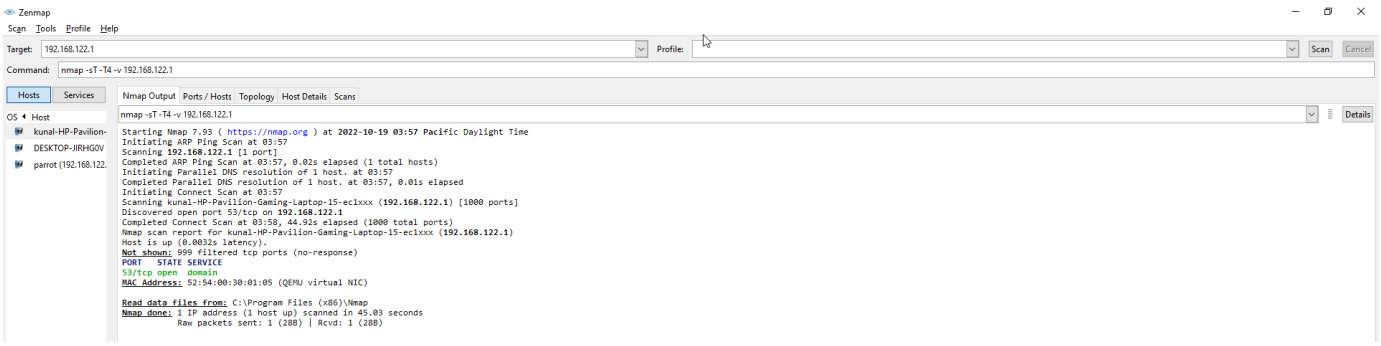
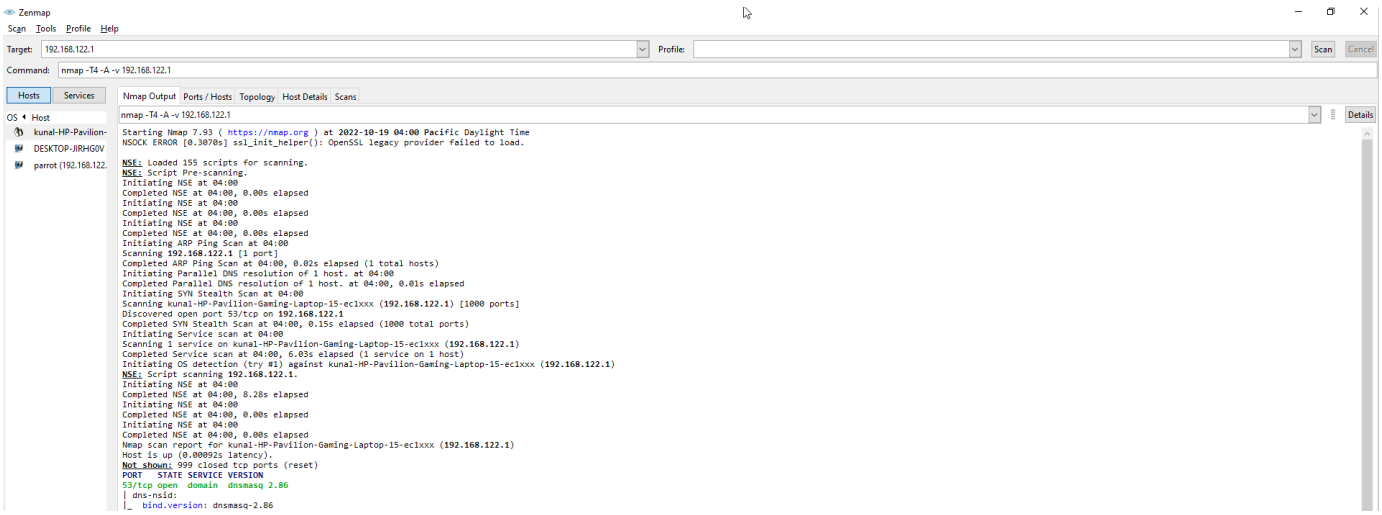
Scanning

Port Discovery using TCP (SYN) (3-way handshake)



Aggersive Scanning (OS,hosts,Port)



Script for OS Detection

Nmap Script for OS Detection

```
nmap --script smb-os-discovery.nse 10.10.10.x
```

Basic Command

Basic command

```
nmap -p- -sC -sV -O -A -T4 -oA nmapOutputfile 10.10.X.X
```

- -p- -> Scans all the ports from 0 to 65535 available on the IP
- -sC -> Runs default scripts
- -sV -> version enumeration or service version
- -O -> OS enumeration
- -A -> Enumerate all the stuff as much as it can
- -T4 -> fast as time 4 (default is 3)
- -oA -> store the output on 3 types of format(nmap, gnmap, xml)

To check ports in use

```
sudo lsof -i -P -n | grep LISTEN
```