Task 1: Scan Your Local Network for Open Ports Objective: Learn to discover open ports on devices in your local network to understand network exposure.

Tools: Nmap (free), Wireshark (optional).

Hints/Mini Guide:

1.Install Nmap from official website.

2.Find your local IP range (e.g., 192.168.1.0/24).

3.Run: nmap -sS 192.168.1.0/24 to perform TCP SYN scan.

4.Note down IP addresses and open ports found.

5.Optiona ly analyze packet capture with Wireshark.

6.Research common services running on those ports.

7.Identify potential security risks from open ports.

8.Save scan results as a text or HTML file.

Outcome: Basic network reconnaissance skills; understanding network service exposure.

┌──(root㉿LAPTOP-9876DSAW)-[/home/kali]

└─# ip a

1: lo: <LOOPBACK,UP,LOWER\_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000

link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00

inet 127.0.0.1/8 scope host lo

valid\_lft forever preferred\_lft forever

inet 10.255.255.254/32 brd 10.255.255.254 scope global lo

valid\_lft forever preferred\_lft forever

inet6 ::1/128 scope host

valid\_lft forever preferred\_lft forever

2: eth0: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1472 qdisc mq state UP group default qlen 1000

link/ether 00:15:5d:75:7a:37 brd ff:ff:ff:ff:ff:ff

inet 172.0.0.1/20 brd 172.30.31.255 scope global eth0

valid\_lft forever preferred\_lft forever

inet6 fe80::215:5dff:fe75:7a37/64 scope link

valid\_lft forever preferred\_lft forever

3: wg0: <POINTOPOINT,NOARP,UP,LOWER\_UP> mtu 1392 qdisc noqueue state UNKNOWN group default qlen 1000

link/none

inet 10.66.66.1/24 scope global wg0

valid\_lft forever preferred\_lft forever

4: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default

link/ether 86:48:ff:3b:82:75 brd ff:ff:ff:ff:ff:ff

inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0

valid\_lft forever preferred\_lft forever

┌──(root㉿LAPTOP-9876DSAW)-[/home/kali]

└─# nmap -sS 172.0.0.1/20

Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-20 19:19 IST

Stats: 0:00:10 elapsed; 4094 hosts completed (1 up), 1 undergoing SYN Stealth Scan

SYN Stealth Scan Timing: About 0.50% done

Nmap scan report for LAPTOP-9876DSAW.mshome.net (172.30.16.1)

Host is up (0.00044s latency).

All 1000 scanned ports on LAPTOP-9876DSAW.mshome.net (172.30.16.1) are in ignored states.

Not shown: 1000 filtered tcp ports (no-response)

MAC Address: 00:15:5D:76:28:A3 (Microsoft)

Nmap scan report for 172.0.0.1

Host is up (0.0000040s latency).

Not shown: 996 closed tcp ports (reset)

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

3306/tcp open mysql

5901/tcp open vnc-1

Nmap done: 4096 IP addresses (2 hosts up) scanned in 30.98 seconds

┌──(root㉿LAPTOP-9876DSAW)-[/home/kali]

└─# nmap -sS 172.0.0.1

Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-20 19:30 IST

Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn

Nmap done: 1 IP address (0 hosts up) scanned in 3.22 seconds

┌──(root㉿LAPTOP-9876DSAW)-[/home/kali]

└─# nmap -sS -Pn 172.0.0.1

Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-20 19:30 IST

Nmap scan report for 172.0.0.1

Host is up (0.019s latency).

All 1000 scanned ports on 172.0.0.1 are in ignored states.

Not shown: 998 filtered tcp ports (no-response), 2 filtered tcp ports (admin-prohibited)

Nmap done: 1 IP address (1 host up) scanned in 47.87 seconds

┌──(root㉿LAPTOP-9876DSAW)-[/home/kali]

└─# nmap -sV --script vuln 172.0.0.1

Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-20 19:34 IST

Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn

Nmap done: 1 IP address (0 hosts up) scanned in 13.27 seconds

┌──(root㉿LAPTOP-9876DSAW)-[/home/kali]

└─# nmap -sV -Pn 172.0.0.1

Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-20 19:35 IST

Nmap scan report for 172.0.0.1

Host is up (0.017s latency).

All 1000 scanned ports on 172.0.0.1 are in ignored states.

Not shown: 995 filtered tcp ports (no-response), 5 filtered tcp ports (admin-prohibited)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 27.47 seconds

┌──(root㉿LAPTOP-9876DSAW)-[/home/kali]

└─# nmap -sV --script vuln 172.0.0.1

Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-20 19:53 IST

Nmap scan report for 172.0.0.1

Host is up (0.0000050s latency).

Not shown: 996 closed tcp ports (reset)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 10.0p2 Debian 8 (protocol 2.0)

| vulners:

| cpe:/a:openbsd:openssh:10.0p2:

| CVE-2025-61985 3.6 https://vulners.com/cve/CVE-2025-61985

| CVE-2025-61984 3.6 https://vulners.com/cve/CVE-2025-61984

| B7EACB4F-A5CF-5C5A-809F-E03CCE2AB150 3.6 https://vulners.com/githubexploit/B7EACB4F-A5CF-5C5A-809F-E03CCE2AB150 EXPLOIT

|\_ 4C6E2182-0E99-5626-83F6-1646DD648C57 3.6 https://vulners.com/githubexploit/4C6E2182-0E99-5626-83F6-1646DD648C57 EXPLOIT

80/tcp open http Apache httpd 2.4.65 ((Debian))

|\_http-dombased-xss: Couldn't find any DOM based XSS.

|\_http-csrf: Couldn't find any CSRF vulnerabilities.

|\_http-server-header: Apache/2.4.65 (Debian)

|\_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

| http-enum:

| /test.php: Test page

| /info.php: Possible information file

|\_ /server-status/: Potentially interesting folder

3306/tcp open mysql MySQL (unauthorized)

5901/tcp open vnc VNC (protocol 3.8)

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 42.66 seconds