



HACKTHEBOX

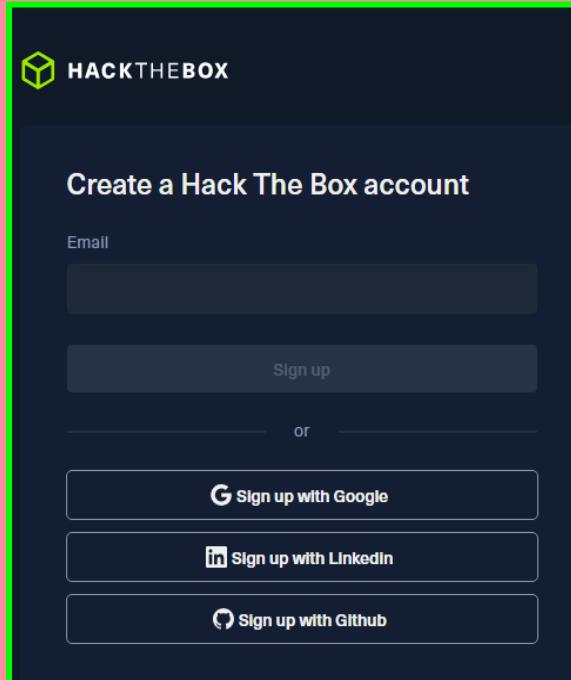


Guía inicial para dar los primeros pasos en la plataforma **HACK THE BOX (HTB)** y completar el primer laboratorio.

Preparación del Entorno y Conexión a la VPN de HTB

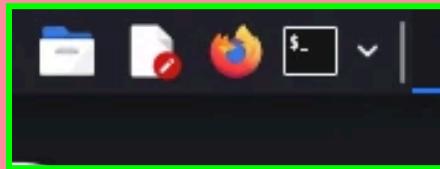
1. Crear cuenta en Hack The Box

- a. Ingresa a [Hack The Box](#) y regístrate con tu cuenta.
- b. Si ya tienes cuenta, perfecto!. *Continua el paso 2.*



2. Entrar a Hack The Box desde la Máquina Virtual

- Abrir la máquina virtual (VM): Una vez estando dentro de tu VM, puedes abrir cualquier navegador ya sea Google, Opera, etc. En nuestro caso, utilizamos Firefox.

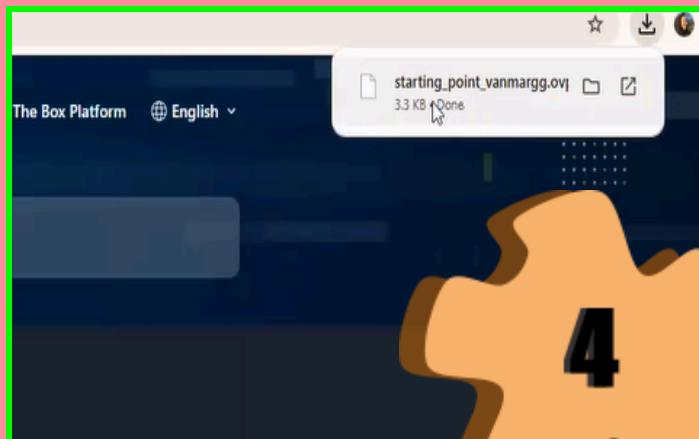
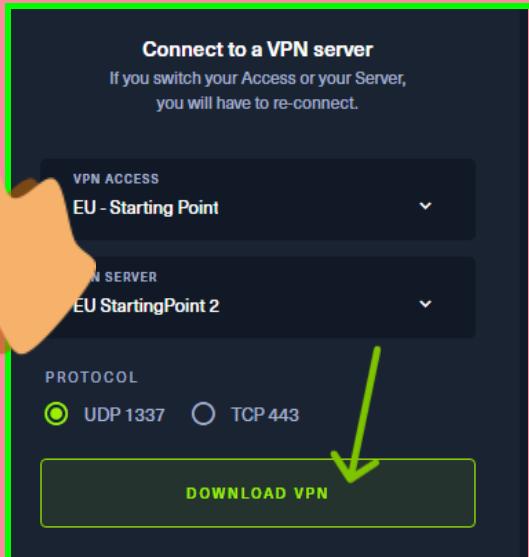


- Acceder a Hack The Box: En el paso 1.1 ya habías creado tu cuenta, ahora debes ingresar a **Hack The Box** desde tu VM.

3. Descargar el archivo de configuración .ovpn:

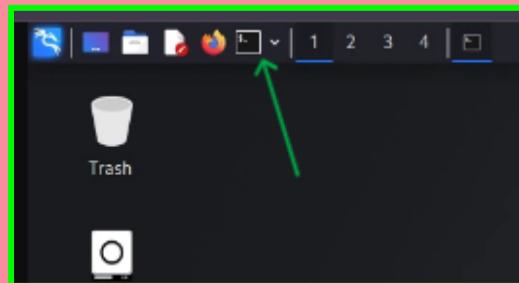
- Ingresa a tu perfil y luego a HTB Labs. Luego habrá una sección que dice **CONNECT TO HTB**, y desde ahí **descarga el archivo de configuración de la VPN**. Abajo está indicado qué seleccionar en cada paso.
- Este archivo es lo que te permitirá conectarte a la red de HTB, y trabajar en las máquinas de laboratorio de manera **SEGURA Y SIN PROBLEMAS**.

