HACKTHEBOX

Hack The Box 101

Lorenzo Pisu, Giorgio Giacinto

Università degli Studi di Cagliari

lorenzo.pisu@unica.it giorgio.giacinto@unica.it

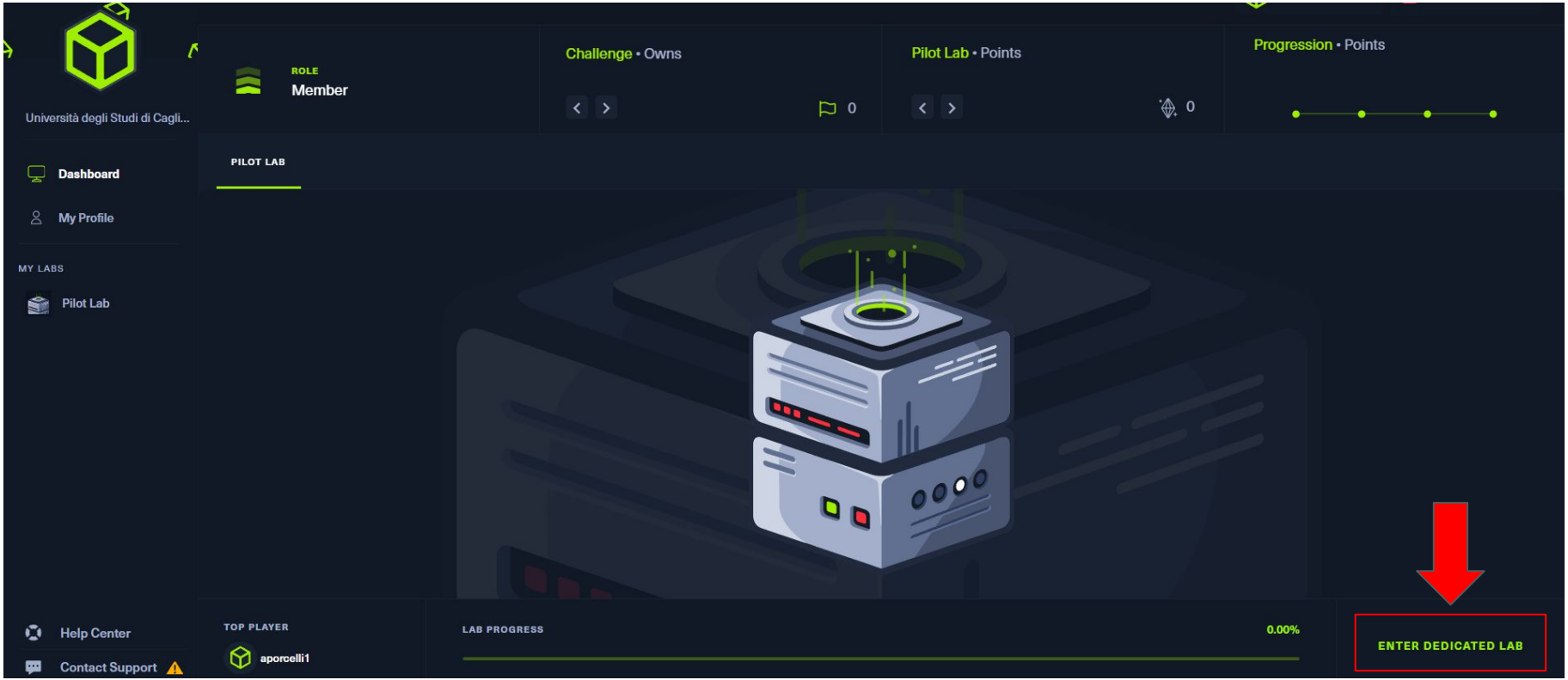
Hack The Box
PEN-TESTING LABS

Capture The Flag - CTF

CTFs are competitions where you must find a flag which is a string with a specific format (e.g. HTB{I_am_a_flag})

