Nmap Host Discovery

Nmap (Network Mapper) is a powerful open-source network scanning tool used for network exploration and security auditing. It allows users to discover hosts, services, and their details on a computer network, thus creating a map of the network topology. Nmap utilizes raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and numerous other characteristics. It is widely used by network administrators, security professionals, and ethical hackers for tasks ranging from network inventory, managing service upgrade schedules, and monitoring host or service uptime to penetration testing and identifying vulnerabilities.

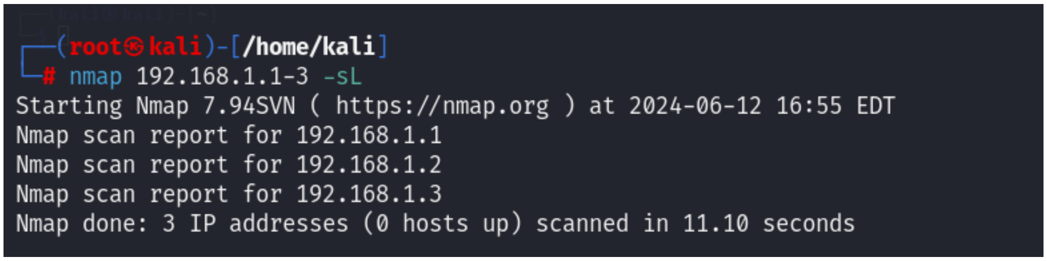
An Nmap host scan refers to the process of using Nmap's capabilities to determine which hosts are active and reachable on a network. This type of scan focuses on identifying live hosts without necessarily probing for open ports or detailed service information. Host scans are essential for network administrators and security professionals to understand the scope and availability of devices on a network, aiding in network management, troubleshooting, and security assessments.

Nmap offers several methods for host scanning, including ICMP echo requests (ping scans), TCP SYN, TCP ACK, and UDP probes. These methods allow Nmap to send different types of packets to hosts and analyze their responses to determine if they are online and responsive. Host scans can be customized with various options to optimize scan speed, accuracy, and stealthiness depending on the network environment and security requirements.

Overall, Nmap host scans serve as a foundational step in network reconnaissance, providing valuable insights into the presence and status of devices within a network infrastructure.

