Nmap Basics

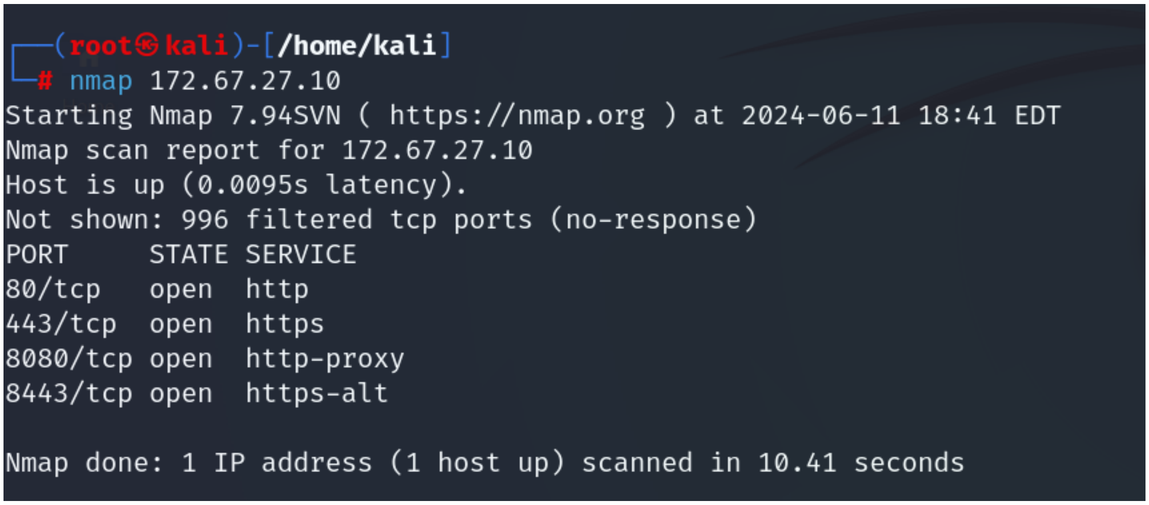
Nmap (Network Mapper) is a powerful open-source tool used for network discovery and security auditing. It was created by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich). Nmap is designed to efficiently scan large networks, but it also works well against single hosts.

Nmap is highly versatile and supports multiple scanning techniques and options, making it a favorite tool among network professionals for both offensive and defensive security tasks.

At the top-level, Nmap is defined as a tool that can detect or diagnose services that are running on an Internet-connected system by a network administrator in their networked system used to identify potential security flaws. It is used to automate redundant tasks, such as monitoring the service.

Example: -

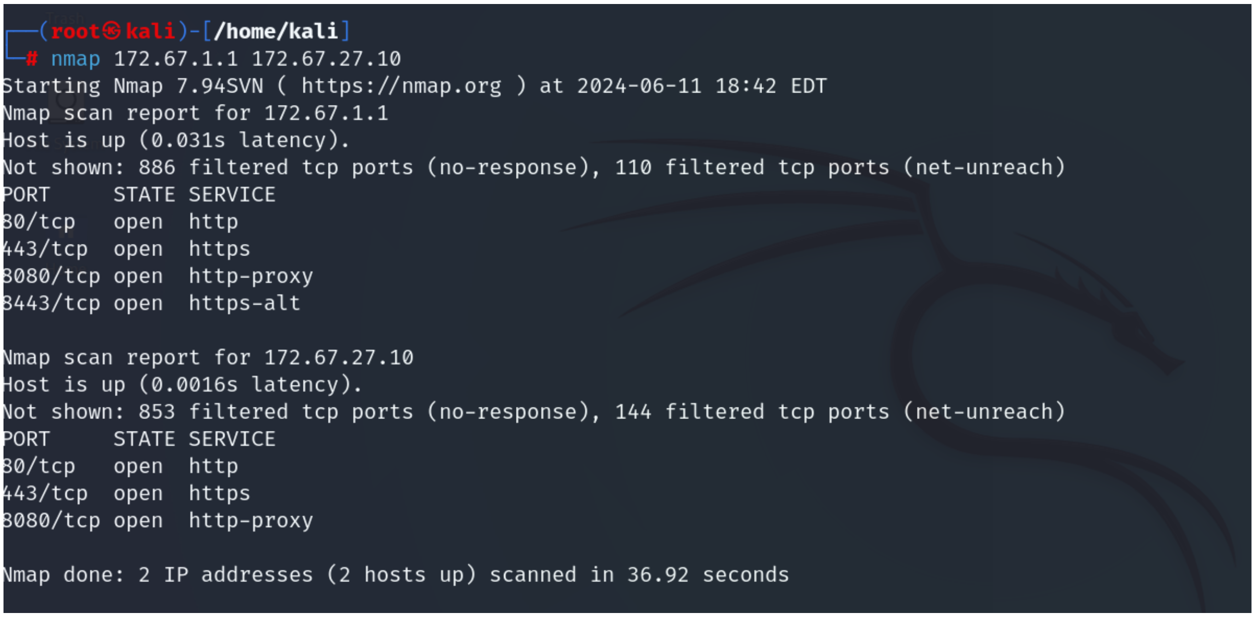
1. To scan a single IP we will use nmap command to the target domain.



```
┌──(root㉿kali)-[/home/kali]
└─# nmap 172.67.27.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-11 18:41 EDT
Nmap scan report for 172.67.27.10
Host is up (0.0095s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 10.41 seconds
```