The image consists of two side-by-side screenshots of the HTB Labs interface. The left screenshot shows the 'Connect to Starting Point' screen, which includes options for 'OpenVPN' and 'Pwnbox'. An orange arrow points upwards from the bottom of the left image towards the 'OpenVPN' icon. The right screenshot shows the 'Connect To Hack The Box' screen, which displays a list of machines: 'Play Machines' (OFFLINE, US FREE 3), 'Starting Point' (Play Starting Point Machines, OFFLINE, EU STARTINGPOINT), and 'Seasonal - Backfire' (Compete on the latest released, OFFLINE, US FR). An orange arrow points upwards from the bottom of the right image towards the 'Play Machines' section. Large orange numbers '1' and '2' are overlaid on the bottom corners of the respective screenshots.



4. Conectar la terminal de Linux con la VPN de HTB

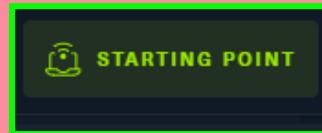
- Abre la terminal en la máquina virtual.



- Escribe el comando **sudo apt update**. (Se descargan las listas de paquetes disponibles, esto ayuda a que se actualicen las versiones, si es la primera vez que usas una terminal).
- Escribe el comando **sudo su**. (Te ayudará el superusuario (root) a obtener privilegios completos).
- Escribe el comando **ls**. (Ayuda a dar el listado de los directorios que tienes para poder **buscar el archivo que descargaste, el .ovpn**).
- Escribe el comando **cd Downloads**. (Lo más seguro es que tu archivo .ovpn esté ahí, si recién se descargó. Sino chequear el Desktop).
- Luego, escribimos el comando **openvpn <nombre del archivo descargado>**.
NOTA: **El comando openvpn debe correr con privilegios**. Como antes te convertiste en root ya los tienes, pero si NO, debes lanzarlo con sudo delante de cada comando, es decir: **sudo openvpn <nombre del archivo descargado>**).

Al final verás que dice Protocol Options en la terminal, y sabrás que el comando funcionó. También quedará titilando el cursor.

6. Por último, refresca la página de HTB. Se debería de ver de esta manera arriba a la derecha en la página:



ACLARACIÓN: es súper importante que NO cierres ni uses la terminal en la que ejecutaste el openvpn, porque harías que se caiga la conexión. Tienes que minimizar y no tocarla hasta que termines de usar la plataforma. Una vez terminas, puedes hacer Ctrl+C en la terminal para matar el proceso, o simplemente cerrarla con la cruz roja en la esquina.

A screenshot of the same HTB interface. On the right side, there is a large, semi-transparent callout box with a dark background and light text. It contains several buttons: "Telnet", "Protocols", "Official Writeup", "Video Walk", "Tags" (with sub-options "Reconnaissance", "Weak Credentials", "Misconfiguration"), "Unlimited Access", "Access", and "SPAWN MACHINE". A green arrow points from the bottom right towards the "SPAWN MACHINE" button. The entire screenshot is framed by a thick green border.

PRIMER LABORATORIO

Conectarse al laboratorio

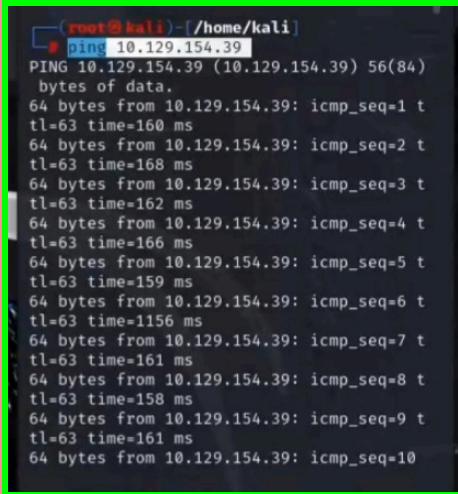
Laboratorio Meow

1. Seleccionar la Máquina Meow

1. En el portal de **Hack The Box** ve a la sección **starting point** y selecciona la máquina Meow.
2. Haz clic en **Spawn Machine** para poder obtener la IP de tu máquina privada.
3. Una vez la tengas puedes empezar a responder el cuestionario que acompaña a la máquina, a la par que realizas los ejercicios prácticos.
4. Desde la consola de tu VM, escribe ping con la IP de la máquina.

