Kevin Huang
CSS 537
Lab 2: Network Scanning using nmap
01/22/2022

Task 1: Getting started with nmap

- -sn: do not do a port scan after host discovery

```
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
```

- -PO: sends an IP packet with the specified protocol number set in it's IP header

```
-PO[protocol list]: IP Protocol Ping
-n/-R: Never do DNS resolution/Always
```

- -PS: sends an empty TCP packet with the SYN flag set

```
             -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to gi
ven ports
```

- -PU: sends a UDP packet to the given ports

```
             -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to gi
ven ports
```

- -sO: determine which IP protocols are supported by target machines

```
-sO: IP protocol scan
```

- -sV: detects the version

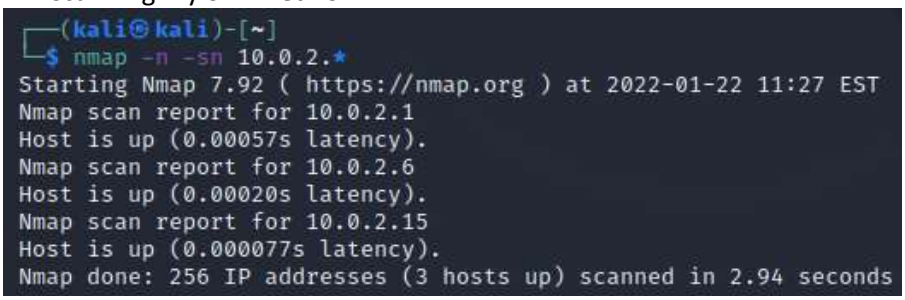
```
           SERVICE/VERSION DETECTION:
             -sV: Probe open ports to determine service/version info
```

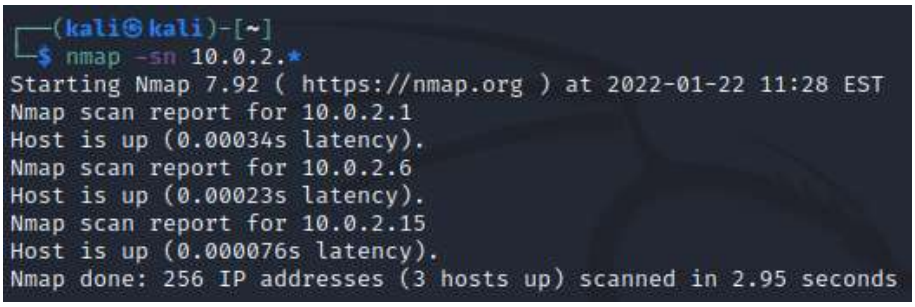
- -O: enables OS detection

```
OS DETECTION:
  -O: Enable OS detection
```

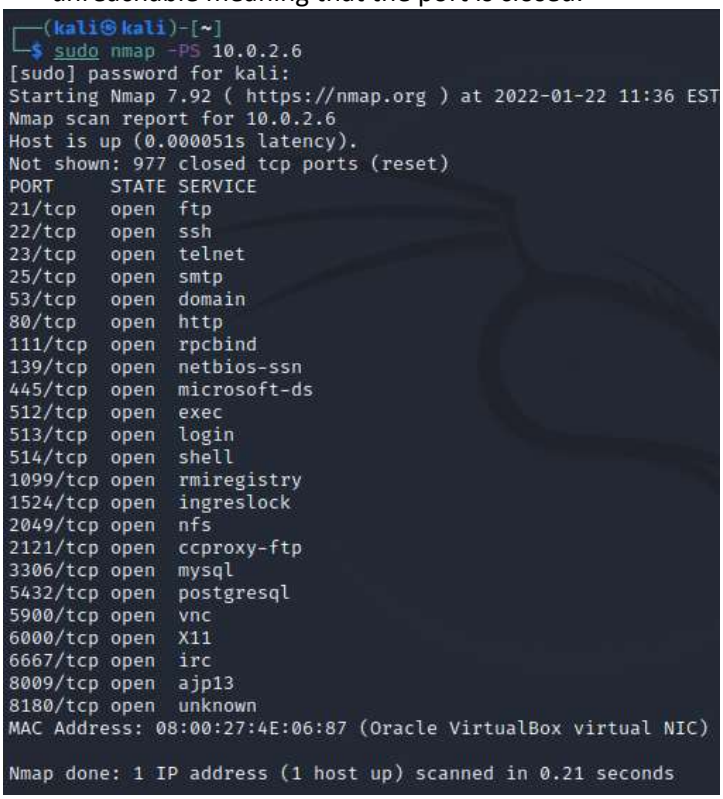
Task 2: Using nmap to conduct a reconnaissance of your network

1. The -n option is used so that the scan does not do DNS resolution. I can see that running without the -n option did not have any noticeable difference since there was no DNS resolution needed when scanning my own network.





