Experiment 7: Network Mapping using Nmap

Name: Akhil Makarand Vaidya **UID**: 2022300131 **Batch**: COMPS B, Batch D

Aim: The objective of this lab assignment is to introduce students to NMAP, a powerful network scanning tool widely used for network discovery and security auditing. Through this assignment, students will gain hands-on experience in using NMAP to scan networks, identify open ports, detect operating systems, and gather valuable information about networked devices.

Theory:

Nmap, short for Network Mapper, is a powerful open-source tool used for network exploration and security auditing. It is designed to discover hosts and services on a computer network, thus creating a "map" of the network. Nmap employs raw IP packets in novel ways to determine what hosts are available on the network, what services those hosts are offering, what operating systems they are running, what type of packet filters/firewalls are in use, and numerous other characteristics.

Problem Statements:

1. Scan a given network range and identify all active hosts.

```
students@spit:~$ nmap -sn 172.16.31.208/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-28 09:47 IST
Nmap scan report for 172.16.31.1
Host is up (0.00056s latency).
Nmap scan report for 172.16.31.11
Host is up (0.00040s latency).
Nmap scan report for 172.16.31.22
Host is up (0.0011s latency).
Nmap scan report for 172.16.31.25
Host is up (0.00043s latency).
Nmap scan report for 172.16.31.30
Host is up (0.00043s latency).
Nmap scan report for 172.16.31.40
Host is up (0.00037s latency).
Nmap scan report for 172.16.31.43
Host is up (0.00027s latency).
Nmap scan report for 172.16.31.44
Host is up (0.00090s latency).
Nmap scan report for 172.16.31.46
Host is up (0.00025s latency).
Nmap scan report for 172.16.31.54
Host is up (0.0017s latency).
Nmap scan report for 172.16.31.55
Host is up (0.00036s latency).
Nmap scan report for 172.16.31.57
Host is up (0.00030s latency).
Nmap scan report for 172.16.31.60
Host is up (0.00034s latency).
Nmap scan report for 172.16.31.62
Host is up (0.00028s latency).
Nmap scan report for 172.16.31.63
Host is up (0.00094s latency).
Nmap scan report for 172.16.31.64
Host is up (0.0043s latency).
Nmap scan report for 172.16.31.65
Host is up (0.00040s latency).
Nmap scan report for 172.16.31.68
Host is up (0.00045s latency).
```

```
Host is up (0.00065s latency).
Nmap scan report for 172.16.31.170
Host is up (0.00081s latency).
Nmap scan report for 172.16.31.172
Host is up (0.00075s latency).
Nmap scan report for 172.16.31.192
Host is up (0.00040s latency).
Nmap scan report for 172.16.31.193
Host is up (0.00037s latency).
Nmap scan report for 172.16.31.208
Host is up (0.00064s latency).
Nmap done: 256 IP addresses (33 hosts up) scanned in 2.12 seconds
students@spit:~$
```

2. Identify the top 5 most commonly open ports on a specific target.

```
students@spit:~$ nmap 172.16.31.208
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-28 09:45 IST
Nmap scan report for 172.16.31.208
Host is up (0.00019s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
25/tcp open  smtp
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
```

3. Determine the MAC address of a target device using NMAP.

```
students@spit:~$ sudo nmap -sP 172.16.31.43
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-28 09:54 IST
Nmap scan report for 172.16.31.43
Host is up (0.00036s latency).
MAC Address: 3C:52:82:61:7E:F4 (Hewlett Packard)
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

4. Perform a scan to detect the presence of HTTP and HTTPS services on a target network.

```
students@spit:~$ nmap -p 80,443 172.16.31.208/25
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-28 10:02 IST
Nmap scan report for 172.16.31.150
Host is up (0.00084s latency).

PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 172.16.31.152
Host is up (0.00038s latency).

PORT    STATE  SERVICE
80/tcp  open   http
443/tcp closed https

Nmap scan report for 172.16.31.170
Host is up (0.0012s latency).

PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for 172.16.31.172
Host is up (0.00044s latency).

PORT    STATE  SERVICE
80/tcp  open   http
443/tcp closed https

Nmap scan report for 172.16.31.192
Host is up (0.00041s latency).

PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https
```

5. Find out if a particular host has FTP service running on it.

```
students@spit:~$ nmap -p 21 172.16.31.208
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-28 10:05 IST
Nmap scan report for 172.16.31.208
Host is up (0.00068s latency).

PORT   STATE SERVICE
21/tcp open  ftp

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
students@spit:~$
```

6. Identify the SSH version running on a given host.

