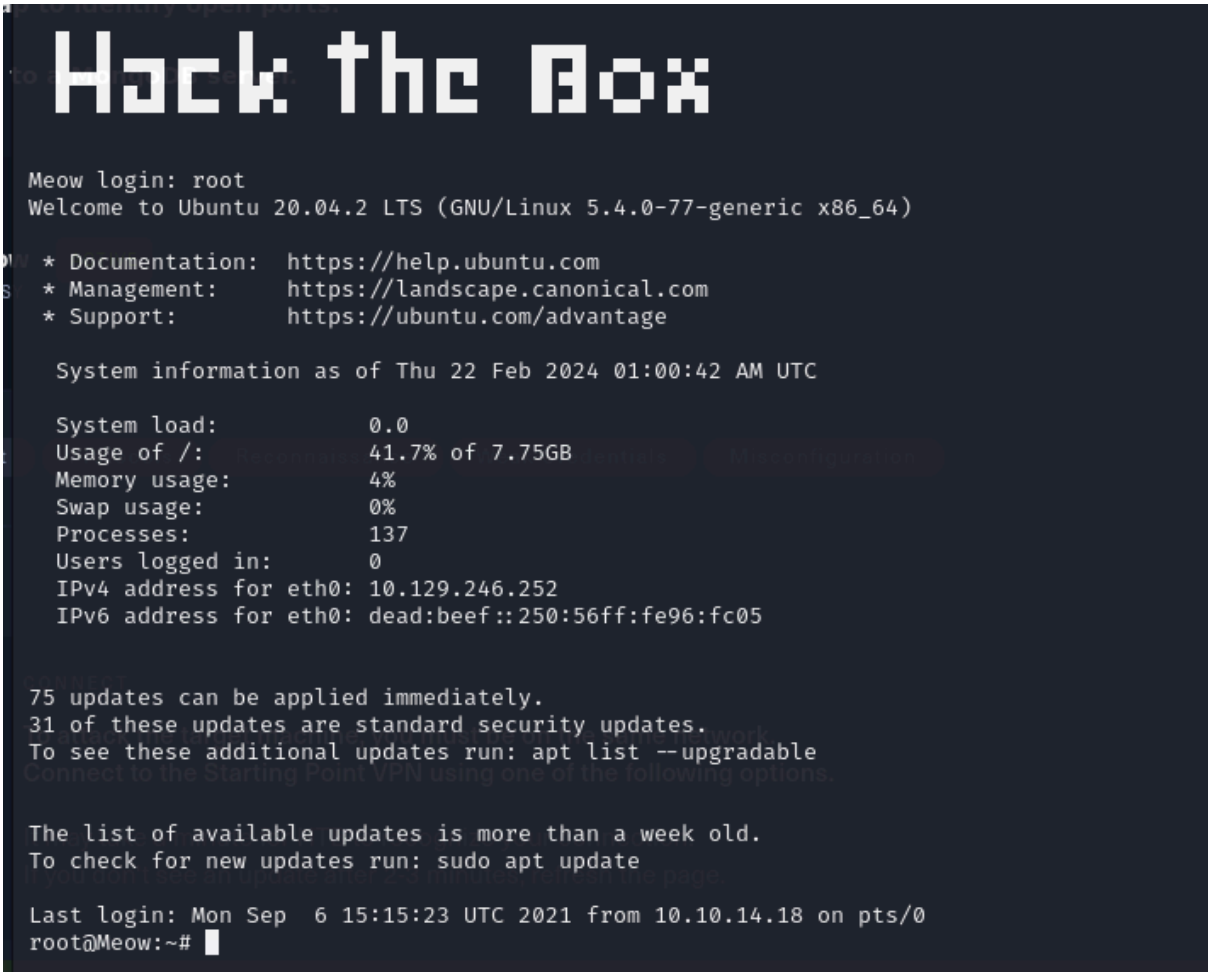
2. Después de tener nuestra ip nos dirigimos a nuestra terminal de kali linux y ejecutamos el siguiente comando, el cual nos permitirá escanear los puertos que se encuentran expuestos.



