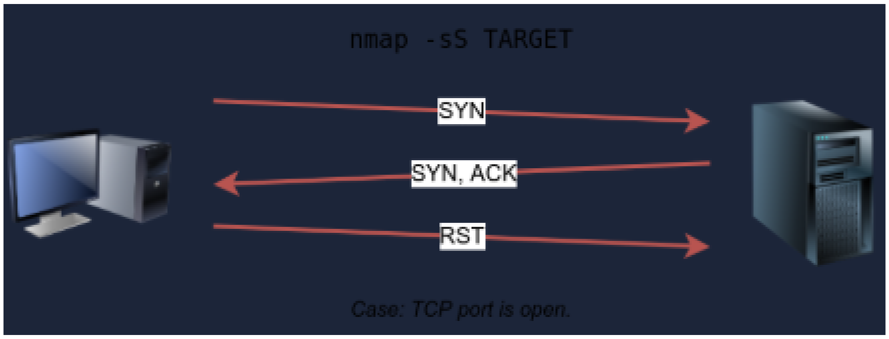
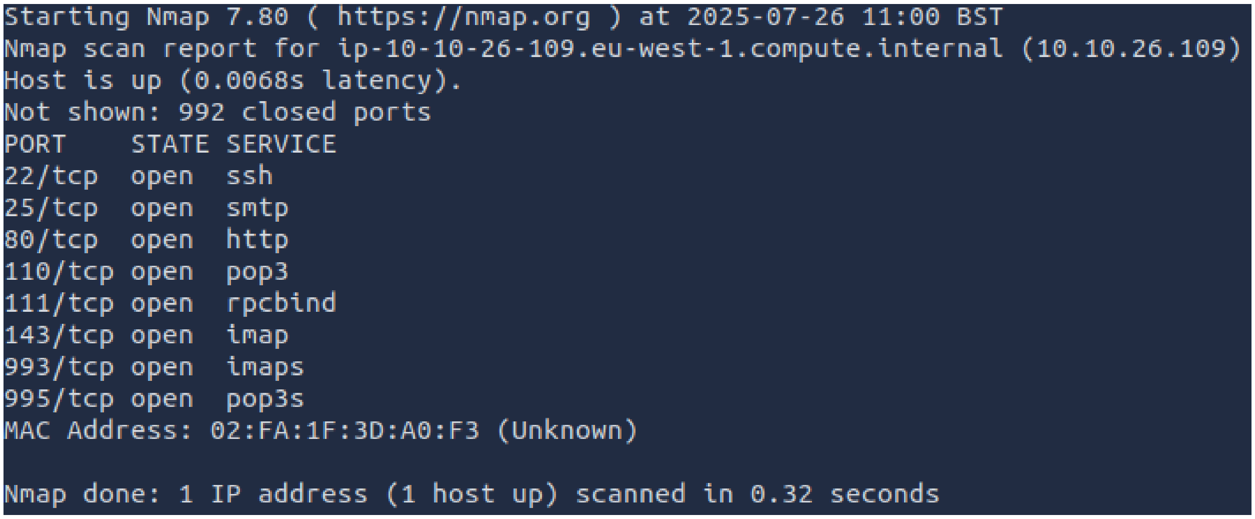
Nmap SYN Scan

A SYN scan or “Syncronized” scan is based on the flag “SYN” used to initiate a 3-way hand shake and synchronize sequence numbers with other hosts. This should be randomly set during a TCP connection, once it is established.

Unprivileged users are limited to connect scan. However, the default scan mode is a SYN scan. **This scan requires a privileged root or sudoer** user to run it. SYN scan does **not need to complete the 3-way handshake** but instead it tears down the connection once it receives a response from the server. Because we **didn’t establish a TCP connection,** this **decreases the chances of the scan being logged.** Which is excellent as an offensive tester!

