In this project I will install NMap in Kali Linux and run a port scan.
First I install Nmap using the command sudo apt-get install nmap, then using nmap –version to make sure it is correctly installed.

```
┌──(root㉿e6567ac6f987)-[/]
└─# nmap --version
Nmap version 7.95 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
```

A default nmap will perform a SYN scan to see if the target system has the ports specified in the command, open, closed or filtered.

```
┌──(root㉿e6567ac6f987)-[/]
└─# nmap scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-27 03:38 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.19s latency).
Other addresses for scanme.nmap.org (not scanned): 45.33.32.156
Not shown: 995 closed tcp ports (reset)
PORT      STATE    SERVICE
19/tcp    filtered chargen
22/tcp    open     ssh
80/tcp    open     http
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 4.23 seconds
```

The -p## tag can be used when wanting to search for a specific port. For example, “nmap -p22,113,139 scanme.nmap.org” will run a SYN scan on only ports 22, 113 and 139.

```
└─# nmap -p22,113,139 scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-27 03:45 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.028s latency).
Other addresses for scanme.nmap.org (not scanned): 45.33.32.156

PORT    STATE  SERVICE
22/tcp  open   ssh
113/tcp closed ident
139/tcp closed netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

Nmap can receive more detailed information through the packet level using the packet-trace option and even further using a higher debug level such as -d5.

```
┌──(root㉿e6567ac6f987)-[/]
└─# nmap -d5 --packet-trace -p22,113,139 scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-27 03:47 UTC
Fetchfile found /usr/share/nmap/nmap-services
Fetchfile found /usr/share/nmap/nmap-protocols
Fetchfile found /usr/share/nmap/nmap.xsl
The max # of sockets we are using is: 0
--------------- Timing report ---------------
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
---------------------------------------------
Warning: Hostname scanme.nmap.org resolves to 2 IPs. Using 45.33.32.156.
Initiating Ping Scan at 03:47
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
```