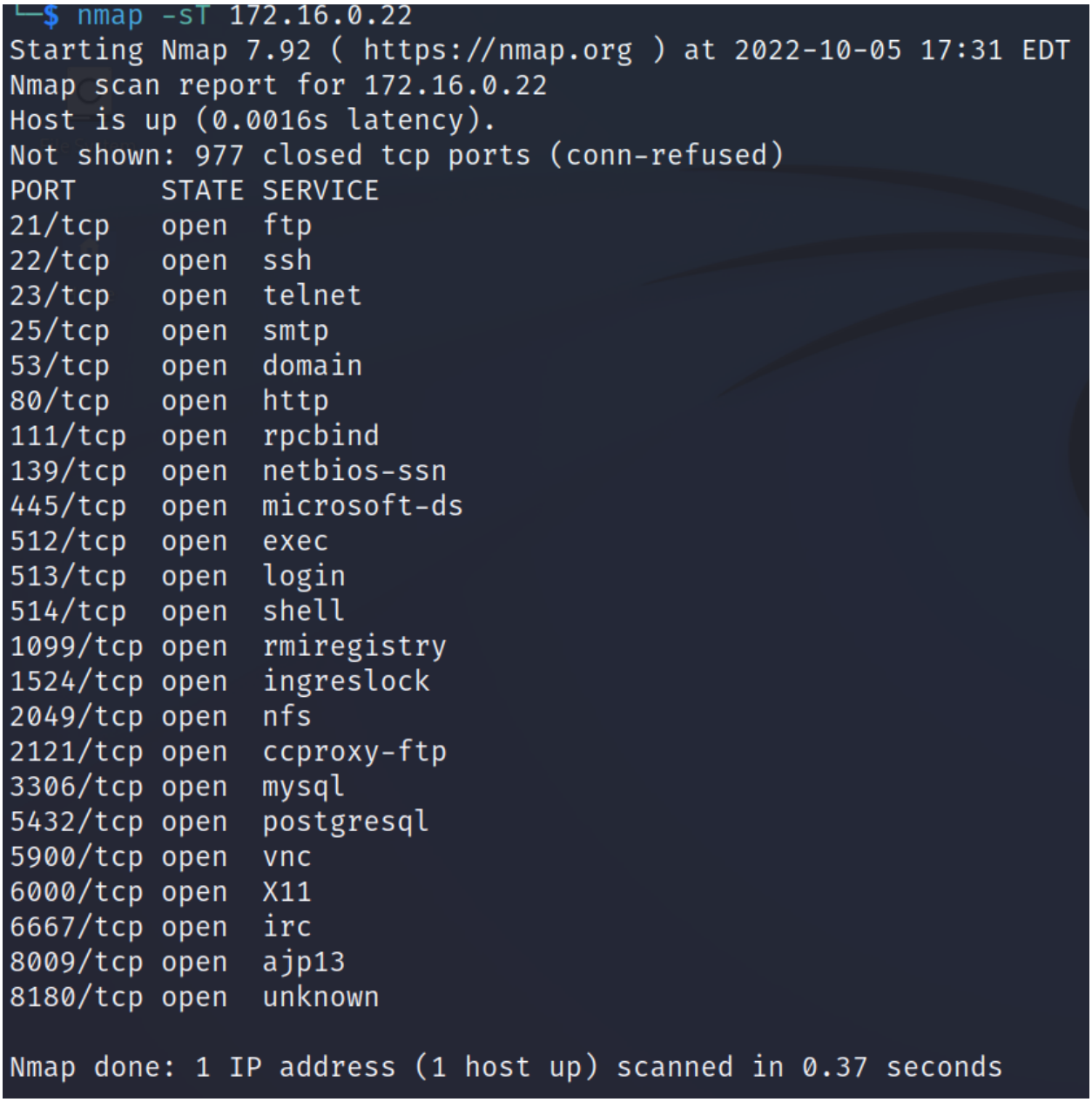
Tully Martin

CS332 Section 1 Armend Mala

Lab 2 Port Scanning

TCP Port Scanning

Nmap -sT



Nmap -sS

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-05 17:33 EDT
Nmap scan report for 172.16.0.22
Host is up (0.00049s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:1F:65:3D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.71 seconds
```

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

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-05 17:39 EDT
Warning: 172.16.0.22 giving up on port because retransmission cap hit (6).
Nmap scan report for 172.16.0.22
Host is up (0.0016s latency).
Not shown: 976 closed udp ports (port-unreach)
PORT      STATE         SERVICE
53/udp    open          domain
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
111/udp   open          rpcbind
137/udp   open          netbios-ns
138/udp   open|filtered netbios-dgm
639/udp   open|filtered msdp
2049/udp  open          nfs
16739/udp open|filtered unknown
17417/udp open|filtered unknown
18605/udp open|filtered unknown
19660/udp open|filtered unknown
20525/udp open|filtered unknown
20710/udp open|filtered unknown
21303/udp open|filtered unknown
21366/udp open|filtered unknown
21625/udp open|filtered unknown
22341/udp open|filtered unknown
24594/udp open|filtered unknown
30975/udp open|filtered unknown
39714/udp open|filtered unknown
40708/udp open|filtered unknown
56141/udp open|filtered unknown
61961/udp open|filtered unknown
MAC Address: 08:00:27:1F:65:3D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1060.02 seconds
```

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

```
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

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

Service Version Detection

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-05 18:05 EDT
Nmap scan report for 172.16.0.22
Host is up (0.00015s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:1F:65:3D (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.01 seconds
```

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