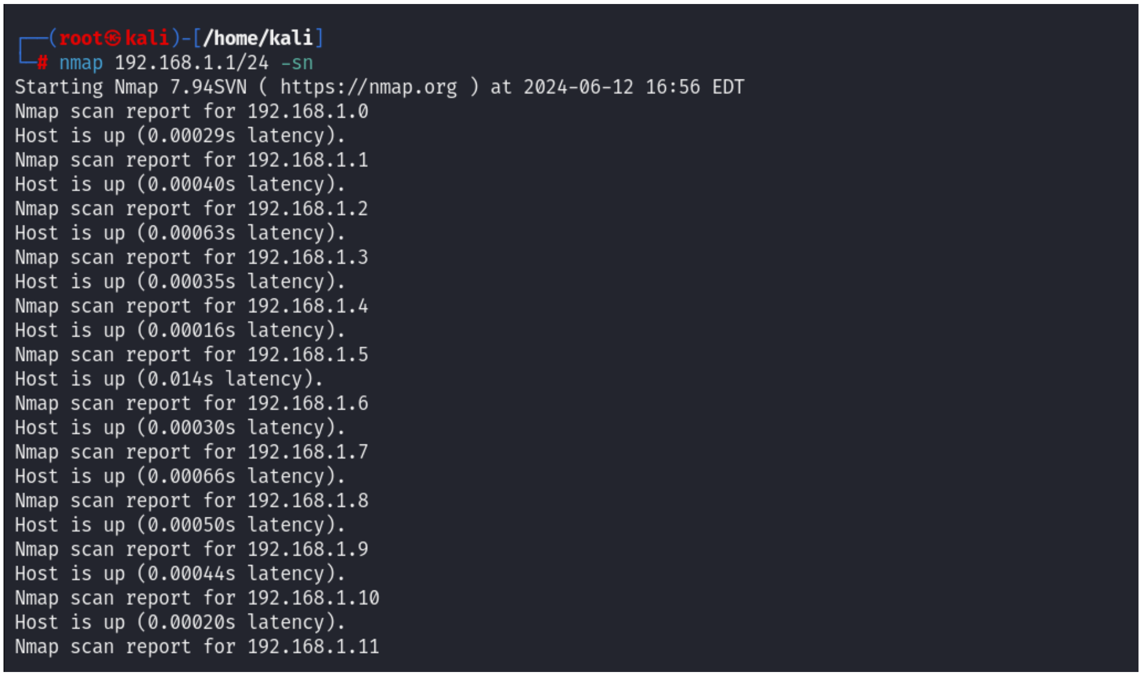
Example: -

1. The -sL switch in nmap performs a "list scan" which simply lists the targets to be scanned without actually scanning them.



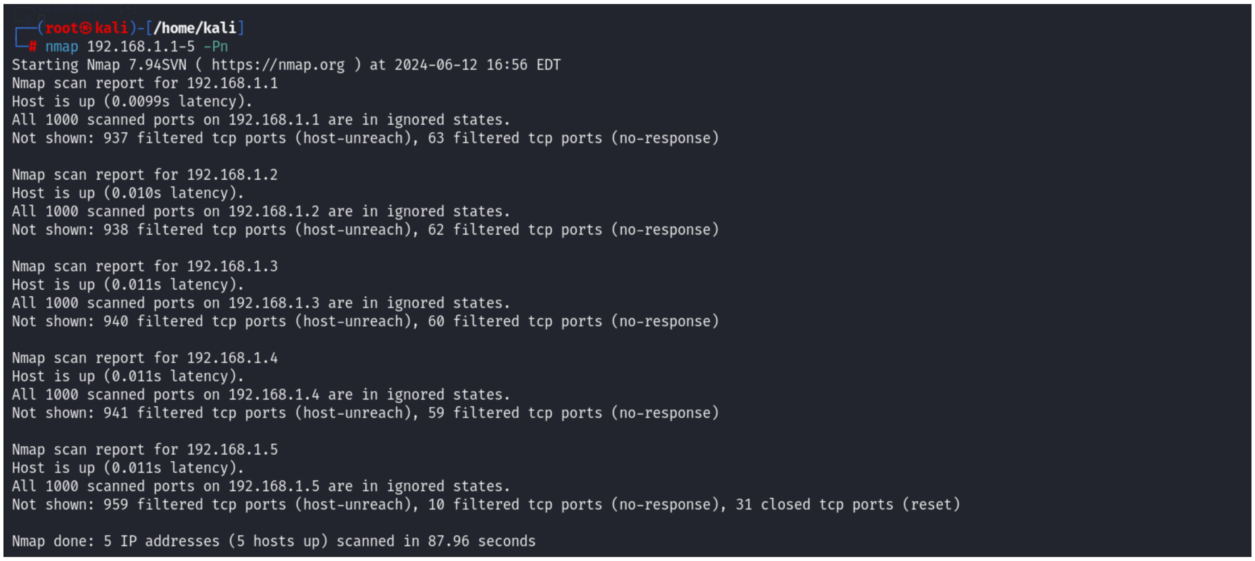
```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.1.1-3 -sL
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-12 16:55 EDT
Nmap scan report for 192.168.1.1
Nmap scan report for 192.168.1.2
Nmap scan report for 192.168.1.3
Nmap done: 3 IP addresses (0 hosts up) scanned in 11.10 seconds
```

