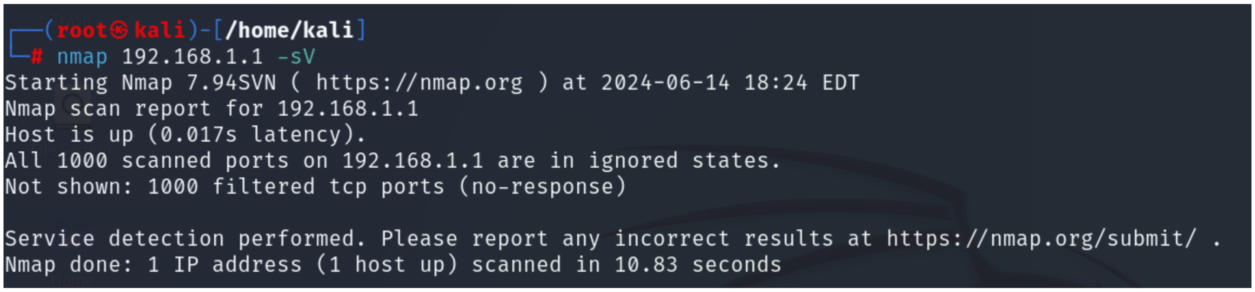
# Nmap Service & OS Detection

Nmap is a crucial tool in network security and administration, providing advanced features for service and version detection as well as operating system (OS) detection. Service and version detection (`-sV`) identifies the specific services running on open ports and their exact versions by sending various probes and analyzing the responses against a comprehensive database of service fingerprints. This allows network administrators to identify vulnerabilities associated with particular service versions, manage network assets effectively, and respond to incidents more efficiently. OS detection (`-O`) determines the operating system and version running on a target host by analyzing attributes from TCP and ICMP probes and matching them against a database of OS fingerprints. This information helps in applying tailored security policies, managing patches, and designing network segmentation strategies. Combining both features with a command like `nmap -sV -O <target>` provides a detailed profile of the target host, enhancing security assessments, network management, and vulnerability management. Overall, Nmap's capabilities in service/version detection and OS detection are indispensable for maintaining a secure and well-managed network infrastructure.

# Examples: -

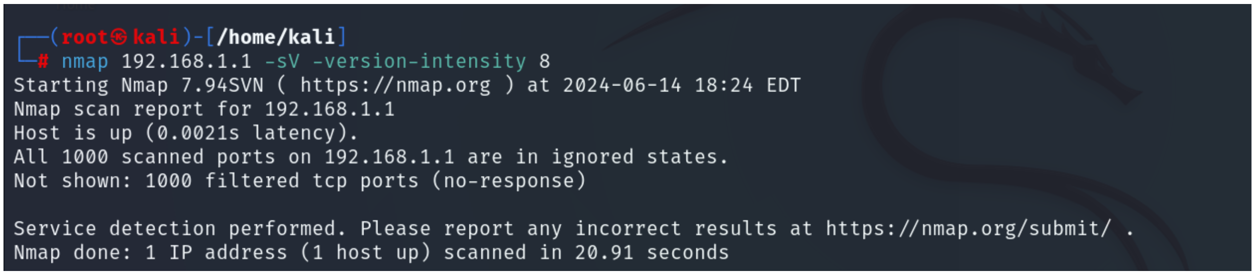
1. This command attempts to determine the version of the service running on port.



```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.1.1 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-14 18:24 EDT
Nmap scan report for 192.168.1.1
Host is up (0.017s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.83 seconds
```

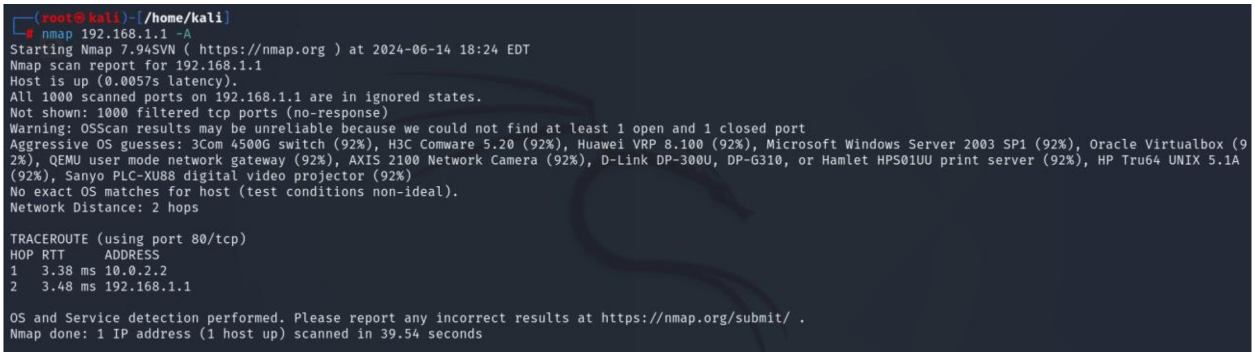
2. In this example the intensity level 0 to 9. Higher number increases possibility of correctness.



```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.1.1 -sV -version-intensity 8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-14 18:24 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0021s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.91 seconds
```

