Joseph Tsai
CSS 537 – Lab 2: NMAP
January 14th, 2021

Task 1: Getting Started with nmap

1) Run: man nmap
2) What do the following switches do?

Switch	**Purpose of switch (taken from the output produced by the "man nmap" command)**
-sn	Tells Nmap to not do a port scan after discovering a host, and only print out available hosts that responded to the scan. This is also known as a "ping scan". -sn stands for no port scan
-PO	Sends IP packets with the specified protocol numbers in the protocol field of the IP headers. The ultimately purpose of this switch is to look for responses in the same protocol as the probes, or ICMP Protocol Unreachable messages that signify that the specified IP protocol isn't supported on the host. -PO stands for IP Protocol Ping
-PS	Sends an empty TCP packet with the SYN flag set. Suggests to remote system that we are trying to establish a connection. If the port is open, we will get back a SYN/ACK TCP packet, to which Nmap will send a RST packet to stop the TCP connection from establishing. -PS stands for portlist, also known as TCP SYN Ping
-sO	Allows us to determine which IP protocols are supported by the target machine. These protocols can include: TCP, ICMP, IGMP, etc. It is not a port scan, because it cycles through IP protocol numbers rather than port numbers.

	-sO stands for IP protocol scan
-sV	This switch enables version detection. Version detection assists with determining which version a server may be running, thus assisting us with determining what the server may be vulnerable to. -sV stands for version detection
-O	This switch enables OS detection. This switch works by sampling TCP/IP options and comparing it to nmap-os-db. Hence, the patterns of responses can be used to figure out if there is a match for a given OS. Similar to -sV, knowing the OS of the target assists with determing what the target may be vulnerable to. -O stands for enabling OS detection

Joseph Tsai
CSS 537 – Lab 2: NMAP
January 14th, 2021

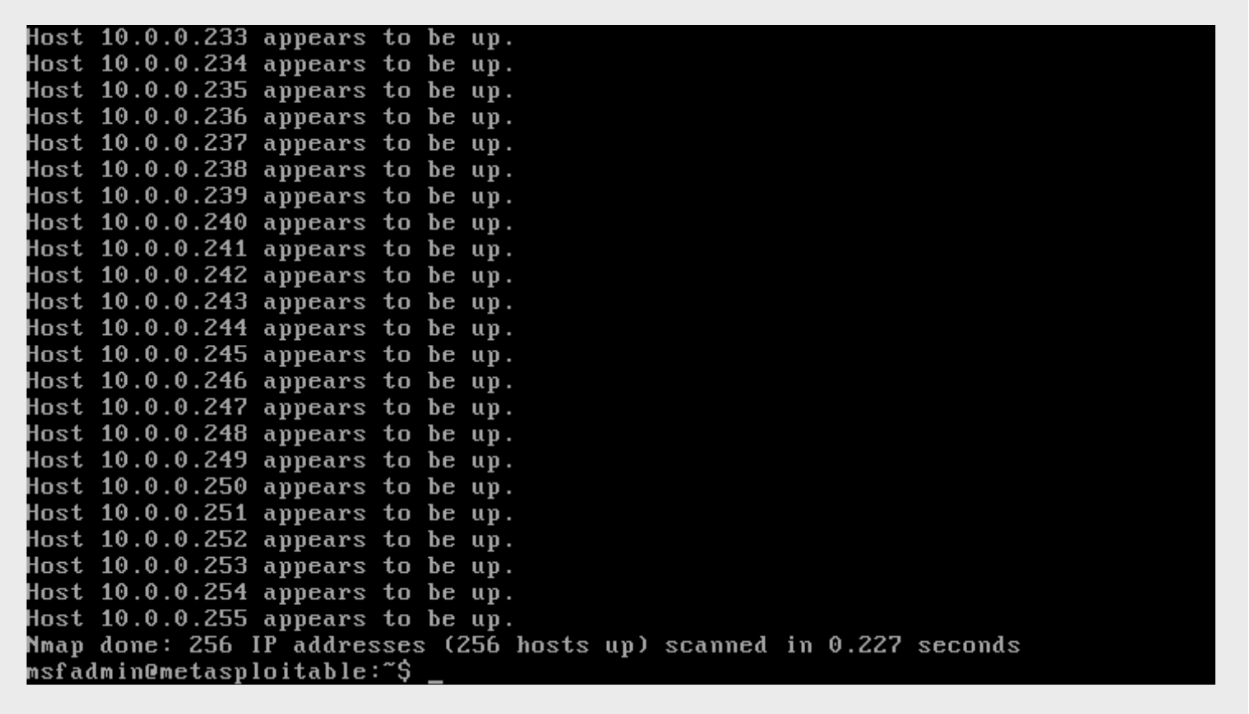
Task 2: Using nmap to conduct a reconnaissance of your network

1. **Use a broad ping scan to determine the hosts that are "up" on a portion of your lab network: nmap -n -sn IPaddress**

   Quick note: I had to use -sP instead of -sn (I think this is because the metasploit machine which I am using is an older version than what the lab asks for, but I am indeed using the machine provided in the PDF for this lab), and I also used 10.0.0.0/24, since I am on my own network and not a lab network with other peers (I believe this is the intent of the ask for ask 1, here).

