

NETWORKING

INTRODUCTION:

Enumeration is the process simply put of, finding as many ways as possible to attack a particular machine/network. Consequently, I want to work on the breadth of my enumeration and exhausting all possible attack vectors. Ultimately in pentesting you are trying to find all possible vulnerabilities in a network, not just one.

+ 1 📦 Based on the last result, find out which operating system it belongs to. Submit the name of the operating system as result.

windows

TTL can help us determine the operating system, and by default, window OS = 128

linux OS = 64

mac OS = 64

Having this knowledge, I managed to determine the OS as windows.

+ 1 📦 Find all TCP ports on your target. Submit the total number of found TCP ports as the answer.

7

I ran an nmap scan of all the ports, and here was the output as shown below.

PORT	STATE	SERVICE
22/tcp	open	ssh
80/tcp	open	http
110/tcp	open	pop3
139/tcp	open	netbios-ssn
143/tcp	open	imap
445/tcp	open	microsoft-ds
31337/tcp	open	Elite

+ 1 📦 Enumerate the hostname of your target and submit it as the answer. (case-sensitive)


nix-nmap-default

To enumerate the hostname, I ran a nmap script for hostname discovery just as shown in the image below.

```
—(root@Kali)-[/home/scr34tur3]
—# nmap --script smb-os-discovery 10.129.168.252
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-29 13:33 EAT
Nmap scan report for 10.129.168.252
Host is up (0.16s latency).
Not shown: 987 closed tcp ports (reset)
PORT      STATE      SERVICE
22/tcp    open      ssh
80/tcp    open      http
110/tcp   open      pop3
139/tcp   open      netbios-ssn
143/tcp   open      imap
445/tcp   open      microsoft-ds
999/tcp   filtered  garcon
1010/tcp  filtered  surf
3871/tcp  filtered  avocent-adsap
5221/tcp  filtered  3exmp
8031/tcp  filtered  unknown
81337/tcp open      Elite
82778/tcp filtered  sometimes-rpc19

Host script results:
  smb-os-discovery:
    OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
    Computer name: nix-nmap-default
    NetBIOS computer name: NIX-NMAP-DEFAULT\x00
    Domain name: \x00
    FQDN: nix-nmap-default
    _ System time: 2024-05-29T12:33:20+02:00

Nmap done: 1 IP address (1 host up) scanned in 6.08 seconds
```

+ 1  Enumerate all ports and their services. One of the services contains the flag you have to submit as the answer.

HTB{pr0F7pDv3r510nb4nn3r}

```
(root@Kali)-[/home/scr34tur3]
# nmap --min-rate 1000 -p- -A 10.129.97.166
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-29 14:16 EAT
Warning: 10.129.97.166 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.129.97.166
Host is up (0.24s latency).
Not shown: 65352 closed tcp ports (reset), 176 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 71:c1:89:90:7f:fd:4f:60:e0:54:f3:85:e6:35:6c:2b (RSA)
|   256 e1:8e:53:18:42:af:2a:de:c0:12:1e:2e:54:06:4f:70 (ECDSA)
|_  256 1a:cc:ac:d4:94:5c:d6:1d:71:e7:39:de:14:27:3c:3c (ED25519)
80/tcp    open  http         Apache httpd 2.4.29 ((Ubuntu))
|_ http-title: Apache2 Ubuntu Default Page: It works
|_ http-server-header: Apache/2.4.29 (Ubuntu)
110/tcp   open  pop3         Dovecot pop3d
|_ pop3-capabilities: PIPELINING SASL UIDL AUTH-RESP-CODE CAPA TOP RESP-CODES
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap         Dovecot imapd (Ubuntu)
|_ imap-capabilities: have listed post-login more Pre-login IDLE capabilities OK LITERAL+ SASL-IR LOGIN-REFERRALS IMAP4rev1 LOGINDISABLEDA0001 ENABLE ID
445/tcp   open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
31337/tcp open  Elite?
|_ fingerprint-strings:
|   GetRequest:
|_    220 HTB{pr0F7pDv3r510nb4nn3r}
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 :
SF-Port31337-TCP:V=7.94SVN%I=7%D=5/29%Time=66570EDE%P=x86_64-pc-linux-gnu%
SF:r(GetRequest,1F,"220\x20HTB{pr0F7pDv3r510nb4nn3r}\r\n");
```

+ 1  Use NSE and its scripts to find the flag that one of the services contain and submit it as the answer.

