

Nmap More Detail

We could add `-reason` if we want Nmap to provide more details regarding its reasoning and conclusions eg:

```
pentester@TryHackMe$ sudo nmap -sS 10.10.252.27

Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-30 10:39 BST
Nmap scan report for ip-10-10-252-27.eu-west-1.compute.internal (10.10.252.27)
Host is up (0.0020s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
111/tcp   open  rpcbind
143/tcp   open  imap
MAC Address: 02:45:BF:8A:2D:6B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
```

```
Pentester Terminal

pentester@TryHackMe$ sudo nmap -sS --reason 10.10.252.27

Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-30 10:40 BST
Nmap scan report for ip-10-10-252-27.eu-west-1.compute.internal (10.10.252.27)
Host is up, received arp-response (0.0020s latency).
Not shown: 994 closed ports
Reason: 994 resets
PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack ttl 64
25/tcp    open  smtp    syn-ack ttl 64
80/tcp    open  http    syn-ack ttl 64
110/tcp   open  pop3    syn-ack ttl 64
111/tcp   open  rpcbind syn-ack ttl 64
143/tcp   open  imap    syn-ack ttl 64
MAC Address: 02:45:BF:8A:2D:6B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds
```

--reason allowed us to identify the type of packet sent, eg SYN-ACK. We could also use -vv or -v for verbose or very verbose.

```
Pentester Terminal

pentester@TryHackMe$ sudo nmap -sS -vv 10.10.252.27

Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-30 10:41 BST
Initiating ARP Ping Scan at 10:41
Scanning 10.10.252.27 [1 port]
Completed ARP Ping Scan at 10:41, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:41
Completed Parallel DNS resolution of 1 host. at 10:41, 0.00s elapsed
Initiating SYN Stealth Scan at 10:41
Scanning ip-10-10-252-27.eu-west-1.compute.internal (10.10.252.27) [1000 ports]
Discovered open port 22/tcp on 10.10.252.27
Discovered open port 25/tcp on 10.10.252.27
Discovered open port 80/tcp on 10.10.252.27
Discovered open port 110/tcp on 10.10.252.27
Discovered open port 111/tcp on 10.10.252.27
Discovered open port 143/tcp on 10.10.252.27
Completed SYN Stealth Scan at 10:41, 1.25s elapsed (1000 total ports)
Nmap scan report for ip-10-10-252-27.eu-west-1.compute.internal (10.10.252.27)
Host is up, received arp-response (0.0019s latency).
Scanned at 2021-08-30 10:41:02 BST for 1s
Not shown: 994 closed ports
Reason: 994 resets
PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack ttl 64
25/tcp    open  smtp    syn-ack ttl 64
80/tcp    open  http    syn-ack ttl 64
110/tcp   open  pop3    syn-ack ttl 64
111/tcp   open  rpcbind syn-ack ttl 64
143/tcp   open  imap    syn-ack ttl 64
MAC Address: 02:45:BF:8A:2D:6B (Unknown)

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds
Raw packets sent: 1002 (44.072KB) | Rcvd: 1002 (40.092KB)
```

If -vv does not satisfy, use -d for debugging details or -dd for even more details.

```
root@ip-10-10-170-242:~# nmap -sS -F --reason 10.10.149.1
Starting Nmap 7.80 ( https://nmap.org ) at 2025-07-26 13:58 BST
Nmap scan report for ip-10-10-149-1.eu-west-1.compute.internal (10.10.149.1)
Host is up, received arp-response (0.0059s latency).
Not shown: 91 closed ports
Reason: 91 resets
PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack ttl 64
25/tcp    open  smtp    syn-ack ttl 64
53/tcp    open  domain  syn-ack ttl 64
80/tcp    open  http    syn-ack ttl 64
110/tcp   open  pop3    syn-ack ttl 64
111/tcp   open  rpcbind syn-ack ttl 64
143/tcp   open  imap    syn-ack ttl 64
993/tcp   open  imaps   syn-ack ttl 64
995/tcp   open  pop3s   syn-ack ttl 64
MAC Address: 02:66:04:D9:98:39 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
root@ip-10-10-170-242:~#
```

There is our attack information.

Answer the questions below

Launch the AttackBox if you haven't done so already. After you make sure that you have terminated the VM from Task 4, start the VM for this task. Wait for it to load completely, then open the terminal on the AttackBox and use Nmap with `nmap -sS -F --reason 10.10.149.1` to scan the VM. What is the reason provided for the stated port(s) being open?

✓ Correct Answer