2. The -sn switch in nmap performs a "ping scan," which checks whether hosts are up without doing a port scan.



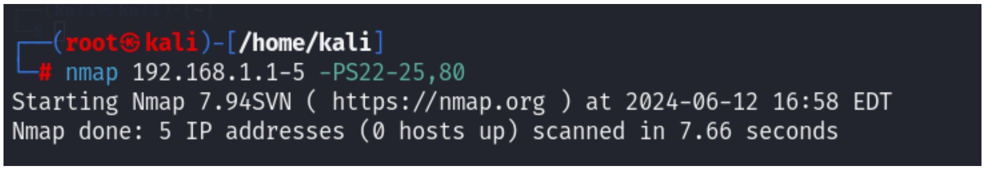
```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.1.1/24 -sn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-12 16:56 EDT
Nmap scan report for 192.168.1.0
Host is up (0.00029s latency).
Nmap scan report for 192.168.1.1
Host is up (0.00040s latency).
Nmap scan report for 192.168.1.2
Host is up (0.00063s latency).
Nmap scan report for 192.168.1.3
Host is up (0.00035s latency).
Nmap scan report for 192.168.1.4
Host is up (0.00016s latency).
Nmap scan report for 192.168.1.5
Host is up (0.014s latency).
Nmap scan report for 192.168.1.6
Host is up (0.00030s latency).
Nmap scan report for 192.168.1.7
Host is up (0.00066s latency).
Nmap scan report for 192.168.1.8
Host is up (0.00050s latency).
Nmap scan report for 192.168.1.9
Host is up (0.00044s latency).
Nmap scan report for 192.168.1.10
Host is up (0.00020s latency).
Nmap scan report for 192.168.1.11
```

3. The -Pn switch in nmap skips the host discovery phase, assuming all hosts are up and scanning them directly.



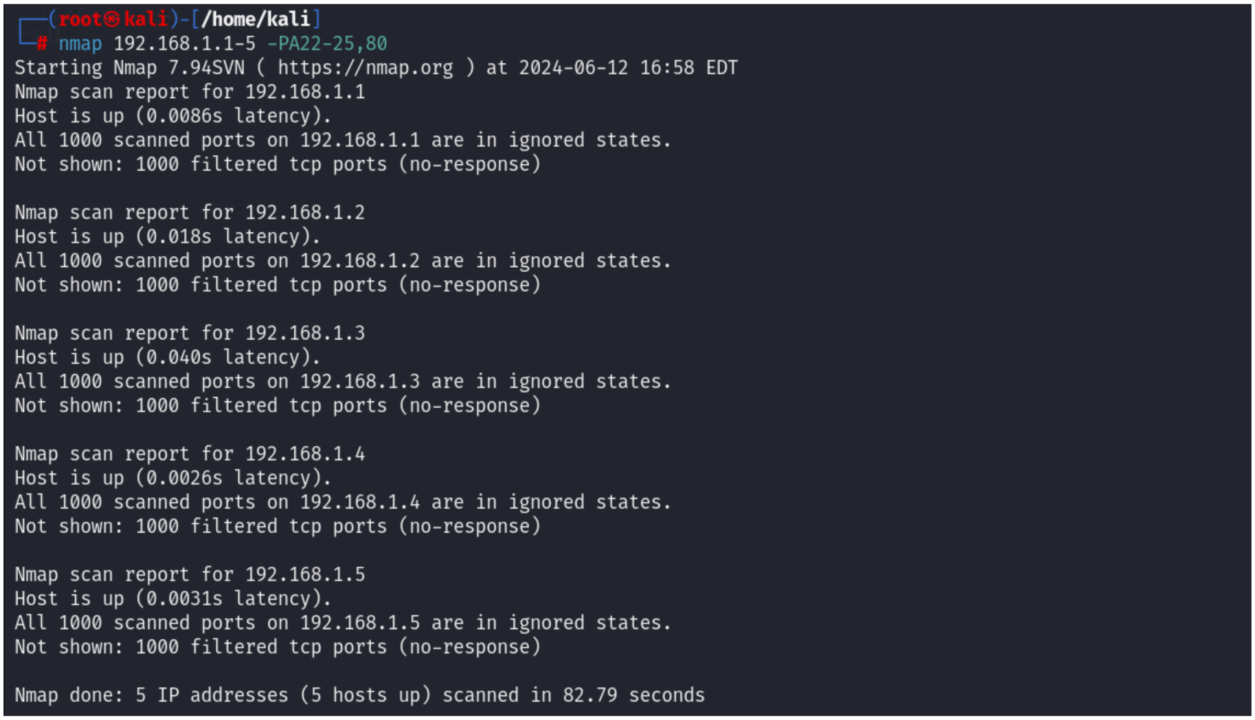
```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.1.1-5 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-12 16:56 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0099s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 937 filtered tcp ports (host-unreach), 63 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.2
Host is up (0.010s latency).
All 1000 scanned ports on 192.168.1.2 are in ignored states.
Not shown: 938 filtered tcp ports (host-unreach), 62 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.3
Host is up (0.011s latency).
All 1000 scanned ports on 192.168.1.3 are in ignored states.
Not shown: 940 filtered tcp ports (host-unreach), 60 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.4
Host is up (0.011s latency).
All 1000 scanned ports on 192.168.1.4 are in ignored states.
Not shown: 941 filtered tcp ports (host-unreach), 59 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.5
Host is up (0.011s latency).
All 1000 scanned ports on 192.168.1.5 are in ignored states.
Not shown: 959 filtered tcp ports (host-unreach), 10 filtered tcp ports (no-response), 31 closed tcp ports (reset)

Nmap done: 5 IP addresses (5 hosts up) scanned in 87.96 seconds
```

