USE OF NMAP

Nmap: Nmap is a tool used to discover hosts and services an a computer network by sending packets and analysing the responses. Also called as “Swiss Army Knife” for Network scanning.
Host discovery
Port Scanning
Service detection
OS Detection
Vulnerability Scanning

To scan a single host
nmap 192.168.xx.xx
To scan a range of Ips
nmap 192.168.1.1-50
To detect Services and OS
nmap -sV -O 192.168.x.x

COMMON NMAP SCAN TYPES

-sT = TCP connect (simple, but noisy)

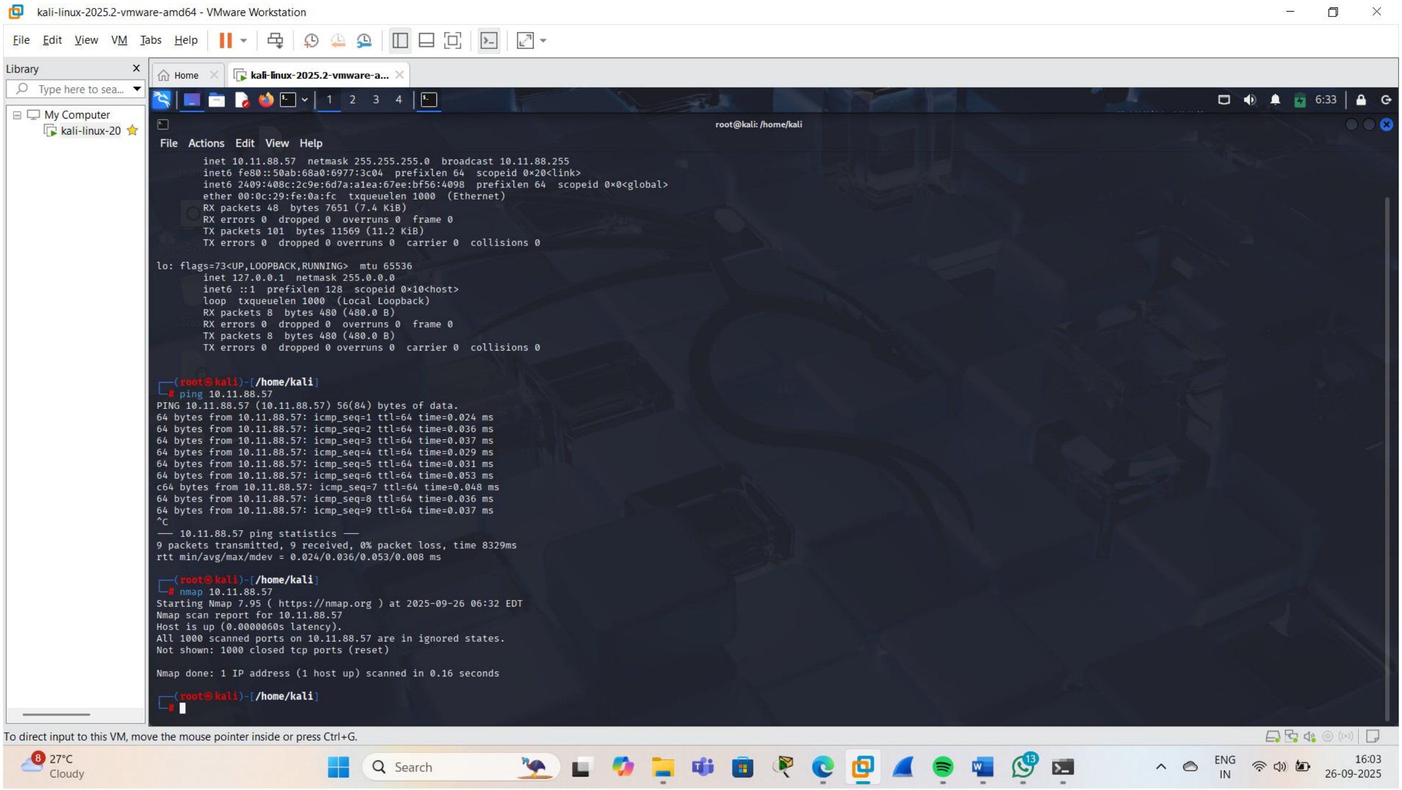
-sS = SYN scan (fast + stealthy, default)

