

TryHackMe

Intermediate Nmap

Md Tajdar Alam Ansari






Introduction

This is my writeup for Intermediate Nmap. The purpose of this writeup is to document the steps I took to complete Intermediate Nmap, a vulnerable Machine. Which is created by cmnatic in [TryHackMe](#). This room was deployed on 17th September.

Steps are followed

Connect to the TryHackMe network! Please note that this machine could be exploited via attack box and your host Kali and may take a few minutes to boot up.

Deploy machine

Active Machine Information				
Title	IP Address	Expires		
Intermediate Nmap	10.10.207.102	1h 10m 44s		 

This room took me around 30 mins to figure out the process.

Scanning

```
mactavish@kali: ~  
└─(mactavish@kali)-[~]  
└─$ nmap -sC -sV -A -O 10.10.207.102  
TCP/IP fingerprinting (for OS scan) requires root privileges.  
QUITTING!  
  
└─(mactavish@kali)-[~]  
└─$ sudo nmap -sC -sV -A -O 10.10.207.102  
[sudo] password for mactavish:  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-19 00:03 IST  
Nmap scan report for 10.10.207.102  
Host is up (0.17s latency).  
Not shown: 997 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
| 3072 7d:dc:eb:90:e4:af:33:d9:0b:21:9a:fc:d5:77:f2 (RSA)  
| 256 83:a7:4a:61:ef:93:a3:57:1a:57:38:5c:48:2a:eb:16 (ECDSA)  
|_ 256 30:bf:ef:94:08:86:07:00:f7:fc:df:e8:ed:fe:07:af (ED25519)  
2222/tcp  open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
| 3072 cd:6b:77:c1:de:24:3d:24:5f:fc:b8:81:c1:b2:df:b9 (RSA)  
| 256 1a:64:54:f2:f6:0d:4d:7e:81:80:00:1f:1f:47:71:a1 (ECDSA)  
|_ 256 0f:04:de:ef:3d:d8:38:ee:67:19:30:32:a3:14:ef:44 (ED25519)  
31337/tcp open  Elite?  
| fingerprint-strings:  
|_ DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, Kerberos, LANDesk-RC, LDAPBindReq, LDAPSearchReq, LPDString, NULL, RPCCheck, RTSPRequest, SIPOptions, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServer, TerminalServerCookie, X11Probe:  
|_ In case I forget - user:pass  
|_ ubuntu:Dafdas!!/str0ng  
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service:  
e :  
SF-Port31337-TCP:V=7.92%E=4%0=9/19%T=22%CT=1%CU=43668%PV=Y%DS=2%DC=T%G=Y%TM=6327649%P=x86_64-pc-linux-gnu%r(N  
SF:ULL,35,"In\x20case\x20I\x20forget\x20-\x20user:pass\nubuntu:Dafdas!!/st  
SF:0ng\n\n")%r(GetRequest,35,"In\x20case\x20I\x20forget\x20-\x20user:pass  
SF:\nubuntu:Dafdas!!/str0ng\n\n")%r(SIPOptions,35,"In\x20case\x20I\x20forg  
SF:e\t\x20-\x20user:pass\nubuntu:Dafdas!!/str0ng\n\n")%r(GenericLines,35,"I  
SF:n\x20case\x20I\x20forget\x20-\x20user:pass\nubuntu:Dafdas!!/str0ng\n\n"  
SF:%r(HTTPOptions,35,"In\x20case\x20I\x20forget\x20-\x20user:pass\nubuntu  
SF::Dafdas!!/str0ng\n\n")%r(RTSPRequest,35,"In\x20case\x20I\x20forget\x20-
```

Here I saw something like user:pass ubuntu:Dafdas!!/str0ng

And an unusual port 31337 running some service called Elite?

Upon some research I unnecessarily and unknowingly went down a rabbit hole

31337 elite exploit

About 5,270 results (0.34 seconds)

<https://www.exploit-db.com/exploits/>

Linux/x64 - Bind (31337/TCP) Shell Shellcode (150 bytes)

04-Oct-2012 — Linux/x64 - Bind (31337/TCP) Shell Shellcode (150 bytes).. shellcode exploit for Linux_x86-64 platform.

<https://answers.microsoft.com/windows/forum/all/>

Port 31337 - "Elite"; Is this a hack tool? - Microsoft Community

23-Feb-2016 · 1 post

I looked around the internet and found that is port is associated with trojans and BackOrifice (which is a backdoor **hack** tool). Now I am not ...

<https://www.computerworld.com/article/on-getting-...>

On getting cracked and recovering with NMAP - Computerworld

NMAP uses the service name "Elite" for anything running on port 31337. Port 31337 is the one Back Orifice most often uses. The handwriting was on the wall.

