TASK-1 Report

Date: 32/06/2025

If I download the Nmap tool from the official website on my laptop and perform the TCP SYN scan on my local range that would lead to disturb devices in my local range and might trigger security tools or be against the network policy. Thus performing the task on a Virtual Machine is important

Here I have used the virtual machine “Attack the Box” on TryHackMe to perform the task.

After starting the Nmap tool I used the ifconfig command to know the IP address and the Subnet mask of the VM I am using.

```
root@ip-10-10-3-239:~# ifconfig
docker0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        inet6 fe80::42:15ff:fe09:2d0  prefixlen 64  scopeid 0x20<link>
        ether 02:42:15:09:02:d0  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 74  bytes 10194 (10.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens5: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9001
        inet 10.10.3.239  netmask 255.255.0.0  broadcast 10.10.255.255
        inet6 fe80::eb:24ff:fee0:e6ad  prefixlen 64  scopeid 0x20<link>
        ether 02:eb:24:e0:e6:ad  txqueuelen 1000  (Ethernet)
        RX packets 42348  bytes 15692051 (15.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 26166  bytes 21120369 (21.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

the Ips I have got it 172.17.0.1 of docker to communicate with local containers so the range becomes 172.17.0.1/16 which will include total 65,534 usable IPs which will be too much so we will scan for the range 172.17.0.1/24 which will have total 254 usable Ips.

```
root@ip-10-10-3-239:~# nmap -sS 172.17.0.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2025-06-23 16:34 BST
Nmap scan report for ip-172-17-0-2.eu-west-1.compute.internal (172.17.0.2)
Host is up (0.0000050s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 02:42:AC:11:00:02 (Unknown)

Nmap scan report for ip-172-17-0-3.eu-west-1.compute.internal (172.17.0.3)
Host is up (0.0000040s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
8000/tcp open  http-alt
MAC Address: 02:42:AC:11:00:03 (Unknown)
```

The scan will be carried out using the command nmap -sS 172.17.0.1/24

Out of all the Ips 172.17.0.1, 172.17.0.2 and 172.17.0.3 responded. From the screenshot we can see port 80 and port 8000 which is the alternate for port 80 being open for both the hosts. Port 80 and port 8000 is responsible for Hypertext transfer protocol.

Now I will scan the ens5 IP 10.10.3.239 in the range 10.10.3.239/24.

```
root@ip-10-10-3-239:~# nmap -sS 10.10.3.239/24
Starting Nmap 7.80 ( https://nmap.org ) at 2025-06-23 16:35 BST
Nmap scan report for ip-10-10-3-11.eu-west-1.compute.internal (10.10.3.11)
Host is up (0.00021s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3000/tcp open  ppp
7777/tcp open  cbt
MAC Address: 02:31:82:88:A3:0F (Unknown)

Nmap scan report for ip-10-10-3-30.eu-west-1.compute.internal (10.10.3.30)
Host is up (0.00015s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
81/tcp   open  hosts2-ns
111/tcp  open  rpcbind
389/tcp  open  ldap
3389/tcp open  ms-wbt-server
```

```
Nmap scan report for ip-10-10-3-239.eu-west-1.compute.internal (10.10.3.239)
Host is up (0.0000060s latency).
Not shown: 990 closed ports
PORT     STATE    SERVICE
22/tcp   open     ssh
80/tcp   open     http
81/tcp   open     hosts2-ns
111/tcp  open     rpcbind
389/tcp  open     ldap
3389/tcp open     ms-wbt-server
5901/tcp open     vnc-1
6001/tcp open     X11:1
7777/tcp filtered cbt
7778/tcp filtered interwise

Nmap done: 256 IP addresses (11 hosts up) scanned in 6.00 seconds
```

Total 256 IP addresses scanned from which 11 hosts were up. Most common ports open were Port 22 is for ssh which is secure shell which allows the host to access a remote server. Port 80 for HTTP, Port 81 for hosts2-ns.