

FACULTAD DE INGENIERÍA



TALLER 1

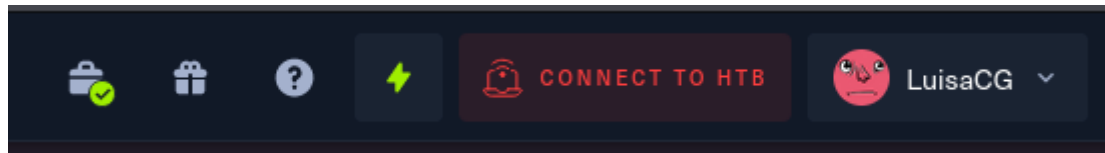
LUISA FERNANDA CELIS GONZÁLEZ

INGENIERÍA DE SOFTWARE

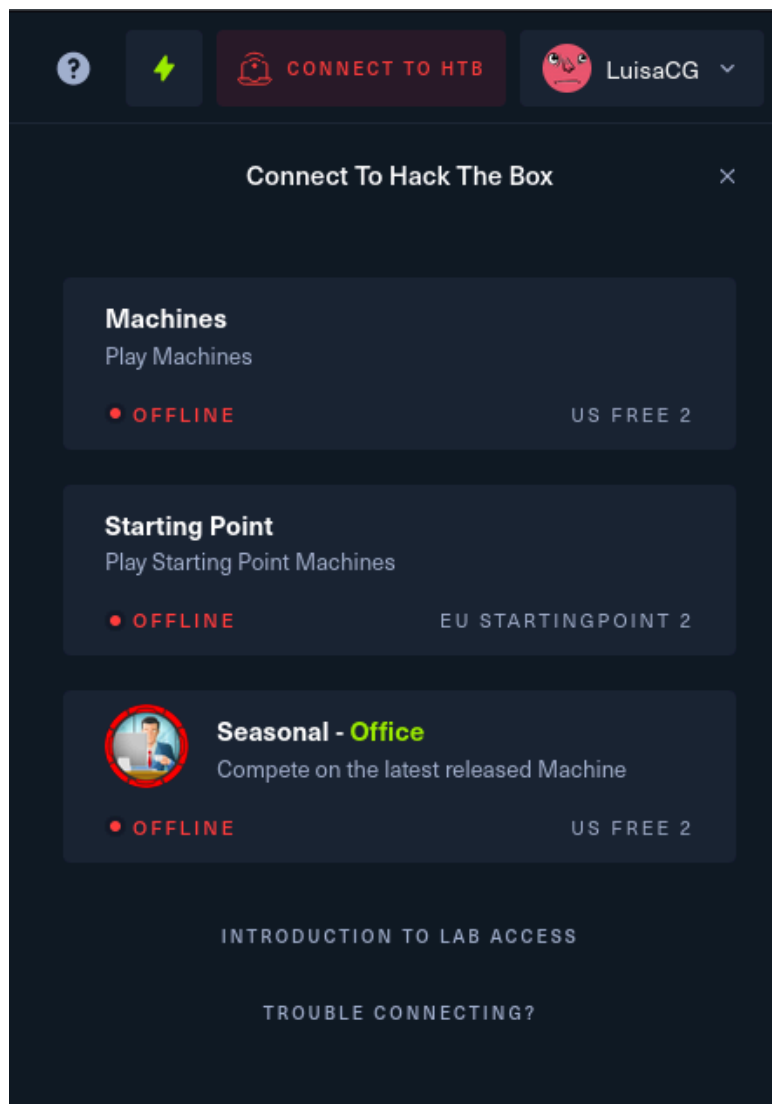
2024

Conexión a la VPN de Hack The Box

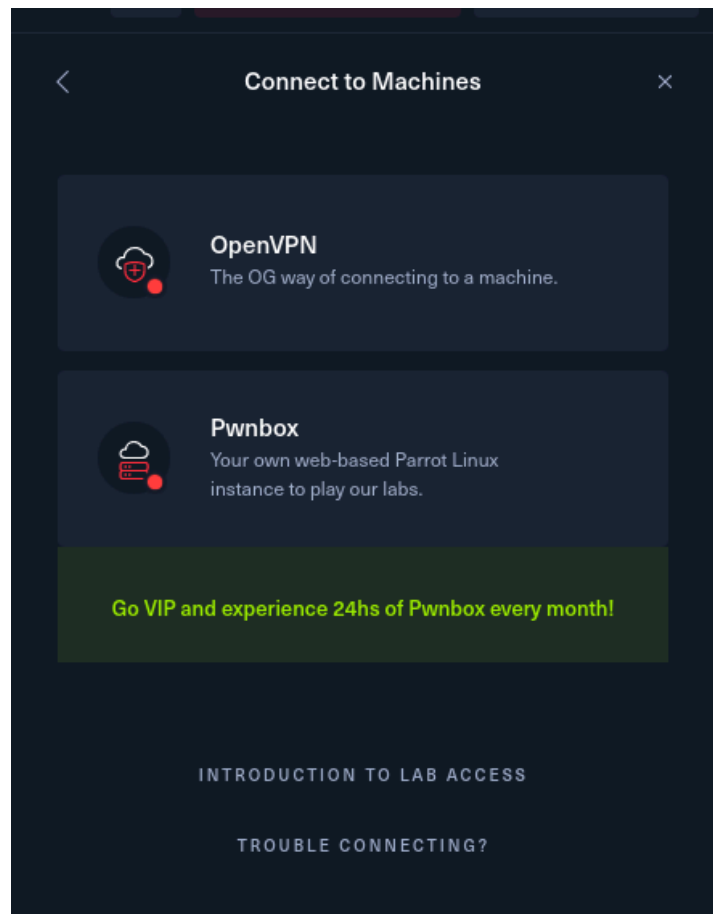
1. Para conectarnos a la VPN de Hack The Box, lo primero que debemos hacer es dirigirnos a la parte superior derecha del navbar y dar clic en la opción "CONNECT TO HTB"



