Meow Write-up

Prepared by: 0ne-nine9

Setting Up

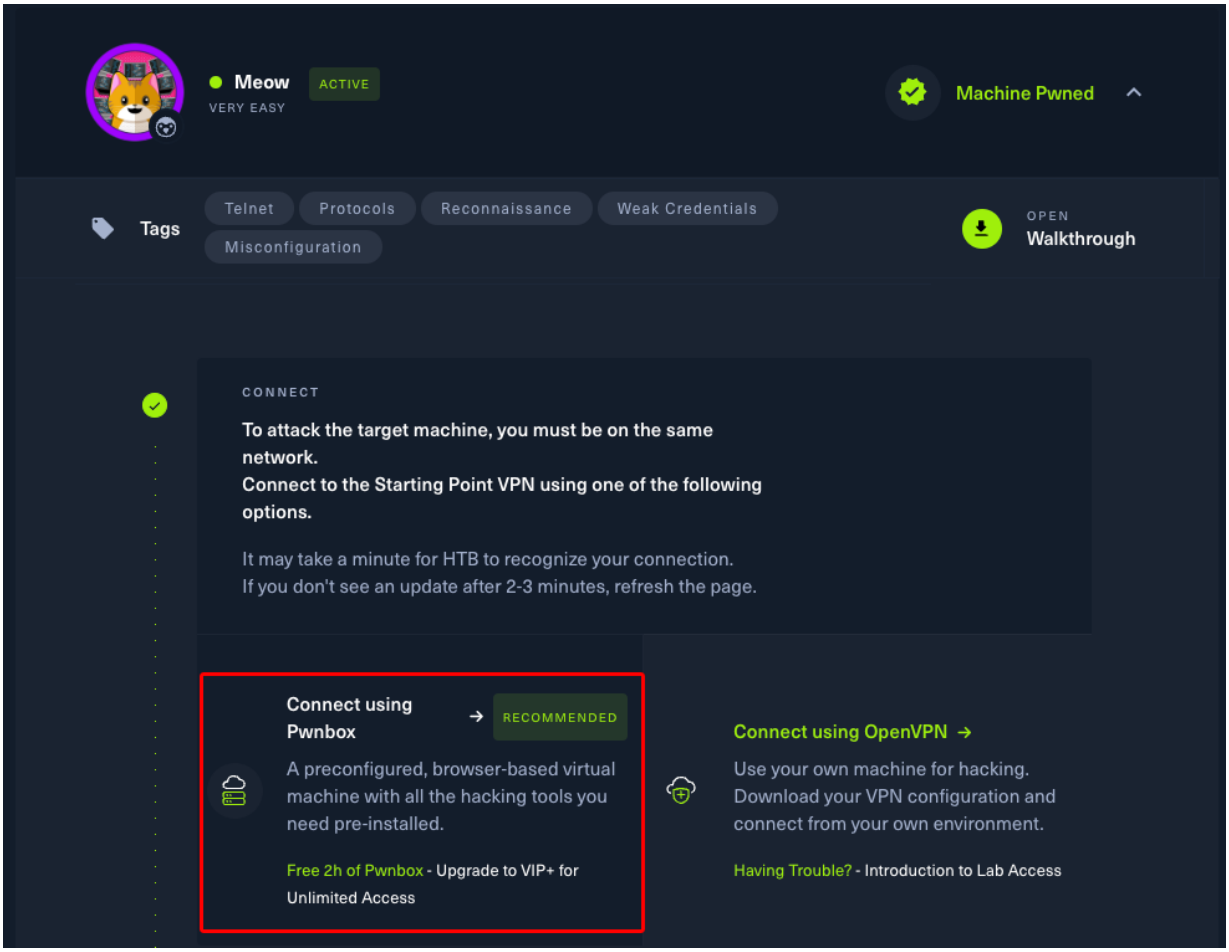
Welcome to Hack The Box!

Before we start with your very first vulnerable machine, let us make sure you are connected to the target's network and know your way around a terminal. When visiting the Starting Point lab's page, you might have been prompted to pick between a Pwnbox connection or a VPN configuration file that you can download and run on your Virtual Machine. The recommended and simplest method is using Pwnbox, which provides a fully configured virtual machine directly in your browser.