I. Record the results.

Exhibit 1: The results of running the command, "nmap -n -sP 10.0.0.0/24"



```
Host 10.0.0.233 appears to be up.
Host 10.0.0.234 appears to be up.
Host 10.0.0.235 appears to be up.
Host 10.0.0.236 appears to be up.
Host 10.0.0.237 appears to be up.
Host 10.0.0.238 appears to be up.
Host 10.0.0.239 appears to be up.
Host 10.0.0.240 appears to be up.
Host 10.0.0.241 appears to be up.
Host 10.0.0.242 appears to be up.
Host 10.0.0.243 appears to be up.
Host 10.0.0.244 appears to be up.
Host 10.0.0.245 appears to be up.
Host 10.0.0.246 appears to be up.
Host 10.0.0.247 appears to be up.
Host 10.0.0.248 appears to be up.
Host 10.0.0.249 appears to be up.
Host 10.0.0.250 appears to be up.
Host 10.0.0.251 appears to be up.
Host 10.0.0.252 appears to be up.
Host 10.0.0.253 appears to be up.
Host 10.0.0.254 appears to be up.
Host 10.0.0.255 appears to be up.
Nmap done: 256 IP addresses (256 hosts up) scanned in 0.227 seconds
msfadmin@metasploitable:~$ _
```

II. Why is the -n option used? What happens if you rerun this command without the -n option?

According to the nmap manual, the -n option tells the scan to not perform a DNS resolution on the active IP addresses that are found. Hence, rerunning the command without the -n option makes the scanning time much longer, as nmap is attempting to perform the DNS resolution for each IP address which is "up".

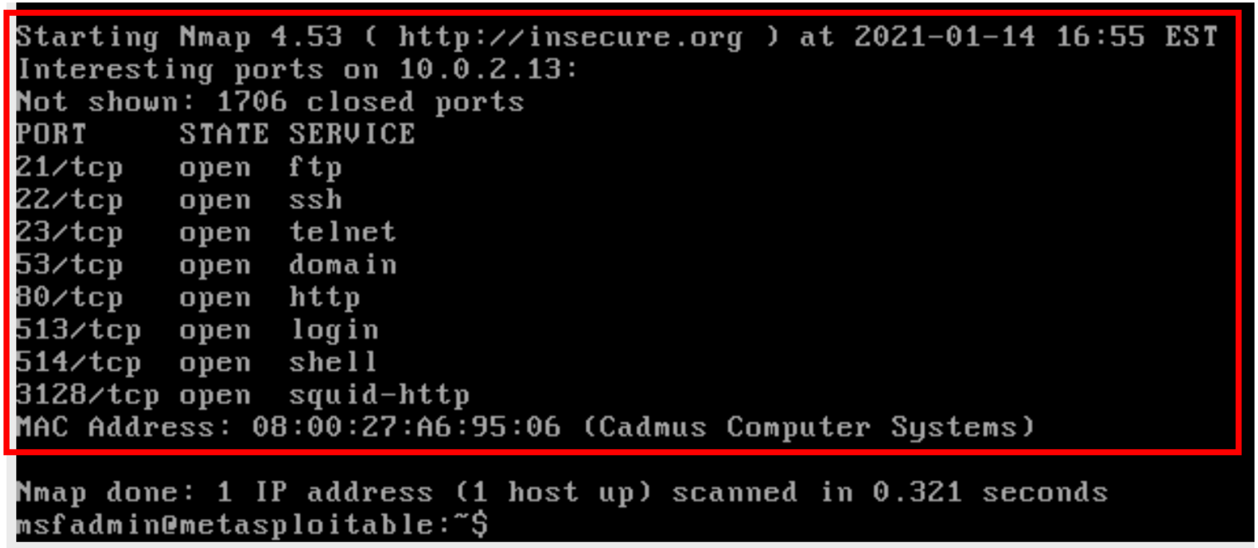
Joseph Tsai
CSS 537 – Lab 2: NMAP
January 14th, 2021

2. **Conduct an IP protocol ping (switch -PO / -PS / -PU) on the Common Network hosts.**

   Quick Note: I believe that the common network is perhaps in reference to a network which other peers would be using. Perhaps such a network would share Common Network hosts, as mentioned in this question. To emulate this, I spun up another VM with the IP address of 10.0.2.13 and performed the protocol ping on this IP address.

   I. There are 8 TCP ports that are open
   II. There does not seem to be any UDP ports open.

Exhibit 2: Results of performing the IP protocol ping on my common network host.