2. To scan for specific Ips we will use the below command.

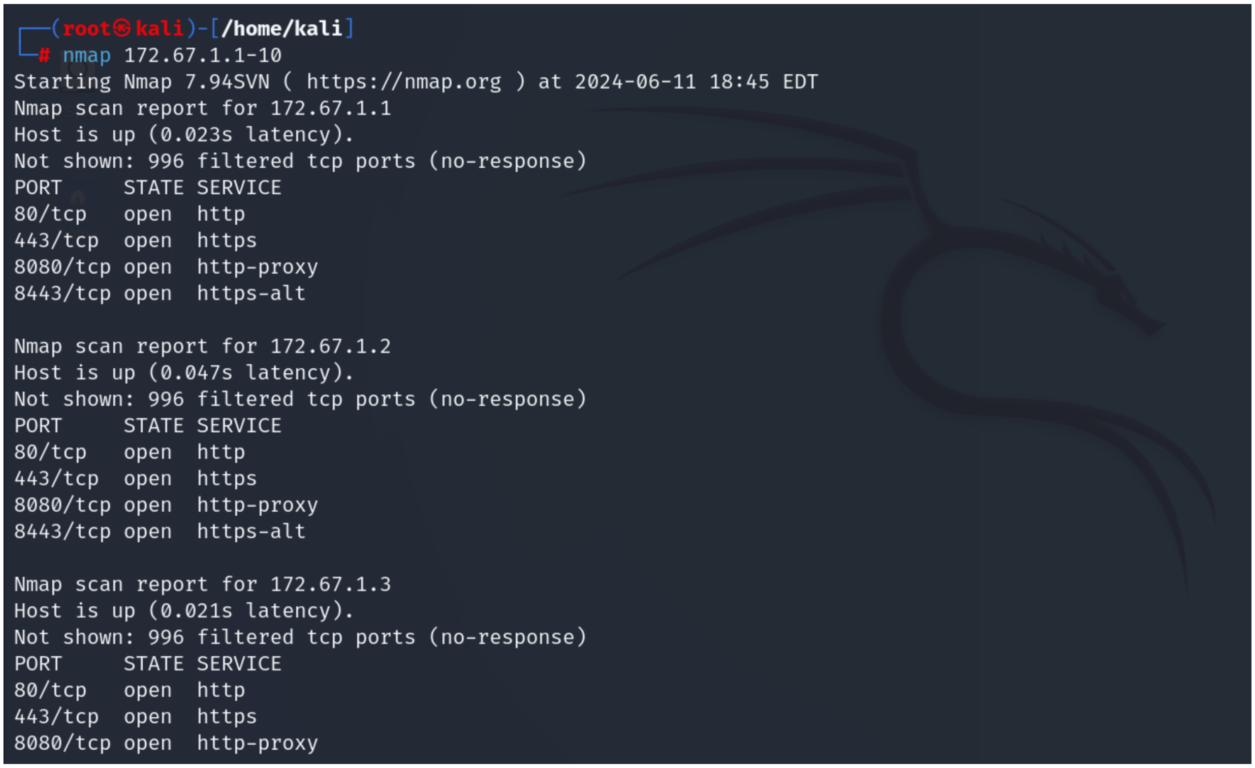


```
┌──(root㉿kali)-[/home/kali]
└─# nmap 172.67.1.1 172.67.27.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-11 18:42 EDT
Nmap scan report for 172.67.1.1
Host is up (0.031s latency).
Not shown: 886 filtered tcp ports (no-response), 110 filtered tcp ports (net-unreach)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap scan report for 172.67.27.10
Host is up (0.0016s latency).
Not shown: 853 filtered tcp ports (no-response), 144 filtered tcp ports (net-unreach)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy

Nmap done: 2 IP addresses (2 hosts up) scanned in 36.92 seconds
```

