**Task 1-Scan your Local Network for Open Ports**

**1.Installing nmap on Kali Linux**

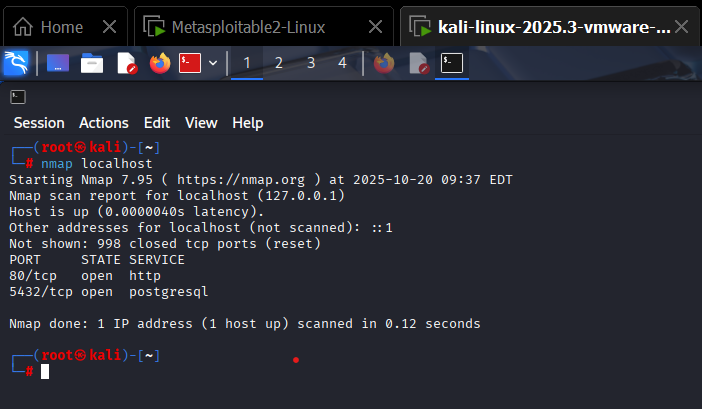
$sudo apt-get update

$sudo apt-get install nmap

$nmap -V or $nmap –version

**2.Finding local IP ranges**

**=> nmap localhost**



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

**=>nmap -sS 192.168.1.1-10**

Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-20 07:17 EDT

Stats: 0:06:43 elapsed; 0 hosts completed (10 up), 10 undergoing SYN Stealth Scan

SYN Stealth Scan Timing: About 86.66% done; ETC: 07:25 (0:01:01 remaining)

Nmap scan report for 192.168.1.1

Host is up (0.00018s latency).

All 1000 scanned ports on 192.168.1.1 are in ignored states.

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

Nmap scan report for 192.168.1.2

Host is up (0.00014s latency).

All 1000 scanned ports on 192.168.1.2 are in ignored states.

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

Nmap scan report for 192.168.1.3

Host is up (0.00016s latency).

All 1000 scanned ports on 192.168.1.3 are in ignored states.

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

Nmap scan report for 192.168.1.4

Host is up (0.00021s latency).

All 1000 scanned ports on 192.168.1.4 are in ignored states.

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

Nmap scan report for 192.168.1.5

Host is up (0.00020s latency).

All 1000 scanned ports on 192.168.1.5 are in ignored states.

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

Nmap scan report for 192.168.1.6

Host is up (0.00015s latency).

All 1000 scanned ports on 192.168.1.6 are in ignored states.

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

Nmap scan report for 192.168.1.7

Host is up (0.00015s latency).

All 1000 scanned ports on 192.168.1.7 are in ignored states.

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

Nmap scan report for 192.168.1.8

Host is up (0.00015s latency).

All 1000 scanned ports on 192.168.1.8 are in ignored states.

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

Nmap scan report for 192.168.1.9

Host is up (0.00015s latency).

All 1000 scanned ports on 192.168.1.9 are in ignored states.

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

Nmap scan report for 192.168.1.10

Host is up (0.00027s latency).

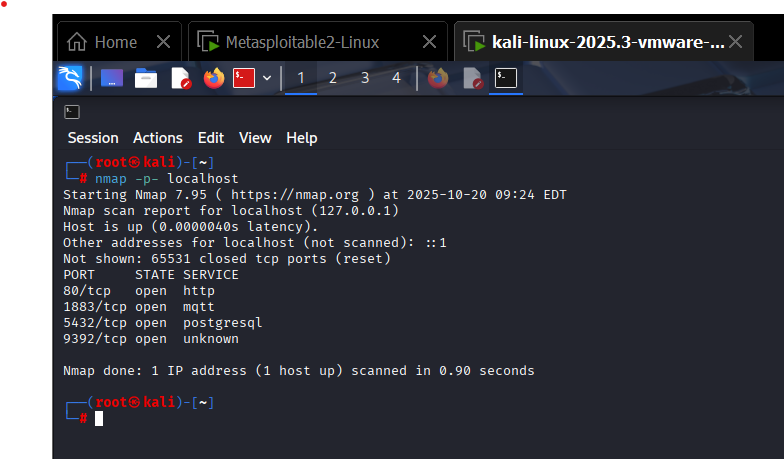
All 1000 scanned ports on 192.168.1.10 are in ignored states.

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

Nmap done: 10 IP addresses (10 hosts up) scanned in 411.91 seconds

**4.IP addresses and open ports found**

**=> nmap -p- localhost**



**5.Analyze packet capture with Wireshark**

**6.Common Services running on above ports**

|  |  |  |
| --- | --- | --- |
| **PORT** | **STATE** | **SERVICE** |
| 80 | open | http-Web Server(Websites,APIs) |
| 1833 | open | No official service is Standard on this port |
| 5432 | open | postgresql |

**7.Potential Risks from open ports**

**NTP(Network Time Protocol):**

1.Misconfigured NTP Servers or old NTP implements may be vulnerable to amplification DDoS.

2.If local device is acting as an NTP Server unintentionally,it could be abused.

**ARP(Address Resolution Protocol):**

1.ARP could indicate misconfigured devices or ARP spoofing/poisoning.