<https://www.speedguide.net/port/port=31337>

Port 31337 (tcp/udp) - SpeedGuide

Port(s)	Protocol	Service	Source
31337	tcp,udp	Back Orifice	SG
31337	tcp		Wikipedia
31337	tcp	trojan	Trojans

View 34 more rows

<https://isc.sans.edu/diary/>

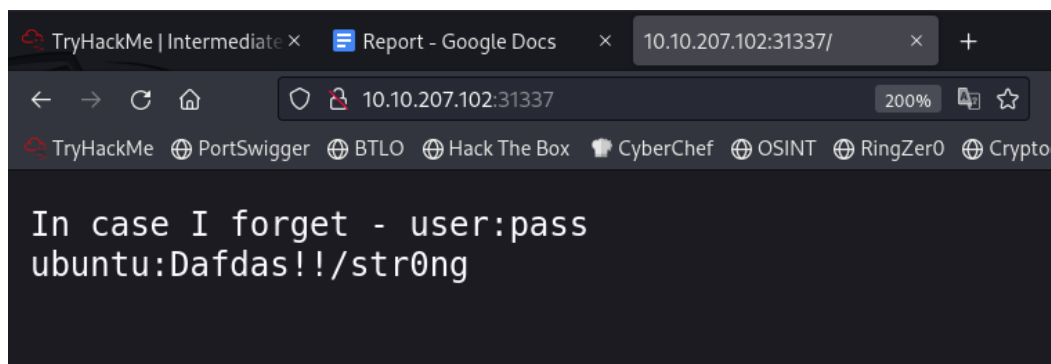
Cyber Security Awareness Month - Day 5 port 31337

Started researching on 31337 and was a lost cause. Eventually started focussing on other ports which ran on ssh and again port 22 was a dead end for me. When I realized that there was another port open port 2222.

```
mactavish@kali: ~  
mactavish@kali)-[~]  
$ ssh nubuntu@10.10.207.102  
The authenticity of host '10.10.207.102 (10.10.207.102)' can't be established.  
ED25519 key fingerprint is SHA256:8VuYgtc5l02sXK+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 '10.10.207.102' (ED25519) to the list of known hosts.  
nubuntu@10.10.207.102's password:  
Permission denied, please try again.  
nubuntu@10.10.207.102's password:  
Permission denied, please try again.  
nubuntu@10.10.207.102's password:
```

```
mactavish@kali: ~  
mactavish@kali)-[~]  
$ wget http://10.10.207.102:2222/  
--2022-09-19 00:27:42-- http://10.10.207.102:2222/  
Connecting to 10.10.207.102:2222... connected.  
HTTP request sent, awaiting response... 200 No headers, assuming HTTP/0.9  
Length: unspecified  
Saving to: 'index.html'  
  
index.html [ <> ] 41 --.-KB/s in 0s  
  
2022-09-19 00:27:42 (832 KB/s) - Read error at byte 41 (Connection reset by peer).Retrying.  
  
--2022-09-19 00:27:43-- (try: 2) http://10.10.207.102:2222/  
Connecting to 10.10.207.102:2222... connected.  
HTTP request sent, awaiting response... 200 No headers, assuming HTTP/0.9  
Length: unspecified  
Saving to: 'index.html'
```

Found some webpage hosted there on port 31117 which had something on the website.



This I found earlier when scanning.

```
mactavish@kali: ~  
mactavish@kali)~  
$ cat index.html  
SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.4  
mactavish@kali)~  
$ ssh 10.10.207.102 -p 2222  
The authenticity of host '[10.10.207.102]:2222 ([10.10.207.102]:2222)' can't be established.  
ED25519 key fingerprint is SHA256:zri8Enf5uf+Z6yWebZ0Sy4rWW5MdRkytw2bJfZlg8VU.  
This key is not known by any other names  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '[10.10.207.102]:2222' (ED25519) to the list of known hosts.  
mactavish@10.10.207.102: Permission denied (publickey).
```

It was time to get into ssh using the user ID and password but port 2222 was restricted, confirming that it runs ssh service. Moving on to port 22.

And voila we are in!

```
mactavish@kali: ~  
mactavish@kali)~  
$ ssh ubuntu@10.10.207.102  
ubuntu@10.10.207.102'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.  
  
The programs included with the Ubuntu system are free software;  
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.  
$ ls
```

```
mactavish@kali: ~  
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.  
  
The programs included with the Ubuntu system are free software;  
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.  
$ ls  
$ cd  
$ cd  
$ ls  
$ ls -la  
total 28  
drwxr-xr-x 1 ubuntu ubuntu 4096 Sep 18 19:01 .  
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 Sep 18 19:01 .cache  
-rw-r--r-- 1 ubuntu ubuntu 807 Feb 25 2020 .profile  
$ cd ..  
$ ls  
ubuntu user  
$ cd user  
$ ls  
flag.txt  
$ cat flag.txt
```

And there we have our flag.

flag{251f309497a18888dde5222761ea88e4}