ping <Tu_Numerito_IP>

<Tu_Numerito_IP> es la IP es la que obtuviste de la página.



```
(root@kali)-[~/home/kali]
# ping 10.129.154.39
PING 10.129.154.39 (10.129.154.39) 56(84) bytes of data.
64 bytes from 10.129.154.39: icmp_seq=1 ttl=63 time=160 ms
64 bytes from 10.129.154.39: icmp_seq=2 ttl=63 time=168 ms
64 bytes from 10.129.154.39: icmp_seq=3 ttl=63 time=162 ms
64 bytes from 10.129.154.39: icmp_seq=4 ttl=63 time=166 ms
64 bytes from 10.129.154.39: icmp_seq=5 ttl=63 time=159 ms
64 bytes from 10.129.154.39: icmp_seq=6 ttl=63 time=1156 ms
64 bytes from 10.129.154.39: icmp_seq=7 ttl=63 time=161 ms
64 bytes from 10.129.154.39: icmp_seq=8 ttl=63 time=158 ms
64 bytes from 10.129.154.39: icmp_seq=9 ttl=63 time=161 ms
64 bytes from 10.129.154.39: icmp_seq=10
```

(Ping es para verificar si la máquina está activa)

5. Escanear la máquina con **nmap** para identificar puertos y servicios abiertos:

```
nmap -p- --open -sCV --min-rate 5000 -n -Pn <Tu_Numerito_ip>
```



```
(root㉿kali)-[~/home/kali]
└─# nmap -p- --open -sCV --min-rate 5000
-n -Pn 10.129.154.39
Starting Nmap 7.94SVN ( https://nmap.org
) at 2025-01-24 20:39 EST
Nmap scan report for 10.129.154.39
Host is up (0.44s latency).
Not shown: 41887 closed tcp ports (reset)
, 23647 filtered tcp ports (no-response)
Some closed ports may be reported as filt
ered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linu
x:linux_kernel

Service detection performed. Please repor
t any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scann
ed in 43.93 seconds

└─#
```

NOTA: La información a la que hay que prestar atención es donde dice **PORT STATE SERVICE** → vemos que el puerto 23 está abierto y que el servicio es telnet.
Telnet es un servicio que nos permite acceder a otra máquina para controlarla de forma remota.

Ahora con el comando `telnet <Tu_Numerito_IP>` nos podemos conectar a la máquina víctima.

The screenshot shows a terminal window with a green border. At the top, it says "root@kali: /home/kali". Below that is a menu bar with "File", "Actions", "Edit", "View", and "Help". The main area of the terminal displays the following text:

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 43.93 seconds

[~(root@kali)-[~/home/kali]
# telnet 10.129.154.39
Trying 10.129.154.39 ...
Connected to 10.129.154.39.
Escape character is '^]'.

Meow login:
Password:

Login incorrect
Meow login:
Login timed out after 60 seconds.
Connection closed by foreign host.

[~(root@kali)-[~/home/kali]
# telnet 10.129.154.39
Trying 10.129.154.39 ...
Connected to 10.129.154.39.
Escape character is '^]'.
```

The terminal shows a telnet session to port 23 of the victim machine. It prompts for a login, which is rejected. It then asks for a password, which is also rejected. The connection is closed by the foreign host. A second attempt is shown below, with the same sequence of events.

3. Una vez que haces ese comando, te va a pedir que **ingreses un usuario y contraseña**.

El usuario que puede ingresar sin contraseña, es root, así que escribes eso y cuando te pida la password solamente das Enter.

4. Con el comando `ls`, puedes listar los contenidos que existe en el lugar donde te encuentras.

5. Con `cat flag.txt` (que es el archivo que verás) puedes obtener la **flag** para poner en la última pregunta de **Hack The Box**.

```
root@Meow:~# ls
flag.txt  snap
root@Meow:~# cat flag.txt
b40abdfc23665f766f9c61ecba8a4c19
root@Meow:~#
```

(Foto tomada de [este](#) writeup de la máquina Meow)



Una vez introducida la flag el laboratorio ya está terminado.

La máquina se desconecta sola (no así la conexión a la VPN, que arriba ya se explicó cómo finalizarla). A partir de aquí puedes intentar resolver la próxima máquina que te aparece, **Fawn**. Solamente tienes que darle a Spawn Machine y utilizar de nuevo los comandos **ping** y **nmap** con la nueva IP que te genere. El resto ya dependerá de la máquina, pero ir siguiendo las preguntas que acompañan a la máquina te ayudará a saber qué hacer.



RECURSOS

Para la conexión de VPN:

<https://territoriohacker.com/como-conectarse-por-vpn-a-htb/>

<https://help.hackthebox.com/en/articles/5185687-introduction-to-lab-access>

Realizar el laboratorio de HTB del meow y apoyarse del walkthrough:

<https://app.hackthebox.com/8d11461d-6f9d-46e4-a37e-6ec420c7933f>

EJERCICIO

Tarea realizar el laboratorio de HTB llamado Fawn: "Fawn" del starting point de Hack de Box: <https://app.hackthebox.com/starting-point>.