**BASIC NETWORK SCAN USING NETWORK MAPPING**

**-SWASTHIK C SHETTY**

**DATE:12 AUGUST 2025**

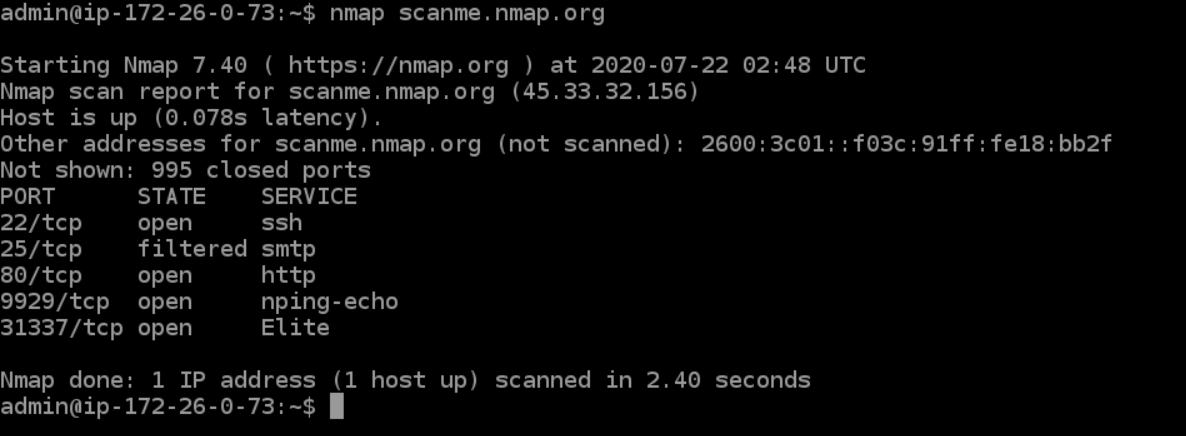
**NMAP**

It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications. It also allows user to know what and all are running in the network and to detect vulnerabilities.

**Commands:**

**Scan a single host —** Scans a single host for 1000 well-known ports. These ports are the ones used by popular services like SQL, SNTP, apache, and others.

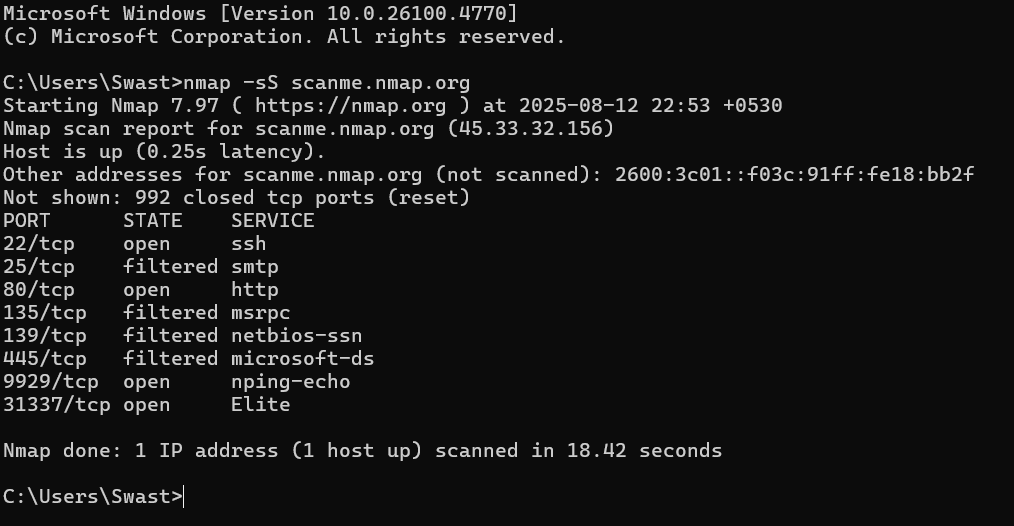
>nmap scanme.nmap.org



**Stealth scan**

Stealth scanning is performed by sending an SYN packet and analyzing the response. If SYN/ACK is received, it means the port is open, and you can open a TCP connection.