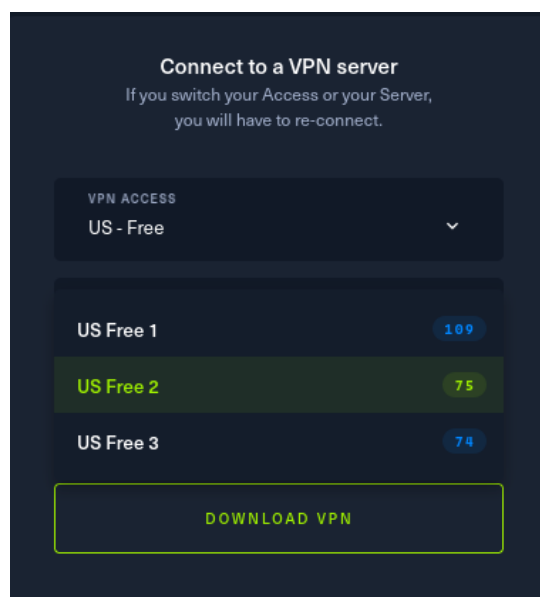
2. Seleccionamos el tipo de vpn a la que nos deseamos conectar o según las necesidad que tengamos.



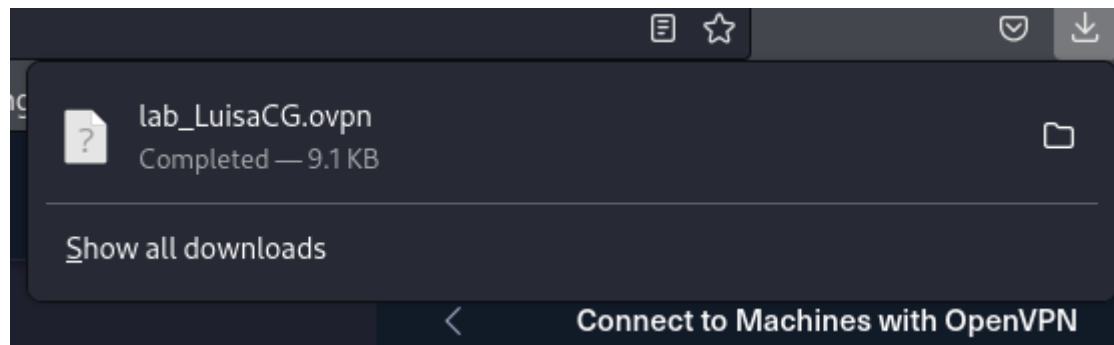
- Después de elegir el tipo de vpn que deseamos vamos a dar clic en la opción de "OpenVPN"



- 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.