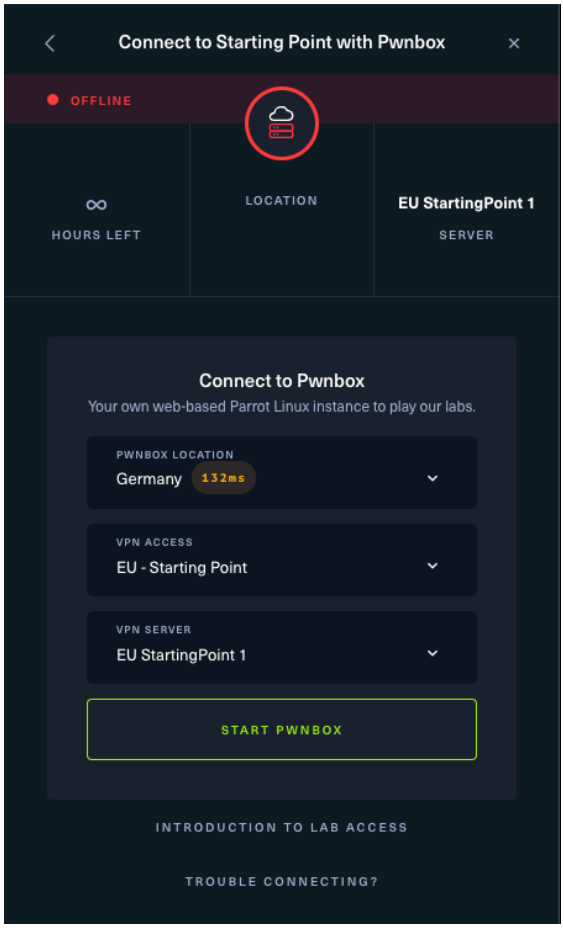
Pwnbox

Running Pwnbox is straightforward and requires no additional steps to connect to the target machine.

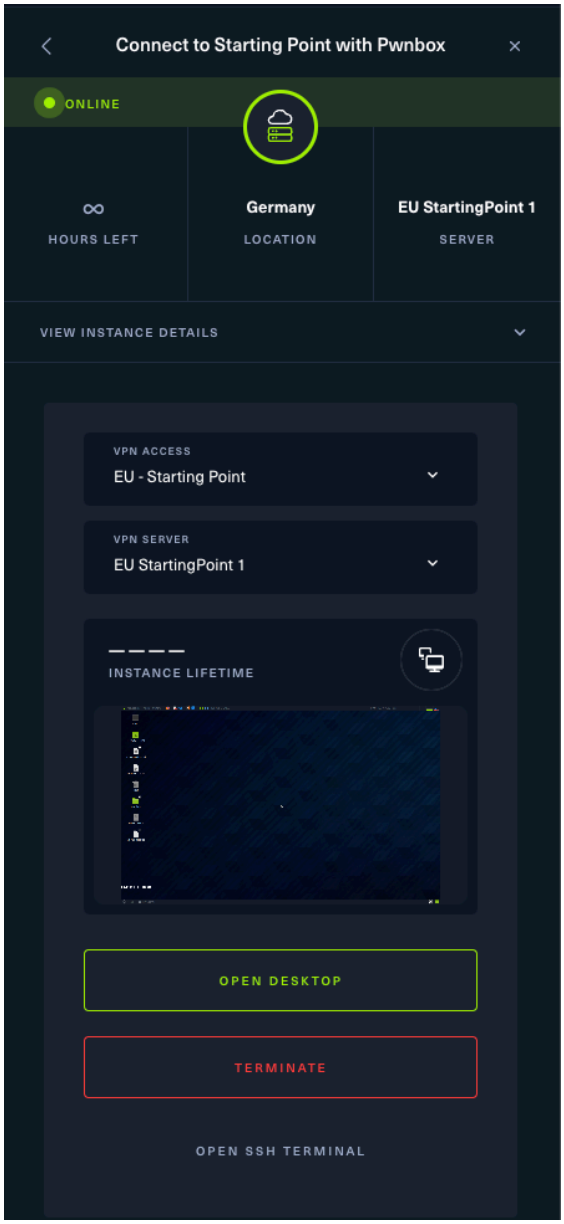
In the machine's dropdown menu, you'll see two options for connecting to the lab.



