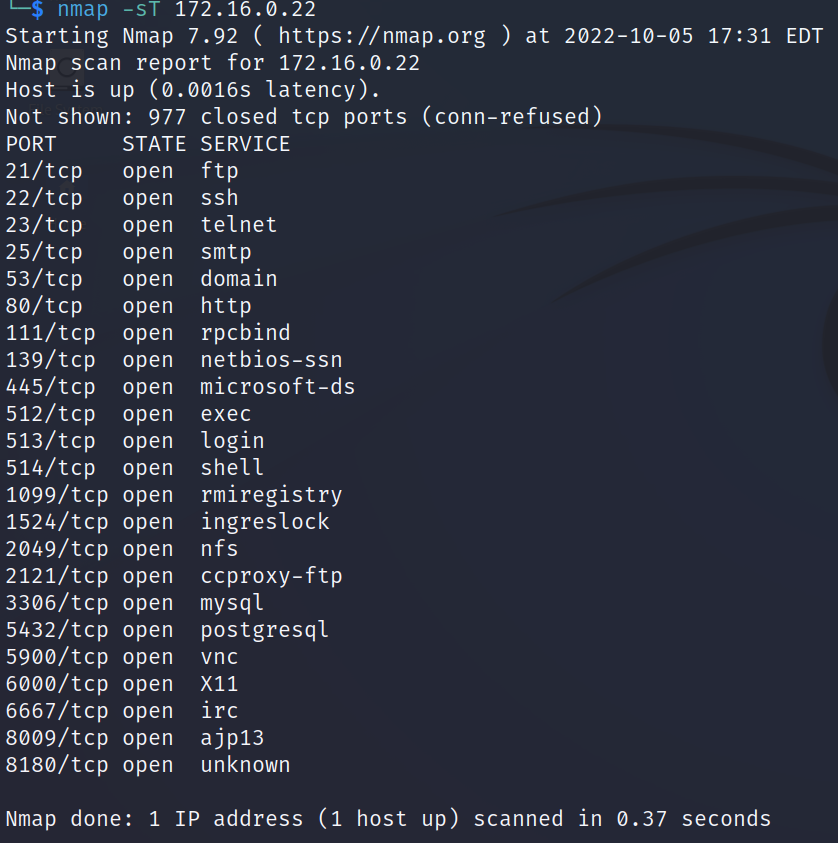
Tully Martin

CS332 Section 1 Armend Mala

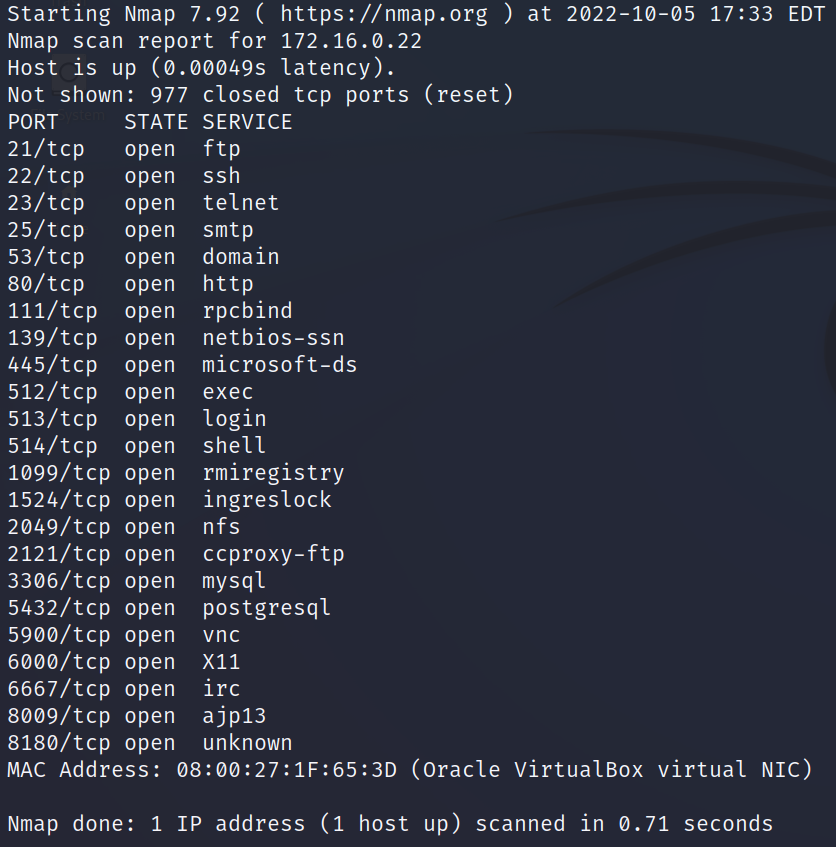
Lab 2 Port Scanning

**TCP Port Scanning**

Nmap -sT