3. It enables OS detection, version detection, script scanning, and traceroute.

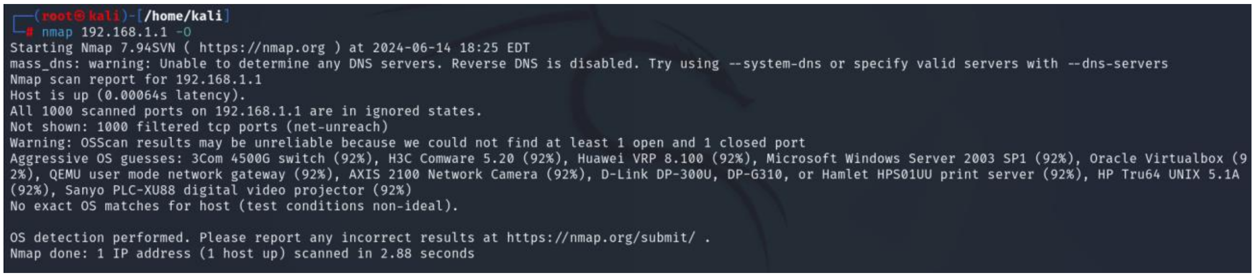


```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.1.1 -A
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-14 18:24 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0057s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: 3Com 4500G switch (92%), H3C Comware 5.20 (92%), Huawei VRP 8.100 (92%), Microsoft Windows Server 2003 SP1 (92%), Oracle Virtualbox (9
2%), QEMU user mode network gateway (92%), AXIS 2100 Network Camera (92%), D-Link DP-300U, DP-G310, or Hamlet HPS01UU print server (92%), HP Tru64 UNIX 5.1A
(92%), Sanyo PLC-XU88 digital video projector (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   3.38 ms 10.0.2.2
2   3.48 ms 192.168.1.1

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 39.54 seconds
```

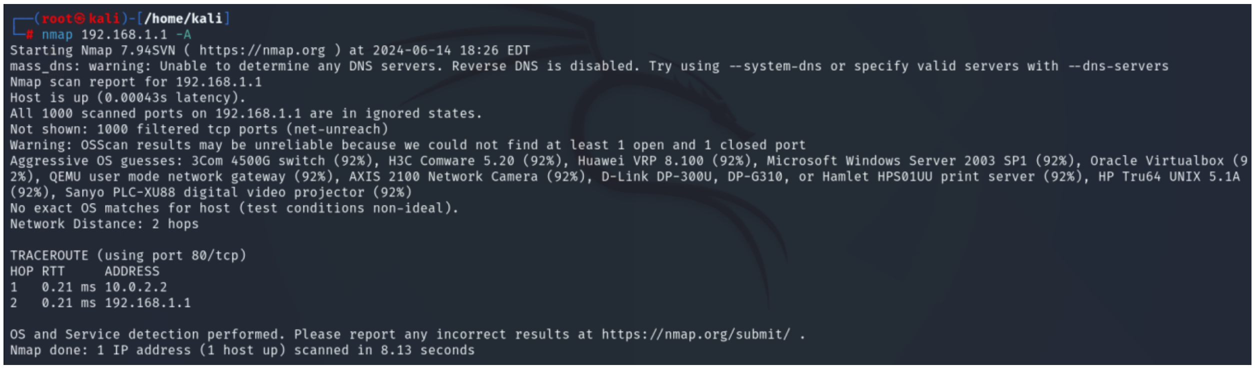
4. This command will do remote OS detection using TCP/IP stack fingerprinting



```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.1.1 -O
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-14 18:25 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.1
Host is up (0.00064s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (net-unreach)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: 3Com 4500G switch (92%), H3C Comware 5.20 (92%), Huawei VRP 8.100 (92%), Microsoft Windows Server 2003 SP1 (92%), Oracle Virtualbox (9
2%), QEMU user mode network gateway (92%), AXIS 2100 Network Camera (92%), D-Link DP-300U, DP-G310, or Hamlet HPS01UU print server (92%), HP Tru64 UNIX 5.1A
(92%), Sanyo PLC-XU88 digital video projector (92%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.88 seconds
```

5. It enables OS detection, version detection, script scanning, and traceroute



```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.1.1 -A
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-14 18:26 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.1
Host is up (0.00043s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (net-unreach)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: 3Com 4500G switch (92%), H3C Comware 5.20 (92%), Huawei VRP 8.100 (92%), Microsoft Windows Server 2003 SP1 (92%), Oracle Virtualbox (9
2%), QEMU user mode network gateway (92%), AXIS 2100 Network Camera (92%), D-Link DP-300U, DP-G310, or Hamlet HPS01UU print server (92%), HP Tru64 UNIX 5.1A
(92%), Sanyo PLC-XU88 digital video projector (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.21 ms 10.0.2.2
2   0.21 ms 192.168.1.1

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.13 seconds
```