

## Beginner level

### Task 1: Basic scanning using nmap

- **Objective:** Perform a network scan to identify open ports and services using **Nmap**.
- **Tools:** Nmap

### Working

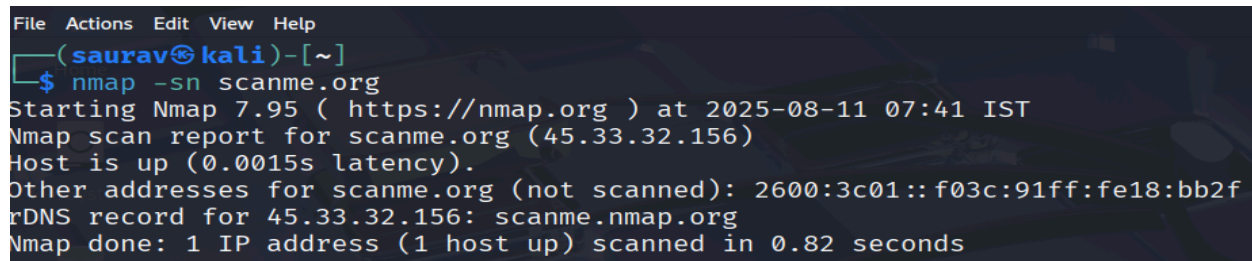
1. Requirements: virtual machine with kali linux installed, as it comes with preinstalled nmap and other tools so check whether it is there or not, if not install nmap using this command line

sudo apt update

sudo apt install nmap -y

2. To identify open ports and services, scanning using nmap for those websites and system which has given permission:

#### 2.1 1. Basic Host Discovery (Ping Scan)

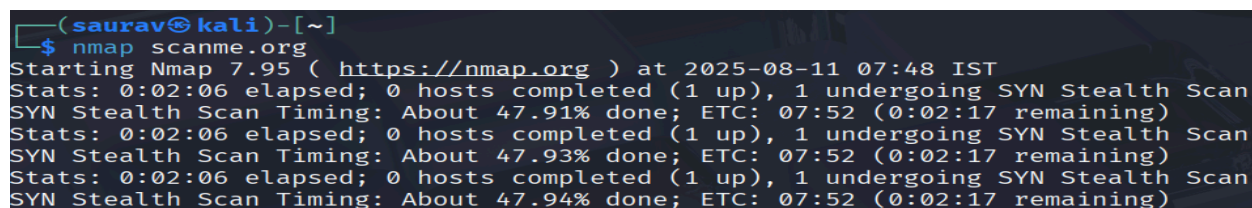


```
File Actions Edit View Help
(saurav@kali)-[~]
$ nmap -sn scanme.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-11 07:41 IST
Nmap scan report for scanme.org (45.33.32.156)
Host is up (0.0015s latency).
Other addresses for scanme.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
rDNS record for 45.33.32.156: scanme.nmap.org
Nmap done: 1 IP address (1 host up) scanned in 0.82 seconds
```

- -sn means *Ping Scan* — it checks if the host is up without scanning ports.
- Useful for confirming if a target is online.

**Output :** Shows whether the host is up, its IP address, and round-trip time.

#### 2.2 Basic Port Scan (Find Open Ports)



```
(saurav@kali)-[~]
$ nmap scanme.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-11 07:48 IST
Stats: 0:02:06 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 47.91% done; ETC: 07:52 (0:02:17 remaining)
Stats: 0:02:06 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 47.93% done; ETC: 07:52 (0:02:17 remaining)
Stats: 0:02:06 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 47.94% done; ETC: 07:52 (0:02:17 remaining)
```

- Scans the most common **1000 TCP ports** on the target.

**Output:** Lists open ports, their state, and the service running.

## 2.3 Scan Specific Ports

```
$ nmap -p 80,443 scanme.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-11 07:54 IST
Nmap scan report for scanme.org (45.33.32.156)
Host is up (0.0038s latency).
Other addresses for scanme.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
rDNS record for 45.33.32.156: scanme.nmap.org

PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https
```

-p lets you scan only specific ports (80 for HTTP, 443 for HTTPS).

**Output:** Shows only the status of the specified ports.

## 2.4 Aggressive Scan (OS + Services)

```
(saurav@kali)-[~]
$ nmap -A -p 80,443 scanme.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-11 08:06 IST
Nmap scan report for scanme.org (45.33.32.156)
Host is up (0.0032s latency).
Other addresses for scanme.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
rDNS record for 45.33.32.156: scanme.nmap.org

PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
|_http-favicon: Nmap Project
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
443/tcp    open  ssl/https?
|_ssl-date: TLS randomness does not represent time
|_ssl-cert: Subject: commonName=45.33.32.156
| Subject Alternative Name: DNS:45.33.32.156
| Not valid before: 2024-04-09T06:04:55
| Not valid after: 2034-04-07T06:04:55
```

-A enables:

- Version detection
- Script scanning
- Traceroute

## 2.5 Service Version Detection

```
(saurav@kali)-[~]
$ nmap -sV --version-intensity 2 -T4 --top-ports 100 -n scanme.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-11 11:05 IST
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 55.67% done; ETC: 11:05 (0:00:03 remaining)
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 62.00% done; ETC: 11:05 (0:00:02 remaining)
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 76.33% done; ETC: 11:05 (0:00:01 remaining)
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 77.67% done; ETC: 11:05 (0:00:01 remaining)
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 25.00% done; ETC: 11:05 (0:00:18 remaining)
Nmap scan report for scanme.org (45.33.32.156)
Host is up (0.073s latency).
Other addresses for scanme.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 77 closed tcp ports (reset)

```

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp	open	http	Apache httpd 2.4.7 ((Ubuntu))
31/tcp	open	http-proxy	Squid http proxy 6.9
139/tcp	filtered	netbios-ssn	
443/tcp	open	ssl/https?	
445/tcp	filtered	microsoft-ds	
513/tcp	filtered	login	
1025/tcp	filtered	NFS-or-IIS	
1026/tcp	filtered	LSA-or-nterm	
1027/tcp	filtered	IIS	
1028/tcp	filtered	unknown	
1029/tcp	filtered	ms-lsa	
1720/tcp	filtered	h323q931	
2000/tcp	filtered	cisco-sccp	
5060/tcp	filtered	sip	
10000/tcp	filtered	snet-sensor-mgmt	
32768/tcp	filtered	filenet-tms	
49152/tcp	filtered	unknown	
49153/tcp	filtered	unknown	
49154/tcp	filtered	unknown	
49155/tcp	filtered	unknown	
49156/tcp	filtered	unknown	
49157/tcp	filtered	unknown	

```
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

It detects the version and the service used , the ports and details about that , like open ,close.

-sV detects service versions running on open ports.

## 2.6 Direct ip scanning using nmap

```
(saurav@kali)-[~]
$ nmap 10.0.2.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-11 11:02 IST
Nmap scan report for 10.0.2.15
Host is up (0.0000030s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

It will direct scan the ip address given and tells about the open ports