

Network Enumeration with Nmap: HackTheBox

Name: Daniel Mwendwa Mwithui

ADMNO. CS-SA04-23080

Program: Security Analyst

Date of submission: 16th June 2023

Introduction:

This report will introduce us to the Network Enumeration module offered by HackTheBox Academy. The module focuses on utilizing Nmap, a powerful network scanning tool, to conduct various enumeration tasks. Throughout this module, we will explore essential concepts such as host discovery, host and port scanning, saving results in Nmap, service enumeration, utilizing the Nmap Scripting Engine, and understanding firewall and IDS/IPS evasion techniques.

Task 1: Host Discovery

Host discovery, also known as host enumeration, is a critical step in network enumeration using Nmap (Network Mapper). It involves identifying active hosts on a network by sending various probe packets and analyzing the responses received. During host discovery, Nmap employs different techniques to determine the presence of live hosts. These techniques typically include sending ICMP (Internet Control Message Protocol) Echo Requests (commonly known as "ping") and analyzing the responses.

To complete this section, research in the different Time to live (TTL) offered by different OS. In this case, TTL = 128, which is the value for TTL in windows.

Task 2: Host and Port Scanning.

Host scanning is the process of identifying open and active hosts on a network. Nmap uses the command **nmap -sn <target>** for host scanning, where **-sn** specifies a "ping scan" to determine live hosts.

Port scanning is the act of scanning a host to identify open ports and the services running on them. Nmap employs the command **nmap -p <port(s)> <target>** for port scanning, where **-p** specifies the port(s) to scan. For example, **nmap -p 80,443 <target>** scans ports 80 and 443 on the specified target.

To complete this section, do **nmap <target> -sT** command which performs a TCP connect scan on the specified target. It establishes a full TCP connection with the target's ports to determine their open or closed state. See the screenshot below.

```
[eu-academy-2]-[10.10.15.49]-[htb-ac-820341@htb-v9ehn9skau]-[~]
[*]$ nmap 10.129.113.131 -sT
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-16 12:44 BST
Nmap scan report for 10.129.113.131
Host is up (0.035s latency).
Not shown: 993 closed tcp ports (conn-refused)
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

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
```

To get the hostname info, you can try a number of commands like **nmap -sC -sV <target>** or **sudo nmap -sR <target>**. Here I used **nmap -sR <target>** command. The **-sR** flag in Nmap enables reverse DNS resolution, which attempts to retrieve and display the hostname associated with the scanned IP addresses. This option allows you to see the hostnames of the target systems. See the screenshot below.

```
Parrot Terminal
File Edit View Search Terminal Help
[eu-academy-2]-[10.10.15.49]-[htb-ac-820341@htb-v9ehn9skau]-[~]
[*]$ sudo nmap -sR 10.129.78.14
WARNING: -sR is now an alias for -sV and activates version detection as well as
RPC scan.
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-16 13:08 BST
Nmap scan report for 10.129.78.14
Host is up (0.055s latency).
Not shown: 993 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; prot
ocol 2.0)
80/tcp    open  http         Apache httpd 2.4.18 ((Ubuntu))
110/tcp   open  pop3         Dovecot pop3d
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap         Dovecot imapd
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
31337/tcp open  Elite?
Service Info: Host: NIX-NMAP-DEFAULT; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Task 3: Saving Results in Nmap

In Nmap, saving results refers to the process of storing the output of a scan in a file for future reference or analysis. It allows you to capture and preserve the information gathered during the scan, such as discovered hosts, open ports, and service details. Saving results enables you to review the scan data later or share it with others.

To solve this section, do command `nmap -p- -sT -oX scan_results.xml <target>`. This will save the results of the full TCP scan scan_results as xml file. To convert this file to html, use the command `xsltproc scan_results.xml -o scan_results.html`. xsltproc is a tool that converts xml files to html.