4. The -PS switch in nmap sends TCP SYN packets to discover if hosts are up, similar to a traditional ping but using specified ports.



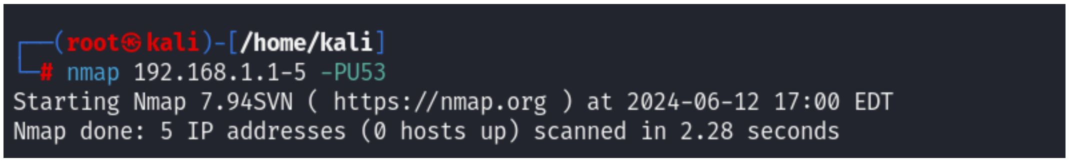
```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.1.1-5 -PS22-25,80
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-12 16:58 EDT
Nmap done: 5 IP addresses (0 hosts up) scanned in 7.66 seconds
```

5. The -PA switch in nmap sends TCP ACK packets to discover if hosts are up, useful for bypassing certain firewalls.



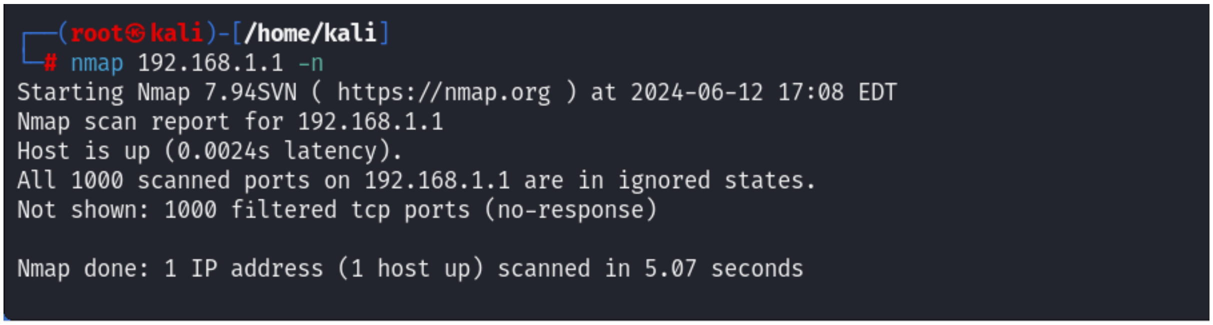
```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.1.1-5 -PA22-25,80
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-12 16:58 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0086s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.2
Host is up (0.018s 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 (0.040s 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 (0.0026s 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 (0.0031s latency).
All 1000 scanned ports on 192.168.1.5 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 5 IP addresses (5 hosts up) scanned in 82.79 seconds
```

6. The -PU switch in nmap sends UDP packets to discover if hosts are up, useful for detecting hosts that do not respond to TCP probes.



```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.1.1-5 -PU53
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-12 17:00 EDT
Nmap done: 5 IP addresses (0 hosts up) scanned in 2.28 seconds
```

7. The -n switch in nmap disables DNS resolution, speeding up the scan by not converting IP addresses to hostnames.



```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.1.1 -n
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-12 17:08 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0024s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 5.07 seconds
```