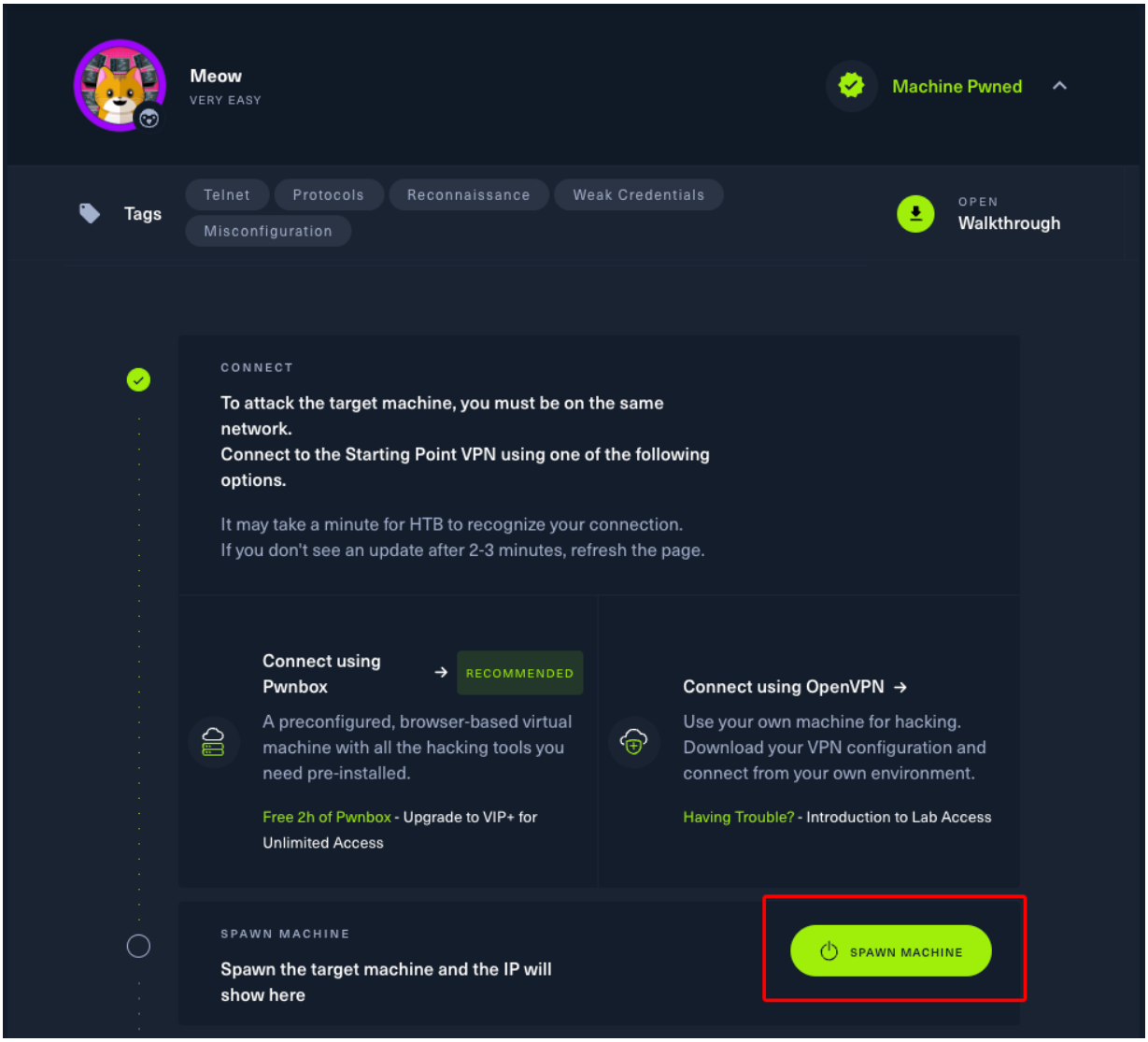
Click on the `Connect using Pwnbox` option to open a tab where you can select a server location. Choose one geographically close to you for lower latency.