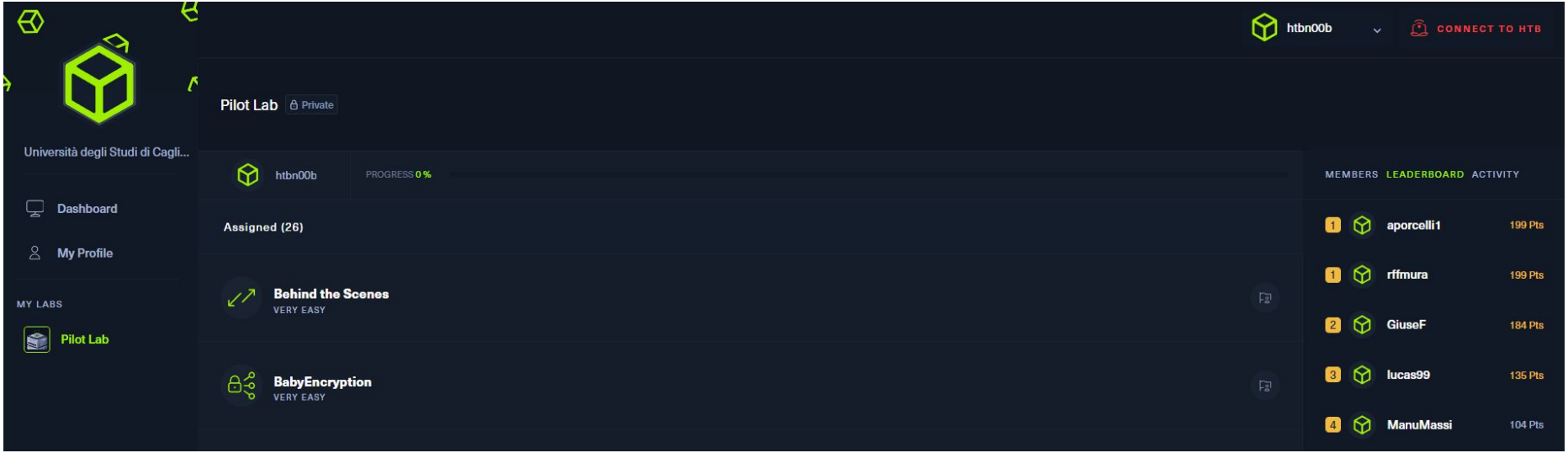
The Platform

https://enterprise.hackthebox.com/



Hack The Box
PEN-TESTING LABS

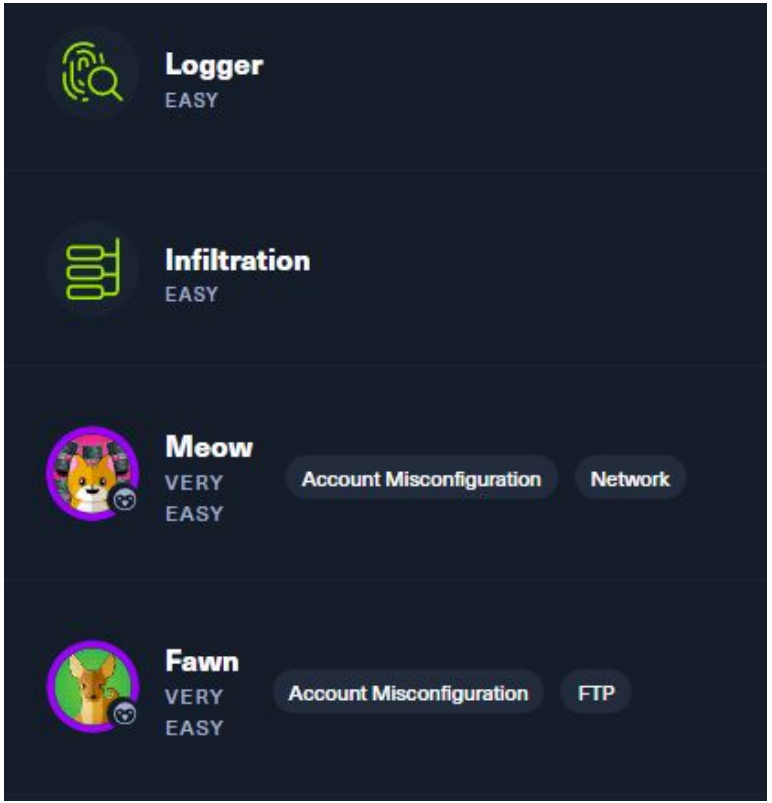
The Platform

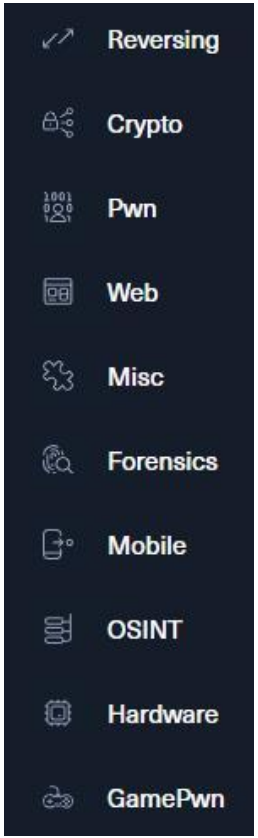


Hack The Box
PEN-TESTING LABS

Challenges VS Machines

- **Challenges** have categories
  - You will need different tools and skills for each category
  - Some categories might be easier for you, others more difficult
- **Machines** have tags
  - There are some must-know tools that you always need in machines
  - You will also need to improvise and search online for other tools and information
- Challenges require you to find a flag