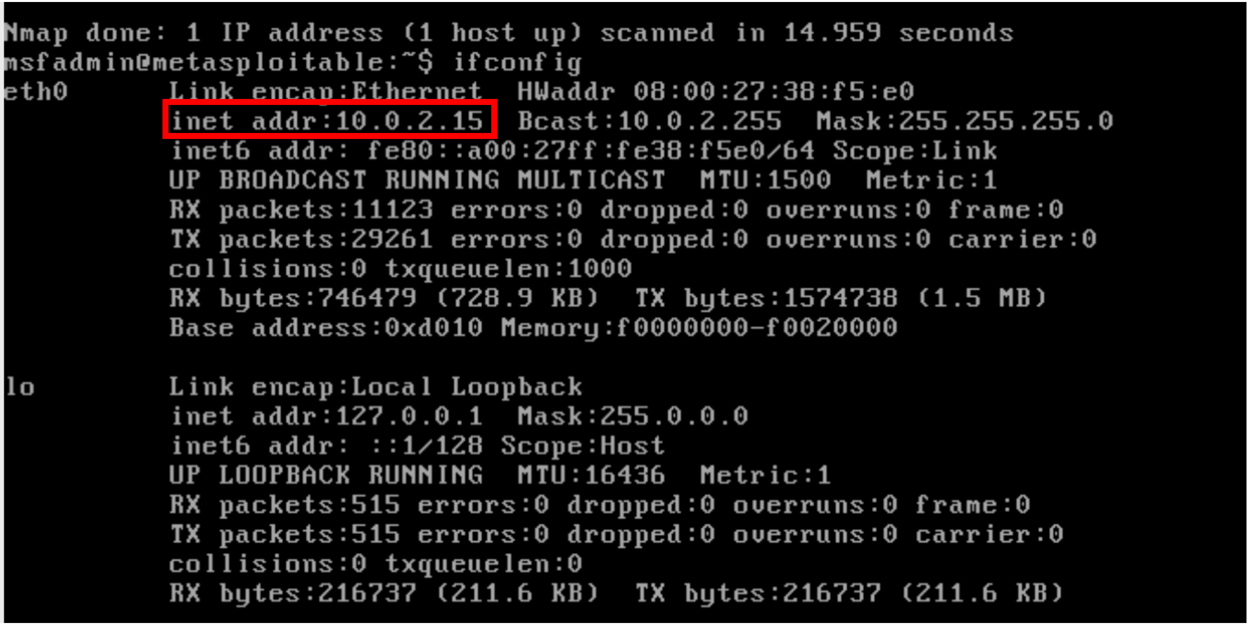


```
Starting Nmap 4.53 ( http://insecure.org ) at 2021-01-14 16:55 EST
Interesting ports on 10.0.2.13:
Not shown: 1706 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
53/tcp   open  domain
80/tcp   open  http
513/tcp  open  login
514/tcp  open  shell
3128/tcp open  squid-http
MAC Address: 08:00:27:A6:95:06 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 0.321 seconds
msfadmin@metasploitable:~$
```

Joseph Tsai
CSS 537 – Lab 2: NMAP
January 14th, 2021

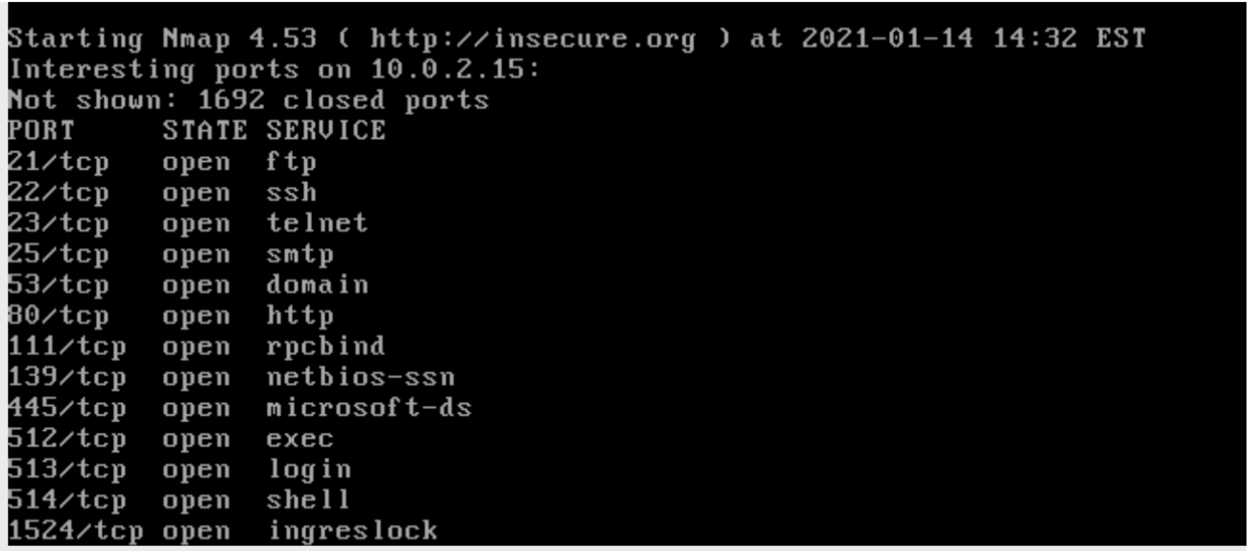
3. **Conduct an IP protocol ping on yourself.**

Exhibit 3: Ifconfig shows that my IP address is: 10.0.2.15.



