



# HACKTHEBOX

## Hack The Box 101

**Lorenzo Pisu, Giorgio Giacinto**

Università degli Studi di Cagliari

lorenzo.pisu@unica.it

giorgio.giacinto@unica.it





# 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 screenshot shows the 'CAPTURE the FLAG' website with a scoreboard. The scoreboard is divided into three columns: CRYPTO, MISC, and PWN. Each challenge is listed with its name, points, and the number of solves.

Category	Challenge Name	Points	Solves
CRYPTO	BETTER ZIP	231pt	38 solves
	DM COLLISION	176pt	63 solves
	DOGESTORE	267pt	27 solves
	MITM	243pt	34 solves
	PERFECT SECRECY	158pt	74 solves
MISC	BOOKSHELF	363pt	10 solves
	FEEL IT	208pt	47 solves
	PHRACK	420pt	5 solves
	TAPE	355pt	11 solves
	WIRED CSV	220pt	42 solves
PWN	DRIVE	500pt	0 solves
	EXECVE SANDBOX	283pt	23 solves
	APT42 - PART 2	420pt	5 solves
	SANDBOX COMPAT	420pt	5 solves
	SFTP	181pt	60 solves



# The Platform

<https://enterprise.hackthebox.com/>

The screenshot displays the Hack The Box Enterprise dashboard for a user named 'aporcelli1'. The interface includes a top navigation bar with sections for 'Challenge - Owns', 'Pilot Lab - Points', and 'Progression - Points'. A left sidebar contains navigation options like 'Dashboard', 'My Profile', and 'MY LABS'. The main content area features a 'PILOT LAB' section with a large illustration of server hardware and a progress bar at the bottom showing '0.00%'. A red arrow points to a button labeled 'ENTER DEDICATED LAB' in the bottom right corner.

ROLE  
Member

Universit  degli Studi di Cagliari...

Dashboard

My Profile

MY LABS

Pilot Lab

Challenge - Owns

Pilot Lab - Points

Progression - Points

PILOT LAB

0.00%

ENTER DEDICATED LAB



Hack The Box  
PEN-TESTING LABS



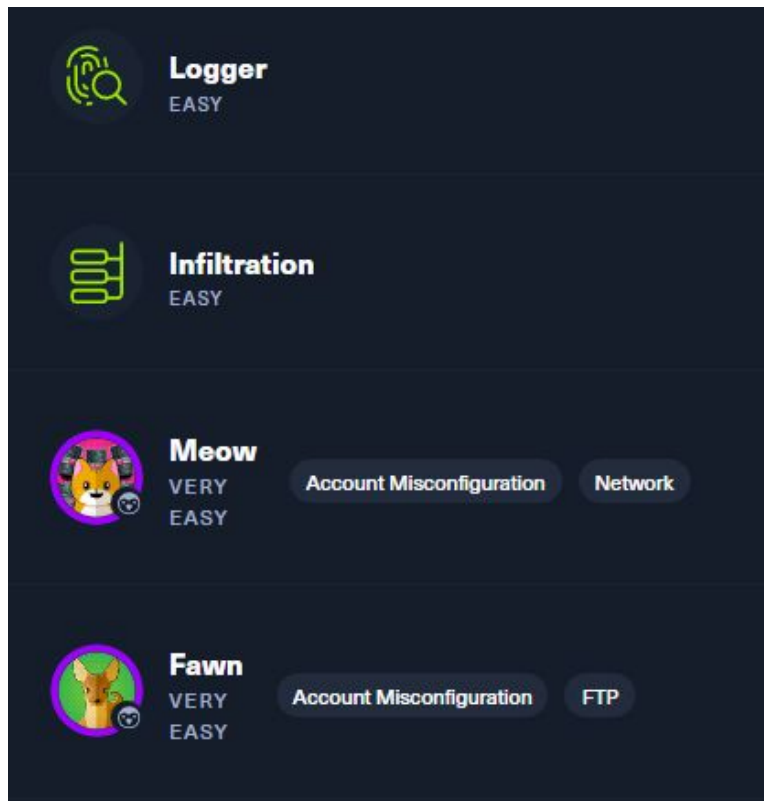
# The Platform

The screenshot displays the Hack The Box platform interface. At the top right, the user is logged in as 'htbn00b' and has a 'CONNECT TO HTB' button. The main content area shows the 'Pilot Lab' (Private) with a progress of 0%. Below this, there are two lab cards: 'Behind the Scenes' and 'BabyEncryption', both marked as 'VERY EASY'. On the right side, a 'LEADERBOARD' is visible, listing members and their scores.