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



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

```
File  Actions  Edit  View  Help
(luisacg@kali)-[~]
$ sudo apt-get install openvpn
[sudo] password for luisacg:
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 1197 not upgraded.

(luisacg@kali)-[~]
$
```

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

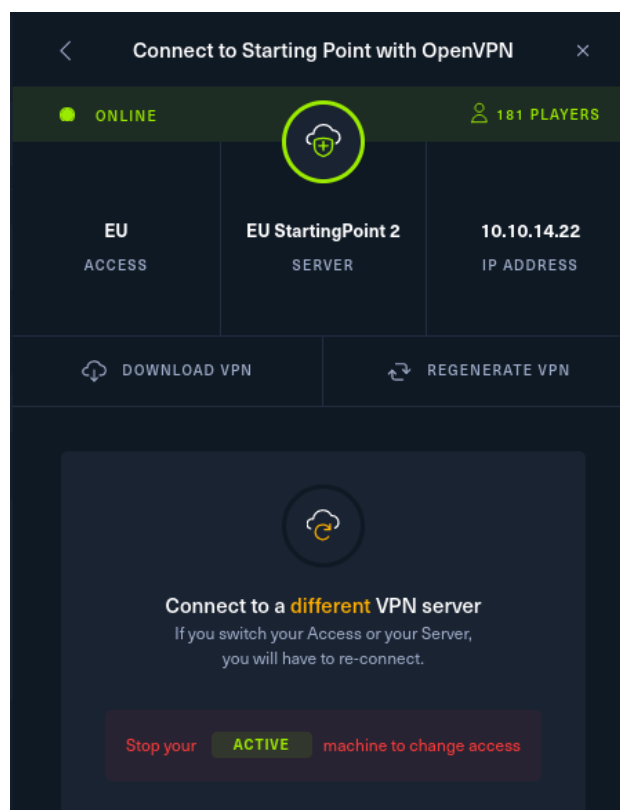
```
(luisacg@kali)-[~]
$ cd Desktop

(luisacg@kali)-[~/Desktop]
$ ls lab_LuisaCG.ovpn
lab_LuisaCG.ovpn
```

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 encryption. 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] [AEAD] [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, emailAddress=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 Authentication
2024-02-20 23:15:31 VERIFY ECU 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 RSA, 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,ping-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,cipher 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
```

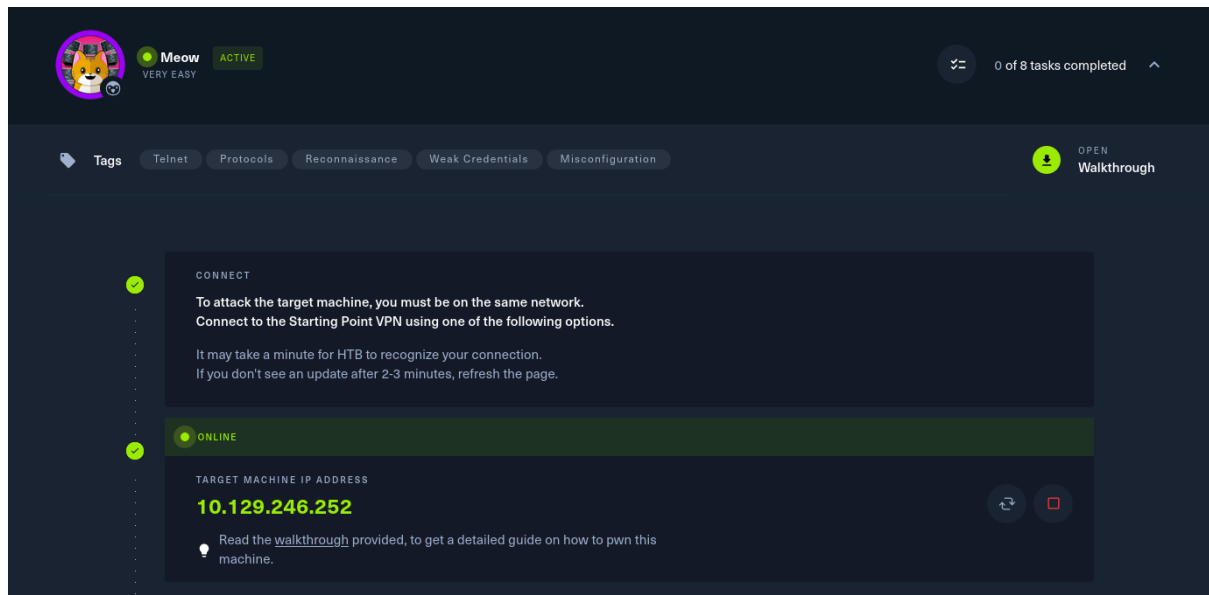
9. Listo, ya estamos conectados a nuestra vpn, para confirmarlo podemos entrar en el sitio web de Hack The Box y dirigirnos al menú donde la descargamos.



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.