```
File Edit View Search Terminal Help
[eu-academy-2]-[10.10.15.49]-[htb-ac-820341@htb-v9ehn9skau]-[~]
[*]$ nmap -p- -sT -oX scan_results.xml 10.129.78.14
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-16 13:31 BST
Nmap scan report for 10.129.78.14
Host is up (0.079s latency).
Not shown: 65528 closed tcp ports (conn-refused)
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

Nmap done: 1 IP address (1 host up) scanned in 34.65 seconds
[eu-academy-2]-[10.10.15.49]-[htb-ac-820341@htb-v9ehn9skau]-[~]
[*]$ ls
Desktop  scan_results.xml  Templates
[eu-academy-2]-[10.10.15.49]-[htb-ac-820341@htb-v9ehn9skau]-[~]
```

```
[eu-academy-2]-[10.10.15.49]-[htb-ac-820341@htb-v9ehn9skau]-[~]
[*]$ xsltproc scan_results.xml -o scan_results.html
[eu-academy-2]-[10.10.15.49]-[htb-ac-820341@htb-v9ehn9skau]-[~]
[*]$ ls
Desktop  scan_results.html  scan_results.xml  Templates
```

Open the .html file on browser

10.129.78.14

Address

- 10.129.78.14 (ipv4)

Ports

The 65528 ports scanned but not shown below are in state: **closed**

- 65528 ports replied with: **conn-refused**

Port	State (toggle closed [0] filtered [0])	Service	Reason	Product	Version	Extra info
22	tcp open	ssh	syn-ack			
80	tcp open	http	syn-ack			
110	tcp open	pop3	syn-ack			
139	tcp open	netbios-ssn	syn-ack			
143	tcp open	imap	syn-ack			
445	tcp open	microsoft-ds	syn-ack			
31337	tcp open	Elite	syn-ack			

Misc Metrics (click to expand)

Task 4: Service Enumeration

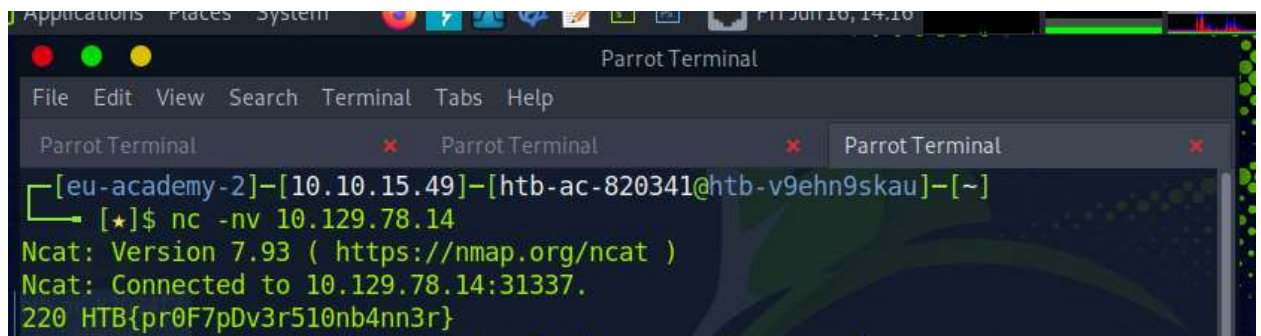
Service enumeration in Nmap means finding out what programs or services are running on a target computer and gathering information about them. It helps to know the software versions and configurations of those services, which can reveal potential vulnerabilities and the overall security of the system. Nmap does this by sending specific requests and analyzing the responses it receives to gather information about the services running on the target computer.

To solve this section, you run a number of commands. First do, *sudo nmap <target> -p- -sV -Pn -n --disable-arp-ping --packet-trace* which performs a detailed scan of all ports on the specified IP address, attempts to identify service versions, treats the target as online, disables DNS resolution, skips ARP ping, and provides a detailed packet trace for the network traffic. Secondly, run the *sudo tcpdump -i eth0 host <ipaddress> and <target>* command that captures and displays network traffic between the network IP addresses and the target on the eth0 interface. Lastly do *nc -nv <target>*. This command initiates a TCP connection to the specified IP

address, allowing you to interact with services or applications running on that system. This lists the flag to answer this section. See the screenshots below for the three commands.