2. The other host machine that I have on the network is 10.0.2.6. I found that there are 23 open TCP ports on this host. UDP is a connectionless protocol, unlike TCP we will not get a response back for a successful request. We can attempt to ping all the UDP ports and if we get a destination unreachable meaning that the port is closed.



3. I was not able to identify any open ports on my own machine. It says that the 1000 scanned ports are in ignored states.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -PS 10.0.2.15
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-22 12:02 EST
Nmap scan report for 10.0.2.15
Host is up (0.0000010s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

4. With the -sO scan, there were additional protocols that were found. There were new protocols found such as igmp, xtp, udplite, and hip.

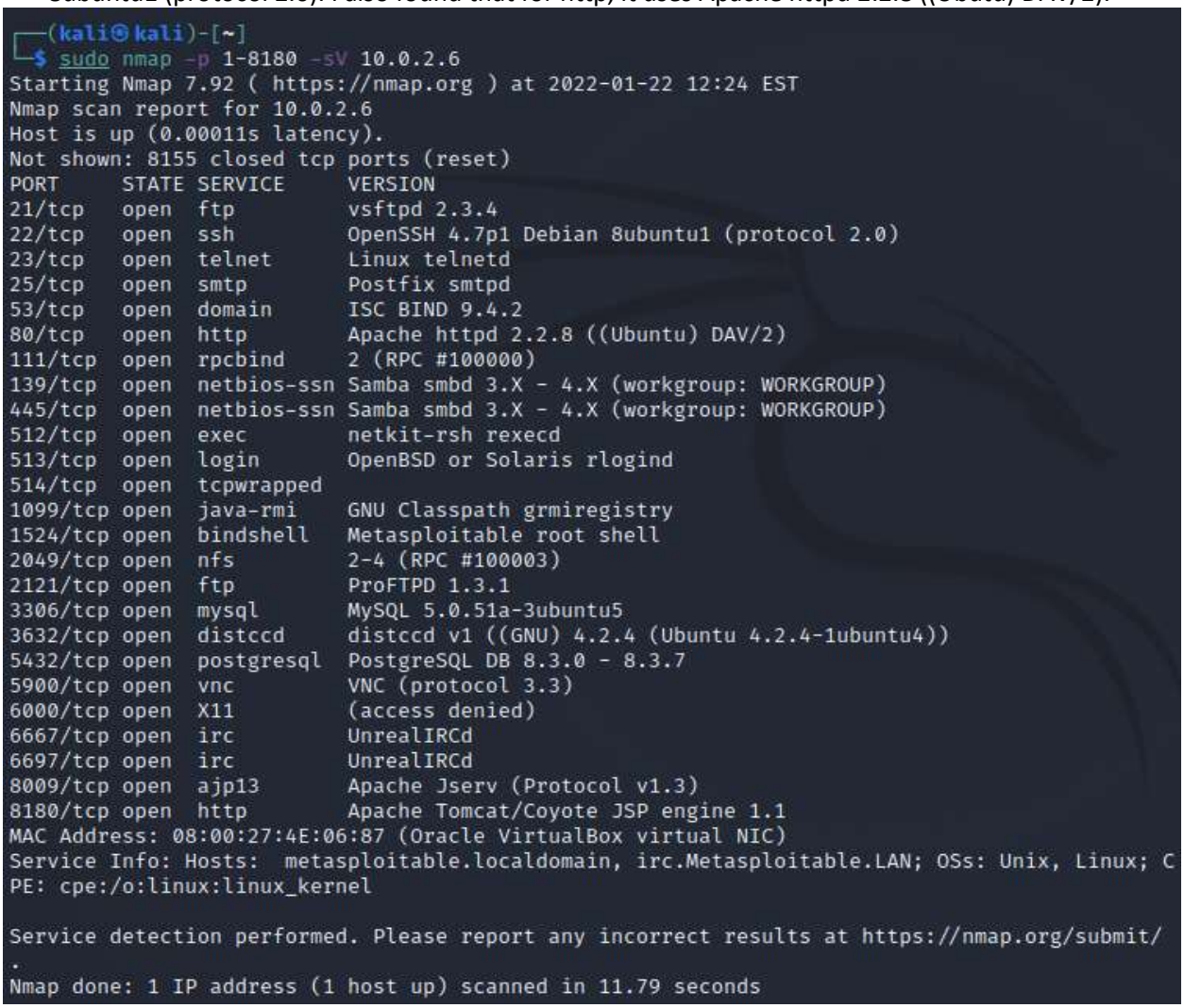
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sO 10.0.2.6
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-22 12:03 EST
Warning: 10.0.2.6 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.0.2.6
Host is up (0.00018s latency).
Not shown: 246 closed n/a protocols (proto-unreach)
PROTOCOL STATE         SERVICE
1        open          icmp
2        open|filtered igmp
6        open          tcp
17       open          udp
36       open|filtered xtp
136      open|filtered udplite
139      open|filtered hip
217      open|filtered unknown
221      open|filtered unknown
227      open|filtered unknown
MAC Address: 08:00:27:4E:06:87 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 271.33 seconds
```

5. Using the -O option when scanning 10.0.2.6, I found that nmap thinks that it is running Linux 2.6.X. Also, it found that the MAC address is 08:00:27:4E:06:87 which matches. It was not able to find what operating system the attacker machine was running.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 10.0.2.6
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-22 12:13 EST
Nmap scan report for 10.0.2.6
Host is up (0.00014s 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: 08:00:27:4E:06:87 (Oracle VirtualBox virtual NIC)
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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.76 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 10.0.2.15
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-22 12:17 EST
Nmap scan report for 10.0.2.15
Host is up (0.0000080s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.72 seconds
```