```
(luisacg@kali) - [~/Desktop/ELECTIVA_VI/Taller_1]
$ sudo nmap -A 10.129.246.252
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 19:52 -05
Nmap scan report for 10.129.246.252
Host is up (0.26s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Linux telnetd
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=2/21%OT=23%CT=1%CU=44274%PV=Y%DS=2%DC=T%G=Y%TM=65D6
OS:9B11%P=x86_64-pc-linux-gnu)SEQ(SP=FD%GCD=1%ISR=10A%TI=Z%CI=Z%TS=A)SEQ(SP
OS:=FE%GCD=1%ISR=10B%TI=Z%CI=Z%TS=A)SEQ(SP=FE%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%
OS:TS=9)SEQ(SP=FE%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M53CST11NW7%O2=M
OS:53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CST11NW7%O6=M53CST11)WIN
OS:(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF
OS:0%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(
OS:R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z
OS:%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=N
OS:)%U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%
OS:DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 256/tcp)
HOP RTT      ADDRESS
1   267.57 ms  10.10.14.1
2   267.86 ms  10.129.246.252

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 44.69 seconds
```

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.

```
(luisacg@kali)-[~/Desktop/ELECTIVA_VI/Taller_1]
$ telnet 10.129.246.252
Trying 10.129.246.252 ...
Connected to 10.129.246.252.
Escape character is '^]'.
Hack the Box

Meow login: █
```

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".

```
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 Thu 22 Feb 2024 01:00:42 AM UTC

System load:          0.0
Usage of /:            41.7% of 7.75GB
Memory usage:         4%
Swap usage:           0%
Processes:            137
Users logged in:      0
IPv4 address for eth0: 10.129.246.252
IPv6 address for eth0: dead:beef::250:56ff:fe96:fc05

75 updates can be applied immediately.
31 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

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

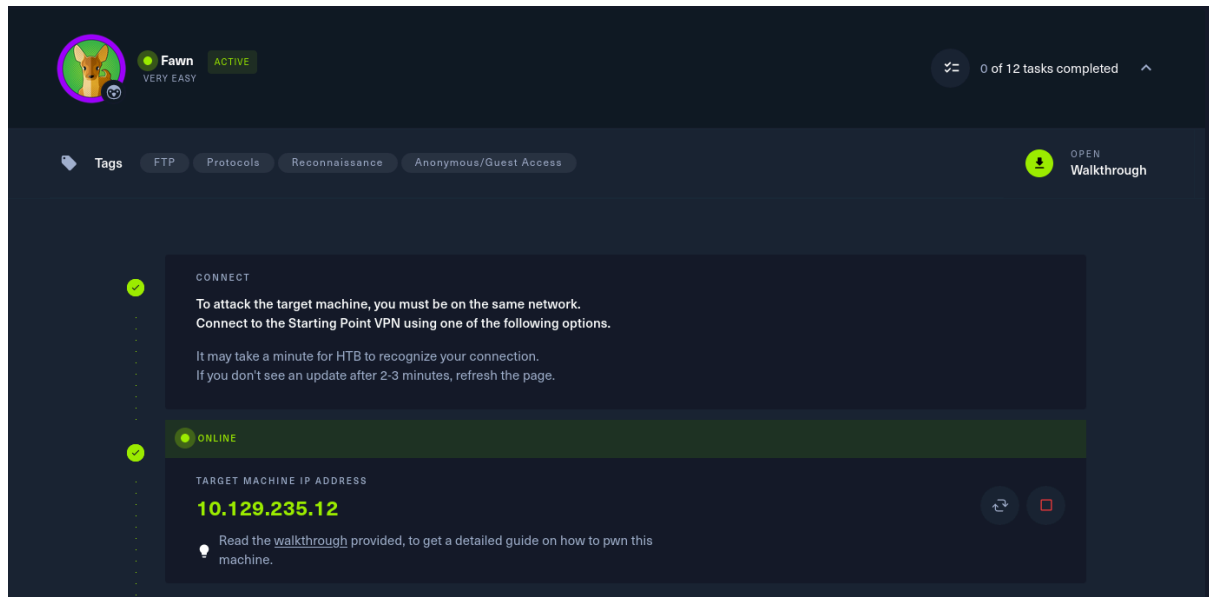
Last login: Mon Sep  6 15:15:23 UTC 2021 from 10.10.14.18 on pts/0
root@Meow:~# █
```

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

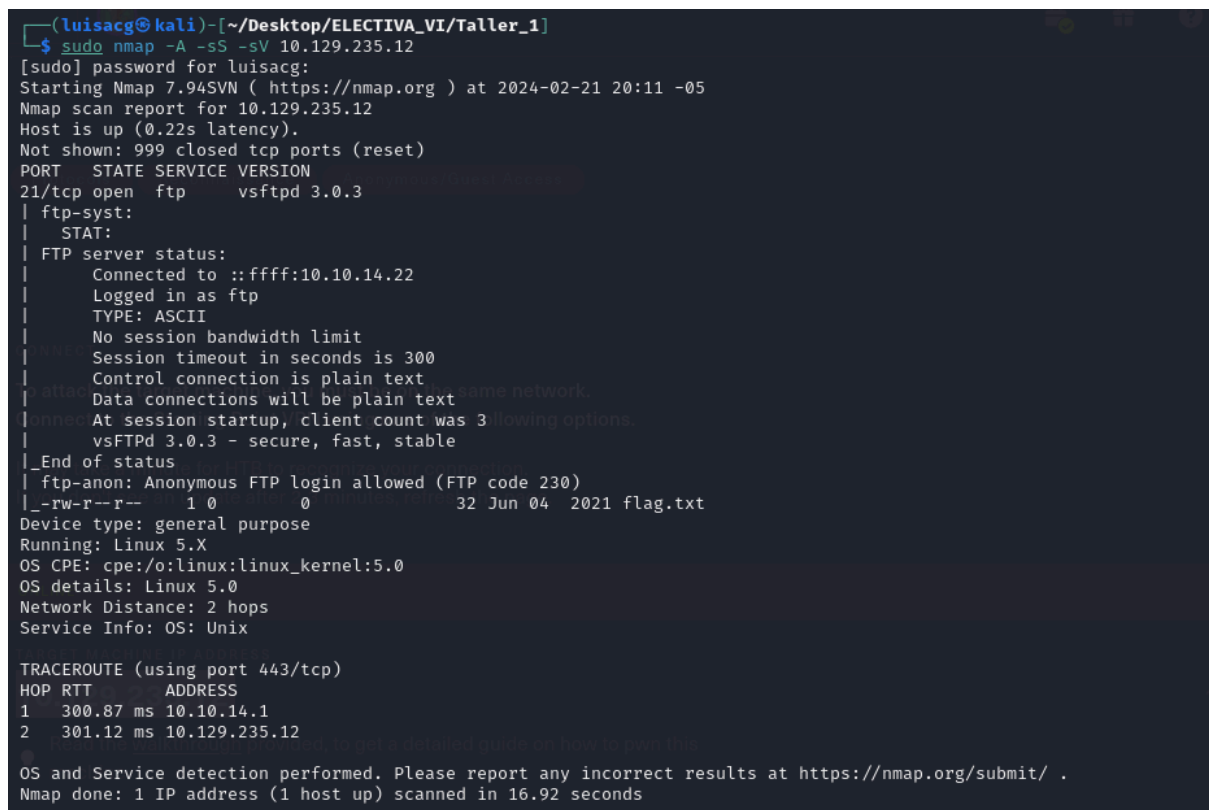
```
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
  