```
[eu-academy-2]-[10.10.15.49]-[htb-ac-820341@htb-v9ehn9skau]-[~]
[*]$ sudo nmap 10.129.78.14 -p- -sV -Pn -n --disable-arp-ping --packet-trace
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-16 14:03 BST
SENT (0.2919s) TCP 10.10.15.49:50855 > 10.129.78.14:445 S ttl=59 id=53670 iplen=
44 seq=570609208 win=1024 <mss 1460>
SENT (0.2919s) TCP 10.10.15.49:50855 > 10.129.78.14:111 S ttl=58 id=29509 iplen=
44 seq=570609208 win=1024 <mss 1460>
SENT (0.2919s) TCP 10.10.15.49:50855 > 10.129.78.14:199 S ttl=58 id=41597 iplen=
44 seq=570609208 win=1024 <mss 1460>
SENT (0.2920s) TCP 10.10.15.49:50855 > 10.129.78.14:8080 S ttl=44 id=36061 iplen=
44 seq=570609208 win=1024 <mss 1460>
SENT (0.2920s) TCP 10.10.15.49:50855 > 10.129.78.14:1723 S ttl=55 id=51194 iplen=
44 seq=570609208 win=1024 <mss 1460>
SENT (0.2920s) TCP 10.10.15.49:50855 > 10.129.78.14:256 S ttl=52 id=28172 iplen=
44 seq=570609208 win=1024 <mss 1460>
```

```
[eu-academy-2]-[10.10.15.49]-[htb-ac-820341@htb-v9ehn9skau]-[~]
[*]$ sudo tcpdump -i eth0 host 10.10.15.49 and 10.129.78.14
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```



The screenshot shows a Parrot Terminal window with three tabs. The active tab shows the following command and output:

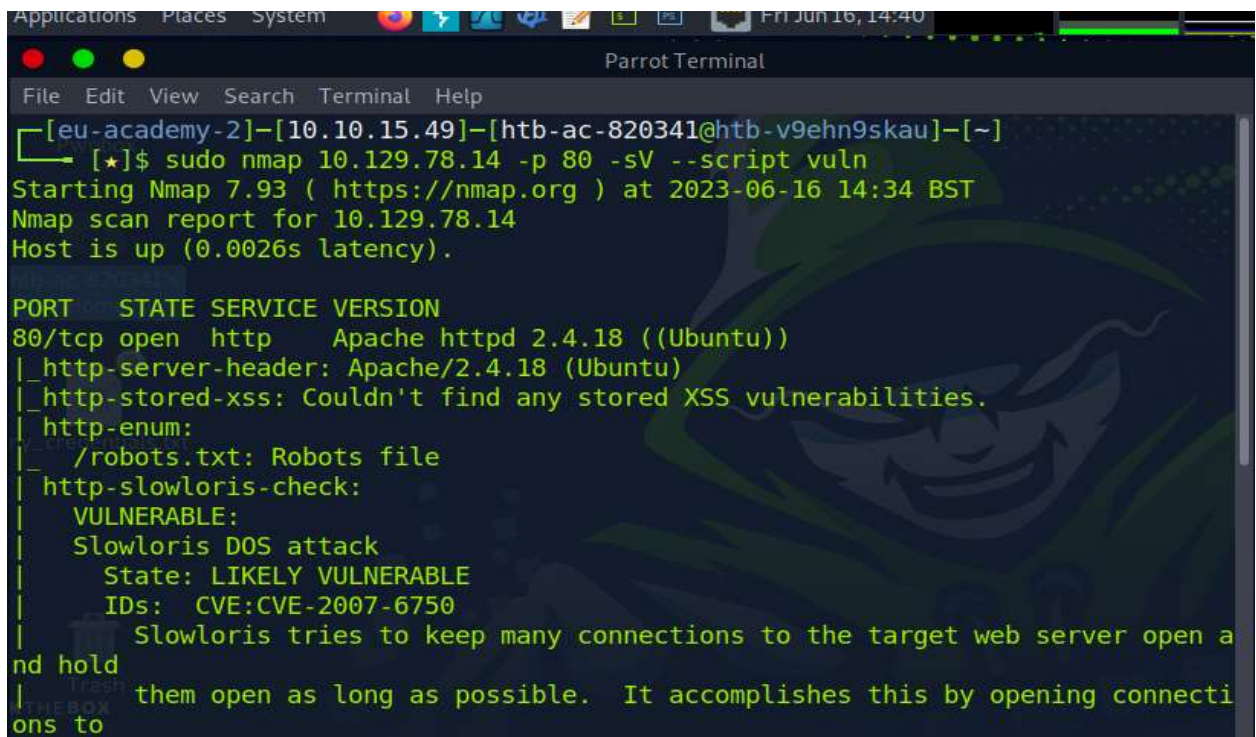
```
[eu-academy-2]-[10.10.15.49]-[htb-ac-820341@htb-v9ehn9skau]-[~]
[*]$ nc -nv 10.129.78.14
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Connected to 10.129.78.14:31337.
220 HTB{pr0F7pDv3r510nb4nn3r}
```