6. I found that I can specify a port range to scan with -p option. I used the version scan option -sV to scan open ports that I found previous. For SSH, the target host uses version OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0). I also found that for http, it uses Apache httpd 2.2.8 ((Ubutu) DAV/2).



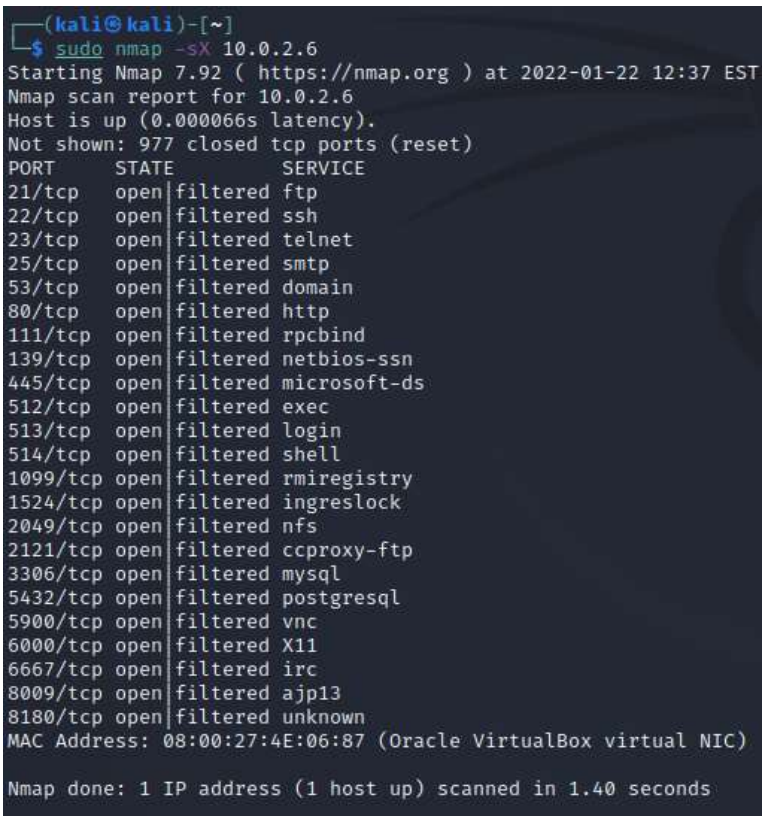
7. TCP Connect scan:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 10.0.2.6
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-22 12:39 EST
Nmap scan report for 10.0.2.6
Host is up (0.00033s latency).
Not shown: 977 closed tcp ports (conn-refused)
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: 08:00:27:4E:06:87 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