MEMBERS	LEADERBOARD	ACTIVITY
1	aporcelli1	199 Pts
1	rffmura	199 Pts
2	GiuseF	184 Pts
3	lucas99	135 Pts
4	ManuMassi	104 Pts

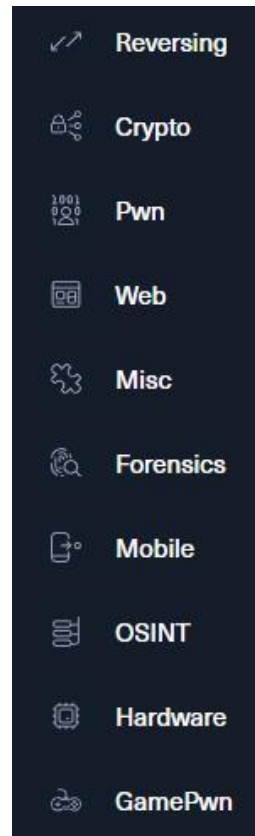
# Challenges VS Machines

- **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)



The screenshot displays the Hack The Box interface with the following challenge categories and machine tags:

- Logger** (EASY): Represented by a magnifying glass icon.
- Infiltration** (EASY): Represented by a document icon.
- Meow** (VERY EASY): Represented by a cat icon. Tags: Account Misconfiguration, Network.
- Fawn** (VERY EASY): Represented by a deer icon. Tags: Account Misconfiguration, FTP.



A vertical sidebar of challenge categories with the following items:

- Reversing
- Crypto
- Pwn
- Web
- Misc
- Forensics
- Mobile
- OSINT
- Hardware
- GamePwn



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

Use this handy web application to test the availability of a device by entering it's **IP address** in the field below. For example, **127.0.0.1**

