



SOCAT

BOOTSTRAP



* apprendre autrement

SOCAT

OpenVPN

Most challenges require to get connected to a Virtual Machine (VM) on TryHackMe.

From this point you have two options:

✓ **AttackBox**

AttackBox is nice but comes with several issues. It is very time limited if you're not a premium subscriber, it takes a long time to load and it forces you to keep your web browser open at all time.

✓ **OpenVPN** on your own machine.

OpenVPN gets you directly connected with your machine to TryHackMe network. This way, you can just use your machine with your favorite tools and payload without relying on something else.



You can choose whichever you prefer, this bootstrap will assume that you choose the OpenVPN way.

Pentesting

Starting a machine and /etc/hosts



We will be using this room: Mustacchio.

From OpenVPN, start the machine and get the machine's ip to connect to it.

Active Machine Information			
Title	IP Address	Expires	
Mustacchio V2	10.10.82.166	1h 57m 16s	? Add 1 hour Terminate



If you don't want to use the ever-changing ip, you can simply use the machine name. But to do so, it needs a bit of configuration. Check `/etc/hosts`.

Enumerating ports



First thing you should do is enumerating the ports. Open ports can all be vectors for attacks.

Nmap is a tool designed to do so.

Here is an example of basic use of nmap:

```
Terminal
T-SEC-600> nmap -vv mustacchio.thm -p-
Scanning mustacchio.thm (10.10.82.166) [65535 ports]
Discovered open port ???/tcp on 10.10.82.166
Discovered open port ???/tcp on 10.10.82.166
Discovered open port ???/tcp on 10.10.82.166
```

What open ports do you find ?

Enumerating a website

Among the open ports, let's find one that is a website

First thing to do is manual enumeration, also called the “happy path”, by navigating the website has a normal user to find out potential issues.

This one however, does not have any special visible issues, so let's get back to enumerating more, with a magic tool: **Gobuster**.



```
Terminal
T-SEC-600> gobuster dir -u mustacchio.thm -w common.txt
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://mustacchio.thm
[+] Method: GET
[+] Wordlist: common.txt
2021/12/01 15:56:02 Starting gobuster in directory enumeration mode
/?????? (Status: 301) [Size: 317] [-> http://mustacchio.thm/?????/]
/?????? (Status: 301) [Size: 317] [-> http://mustacchio.thm/?????/]
/?????? (Status: 301) [Size: 317] [-> http://mustacchio.thm/?????/]
2021/12/01 15:56:19 Finished
```

No fancy icon for this tool, but it will allow you to test many routes on a website, including routes that does not have a direct link to it.

Using this tool, can you find the hidden directory?

Password cracking

If all goes well for you, you found a hash for the `admin` user.

A hash is a one-way function, so you can't reverse a hash.

But you can re-hash a list of potential passwords to see if one of them produces the same hash.

For that you need two things:

- ✓ a good dictionary such as `rockyou.txt`
- ✓ a password cracker tool: either John the Ripper or Hashcat, or both.



Both are equally as good, John is sometimes more useful in cracking zip key file, ssh password file, etc... while hashcat can crack a bit faster and more different types of hash.

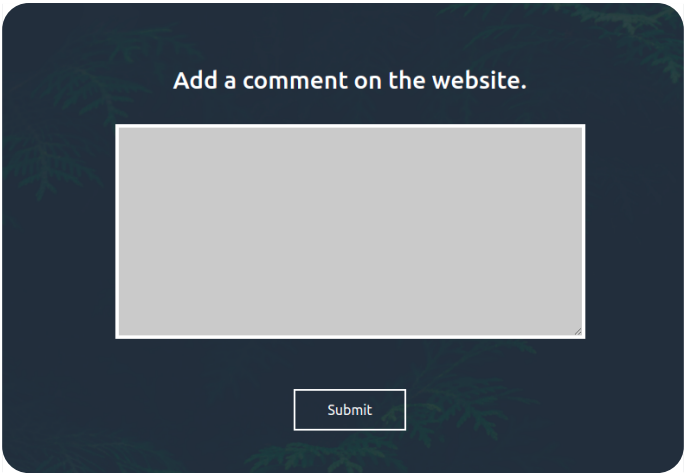
Here is an example of Hashcat:

```
Terminal
T-SEC-600> hashcat -a 0 -m ??? hashes rockyou.txt
1868e36a6d2b17d4c2745f1659433a54d4bc5f4b:????????????
Session.....: hashcat
Status.....: Cracked
Hash.Target.....: 1868e36a6d2b17d4c2745f1659433a54d4bc5f4b
```

Once you find the password, you must find out where to use it.

Common weaknesses and payload

Once logged in on the website, you'll find another point of entry.
Each room will have different way of hacking into the machine, can you identify this one?

A screenshot of a web form. At the top, it says "Add a comment on the website." in white text on a dark blue background. Below this is a large, empty, light gray rectangular box for text input. At the bottom center of the form is a small, white rectangular button with the word "Submit" in black text. The entire form is set against a dark blue background with faint, stylized green leaf patterns.

Once you have exploited this weakness in the website, what can you do with it?
Which file can you read that will be of use to you?

Privilege Escalation

If you made it up to there, congratulations, you are almost done! You should have found the user.txt file.

This proves that you've been able to access the machine instead of just using the web-service.



Now one thing common in boot2root and pentest engagements is going from user to the super admin, root. Every room have different way to do privesc, some obvious, some less obvious and more realistic.

To enumerate yet again the potential weaknesses, we can automate this with a bunch of tools, such as **LinPeas**.

Since you're not on your machine anymore, you have to use scp to copy this tool over ssh or host a simple python server on your machine to fetch it from the compromised host.

Once launched, the script will provide various information about potential weaknesses in the system, potentially allowing a privilege escalation.

In the following example, one can find an unknown SUID binary, which means a custom way to privesc.

```
Terminal
-rwsr-xr-x 1 root root 17K Jun 12 15:48 ???????? (Unknown SUID binary)
```



For more common payload, you can use **gtfobins** to help you find common privesc.

Finish it

With the privesc done, you should now have access to the root flag to validate the whole room, congratulations!

The only way to get better at hacking is by practicing, so work on the **Socat** challenges, read a lot about techniques and tools and train on the easier room on TryHackMe.



{EPITECH}
LEARN DIFFERENT*

* apprendre autrement