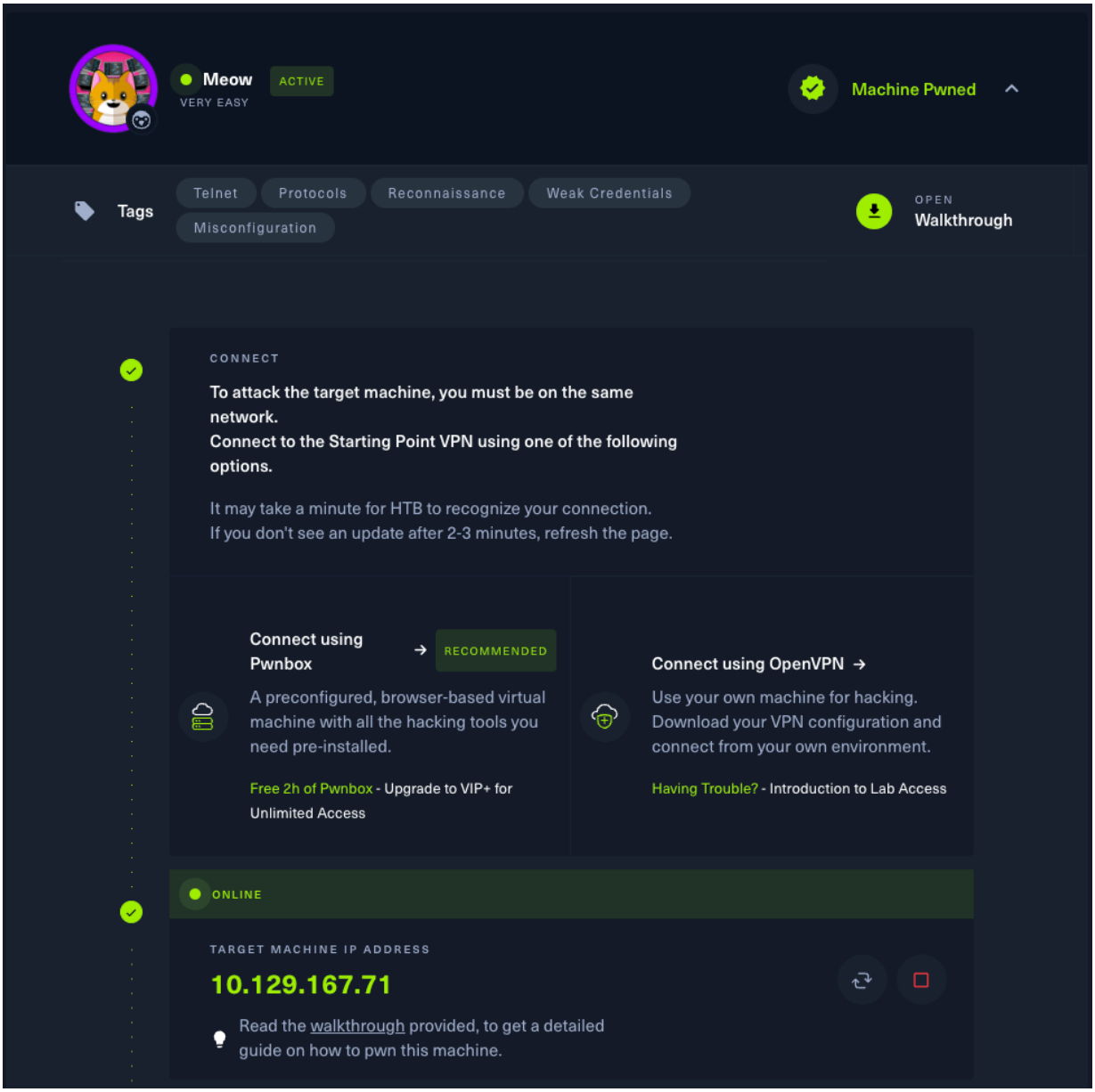
Once you have selected a server, click `START PWNBOX` to spawn the machine. After a few seconds, your dedicated virtual machine will be online.



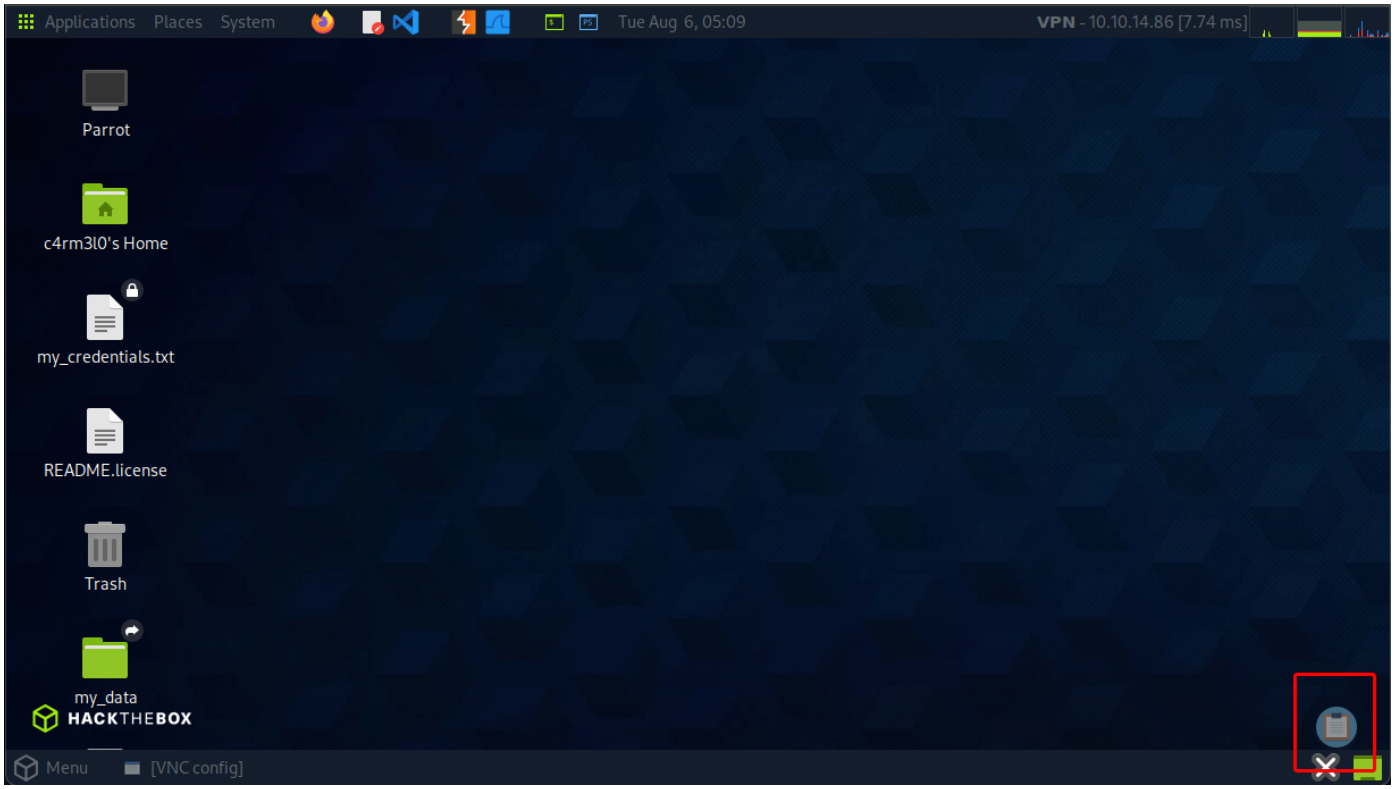
Click on `OPEN DESKTOP` to open a new tab where you can interact with your instance. The last step is to spawn the actual lab machine by clicking on the `SPAWN MACHINE` button in the dropdown menu for `Meow`.