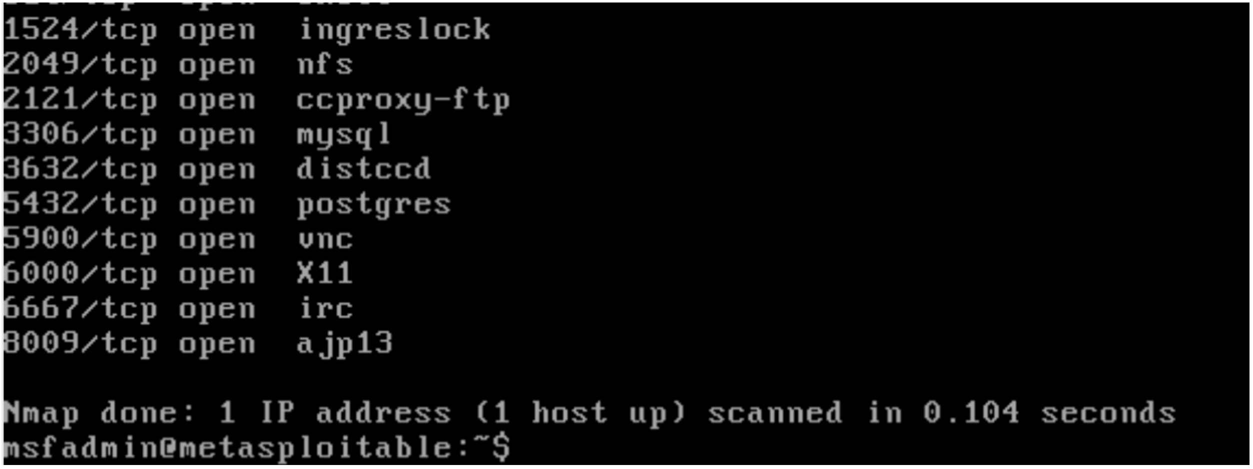
```
Nmap done: 1 IP address (1 host up) scanned in 14.959 seconds
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:38:f5:e0
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe38:f5e0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:11123 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29261 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:746479 (728.9 KB)  TX bytes:1574738 (1.5 MB)
          Base address:0xd010 Memory:f0000000-f0020000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:515 errors:0 dropped:0 overruns:0 frame:0
          TX packets:515 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:216737 (211.6 KB)  TX bytes:216737 (211.6 KB)
```

Exhibit 4: Results of the scan on 10.0.2.15 (part 1 of the scan)



```
Starting Nmap 4.53 ( http://insecure.org ) at 2021-01-14 14:32 EST
Interesting ports on 10.0.2.15:
Not shown: 1692 closed ports
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
1524/tcp open  ingreslock
```

Exhibit 5: Results of the scan on 10.0.2.15 (part 2 of the scan)



```
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
3632/tcp open  distccd
5432/tcp open  postgres
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13

Nmap done: 1 IP address (1 host up) scanned in 0.104 seconds
msfadmin@metasploitable:~$
```

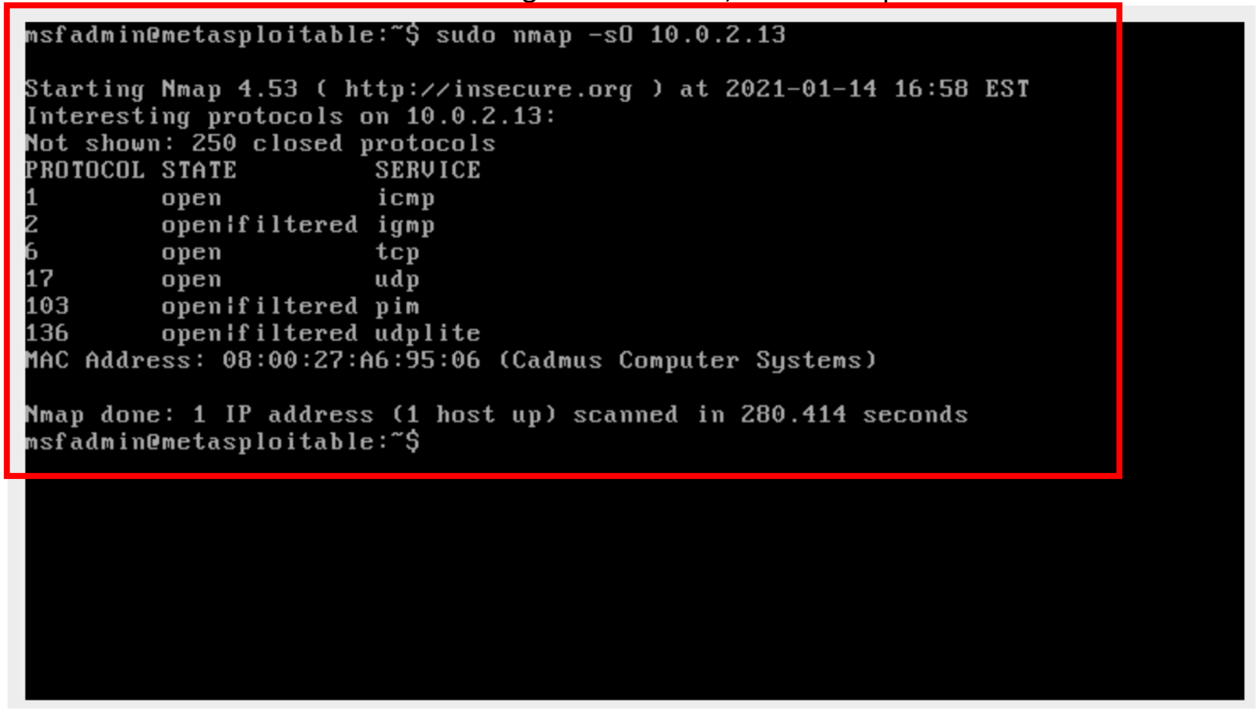
I. How many ports are open?
   i. 22 ports are open.

Joseph Tsai
CSS 537 – Lab 2: NMAP
January 14th, 2021

4. **Conduct an IP protocol scan (switch -sO) on target host.**

   Quick note: I decided to run the command on 10.0.2.13, as I had done for question 2, in order to answer the question below.