- Machines require you to take control over the server and find 1 or 2 flags (user and root flag, they are usually located in a user.txt file and a root.txt file on the machine's file system)



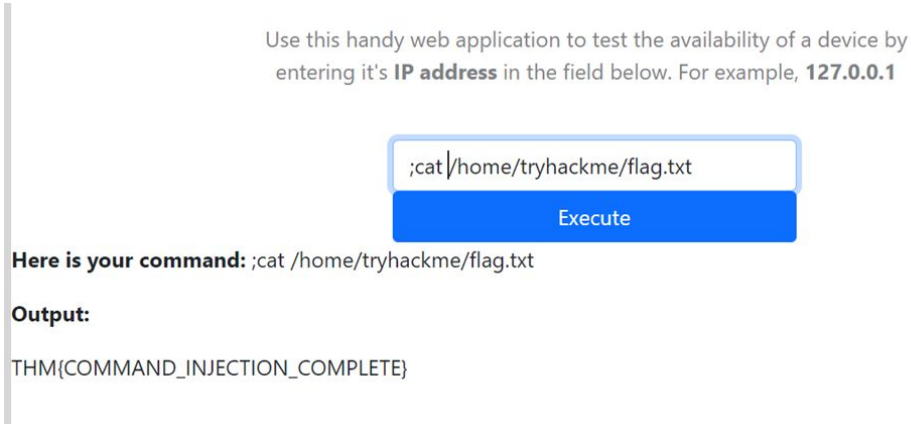


Challenges

Where are **flags** located? It depends on the kind of challenge

- In **web**, they can be in a database, in the file system or even somewhere in the web application
- In **reverse engineering** they are usually in the program but they could be encrypted and you need to understand how the program works to retrieve the flag
- In **pwn**, they are usually in the file system, therefore you need to obtain a bash shell exploiting vulnerabilities in the binary

In general you will find that flags can be hidden in trivial or complicated ways but you always need to bypass some "defences" to obtain it