-sU = UDP scan (for UDP services)

-sF, -sX, -sN = stealth scans (bypass some firewalls)

-sn = host discovery

-sV, -O, NSE = advanced service/OS/vulnerability detection

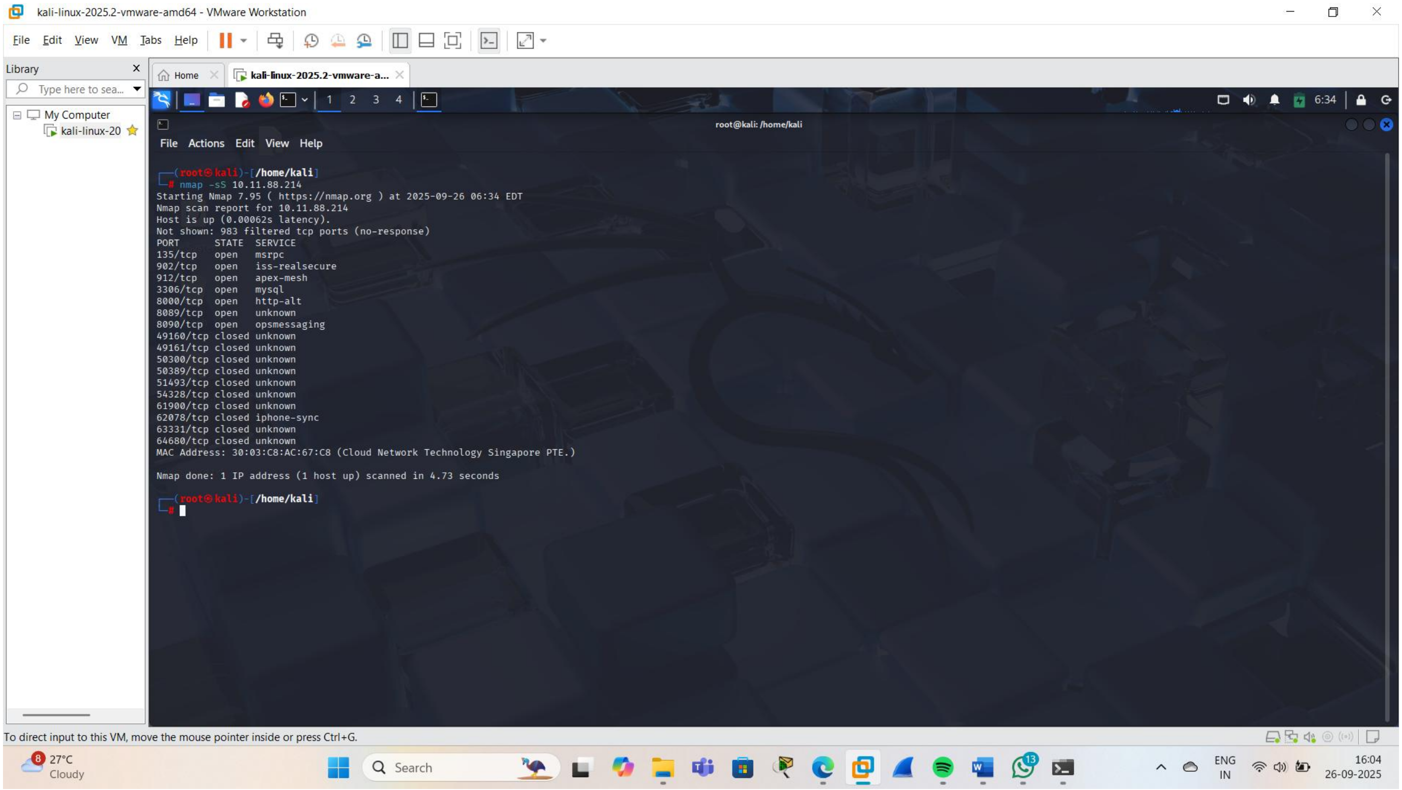

kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
kali-linux-20
Home
kali-linux-2025.2-vmware-a...
1 2 3 4
6:33
root@kali: /home/kali
File Actions Edit View Help

```
        inet 10.11.88.57  netmask 255.255.255.0  broadcast 10.11.88.255
        inet6 fe80::50ab:68a0:6977:3c04  prefixlen 64  scopeid 0×20<link>
        inet6 2409:408c:2c9e:6d7a:a1ea:67ee:bf56:4098  prefixlen 64  scopeid 0×0<global>
        ether 00:0c:29:fe:0a:fc  txqueuelen 1000  (Ethernet)
        RX packets 48  bytes 7651 (7.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 101  bytes 11569 (11.2 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 0×10<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


┌──(root㉿kali)-[/home/kali]
└─# ping 10.11.88.57
PING 10.11.88.57 (10.11.88.57) 56(84) bytes of data.
64 bytes from 10.11.88.57: icmp_seq=1 ttl=64 time=0.024 ms
64 bytes from 10.11.88.57: icmp_seq=2 ttl=64 time=0.036 ms
64 bytes from 10.11.88.57: icmp_seq=3 ttl=64 time=0.037 ms
64 bytes from 10.11.88.57: icmp_seq=4 ttl=64 time=0.029 ms
64 bytes from 10.11.88.57: icmp_seq=5 ttl=64 time=0.031 ms
64 bytes from 10.11.88.57: icmp_seq=6 ttl=64 time=0.053 ms
c64 bytes from 10.11.88.57: icmp_seq=7 ttl=64 time=0.048 ms
64 bytes from 10.11.88.57: icmp_seq=8 ttl=64 time=0.036 ms
64 bytes from 10.11.88.57: icmp_seq=9 ttl=64 time=0.037 ms
^C
—— 10.11.88.57 ping statistics ——
9 packets transmitted, 9 received, 0% packet loss, time 8329ms
rtt min/avg/max/mdev = 0.024/0.036/0.053/0.008 ms

┌──(root㉿kali)-[/home/kali]