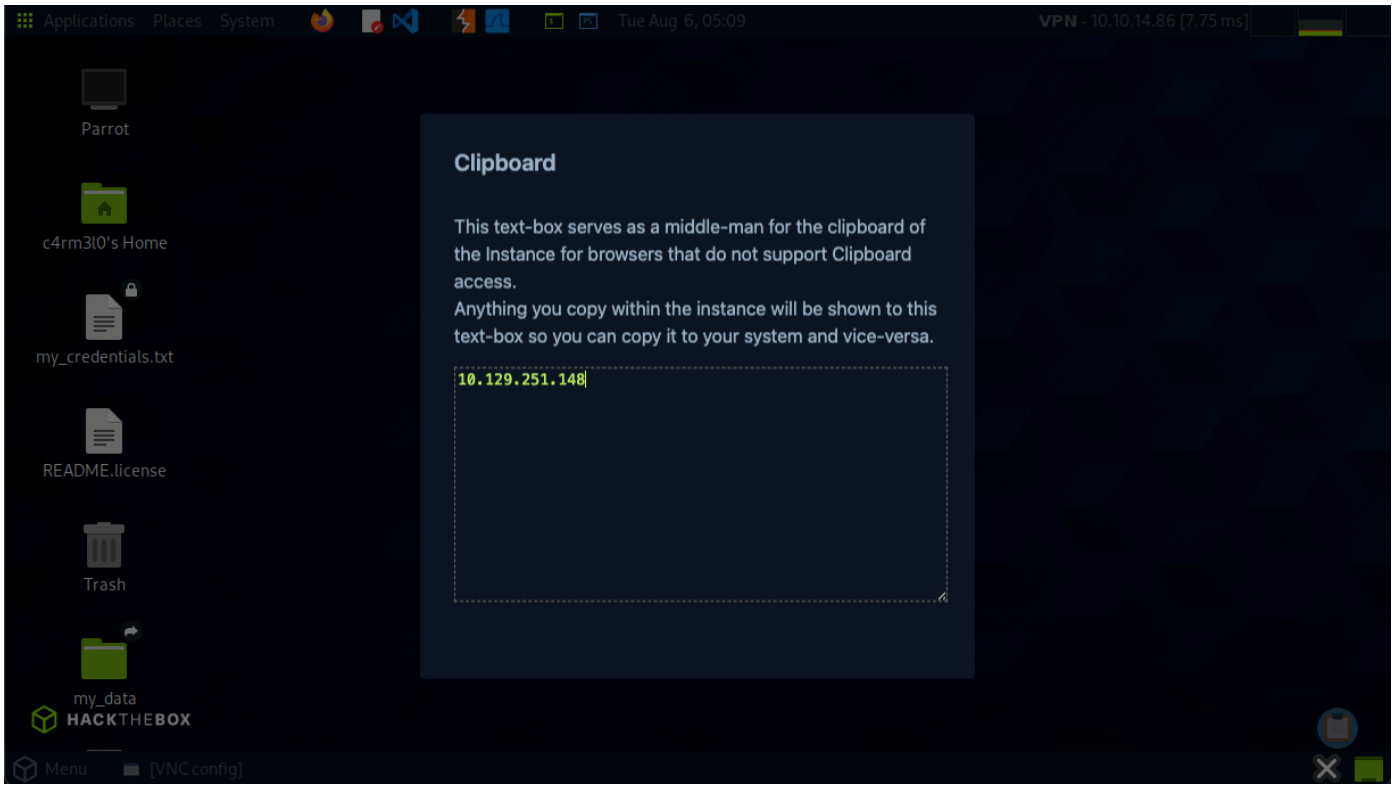
After a few seconds, the target machine will spawn, and you will see its IP address.