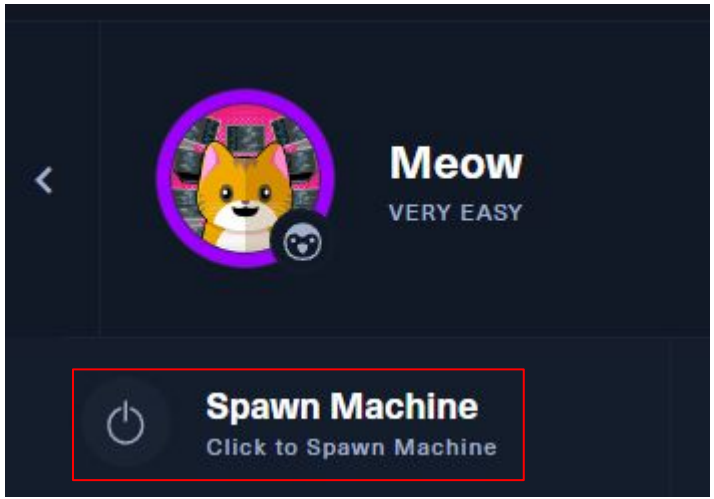


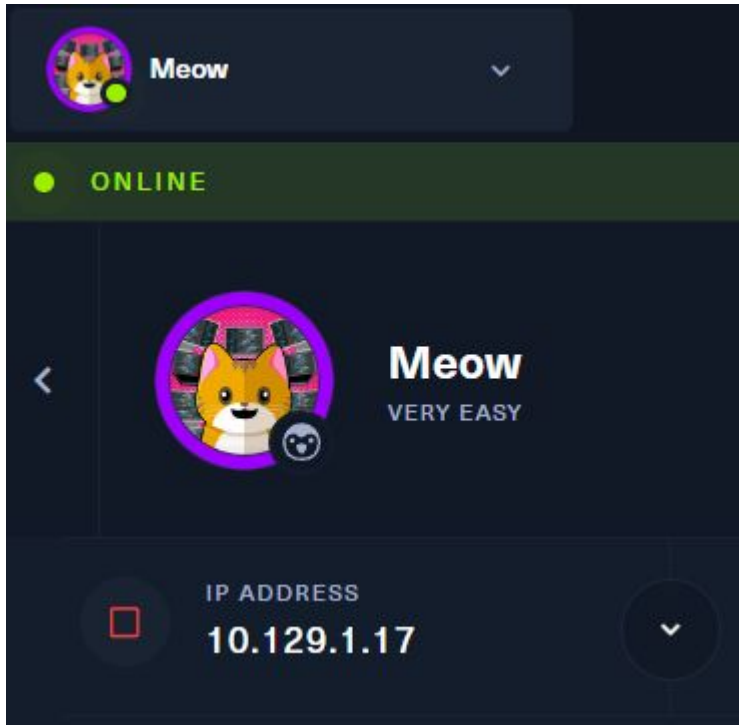
Machines

Machines (and also some challenges) need to be spawned

After the machine spawns you will see an IP address

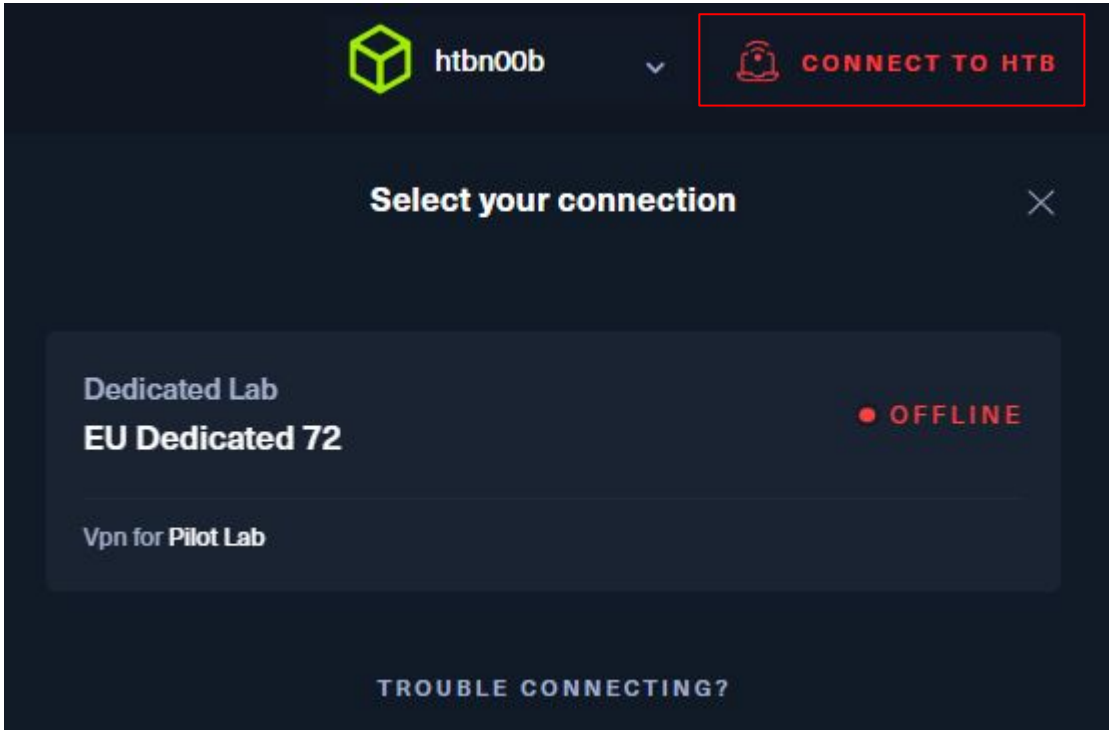
What do we do now?

