CYBER SECURITY PRACTICAL –LAB ASSIGNMENT1

Title: Network Awareness and Port Security Using Nmap
Tool: Nmap
Instructor: Bijesh Thomas

OBJECTIVE

By the end of this 3-hour lab session, students will be able to:

- Identify live hosts in a network
- Detect open and closed ports
- Understand services running on a system
- Create an open port and then close it securely
- Develop basic defensive cybersecurity awareness

Rule: Students are allowed to scan ONLY their own system or college network. Scanning public websites or unknown IPs is strictly prohibited.

IMPORTANT TERMINOLOGIES

Term	Meaning
IP Address	Unique address of a device on a network
Host	Any connected device
Port	Digital door (0–65535)
Open Port	Accepts incoming connection
Closed Port	Exists but locked
Filtered Port	Blocked by firewall
Service	Program using a port
Firewall	Blocks unauthorized access
Subnet	Range of IP addresses
Localhost	Your own system (127.0.0.1)
Nmap	Network scanning tool

Write definitions for any 5 terms in your submission.

PART 1 – SETUP CHECK

Task 1: Check Nmap Installation

nmap --version

```
Nmap version 7.95 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.7 openssl-3.5.2 libssh2-1.11.1 libz-1.3.1 libpcre2-10.45 libpcap-1.10.5 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

Write your Nmap version: 7.95

Task 2: Find Your IP Address

Windows:

ipconfig

Mac/Linux:

ifconfig

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.104  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::f31d:5c4:11f8:6afe  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:1f:b7:23  txqueuelen 1000  (Ethernet)
        RX packets 30  bytes 5140 (5.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 29  bytes 3722 (3.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.3.15  netmask 255.255.255.0  broadcast 10.0.3.255
        inet6 fd17:625c:f037:3:b9ae:a679:73be:9b46  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::85d4:f61b:9299:f033  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:9e:40:30  txqueuelen 1000  (Ethernet)
        RX packets 22  bytes 4043 (3.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 550  bytes 35721 (34.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
```

My IP Address: 10.0.3.15

Task 3: Find Your Network Range

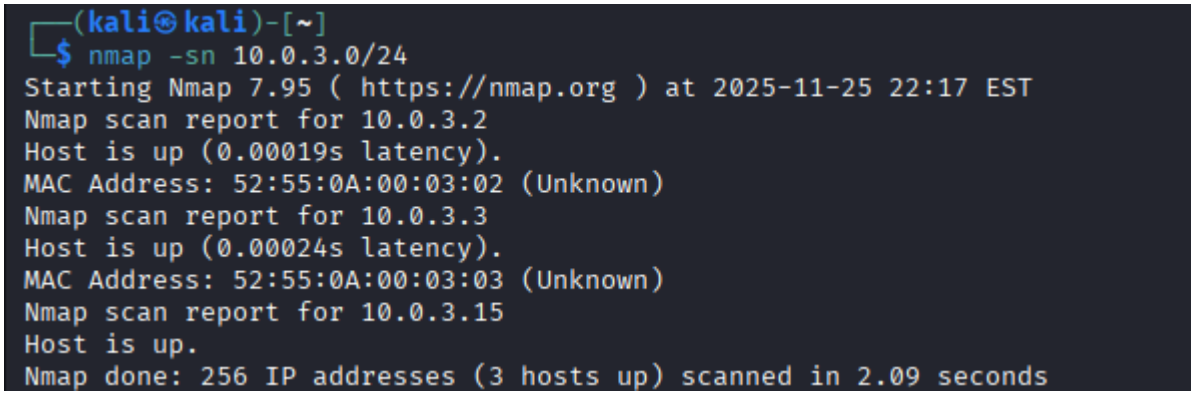
Example:
If IP = 10.67.220.111
Then Network Range = 10.67.220.0/24

My Network Range: 10.0.3.0/24

PART 2 – NETWORK SCANNING

Task 4: Scan for Live Devices

nmap -sn 10.0.3.0/24



Number of live devices found: 3

Write any 5 IP addresses found:

1. 10.0.3.2
2. 10.0.3.3
3. 10.0.3.15

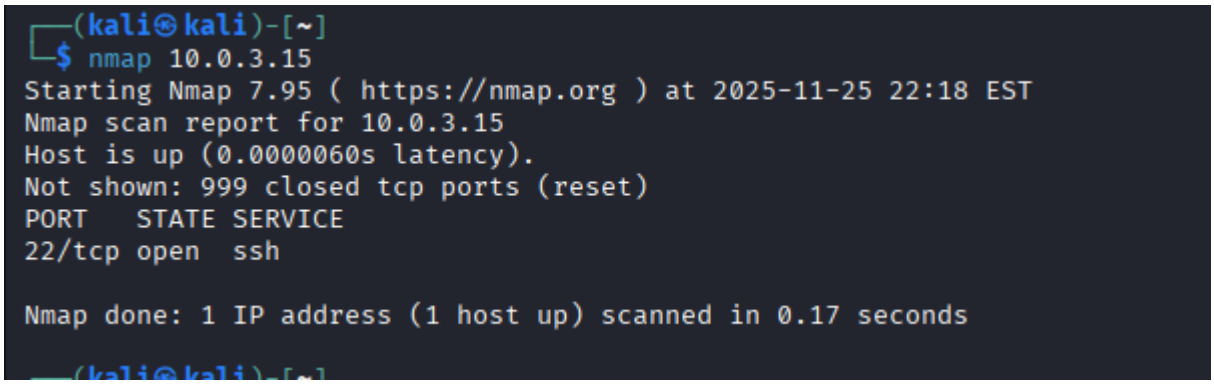
Question:
How many devices are sharing your network?

