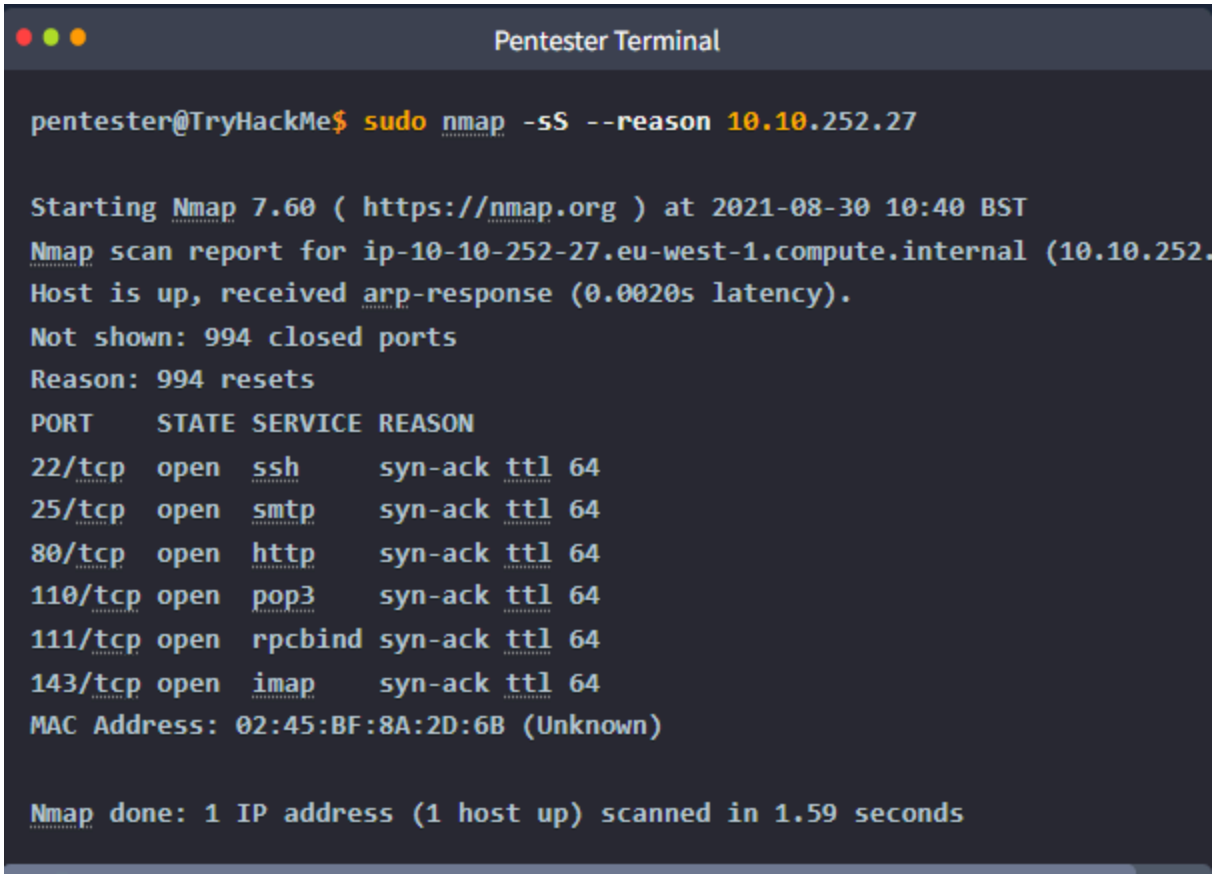
Nmap More Detail

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

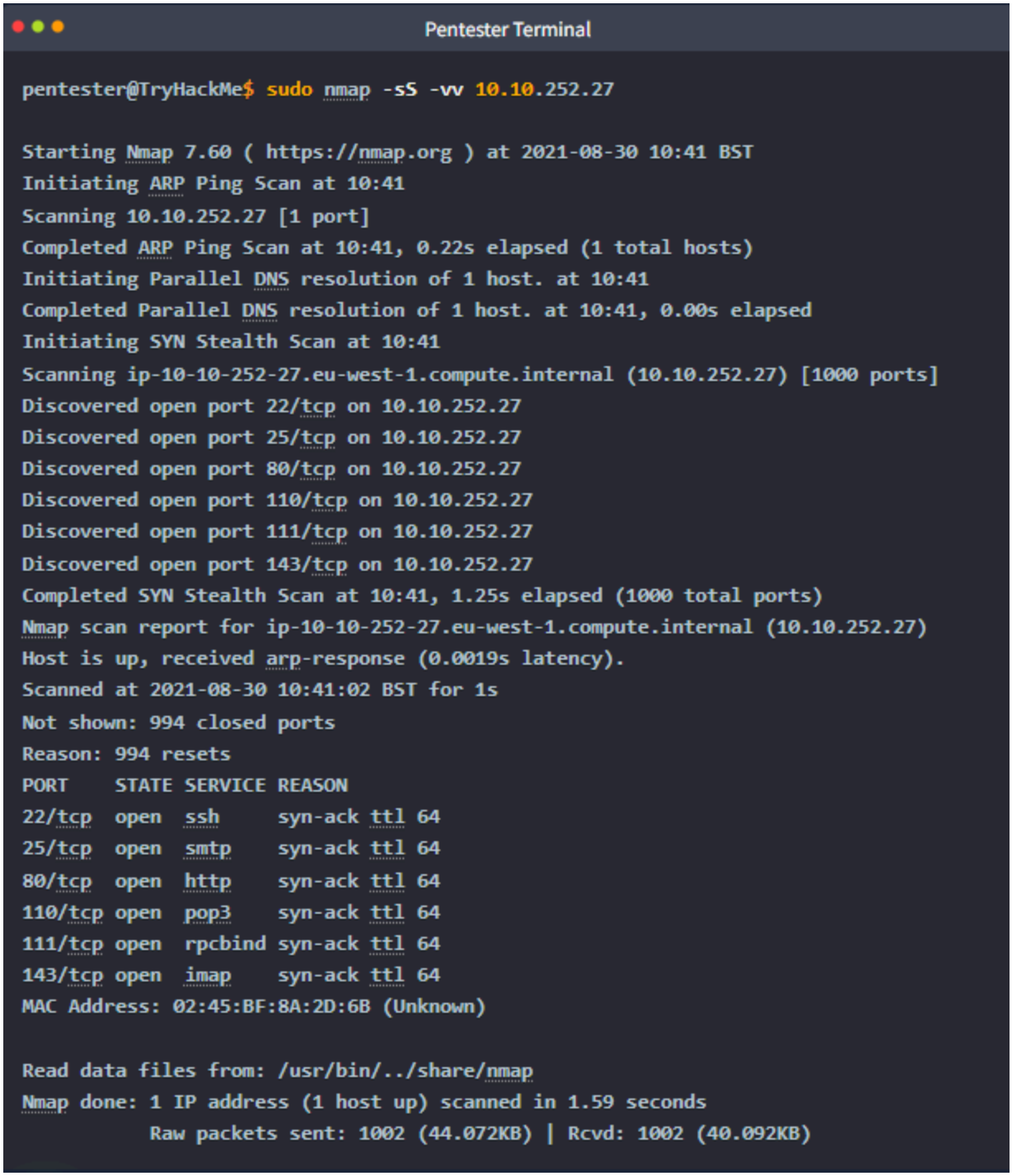
```
pentester@TryHackMe$ sudo nmap -sS 10.10.252.27

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
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
```



--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.



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.