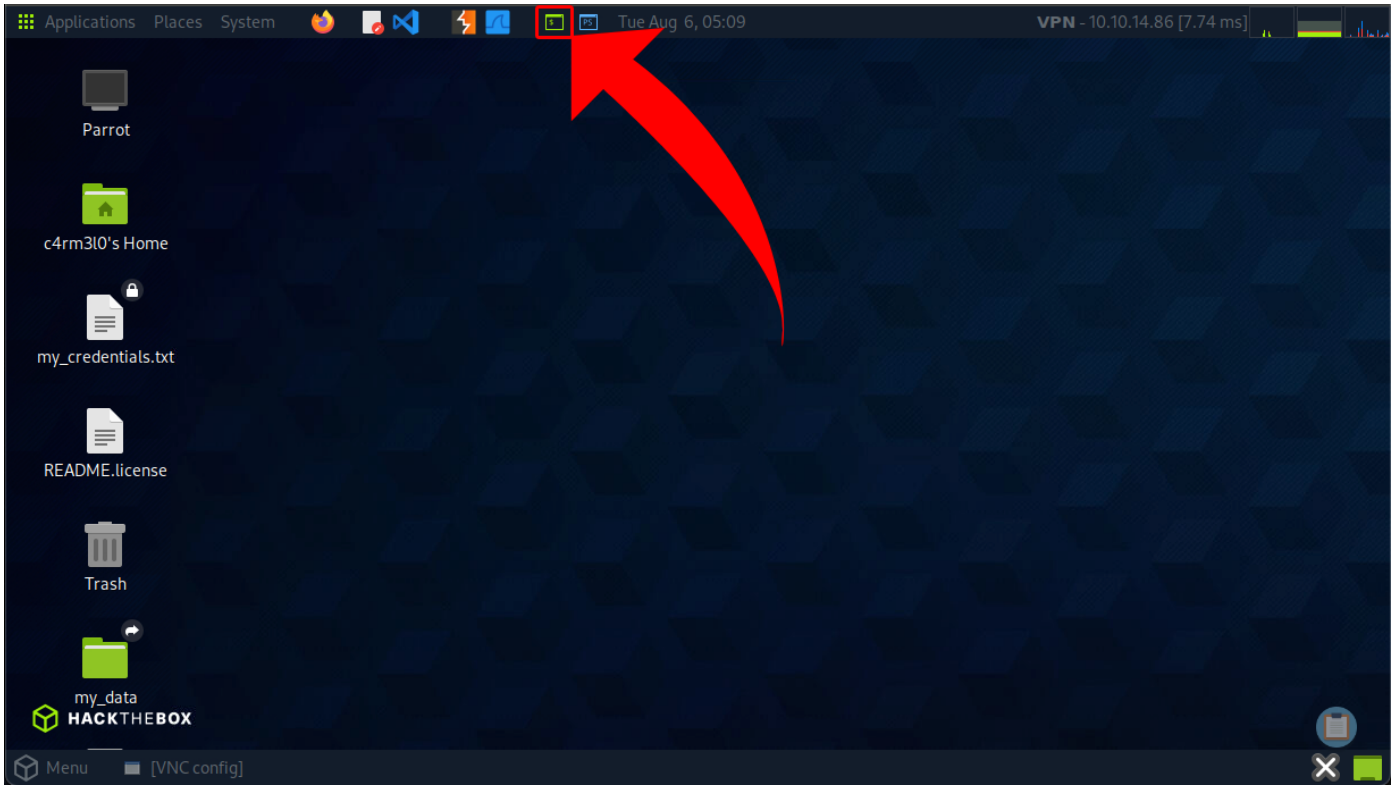
In this case, the IP is `10.129.251.148`, but yours will likely be different. To ensure the lab is set up properly, copy the IP address and return to the Pwnbox tab. In the bottom-right corner, you'll find a clipboard icon:



Clicking on this icon will open a menu where you can copy/paste content to and from Pwnbox. Paste in the target's IP address that you copied earlier.