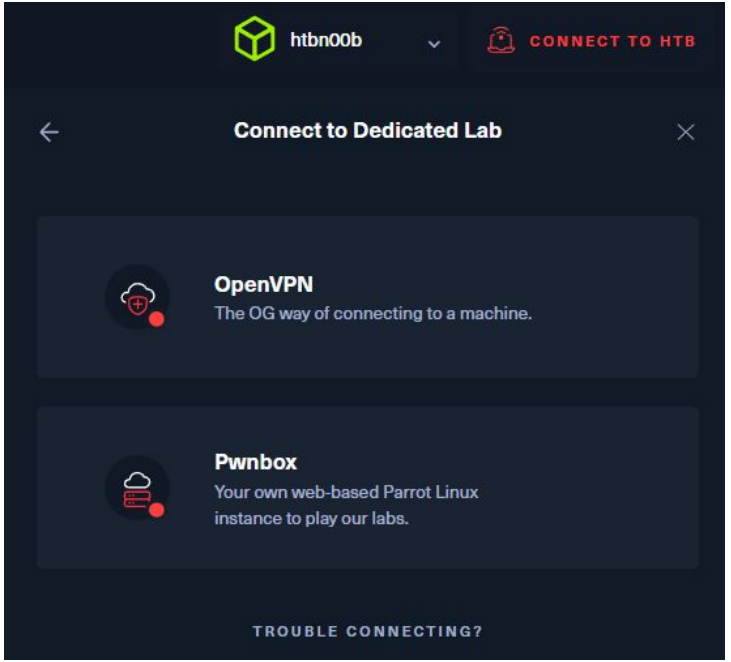




Hack The Box
PEN-TESTING LABS

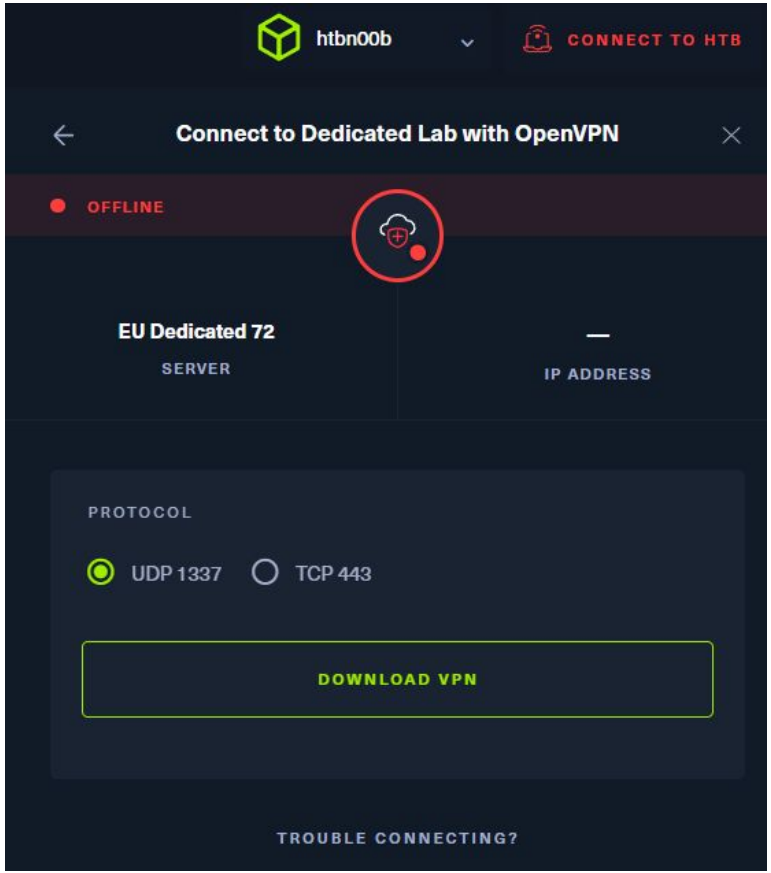
Connecting to HTB

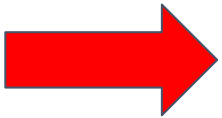


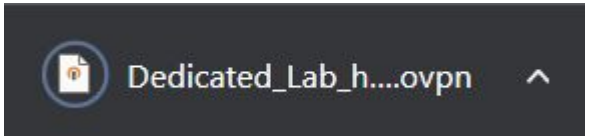


Hack The Box
PEN-TESTING LABS

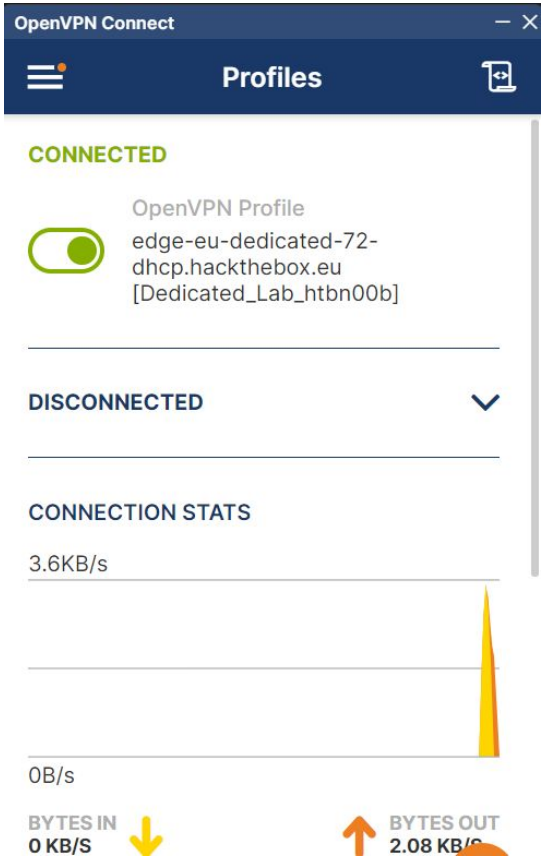