```
students@spit:~$ nmap -sV -p 22 172.16.31.208
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-28 10:06 IST
Nmap scan report for 172.16.31.208
Host is up (0.00061s latency).

PORT   STATE  SERVICE VERSION
22/tcp closed ssh

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.85 seconds
students@spit:~$
```

7. Scan a range of IP addresses and list all hosts that have Telnet service running.

```
students@spit:~$ nmap -p 23 172.16.31.208
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-28 10:08 IST
Nmap scan report for 172.16.31.208
Host is up (0.00059s latency).

PORT   STATE  SERVICE
23/tcp closed telnet

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
students@spit:~$
```

8. Determine the operating system of a target host using NMAP.

```
students@spit:~$ sudo nmap -O 172.16.31.208
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-28 10:09 IST
Nmap scan report for 172.16.31.208
Host is up (0.00068s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
25/tcp open  smtp
80/tcp open  http
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=3/28%OT=21%CT=1%CU=37097%PV=Y%DS=2%DC=I%G=Y%TM=6604F49
OS:D%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=A)SEQ
OS:(SP=104%GCD=1%ISR=109%TI=Z%CI=Z%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O
OS:3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=
OS:FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSN
OS:W7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%D
OS:F=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O
OS:=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W
OS:=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%R
OS:IPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.90 seconds
students@spit:~$
```

9. identify any SQL services running on a given network.

```
students@spit:~$ nmap -p 1433 172.16.31.208/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-28 10:15 IST
Nmap scan report for 172.16.31.1
Host is up (0.0014s latency).

PORT     STATE  SERVICE
1433/tcp closed ms-sql-s

Nmap scan report for 172.16.31.11
Host is up (0.00049s latency).

PORT     STATE  SERVICE
1433/tcp closed ms-sql-s

Nmap scan report for 172.16.31.22
Host is up (0.00065s latency).

PORT     STATE    SERVICE
1433/tcp filtered ms-sql-s

Nmap scan report for 172.16.31.25
Host is up (0.00047s latency).

PORT     STATE  SERVICE
1433/tcp closed ms-sql-s
```

```
Nmap scan report for 172.16.31.193
Host is up (0.00054s latency).

PORT     STATE  SERVICE
1433/tcp closed ms-sql-s

Nmap scan report for 172.16.31.208
Host is up (0.00053s latency).

PORT     STATE  SERVICE
1433/tcp closed ms-sql-s

Nmap scan report for 172.16.31.230
Host is up (0.00064s latency).

PORT     STATE  SERVICE
1433/tcp closed ms-sql-s

Nmap done: 256 IP addresses (36 hosts up) scanned in 2.34 seconds
students@spit:~$
```

10. Find out if a specific host has Remote Desktop Protocol (RDP) enabled.

```
students@spit:~$ nmap -p 3389 172.16.31.208
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-28 10:18 IST
Nmap scan report for 172.16.31.208
Host is up (0.00058s latency).

PORT     STATE  SERVICE
3389/tcp closed ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
students@spit:~$
```

11. Scan a target network and determine if any hosts are running DNS services.

```
Nmap scan report for 172.16.31.192
Host is up (0.00047s latency).

PORT   STATE  SERVICE
53/tcp closed domain

Nmap scan report for 172.16.31.193
Host is up (0.00043s latency).

PORT   STATE  SERVICE
53/tcp closed domain

Nmap scan report for 172.16.31.208
Host is up (0.00040s latency).

PORT   STATE  SERVICE
53/tcp closed domain

Nmap scan report for 172.16.31.230
Host is up (0.00067s latency).

PORT   STATE  SERVICE
53/tcp closed domain

Nmap done: 256 IP addresses (36 hosts up) scanned in 2.34 seconds
students@spit:~$
```

12. Detect if a host has SNMP (Simple Network Management Protocol) enabled.

```
students@spit:~$ nmap -p 161 172.16.31.208
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-28 10:20 IST
Nmap scan report for 172.16.31.208
Host is up (0.00051s latency).

PORT    STATE  SERVICE
161/tcp closed snmp

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
students@spit:~$
```

13. Perform a scan to identify any SMTP (Simple Mail Transfer Protocol) servers on a network.

```
Nmap scan report for 172.16.31.192
Host is up (0.00062s latency).

PORT   STATE  SERVICE
25/tcp closed smtp

Nmap scan report for 172.16.31.193
Host is up (0.00060s latency).

PORT   STATE  SERVICE
25/tcp closed smtp

Nmap scan report for 172.16.31.208
Host is up (0.00048s latency).

PORT   STATE SERVICE
25/tcp open  smtp

Nmap scan report for 172.16.31.230
Host is up (0.00051s latency).