Exhibit 6: Results of running the command, "sudo nmap -sO 10.0.2.13"



```
msfadmin@metasploitable:~$ sudo nmap -sO 10.0.2.13

Starting Nmap 4.53 ( http://insecure.org ) at 2021-01-14 16:58 EST
Interesting protocols on 10.0.2.13:
Not shown: 250 closed protocols
PROTOCOL STATE         SERVICE
1        open          icmp
2        open|filtered igmp
6        open          tcp
17       open          udp
103      open|filtered pim
136      open|filtered udplite
MAC Address: 08:00:27:A6:95:06 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 280.414 seconds
msfadmin@metasploitable:~$
```

I. Are the results different than that attained with the IP protocol ping? Explain.

   Yes, the results are different than those which were attained with the IP protocol ping. Specifically, the scan seems to return more general services than the specific protocols that were returned in the protocol ping.

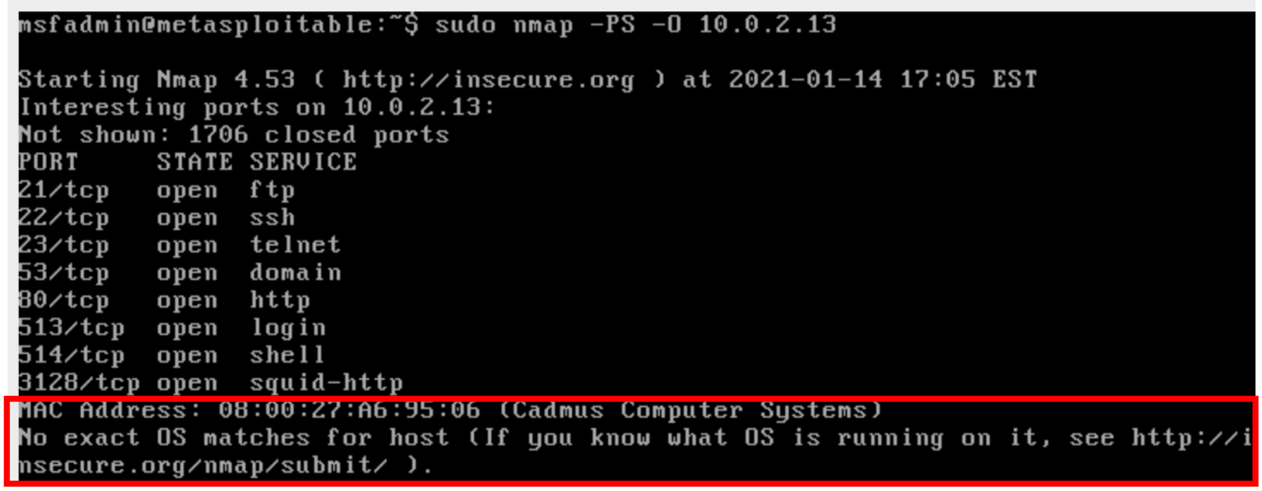
   For example, rather than listing each tcp service, the IP protocol scan returned other services such as icmp, igmp, udp, and udplite. Also, the protocol scan returned whether the service had a state of "open" or "open:filtered", which was not seen within the scan shown within exhibit 4 or 5.

5. **Performing OS detection on the host**

I. What operating system does nmap think your Server VM is running?

Quick note: To run this command, I ran it against my other VM running on the IP address of 10.0.2.13. Interestingly, nmap was unable to fingerprint the given VM. It is running Ubuntu 16.04, and is the VM which was provided to our class for purposes of the SEED labs.

Exhibit 7: Attempting to find the OS of the Server VM running on 10.0.2.13. I noted that the message returned indicates that nmap was unable to determine the OS.



```
msfadmin@metasploitable:~$ sudo nmap -PS -O 10.0.2.13

Starting Nmap 4.53 ( http://insecure.org ) at 2021-01-14 17:05 EST
Interesting ports on 10.0.2.13:
Not shown: 1706 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
53/tcp   open  domain
80/tcp   open  http
513/tcp  open  login
514/tcp  open  shell
3128/tcp open  squid-http
MAC Address: 08:00:27:A6:95:06 (Cadmus Computer Systems)
No exact OS matches for host (If you know what OS is running on it, see http://i
nsecure.org/nmap/submit/ ).
```

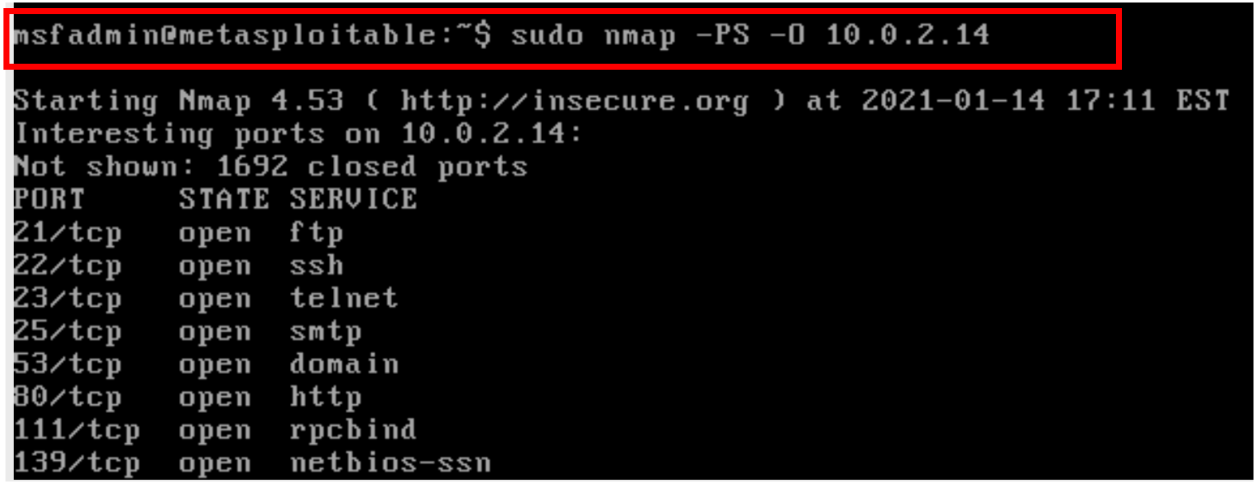
II. What is its MAC address?