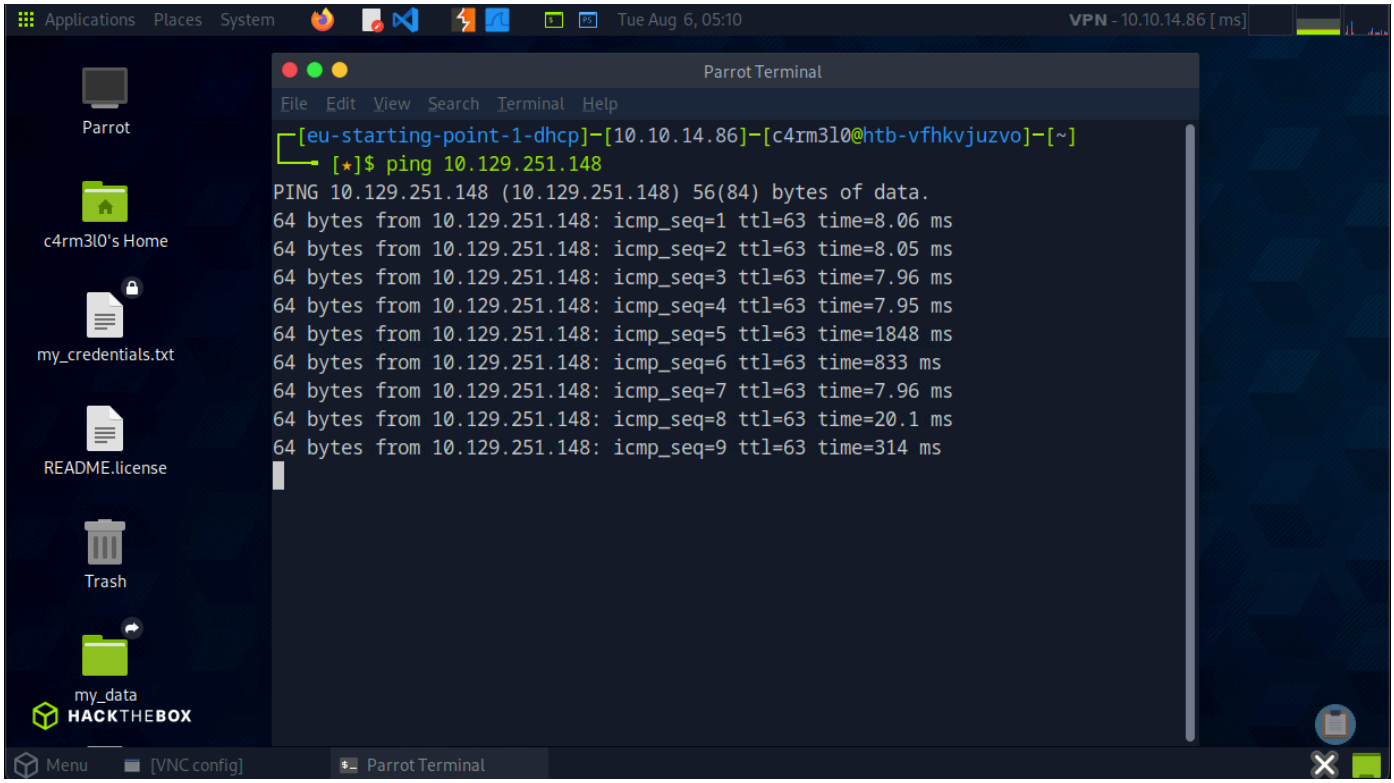


Next, start a terminal by clicking on the green console icon in the navigation bar.



The final step is to check whether you can reach the machine. To test this, ping the target's IP address using the following command:

```
ping {TARGET_IP}
```



If you get responses back like in the screenshot above, you can reach the machine and are ready to start hacking.

For more detailed explanations on Pwnbox and troubleshooting, visit the Introduction to Pwnbox page. Alternatively, if you prefer to set up your own Virtual Machine and connect via `OpenVPN`, check out the Setting Up module on HTB Academy.

Introduction

When first starting a penetration test or any security evaluation on a target, a primary step is known as `Enumeration`. This step consists of documenting the current state of the target to learn as much as possible about it.

Since you are now on the same Virtual Private Network (VPN) as the target, you can directly access it as any user would. If the target is a web server, running a public web page, you can navigate to its IP address to see what the page contains. If the target is a storage server, you can connect to it using the same IP address to explore the files and folders stored on it, provided that you have the necessary credentials. The question is, how do you find these services? You cannot manually search for them because it would take a long time.

Every server uses `ports` in order to serve data to other clients. The first steps in the Enumeration phase involve scanning these open ports to see the purpose of the target on the network and what potential vulnerabilities might appear from the services running on it. In order to quickly scan for ports, we can use a tool called `nmap`, which we will detail more in the Enumeration chapter of this write-up.

After finding the open ports on the target, we can manually access each of them using different tools to find out if we have access to their contents or not. Different services will use different tools or scripts to be accessed. These can be discovered and learned by a beginner penetration tester only with time and practice (and some diligent Googling). 90% of penetration testing consists of research done on the internet about the product you are testing. Since the technological ecosystem is continuously evolving, it is impossible to know everything about everything. The key is to know how to look for the information you need. The ability to research effectively is the skill you need to continuously adapt and evolve into your top quality.

The objective here is not speed but meticulousness. If a resource on the target is missed during the Enumeration phase of your test, you might lose a vital attack vector which would have potentially cut your worktime on the target in half or even less.