Connecting by VPN

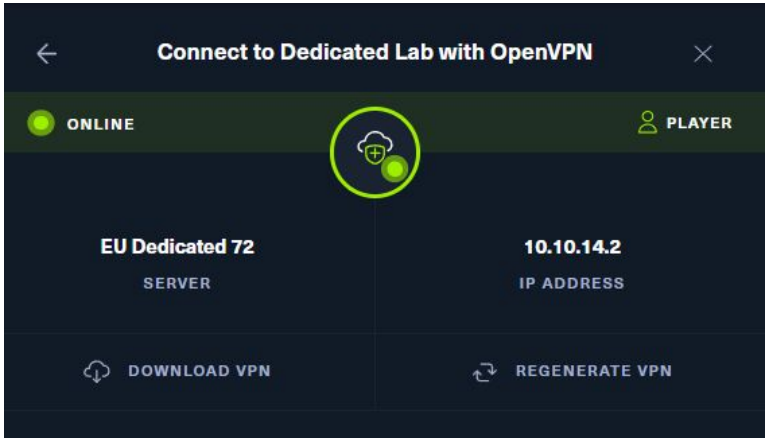






Connecting by VPN

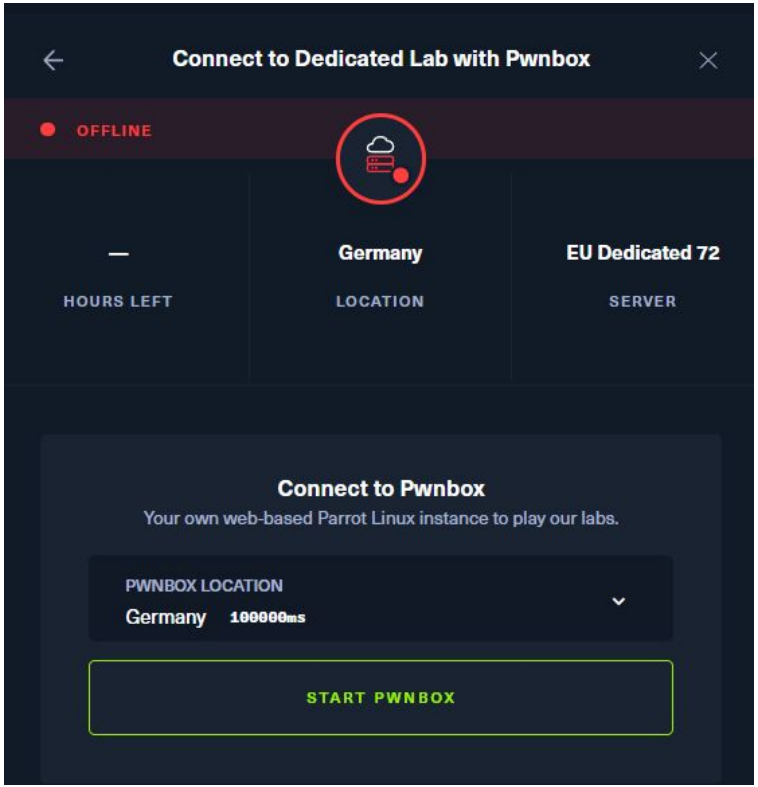


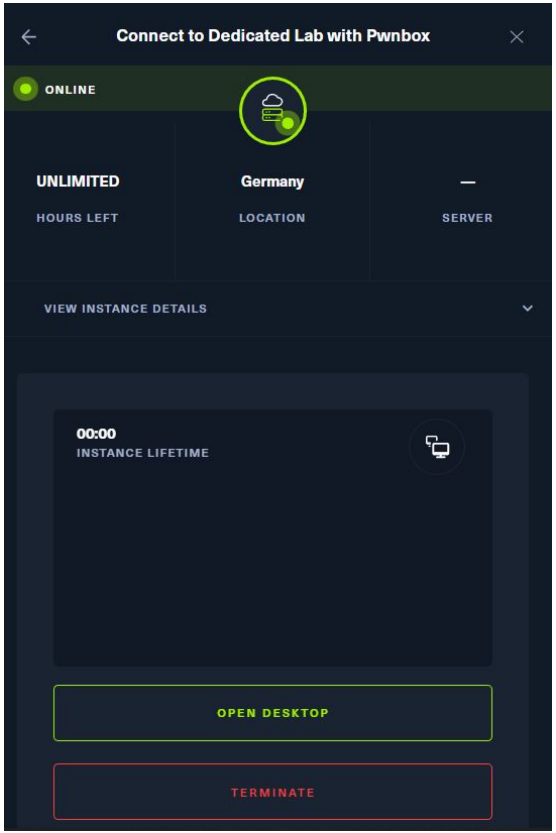



```
C:\Users\loren>ping 10.129.1.17

Pinging 10.129.1.17 with 32 bytes of data:
Reply from 10.129.1.17: bytes=32 time=43ms TTL=63
Reply from 10.129.1.17: bytes=32 time=43ms TTL=63
Reply from 10.129.1.17: bytes=32 time=43ms TTL=63
Reply from 10.129.1.17: bytes=32 time=492ms TTL=63

Ping statistics for 10.129.1.17:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 43ms, Maximum = 492ms, Average = 155ms
```