Last login: Mon Sep  6 15:15:23 UTC 2021 from 10.10.14.18 on pts/0  
root@Meow:~# ls  
flag.txt  snap  
root@Meow:~# cat flag.txt  
b40abdfе23665f766f9c61ecba8a4c19  
root@Meow:~# █
```


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.



- 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.

```
(luisacg@kali)~[/Desktop/ELECTIVA_VI/Taller_1]
$ ftp -h
ftp: -h: unknown option
usage: ftp [-46AaefginpRtVv] [-N NETRC] [-o OUTPUT] [-P PORT] [-q QUITTIME]
        [-r RETRY] [-s SRCADDR] [-T DIR,MAX[,INC]] [-x XFERSIZE]
        [[USER@]HOST [PORT]]
        [[USER@]HOST:[PATH][/]
        [file:///PATH]
        [ftp://[USER[:PASSWORD]@]HOST[:PORT]/PATH[/];type=TYPE]]
        [http://[USER[:PASSWORD]@]HOST[:PORT]/PATH]
        [https://[USER[:PASSWORD]@]HOST[:PORT]/PATH]
        ...
ftp -u URL FILE ...
ftp -?
```

```
(luisacg@kali)~[/Desktop/ELECTIVA_VI/Taller_1]
$ ftp -v 10.129.235.12
Connected to 10.129.235.12.
220 (vsFTPD 3.0.3)
```

- 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

```
(luisacg@kali)~[/Desktop/ELECTIVA_VI/Taller_1]
$ ftp -v 10.129.235.12
Connected to 10.129.235.12.
220 (vsFTPD 3.0.3)
Name (10.129.235.12:luisacg): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||23646|)
150 Opening BINARY mode data connection for flag.txt (32 bytes).
100% |*****| 32 6.63 KiB/s 00:00 ETA
226 Transfer complete.
32 bytes received in 00:00 (0.13 KiB/s)
ftp>
```

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