Execute

**Here is your command:** ;cat /home/tryhackme/flag.txt

**Output:**

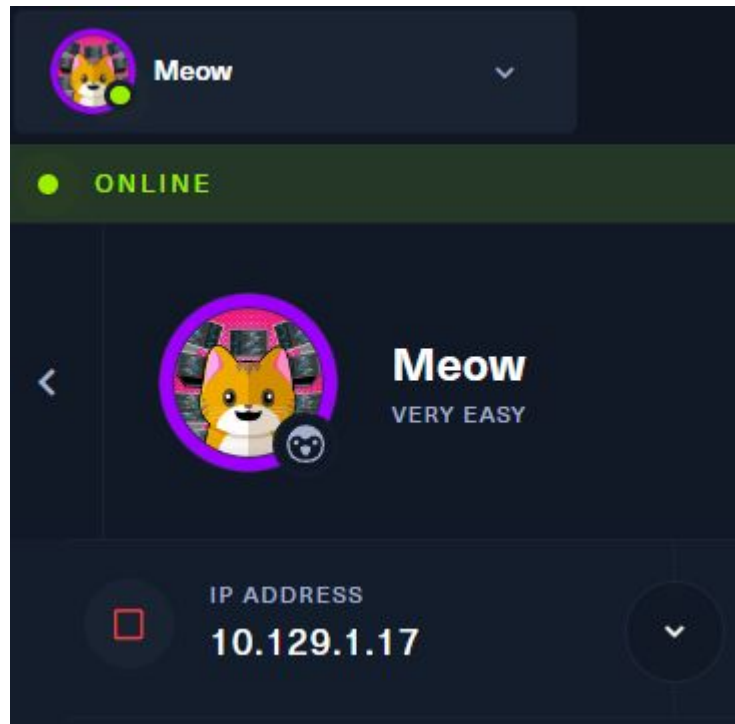
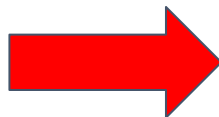
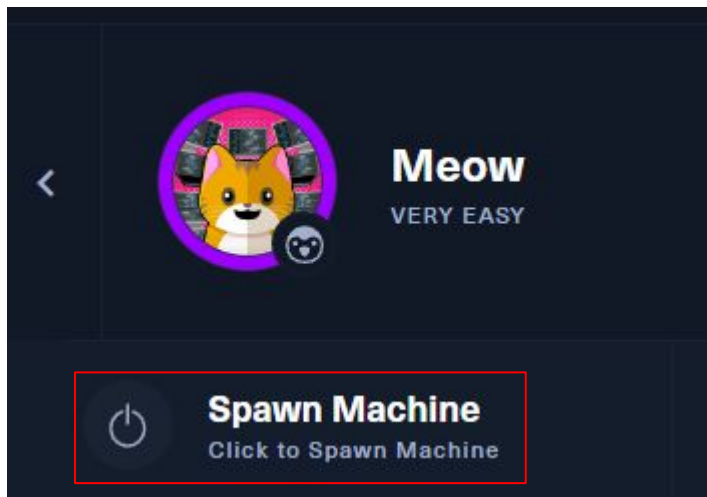
THM{COMMAND\_INJECTION\_COMPLETE}



Machines (and also some challenges) need to be spawned

After the machine spawns you will see an IP address

What do we do now?





# Connecting to HTB



htbn00b



CONNECT TO HTB

## Select your connection



Dedicated Lab  
EU Dedicated 72

● OFFLINE

Vpn for Pilot Lab

TROUBLE CONNECTING?



htbn00b



CONNECT TO HTB



## Connect to Dedicated Lab



### OpenVPN

The OG way of connecting to a machine.



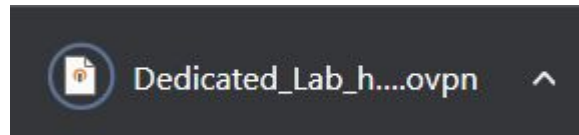
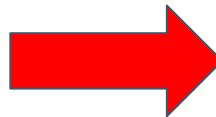
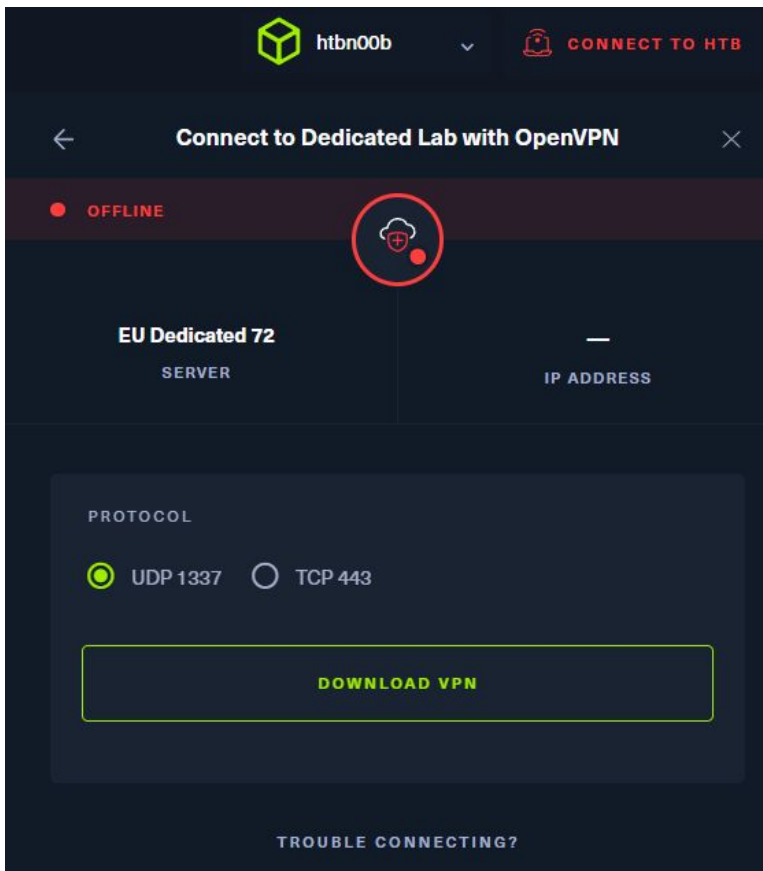
### Pwnbox