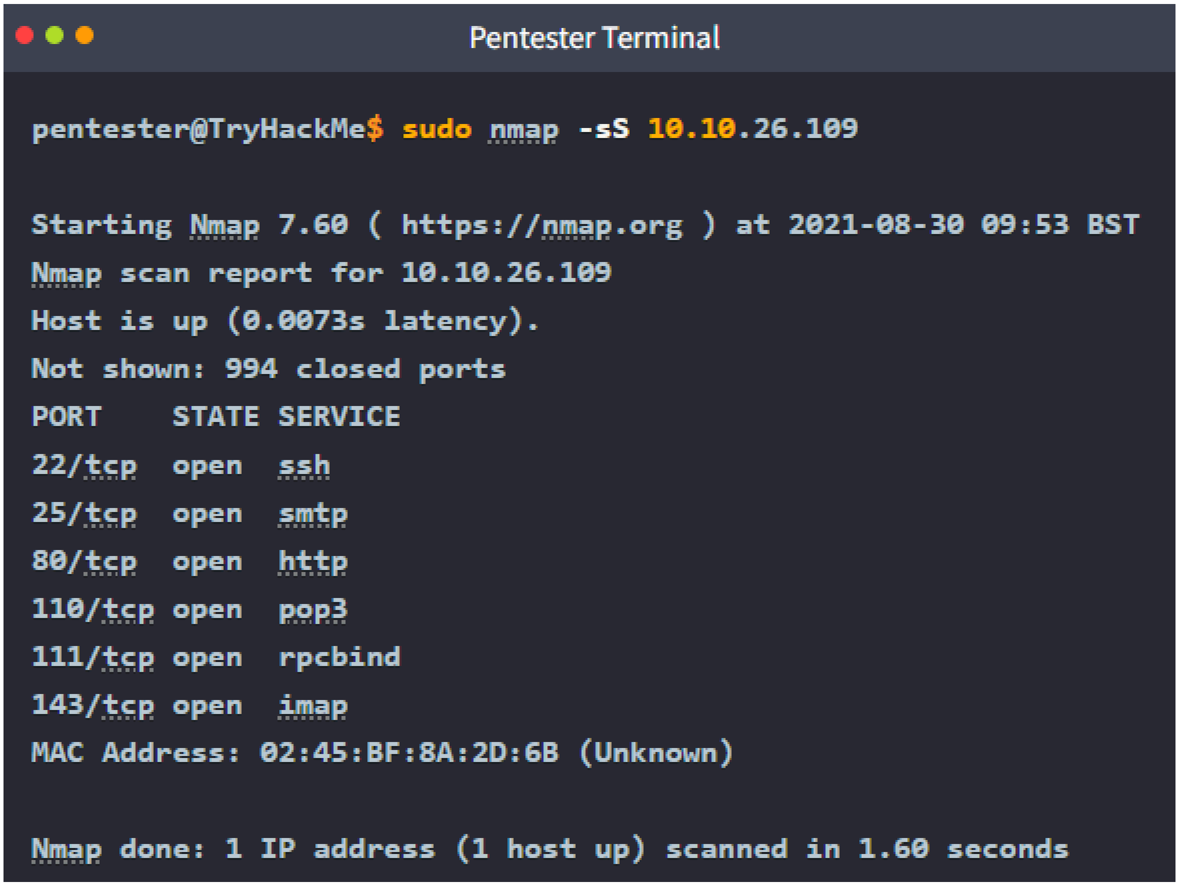


So how do we do this?
Nmap - sS 10.10.26.109 - We will use this for example and see what happens.



```
Starting Nmap 7.80 ( https://nmap.org ) at 2025-07-26 11:00 BST
Nmap scan report for ip-10-10-26-109.eu-west-1.compute.internal (10.10.26.109)
Host is up (0.0068s latency).
Not shown: 992 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
993/tcp open  imaps
995/tcp open  pop3s
MAC Address: 02:FA:1F:3D:A0:F3 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
```



```
pentester@TryHackMe$ sudo nmap -sS 10.10.26.109

Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-30 09:53 BST
Nmap scan report for 10.10.26.109
Host is up (0.0073s 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
```

So we are comparing examples again, similarly to our previous "Nmap Port Scan". The example as opposed to our scan shows comparable differences. Such as our example yielded 8 open ports, whereas the example only yielded 6. A sizable difference.

So in our test the ports opened that wasn't open on the example were:

IMAPS and POP3S note these ports are on **993 and 995.** So the secure connections were missed.