i. 08:00:27:A6:95:06 (see exhibit 7)

III. What OS does nmap think your Linux VM is running?

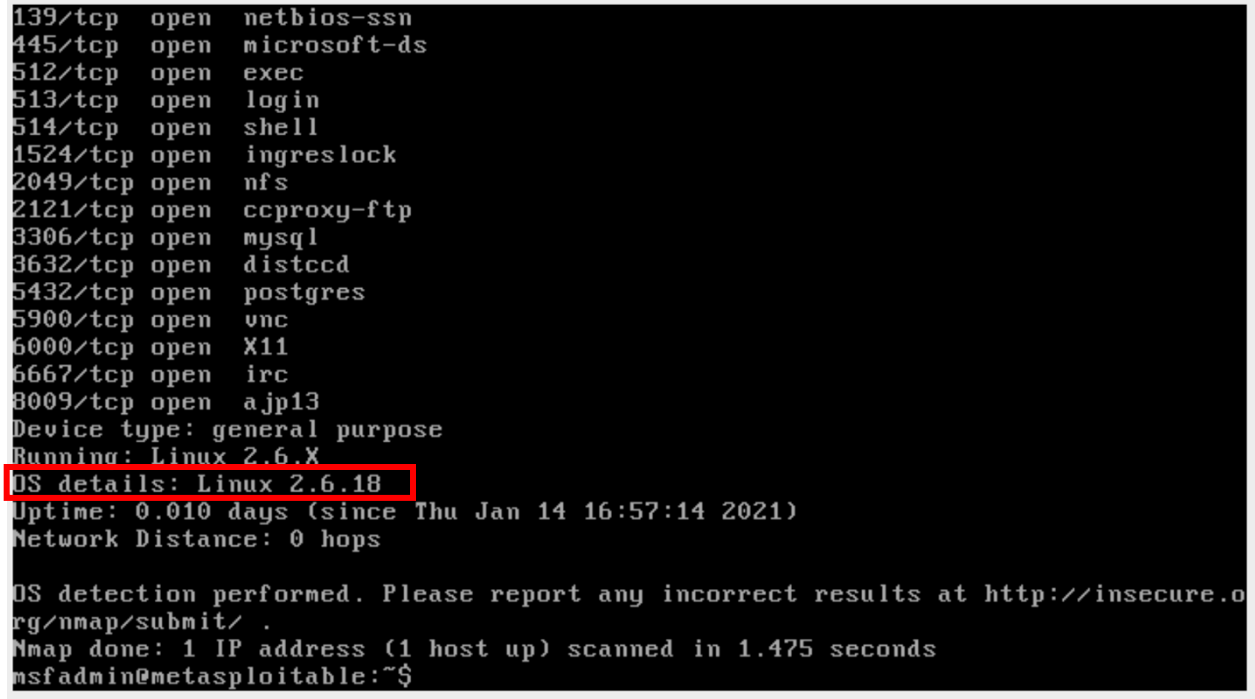
i. Linux 2.6.18

Exhibit 8: The command which was run against the Linux VM to determine the OS that nmap thought the VM was running.



```
msfadmin@metasploitable:~$ sudo nmap -PS -O 10.0.2.14

Starting Nmap 4.53 ( http://insecure.org ) at 2021-01-14 17:11 EST
Interesting ports on 10.0.2.14:
Not shown: 1692 closed ports
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
```

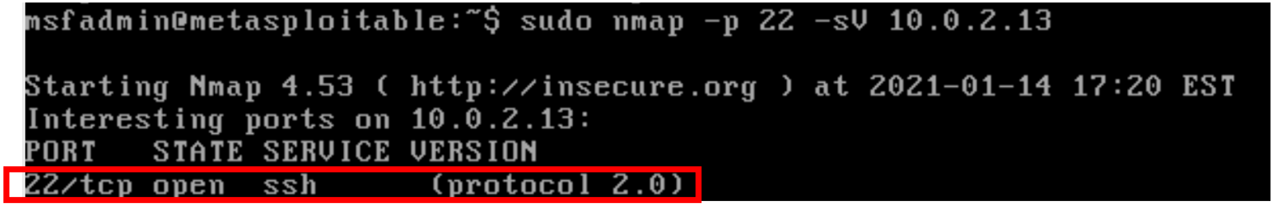
Exhibit 9: Presented OS details from nmap



```
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
3632/tcp open  distccd
5432/tcp open  postgres
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.18
Uptime: 0.010 days (since Thu Jan 14 16:57:14 2021)
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at http://insecure.o
rg/nmap/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.475 seconds
msfadmin@metasploitable:~$
```

6. **Using nmap to perform services/version detection**
   I. What version of ssh is running on your target host?
      i. 2.0
      ii. Quick Note: I had restarted my computer which resulted in my target host's ip changing from 10.0.2.15 to 10.0.2.13.