> nmap -sS scanme.nmap.org



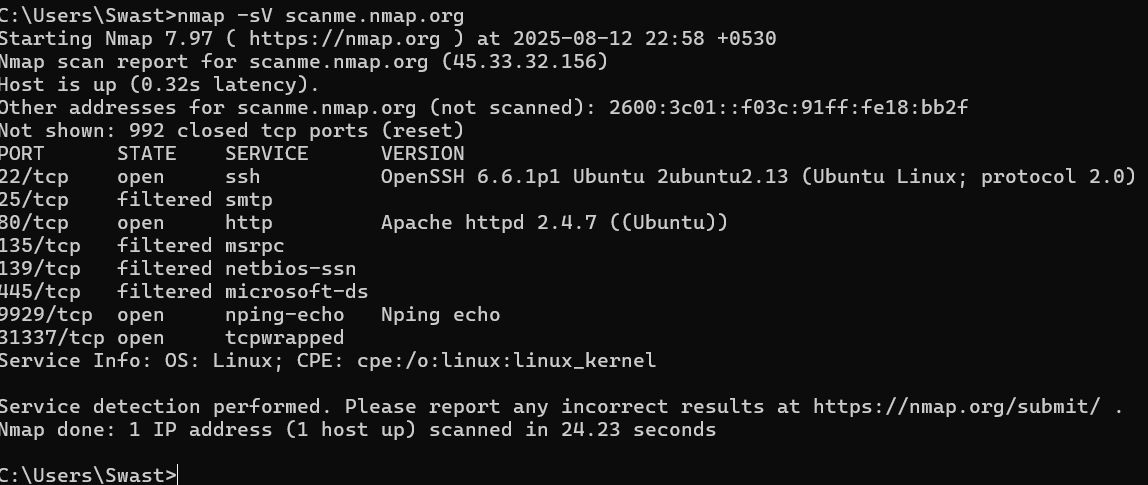
We can use the **‘-sS’** command to perform a stealth scan.

**Version scanning**

Finding application versions is a crucial part in penetration testing.

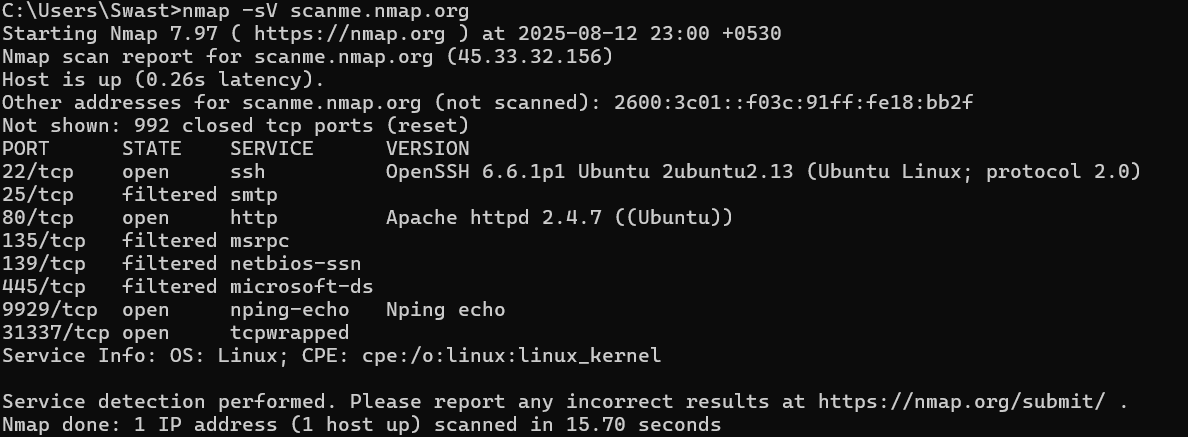
It makes your life easier since you can find an existing vulnerability from CVE database for a particular version of the service.