3. To scan a range for a range of ip addresses use – flag.

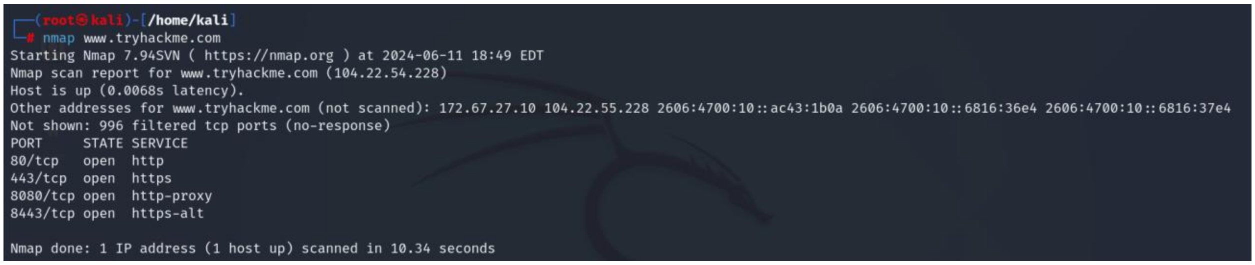


```
┌──(root㉿kali)-[/home/kali]
└─# nmap 172.67.1.1-10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-11 18:45 EDT
Nmap scan report for 172.67.1.1
Host is up (0.023s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap scan report for 172.67.1.2
Host is up (0.047s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap scan report for 172.67.1.3
Host is up (0.021s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
```

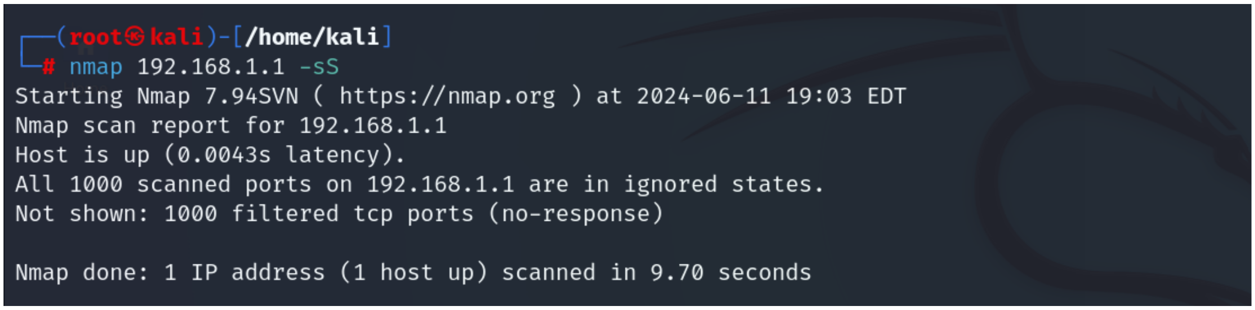
4. To scan for a domain use the below command.



```
┌──(root㉿kali)-[/home/kali]
└─# nmap www.tryhackme.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-11 18:49 EDT
Nmap scan report for www.tryhackme.com (104.22.54.228)
Host is up (0.0068s latency).
Other addresses for www.tryhackme.com (not scanned): 172.67.27.10 104.22.55.228 2606:4700:10::ac43:1b0a 2606:4700:10::6816:36e4 2606:4700:10::6816:37e4
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 10.34 seconds
```

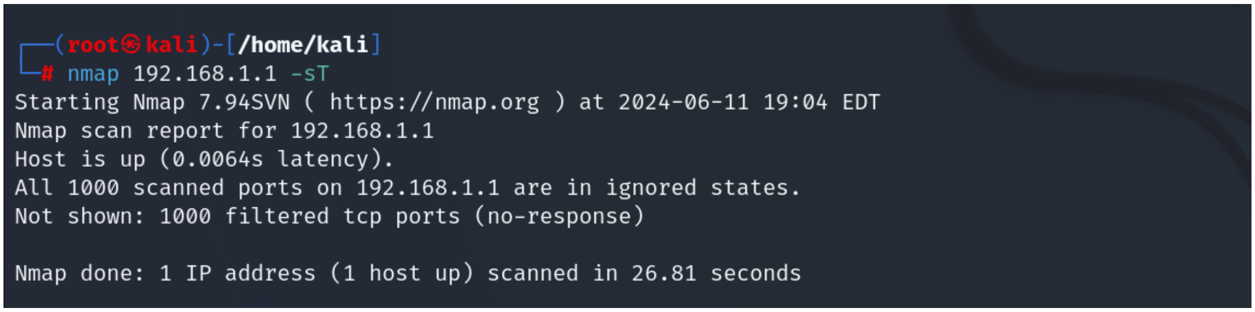
5. To scan for TCP SYN port scan (Default)



```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.1.1 -sS
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-11 19:03 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0043s 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 9.70 seconds
```