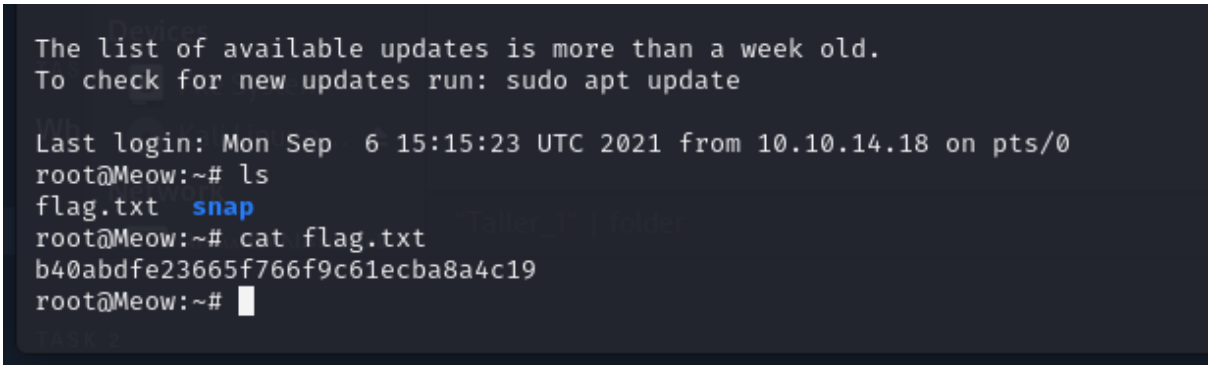
3. En nuestra terminal podemos observar que el puerto que se encuentra expuesto es el 23/tcp, por ello, ingresamos a ese puerto a través del siguiente comando.



4. Como se puede observar ya tenemos una conexión hacia la máquina, pero para poder ingresar a este debemos iniciar sesión, para ello trataremos de iniciar con el más común que es “root”.

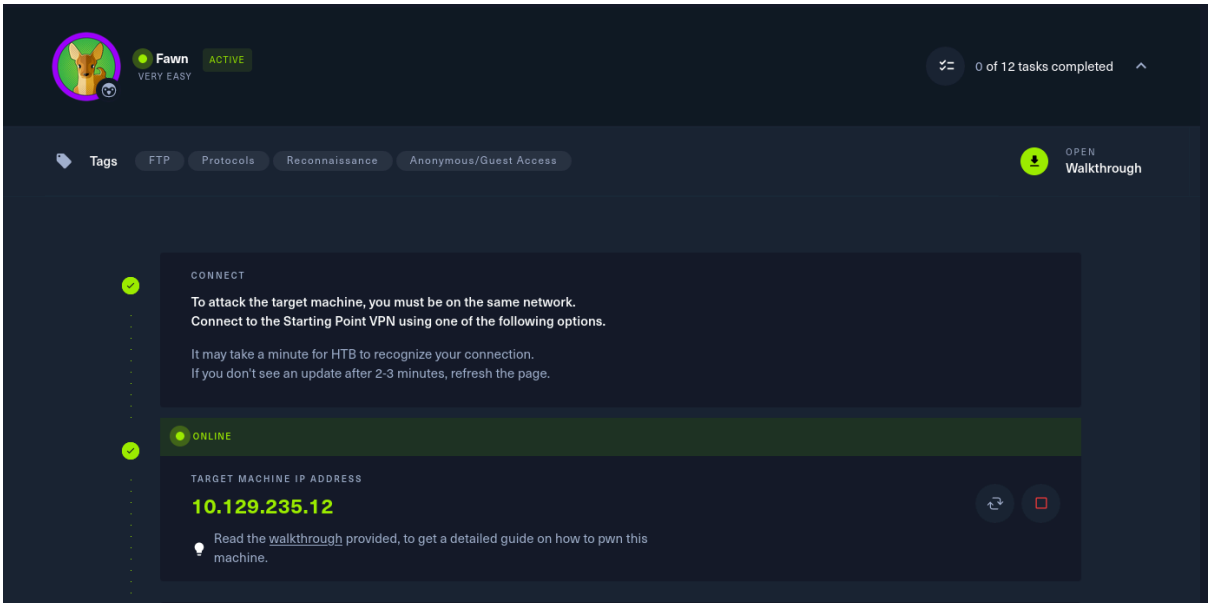


5. Listo, ya nos hemos conectado a la máquina, ahora obtendremos su flag con el siguiente comando y listo, hemos conseguido nuestra primera flag.