PORT   STATE  SERVICE
25/tcp closed smtp

Nmap done: 256 IP addresses (37 hosts up) scanned in 2.34 seconds
students@spit:~$
```

14. Determine if a target network has any active FTP servers allowing anonymous login.

```
students@spit:~$ nmap -p 21 --script ftp-anon 172.16.30.125/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-28 10:32 IST
Nmap scan report for _gateway (172.16.30.1)
Host is up (0.00048s latency).

PORT   STATE  SERVICE
21/tcp closed ftp

Nmap scan report for 172.16.30.4
Host is up (0.081s latency).

PORT   STATE  SERVICE
21/tcp closed ftp
```

```
Nmap scan report for 172.16.30.35
Host is up (0.00069s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 0        0              26 Mar 16  2022 sample.txt
|_-rw-r--r--    1 0        0              46 Mar 16  2022 sample.txt~
```

15. Find out if any hosts in a network are running vulnerable versions of the Apache HTTP server.

```
students@spit:~$ nmap -p 80 --script http-vuln-cve2017-5638 172.16.31.0/
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-28 10:36 IST
Nmap scan report for _gateway (172.16.31.1)
Host is up (0.00035s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap scan report for 172.16.31.11
Host is up (0.00015s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap scan report for 172.16.31.22
Host is up (0.00100s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 172.16.31.25
Host is up (0.00021s latency).

PORT   STATE  SERVICE
80/tcp closed http

Nmap scan report for 172.16.31.27
Host is up (0.00020s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 172.16.31.30
Host is up (0.00031s latency).
```

16. Detect if a target host has any open NFS (Network File System) shares.

```
Nmap scan report for 172.16.31.192
Host is up (0.00037s latency).
All 1000 scanned ports on 172.16.31.192 are closed

Nmap scan report for 172.16.31.193
Host is up (0.00032s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
5900/tcp open  vnc

Nmap scan report for 172.16.31.208
Host is up (0.00030s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
25/tcp open  smtp
80/tcp open  http

Nmap scan report for 172.16.31.238
Host is up (0.00030s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 256 IP addresses (37 hosts up) scanned in 71.88 seconds
students@spit:~$
```

```
students@spit:~$ nmap --script nfs-showmount 172.16.31.208
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-28 10:34 IST
Nmap scan report for 172.16.31.208
Host is up (0.00024s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
25/tcp open  smtp
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

17. Identify the presence of any MySQL database servers on a given network.

```
Nmap scan report for 172.16.31.192
Host is up (0.00053s latency).

PORT     STATE  SERVICE VERSION
3306/tcp closed mysql

Nmap scan report for 172.16.31.193
Host is up (0.00041s latency).

PORT     STATE  SERVICE VERSION
3306/tcp closed mysql

Nmap scan report for 172.16.31.208
Host is up (0.00040s latency).

PORT     STATE  SERVICE VERSION
3306/tcp closed mysql

Nmap scan report for 172.16.31.230
Host is up (0.00045s latency).

PORT     STATE  SERVICE VERSION
3306/tcp closed mysql

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (36 hosts up) scanned in 2.60 seconds
students@spit:~$
```

18. Scan a network to determine if any hosts have the Remote Procedure Call (RPC) service running.

```
students@spit:~$ nmap -sV -p 111 172.16.31.208
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-28 10:44 IST
Nmap scan report for 172.16.31.208
Host is up (0.00063s latency).

PORT    STATE  SERVICE VERSION
111/tcp closed rpcbind

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
students@spit:~$
```

19. Detect if a specific host has any open VNC (Virtual Network Computing) ports.

```
students@spit:~$ nmap -p 5000 172.16.31.208
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-28 10:46 IST
Nmap scan report for 172.16.31.208
Host is up (0.00059s latency).

PORT     STATE  SERVICE
5000/tcp closed upnp

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
students@spit:~$
```

20. Perform a scan to identify any hosts with the Secure Shell (SSH) service running on non-default ports.

```
students@spit:~$ nmap -p 2222 --script ssh-hostkey 172.16.31.208/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-28 10:51 IST
Nmap scan report for 172.16.31.1
Host is up (0.0013s latency).

PORT     STATE  SERVICE
2222/tcp closed EtherNetIP-1

Nmap scan report for 172.16.31.11
Host is up (0.00057s latency).

PORT     STATE  SERVICE
2222/tcp closed EtherNetIP-1

Nmap scan report for 172.16.31.22
Host is up (0.0017s latency).

PORT     STATE    SERVICE
2222/tcp filtered EtherNetIP-1
```

Conclusion:

1. Understood the use of nmap to perform various types of network exploration tasks.
2. Identified and observed various ports present on different end systems in the given network.