HTB{873nniuc71bu6usbs1i96as6dsv26}

Running an nmap script to enumerate port 80, I found a directory /robots.txt just as shown below.

```
(root@Kali)-[/home/scr34tur3]
# nmap --script http-enum -p 80 --min-rate 1000 10.129.18.228
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-31 07:16 EAT
Nmap scan report for 10.129.18.228
Host is up (1.0s latency).

PORT      STATE SERVICE
80/tcp    open  http
| http-enum:
|_ /robots.txt: Robots file

Nmap done: 1 IP address (1 host up) scanned in 29.82 seconds
```

visiting that path url I find this flag.

```
(root@Kali)-[/home/scr34tur3]
# cat robots.txt-flag

HTB{873nniuc71bu6usbs1i96as6dsv26}
```

+1 🟢 Perform a full TCP port scan on your target and create an HTML report. Submit the number of the highest port as the answer.

31337

From my initial nmap scan to find all tcp ports on the target, I found port 31337 to be the highest port.

```
(root@Kali)-[/home/scr34tur3]
# nmap -p- --min-rate 1000 10.129.18.228
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-31 08:10 EAT
Warning: 10.129.18.228 giving up on port because retransmission cap hit (10)
Nmap scan report for 10.129.18.228
Host is up (0.15s latency).
Not shown: 65525 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
110/tcp   open  pop3
139/tcp   open  netbios-ssn
143/tcp   open  imap
445/tcp   open  microsoft-ds
31337/tcp open  Elite
37485/tcp filtered unknown
37980/tcp filtered unknown
44270/tcp filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 79.09 seconds
```

+1 🟢 Our client wants to know if we can identify which operating system their provided machine is running on. Submit the OS name as the answer.

Ubuntu

```
(root@Kali)-[/home/scr34tur3]
# nmap --min-rate 1000 -sV 10.129.161.213
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-31 08:30 EAT
Nmap scan report for 10.129.161.213
Host is up (0.20s latency).
Not shown: 869 closed tcp ports (reset), 128 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.29 ((Ubuntu))
10001/tcp open  scp-config?
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 :
SF-Port10001-TCP:V=7.94SVN%I=7%D=5/31%Time=66596081%P=x86_64-pc-linux-gnu%
SF:r(GetRequest,1F,"220\x20HTB{pr0F7pDv3r510nb4nn3r}\r\n");
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 184.86 seconds
```


+ 1 🟢 After the configurations are transferred to the system, our client wants to know if it is possible to find out our target's DNS server version. Submit the DNS server version of the target as the answer.

HTB{GoTtgUnyze9Psw4vGjcuMpHRp}

So I decided to use a different approach to find this flag. Instead of running an nmap scan, I used dig to dig for dns server version just as shown in the image below.

```
(root@Kali)-[/home/scr34tur3]
# dig @10.129.2.48 version.bind CH TXT
;; communications error to 10.129.2.48#53: timed out
;; communications error to 10.129.2.48#53: timed out

; <<>> DiG 9.19.21-1+b1-Debian <<>> @10.129.2.48 version.bind CH TXT
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59523
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags;; udp: 4096
; COOKIE: adebef46be95dc50663e02ff66596472940970f2674f84a2 (good)
;; QUESTION SECTION:
;version.bind.                CH      TXT

;; ANSWER SECTION:
version.bind.                0      CH      TXT      "HTB{GoTtgUnyze9Psw4vGjcuMpHRp}"

;; AUTHORITY SECTION:
version.bind.                0      CH      NS      version.bind.

;; Query time: 159 msec
;; SERVER: 10.129.2.48#53(10.129.2.48) (UDP)
;; WHEN: Fri May 31 08:47:31 EAT 2024
;; MSG SIZE rcvd: 126
```

+ 2 🟢 Now our client wants to know if it is possible to find out the version of the running services. Identify the version of service our client was talking about and submit the flag as the answer.

HTB{kjnsdf2n982n1827eh76238s98di1w6}

This task hinted at large amounts of data and so a full port scan (-p-) reveals port 50000. Above we set up a netcat listener between DNS port 53 and this new mysterious port 50000. Let the netcat listener run for a second or two and the flag presents itself with a successful 220 request.

```
(root@Kali)-[/home/scr34tur3]  
# nc -nv -p 53 10.129.36.237 50000  
UNKNOWN) [10.129.36.237] 50000 (?) open  
220 HTB{kjnsdf2n982n1827eh76238s98di1w6}
```

Great job SCr34tur3!




Network Enumeration with Nmap

Congratulations **SCr34tur3!**

You have just completed the Network Enumeration with Nmap module!

Let's share your success with everyone!

 Share on LinkedIn

 Share on X

 Share on Facebook



Get a shareable link

<https://academy.hackthebox.com/achievement/1287818/19>

CONCLUSION

This module required a lot of outside research, but I feel it's part of the job. It's not a memory of everything game, but knowing where to look for the tool you need to do the job you want.