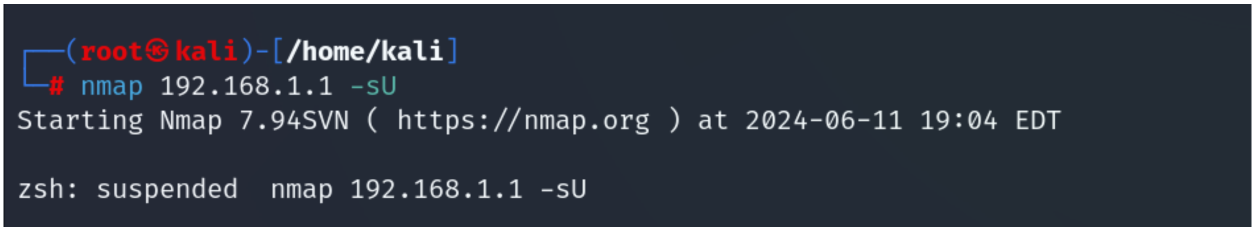
6. To TCP connect port scan (Default without root privilege)



```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.1.1 -sT
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-11 19:04 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0064s 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 26.81 seconds
```

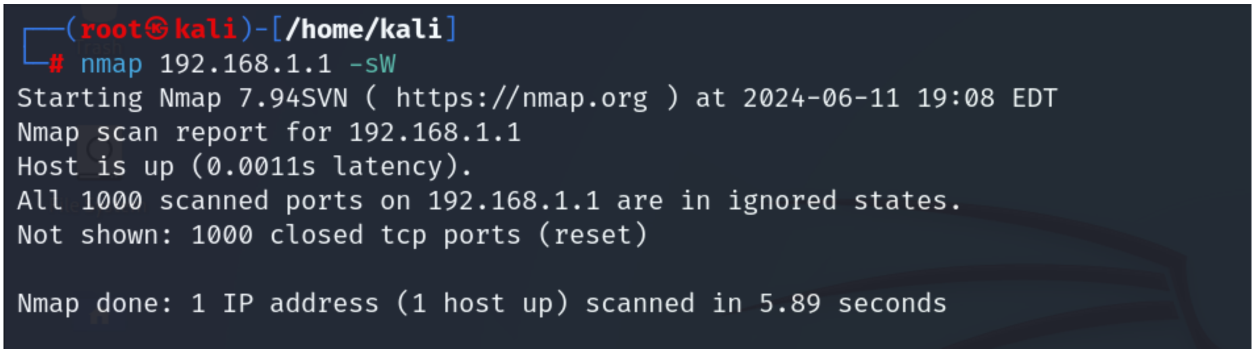
7. To scan for UDP port



```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.1.1 -sU
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-11 19:04 EDT

zsh: suspended  nmap 192.168.1.1 -sU
```

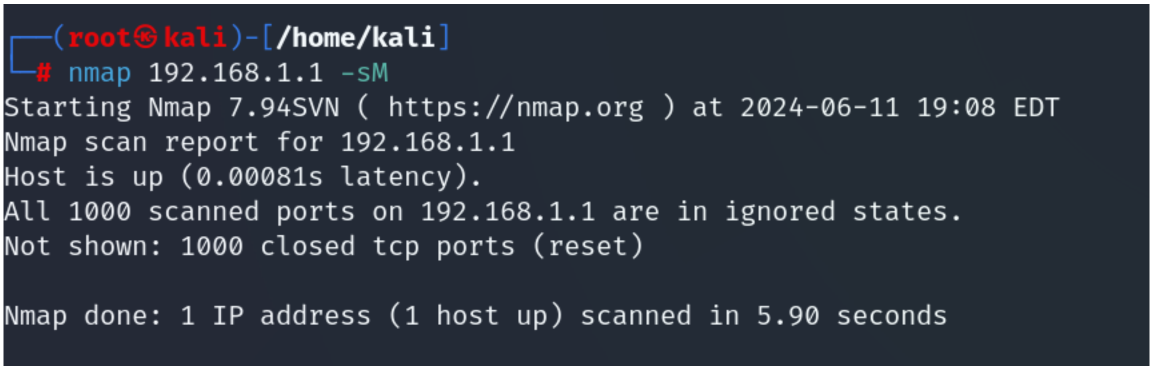
8. To scan TCP Window port



```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.1.1 -sW
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-11 19:08 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 5.89 seconds
```

9. To scan TCP Maimon port



```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.1.1 -sM
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-11 19:08 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00081s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 5.90 seconds
```