Hack The Box
PEN-TESTING LABS

Connecting using a Pwnbox



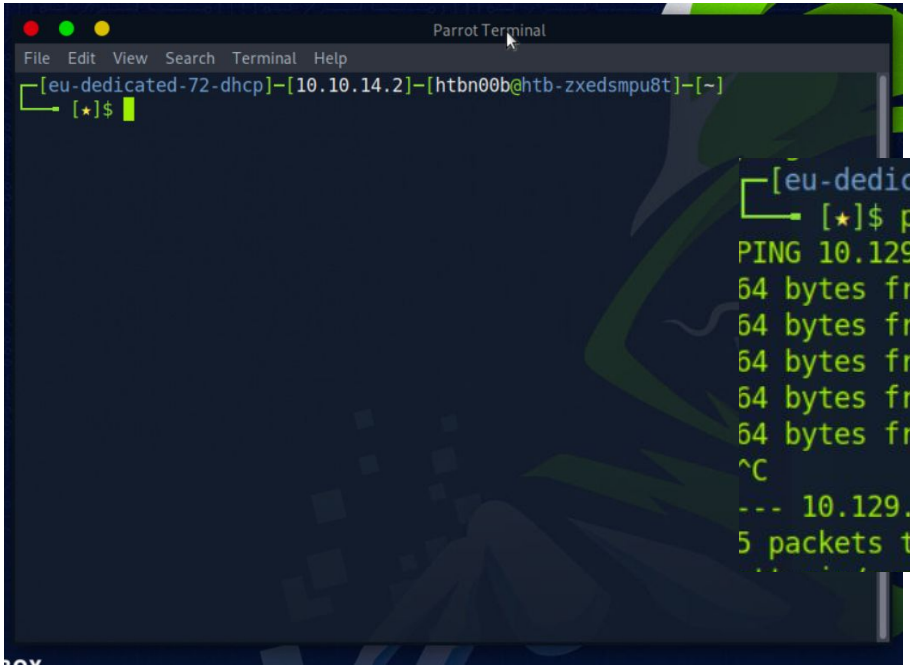


Hack The Box
PEN-TESTING LABS

Connecting using a Pwnbox

Hack The Box
PEN-TESTING LABS

Connecting using a Pwnbox




```
[eu-dedicated-72-dhcp]-[10.10.14.2]-[htbn00b@htb-zxedsmpu8t]-[~]
[★]$ ping 10.129.1.17
PING 10.129.1.17 (10.129.1.17) 56(84) bytes of data.
64 bytes from 10.129.1.17: icmp_seq=1 ttl=63 time=15.9 ms
64 bytes from 10.129.1.17: icmp_seq=2 ttl=63 time=15.9 ms
64 bytes from 10.129.1.17: icmp_seq=3 ttl=63 time=16.0 ms
64 bytes from 10.129.1.17: icmp_seq=4 ttl=63 time=15.9 ms
64 bytes from 10.129.1.17: icmp_seq=5 ttl=63 time=15.9 ms
^C
--- 10.129.1.17 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
```

Tools

Nmap is a tool that allows to scan for open ports

It is the first tool you must use when solving a machine

There are many options that can be used, enter the command “man nmap” to discover them

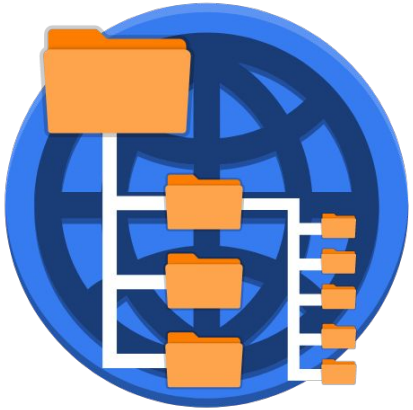
This is the base command: **nmap <MACHINE_IP>**


```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-21 11:25 EDT
Nmap scan report for 10.129.228.60
Host is up (0.0092s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 16.39 seconds
```

Tools

Other tools, protocols or commands that you might need are:

- Metasploit
- Dirbuster
- wfuzz
- FTP
- SMB
- Telnet
- SSH



Tools - For challenges

Challenges require you to use different tools depending on the category (this list is not complete, there are countless tools for each category)

- Web -> Burp, ZAP, Browser developer tools
- Crypto -> Python
- Reversing -> IDA, Ghidra
- Pwn -> IDA, Ghidra, pwntools
- Forensics -> wireshark, volatility

Hack The Box
PEN-TESTING LABS

An example

Let’s try to solve our first challenge and our first machine together!

Some additional references

- https://book.hacktricks.xyz/ (collection of vulnerabilities and tool explanations)
- https://academy.hackthebox.com/ (some guided paths for starting with HTB)
- https://www.metasploit.com/ (tool for automatic exploitation)
- https://www.revshells.com/ (when you need to open a reverse shell)