Ans: there are total of 3 devices active in my NAT.

PART 3 – PORT SCANNING

Task 5: Scan Your Own System

Nmap 10.0.3.15



Port	State	Service
22/tcp	open	ssh

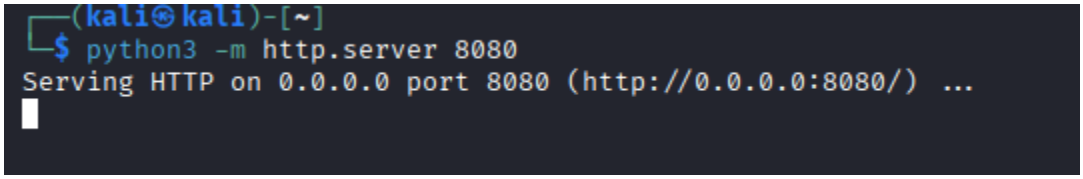
Question:
Why is it risky to have too many open ports?

Ans: Because there are vulnerabilities for many ports, and services that are running in them.

PART 4 – CREATE YOUR OWN OPEN PORT

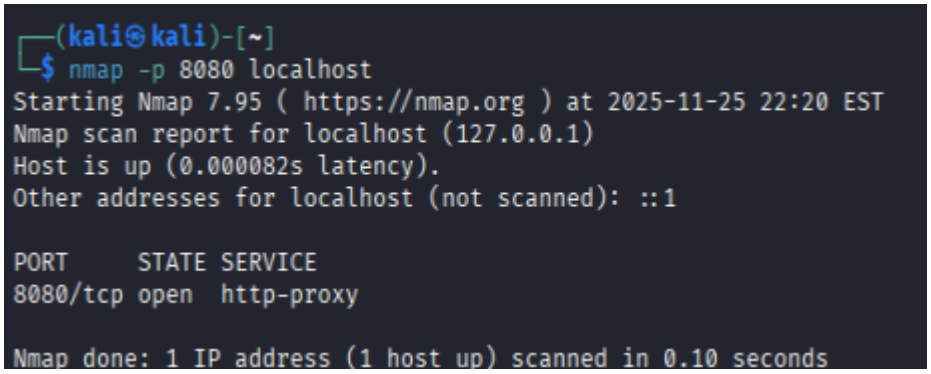
Task 6: Open Port 8080

python3 -m http.server 8080



Task 7: Confirm Port is OPEN

nmap -p 8080 localhost



What happened to port 8080?

Ans: A service started running in that.

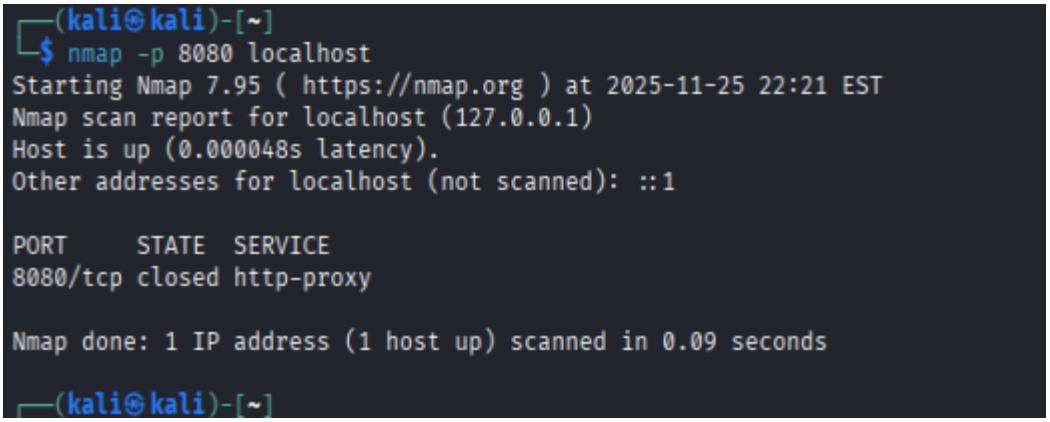
PART 5 – CLOSE THE OPEN PORT

Press in the first terminal window:

CTRL + C

Then run:

nmap -p 8080 localhost



Why must we close unused ports?

Ans: Because Hackers can take advantage of the unmonitored ports to hack us.

FINAL REFLECTION

Write in your own words:

1. What did you learn today?

Ans: what's the basics of the nmap, and can open ports effect out network security.

2. How many unknown devices were on your network?

Ans: Total of 2 unknown devices were there in my network, one known was mine own.

3. Why is Nmap dangerous in the wrong hands?

Ans: Because it will let u know critical information which a hacker can use to cause harm to out networks.

4. How has this lab changed your view on cybersecurity?

Ans: To me it hasn't because, my view towards the Cybersecurity was already in the right direction to begin with.