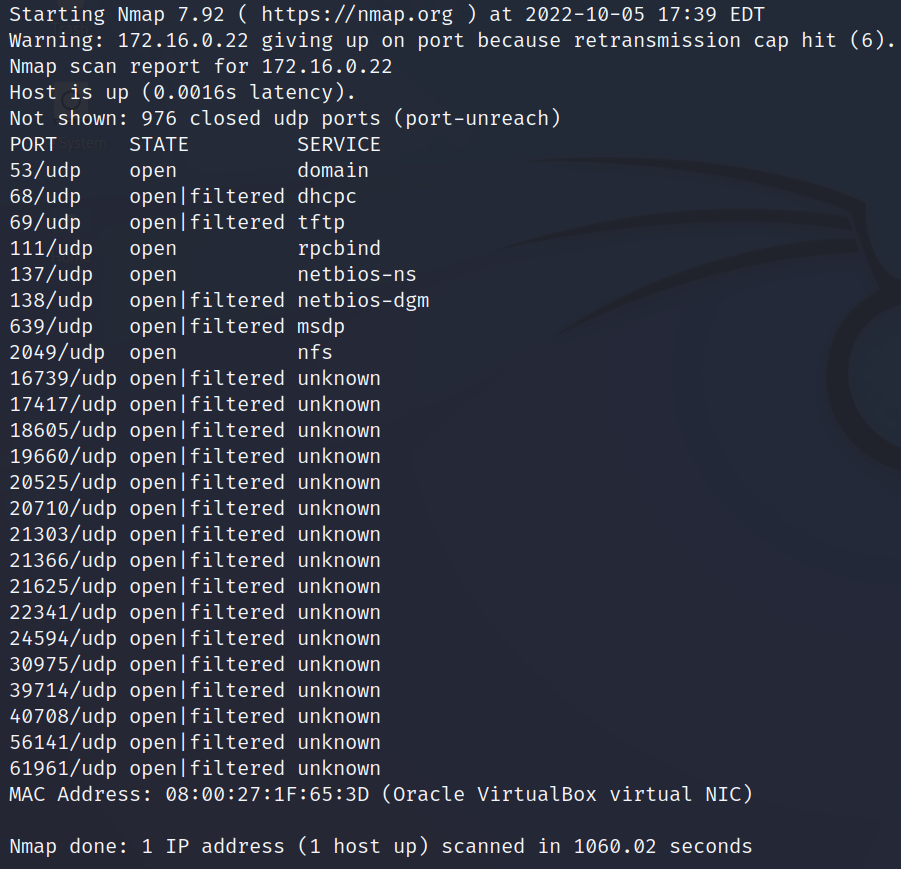


Nmap -sS



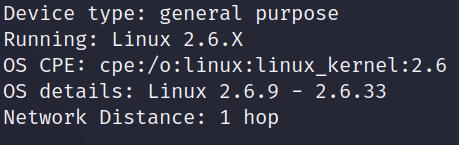
1. There is no difference in the ports and services listed, -sS option shows us MAC Address
2. Telnet
3. http
4. No
5. 5900