Máquina Fawn

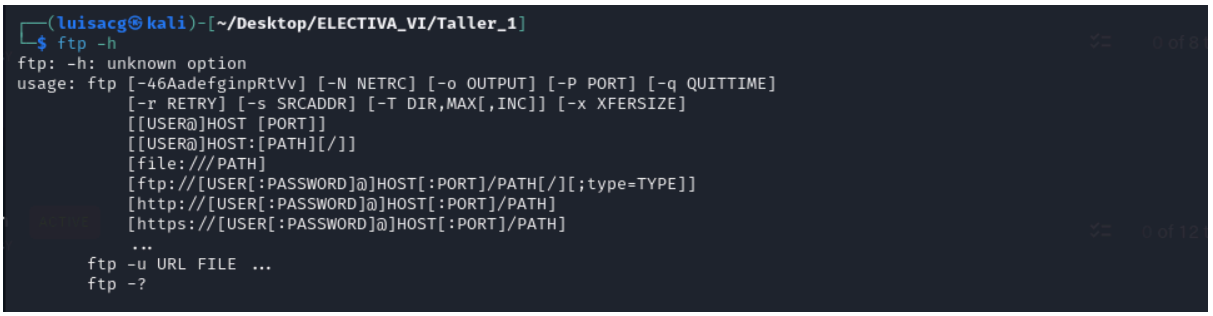
1. Para nuestra segunda máquina realizaremos el mismo proceso que en la anterior, ingresamos a Hack The Box y obtendremos su ip.



2. Ahora haremos un nmap a dicha ip para escanear y obtener aquellos puertos que se encuentran expuestos.

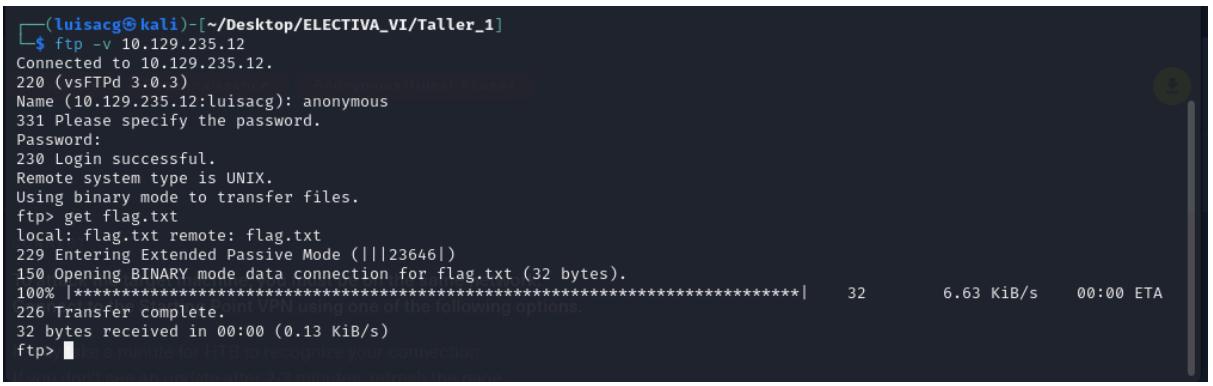
```
┌──(luisacg㉿kali)-[~/Desktop/ELECTIVA_VI/Taller_1]
└─$ sudo nmap -A -sS -sV 10.129.235.12
[sudo] password for luisacg:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 20:11 -05
Nmap scan report for 10.129.235.12
Host is up (0.22s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.10.14.22
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0              32 Jun 04  2021 flag.txt
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5.0
OS details: Linux 5.0
Network Distance: 2 hops
Service Info: OS: Unix

TRACEROUTE (using port 443/tcp)
HOP RTT       ADDRESS
1   300.87 ms 10.10.14.1
2   301.12 ms 10.129.235.12

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.92 seconds
```

3. Como podemos observar en nuestra terminal, en esta ocasión el puerto que se encuentra expuesto es el 21/tcp open ftp, por ello, haremos una conexión ftp a este.



4. Listo, ya nos hemos conectado al puerto, ahora accederemos a la máquina y obtendremos su flag al igual que en la anterior.

Nuestra flag es: 035db21c881520061c53e0536e44f815



Nota: Para conectarnos a las máquinas debemos permanecer conectados a la VPN.