Enumeration

After our VPN connection is successfully established, we can ping the target's IP address to see if our packets reach their destination. You can take the IP address of your current target from the Starting Point lab's page and paste it into your terminal after typing in the `ping` command as illustrated below.

```
$ ping {target_IP}

PING {target_IP} ({target_IP}) 56(84) bytes of data.
64 bytes from {target_IP}: icmp_seq=1 ttl=63 time=20.4 ms
64 bytes from {target_IP}: icmp_seq=2 ttl=63 time=22.0 ms
64 bytes from {target_IP}: icmp_seq=3 ttl=63 time=20.2 ms
64 bytes from {target_IP}: icmp_seq=4 ttl=63 time=19.8 ms
^C
--- {target_IP} ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 19.788/20.603/22.026/0.849 ms
```

After four successful replies from the target, we can determine that our connection is formed and stable. We can cancel the ping command by pressing the `CTRL+C` combination on our keyboard, which will be displayed in the terminal as `^C` marked above in green. This will return control of the terminal tab to us, from where we can proceed with the next step - scanning all of the target's open ports to determine the services running on it. In order to start the scanning process, we can use the following command with the `nmap` script. `nmap` stands for Network Mapper, and it will send requests to the target's ports in hopes of receiving a reply, thus determining if the said port is open or not. Some ports are used by default by certain services. Others might be non-standard, which is why we will be using the service detection flag `-sV` to determine the name and description of the identified services. The text marked in green and curly brackets `{}` is a replacement for your own version of input. In this case, you will need to replace the `{target_IP}` part with the IP address of your own target.

```
$ sudo nmap -sV {target_IP}

Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-24 20:36 BST
Nmap scan report for {target_IP}
Host is up (0.050s latency).
Not shown: 999 closed tcp ports (reset)

PORT   STATE SERVICE VERSION
23/tcp open  telnet  Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 1.82 seconds
```

Following the completion of the scan, we have identified `port 23/tcp` in an `open` state, running the `telnet` service. Following a quick Google search of this protocol, we find out that telnet is an old service used for remote management of other hosts on the network. Since the target is running this service, it can receive telnet connection requests from other hosts in the network (such as ourselves). Usually, connection requests through telnet are configured with username/password combinations for increased security. We

can see this is the case for our target, as we are met with a Hack The Box banner and a request from the target to authenticate ourselves before being allowed to proceed with remote management of the target host.

```
$ telnet {target_IP}

Trying {target_IP}...
Connected to {target_IP}.
Escape character is '^]'.

 Hack The Box

Meow login:
```

We will need to find some credentials that work to continue since there are no other ports open on the target that we could explore.

Foothold

Sometimes, due to configuration mistakes, some important accounts can be left with blank passwords for the sake of accessibility. This is a significant issue with some network devices or hosts, leaving them open to simple brute-forcing attacks, where the attacker can try logging in sequentially, using a list of usernames with no password input.

Some typical important accounts have self-explanatory names, such as:

- admin
- administrator
- root

A direct way to attempt logging in with these credentials in hopes that one of them exists and has a blank password is to input them manually in the terminal when the hosts request them. If the list were longer, we could use a script to automate this process, feeding it a wordlist for usernames and one for passwords. Typically, the wordlists used for this task consist of typical people names, abbreviations, or data from previous database leaks. For now, we can resort to manually trying these three main usernames above.

```
Meow login: admin
Password:

Login incorrect
Meow login: administrator
Password:

Login incorrect
Meow login:
```

The first two were not so lucky for us. When things look down, it is essential to keep going, be persistent. We can't succeed unless we attempt all possibilities. Let us try the last one.

```
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 Mon 06 Sep 2021 03:15:22 PM UTC

  System load:  0.0               Processes:             195
  Usage of /:   41.7% of 7.75GB   Users logged in:       0
  Memory usage: 4%                IPv4 address for eth0: {target_IP}
  Swap usage:   0%

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

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


Last login: Wed Jul  7 10:55:01 UTC 2021 on tty1
```

Success! We have logged into the target system. We can now go ahead and take a look around the directory we landed in using the `ls` command. There is a possibility we might find what we are looking for.

```
# ls
flag.txt  snap

# cat flag.txt
b40abdfe23665f766f9c61ecba8a4c19
```

The `flag.txt` file is our target in this case. Most of Hack The Box's targets will have one of these files, which will contain a hash value called `a flag`. The naming convention for these targeted files varies from lab to lab. For example, weekly and retired machines will have two flags, namely `user.txt` and `root.txt`. CTF targets and other labs will have `flag.txt`. Challenges will, most of the time, not contain an actual file, but rather offer you snippets of the flag as you solve it, the respective parts being embedded into the challenge more homogeneously (text hidden in an image, or other examples).

You can read the file to have the hash value displayed in the terminal using the `cat` command. Copying the flag and pasting it into the Starting Point lab's page will grant you ownership of this machine, completing your very first task.

Congratulations!