**UDP Port Scanning**



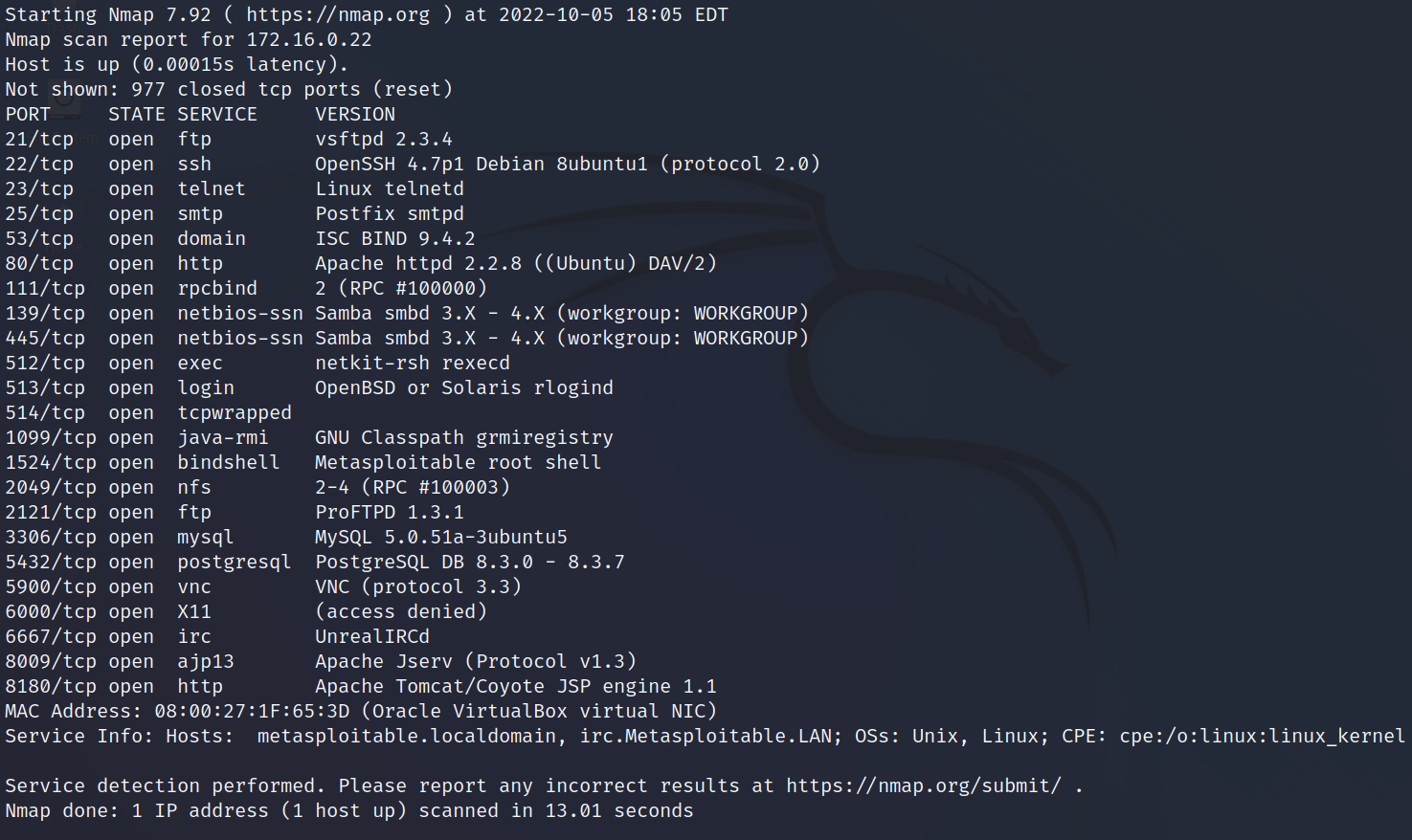
1. -T option is timing templates indicating how aggressive you want your scan to be. A full UDP scan on all the ports is exhaustive so we use the option -T4 which is a scan with aggressive speed.
2. 53, 111, 137, 2049.
3. domain, rpcbind, netbios-ns, nfs.
4. DNS.

**OS Detection**



1. Linux 2.6.X
2. Linux 2.6.9 – 2.6.33

**Service Version Detection**



1. vsftpd 2.3.4
2. VNC (protocol 3.3)
3. ProFTPD 1.3.1