└─# nmap 10.11.88.57
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-26 06:32 EDT
Nmap scan report for 10.11.88.57
Host is up (0.0000060s latency).
All 1000 scanned ports on 10.11.88.57 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds

┌──(root㉿kali)-[/home/kali]
└─# █
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Here the packet transferring through the own device means the connection is good, By using ping command we can check the speed of the packet, TTL (Time to live).

Here by using the nmap is network mapping used to check which ports are open, which services are running including OS information sometimes.



kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-20
Home
kali-linux-2025.2-vmware-a...
root@kali: /home/kali
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
27°C
Cloudy
Search
ENG
IN
16:04
26-09-2025

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 10.11.88.214
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-26 06:34 EDT
Nmap scan report for 10.11.88.214
Host is up (0.00062s latency).
Not shown: 983 filtered tcp ports (no-response)
PORT      STATE  SERVICE
135/tcp   open   msrpc
902/tcp   open   iss-realsecure
912/tcp   open   apex-mesh
3306/tcp  open   mysql
8000/tcp  open   http-alt
8089/tcp  open   unknown
8090/tcp  open   opsmessaging
49160/tcp closed unknown
49161/tcp closed unknown
50300/tcp closed unknown
50389/tcp closed unknown
51493/tcp closed unknown
54328/tcp closed unknown
61900/tcp closed unknown
62078/tcp closed iphone-sync
63331/tcp closed unknown
64680/tcp closed unknown
MAC Address: 30:03:C8:AC:67:C8 (Cloud Network Technology Singapore PTE.)

Nmap done: 1 IP address (1 host up) scanned in 4.73 seconds

┌──(root㉿kali)-[/home/kali]
└─# 
```