> nmap -sV scanme.nmap.org



**OS Scanning**

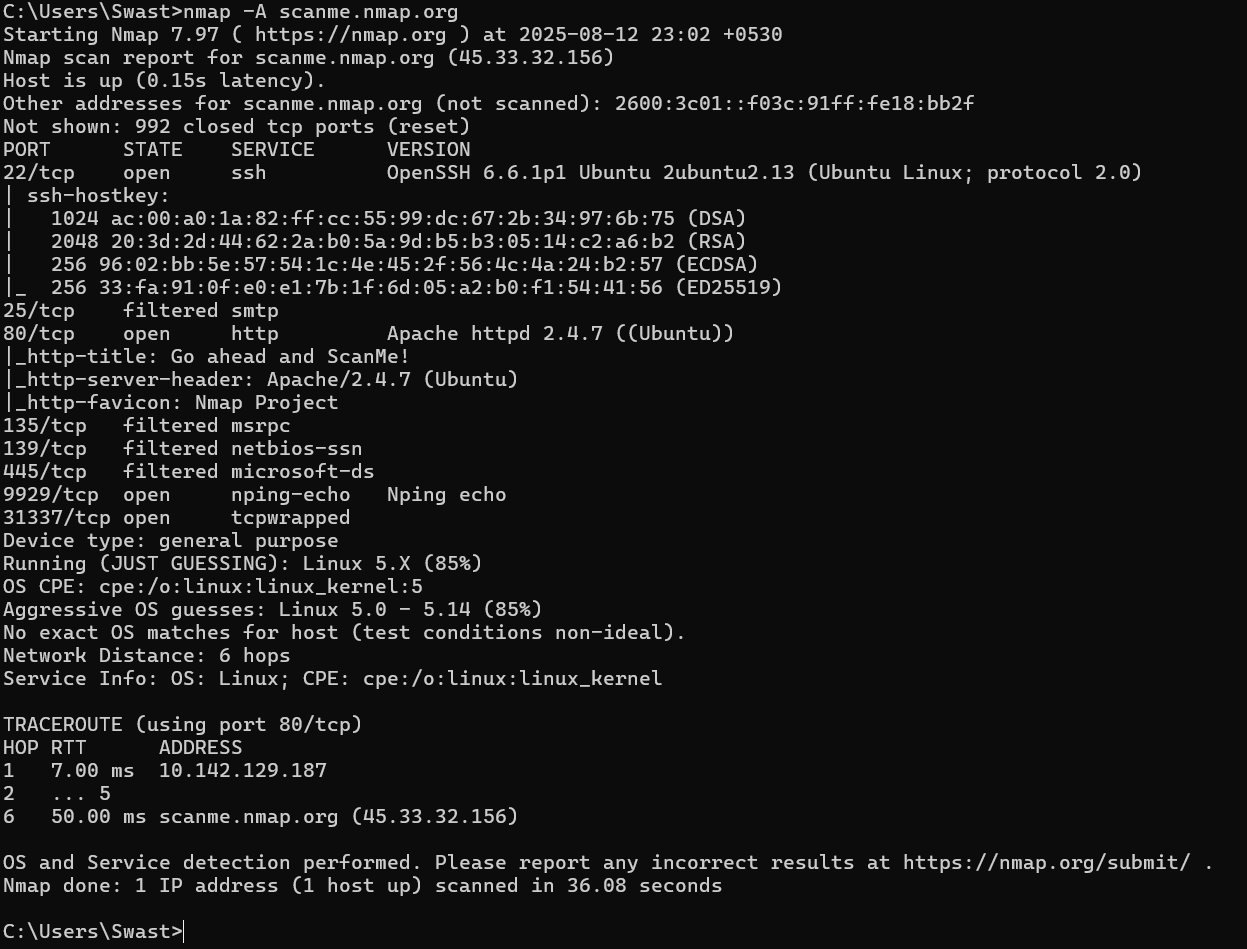
> nmap -sV scanme.nmap.org



**Aggressive Scanning**

> nmap -A scanme.nmap.org

Aggressive scans provide far better information than regular scans. However, an aggressive scan also sends out more probes, and it is more likely to be detected during security audits.



**ALL PORT SCAN:**

Scans all the 65535 TCP ports usually it takes time to complete. It ensures that we are not missing any ports outside 1000 ports.

>nmap -p- scanme.nmap.org

**Nmap Help**

Nmap has a built-in help command that lists all the flags and options you can use. It is often handy given the number of command-line arguments Nmap comes with.

> nmap -h

**Key Observations**

* Open ports indicate the services the server is running.
* Closed ports respond with “RST” packets (service not running).
* No filtered ports were detected in this scan which means no firewall is blocking.

**Conclusion**  
Nmap lets you quickly scan and discover essential information about network, hosts, ports, firewalls, and operating systems.

Nmap has numerous settings, flags, and preferences that help system administrators analyze a network in detail.