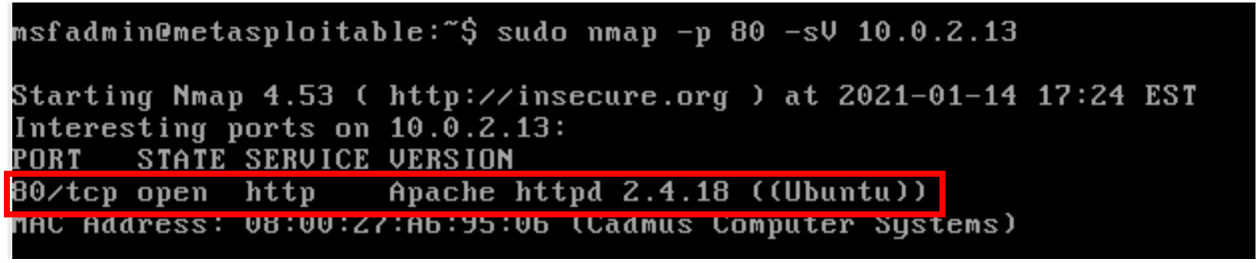
Exhibit 10: Results from attempting to obtain ssh version on target host



```
msfadmin@metasploitable:~$ sudo nmap -p 22 -sV 10.0.2.13

Starting Nmap 4.53 ( http://insecure.org ) at 2021-01-14 17:20 EST
Interesting ports on 10.0.2.13:
PORT   STATE SERVICE VERSION
22/tcp open  ssh      (protocol 2.0)
```

   II. What web server is running on your target host?
      i. http via Apache httpd 2.4.18 (Ubuntu)

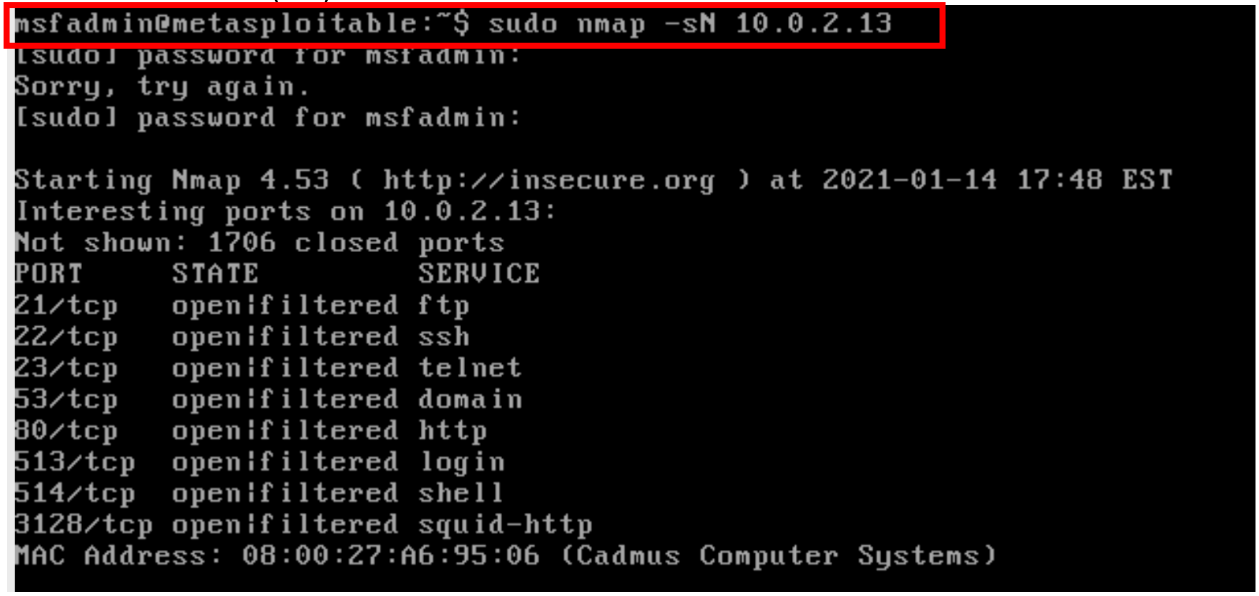
Exhibit 11: Determining the web server that is running on my target host



```
msfadmin@metasploitable:~$ sudo nmap -p 80 -sV 10.0.2.13

Starting Nmap 4.53 ( http://insecure.org ) at 2021-01-14 17:24 EST
Interesting ports on 10.0.2.13:
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 08:00:27:A6:95:06 (Cadmus Computer Systems)
```