Your own web-based Parrot Linux instance to play our labs.

TROUBLE CONNECTING?



# Connecting by VPN





# Connecting by VPN

OpenVPN Connect

Profiles

**CONNECTED**

OpenVPN Profile  
edge-eu-dedicated-72-  
dhcp.hackthebox.eu  
[Dedicated\_Lab\_htbn00b]

**DISCONNECTED**

**CONNECTION STATS**

3.6KB/s

0B/s

BYTES IN 0 KB/S

BYTES OUT 2.08 KB/S

Connect to Dedicated Lab with OpenVPN

ONLINE

PLAYER

**EU Dedicated 72**  
SERVER

**10.10.14.2**  
IP ADDRESS

DOWNLOAD VPN

REGENERATE 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
```



# Connecting using a Pwnbox

Connect to Dedicated Lab with Pwnbox

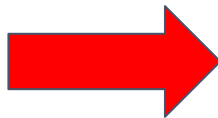
OFFLINE

HOURS LEFT	LOCATION	SERVER
—	Germany	EU Dedicated 72

**Connect to Pwnbox**  
Your own web-based Parrot Linux instance to play our labs.

PWNBOX LOCATION  
Germany 100000ms

START PWNBOX



Connect to Dedicated Lab with Pwnbox

ONLINE

HOURS LEFT	LOCATION	SERVER
UNLIMITED	Germany	—

VIEW INSTANCE DETAILS

00:00  
INSTANCE LIFETIME

OPEN DESKTOP

TERMINATE



# Connecting using a Pwnbox





# Connecting using a Pwnbox

```
Parrot Terminal
File Edit View Search Terminal Help
[eu-dedicated-72-dhcp]-[10.10.14.2]-[htbn00b@htb-zxedsmpt]-[~]
[*]$
```

```
[eu-dedicated-72-dhcp]-[10.10.14.2]-[htbn00b@htb-zxedsmpt]-[~]
[*]$ 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
```

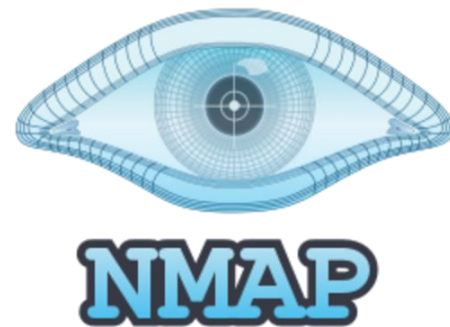


Nmap is a tool that allows to scan for open ports

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>**



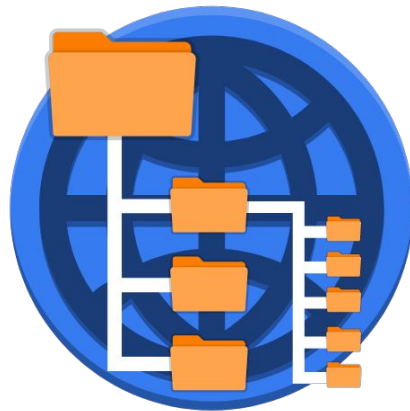
```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-21 11:25 EDT
Nmap scan report for 10.129.228.60
Host is up (0.0092s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

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



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

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





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!



**baby auth**  
EASY



**Photobomb**  
EASY



## 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)