TCP SYN scan:

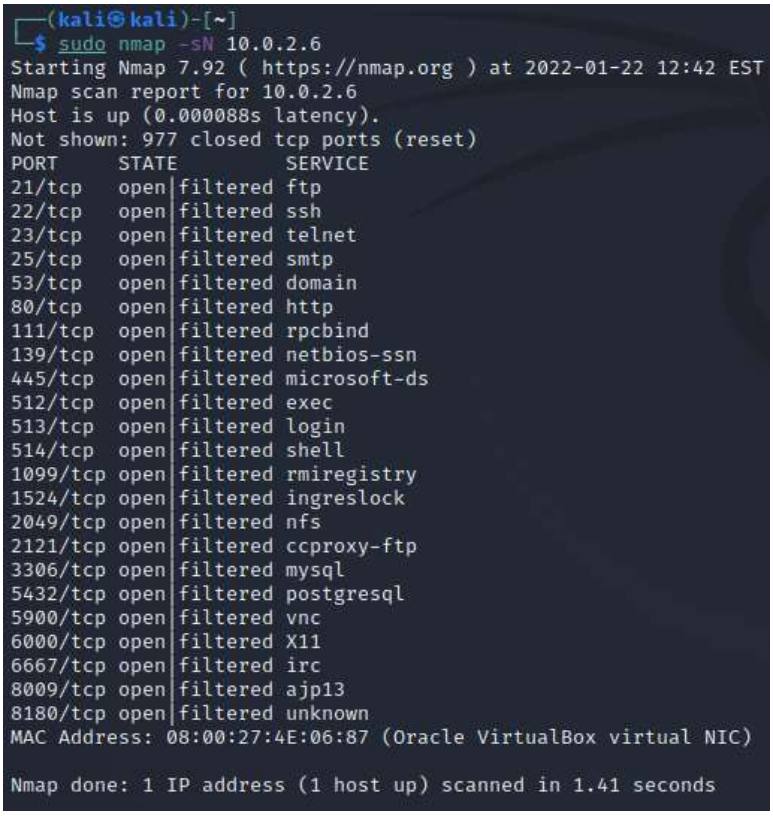
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 10.0.2.6
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-22 12:40 EST
Nmap scan report for 10.0.2.6
Host is up (0.000057s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   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: 08:00:27:4E:06:87 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

Xmas -sX scan:



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sX 10.0.2.6
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-22 12:37 EST
Nmap scan report for 10.0.2.6
Host is up (0.000066s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
53/tcp   open|filtered domain
80/tcp   open|filtered http
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
512/tcp  open|filtered exec
513/tcp  open|filtered login
514/tcp  open|filtered shell
1099/tcp open|filtered rmiregistry
1524/tcp open|filtered ingreslock
2049/tcp open|filtered nfs
2121/tcp open|filtered ccproxy-ftp
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
5900/tcp open|filtered vnc
6000/tcp open|filtered X11
6667/tcp open|filtered irc
8009/tcp open|filtered ajp13
8180/tcp open|filtered unknown
MAC Address: 08:00:27:4E:06:87 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.40 seconds
```

Null scan:



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sN 10.0.2.6
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-22 12:42 EST
Nmap scan report for 10.0.2.6
Host is up (0.000088s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
53/tcp   open|filtered domain
80/tcp   open|filtered http
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
512/tcp  open|filtered exec
513/tcp  open|filtered login
514/tcp  open|filtered shell
1099/tcp open|filtered rmiregistry
1524/tcp open|filtered ingreslock
2049/tcp open|filtered nfs
2121/tcp open|filtered ccproxy-ftp
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
5900/tcp open|filtered vnc
6000/tcp open|filtered X11
6667/tcp open|filtered irc
8009/tcp open|filtered ajp13
8180/tcp open|filtered unknown
MAC Address: 08:00:27:4E:06:87 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.41 seconds
```