Task 5: Nmap Scripting Engine

The Nmap Scripting Engine is a powerful feature of Nmap that allows users to automate and extend the functionality of the scanning tool. It provides a wide range of pre-built scripts that

can be used for various purposes, such as vulnerability detection, service enumeration, and network discovery. These scripts can be used to perform targeted scans, gather additional information about the target, or even exploit known vulnerabilities. The Nmap Scripting Engine offers flexibility and customization options, enabling users to write and execute their own scripts, making it a valuable tool for network security assessments and penetration testing.

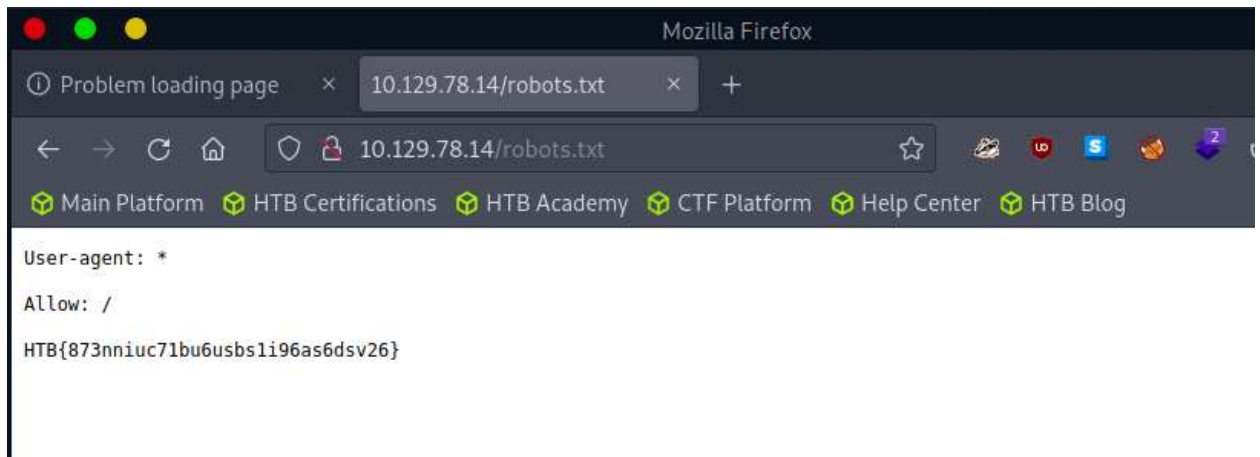
To complete this section, do the `sudo nmap <target> -p 80 -sV --script vuln` that scans the target IP address on port 80, detects the service version, and performs vulnerability scanning using Nmap scripts specifically designed to identify vulnerabilities associated with the target system.



```
[eu-academy-2]-[10.10.15.49]-[htb-ac-820341@htb-v9ehn9skau]-[~]
[*]$ sudo nmap 10.129.78.14 -p 80 -sV --script vuln
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-16 14:34 BST
Nmap scan report for 10.129.78.14
Host is up (0.0026s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-enum:
|_   /robots.txt: Robots file
|_ http-slowloris-check:
|_   VULNERABLE:
|_     Slowloris DOS attack
|_       State: LIKELY VULNERABLE
|_       IDs: CVE:CVE-2007-6750
|_       Slowloris tries to keep many connections to the target web server open a
nd hold
|_       them open as long as possible. It accomplishes this by opening connecti
ons to
```

Identify the robots.txt. use target/robots.txt on browser to view the file.



Task 6: Firewall and IDS/IPS Evasion

Firewall evasion on nmap involves techniques like fragmentation, timing, and port manipulation to bypass or circumvent firewall security measures. IDS/IPS evasion on nmap involves methods such as traffic fragmentation, TCP/IP stack fingerprinting, slow scanning, delays, and traffic obfuscation to avoid detection by intrusion detection and prevention systems.

This section involves solving a lab ranging from easy to hard lab. The `nmap -sC -sV <target>` command helped me to solve the simple lab in this section as shown below.

```
[ed-academy-2]~[10.10.14.155]~[htb-ac-820341@htb-nvewunch19]~[~]
[*]$ nmap -sC -sV 10.129.2.80
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-17 17:36 BST
Nmap scan report for 10.129.2.80
Host is up (0.014s latency).
Not shown: 869 closed tcp ports (conn-refused), 128 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 71c189907ffd4f60e054f385e6356c2b (RSA)
|   256 e18e531842af2adec0121e2e54064f70 (ECDSA)
|_  256 1accacd4945cd61d71e739de14273c3c (ED25519)
```

The medium lab can be solved using the command `sudo nmap -sSU -p 53 --script dns-nsid <target>`. This command conducts a network scan on the target, specifically targeting port 53, using both TCP and UDP protocols. It also runs the "dns-nsid" script to determine if the DNS server supports the NSID feature. See the screenshot below.

```
[eu-academy-2]-[10.10.14.153]-[htb-ac-820341@htb-nvewuhcnf9]-[~]
[*]$ sudo nmap -sSU -p 53 --script dns-nsid 10.129.2.48
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-17 17:51 BST
Nmap scan report for 10.129.2.48
Host is up (0.0058s latency).

PORT      STATE      SERVICE
53/tcp    filtered  domain
53/udp    open       domain
| dns-nsid:
|_  bind.version: HTB{GoTtgUnyze9Psw4vGjcuMpHRp}

Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds
[eu-academy-2]-[10.10.14.153]-[htb-ac-820341@htb-nvewuhcnf9]-[~]
```

The hard lab in this section can be solved using the command `sudo nc -nv -p 53 <target> 50000` which initiates a connection from the local machine's port 53 to the remote IP address 10.129.99.25 on port 50000 using the netcat utility. We use the port 53 which is the port associated with DNS and 50000 which is the hinted port. See the screenshot below.

```
[eu-academy-2]-[10.10.14.153]-[htb-ac-820341@htb-nvewuhcnf9]-[~]
[*]$ sudo nc -nv -p 53 10.129.99.25 50000
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Connected to 10.129.99.25:50000.
220 HTB{kjnsdf2n982n1827eh76238s98di1w6}
```

Completion:

See the completion screenshot and the sharable link.



Link: <https://academy.hackthebox.com/achievement/820341/19>

Conclusion

In conclusion, the Network Enumeration module on HackTheBox Academy has been a valuable learning experience. I acquired practical skills in network scanning and enumeration using Nmap, learned how to save and analyze scan results, explored the Nmap Scripting Engine, and gained insights into overcoming network security measures. This module has enhanced my understanding of network security and equipped me with practical skills applicable to real-world scenarios.