7. Testing for vulnerable services via port scanning:

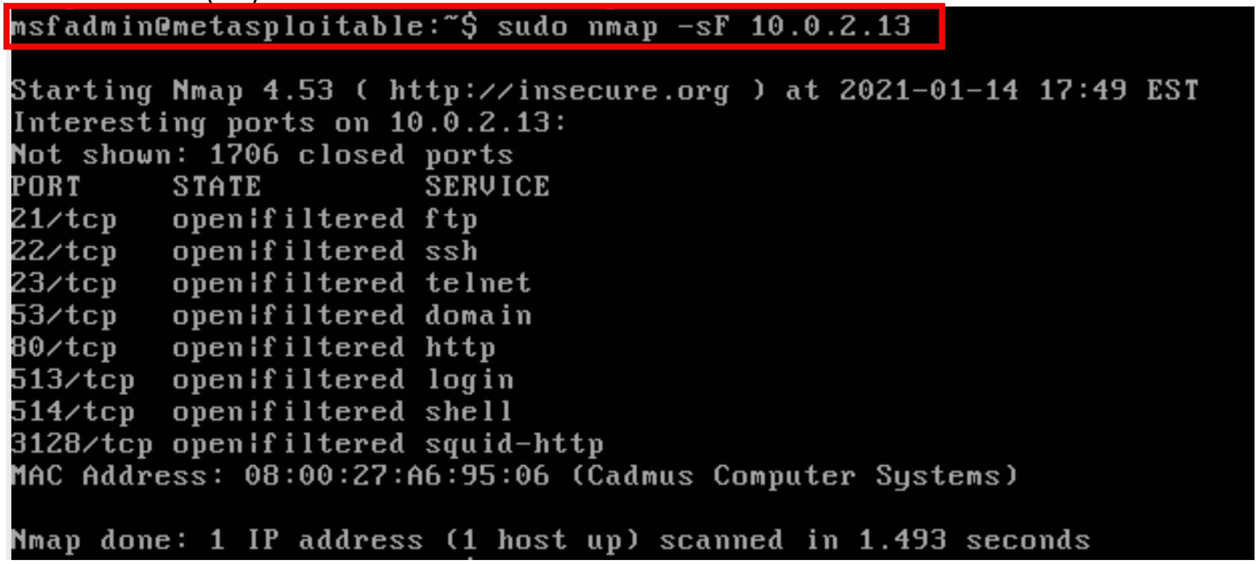
Exhibit 12: TCP Null (-sN) scan



```
msfadmin@metasploitable:~$ sudo nmap -sN 10.0.2.13
[sudo] password for msfadmin:
Sorry, try again.
[sudo] password for msfadmin:

Starting Nmap 4.53 ( http://insecure.org ) at 2021-01-14 17:48 EST
Interesting ports on 10.0.2.13:
Not shown: 1706 closed ports
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
53/tcp   open|filtered domain
80/tcp   open|filtered http
513/tcp  open|filtered login
514/tcp  open|filtered shell
3128/tcp open|filtered squid-http
MAC Address: 08:00:27:A6:95:06 (Cadmus Computer Systems)
```

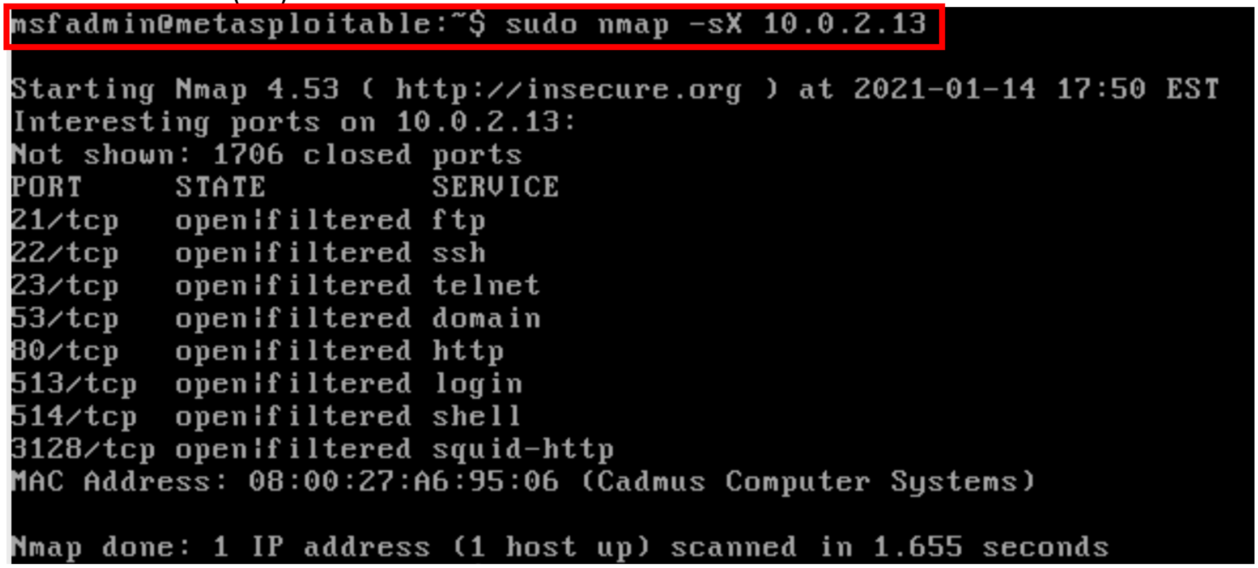
Joseph Tsai
CSS 537 – Lab 2: NMAP
January 14th, 2021

Exhibit 13: FIN (-sF) scan



```
msfadmin@metasploitable:~$ sudo nmap -sF 10.0.2.13

Starting Nmap 4.53 ( http://insecure.org ) at 2021-01-14 17:49 EST
Interesting ports on 10.0.2.13:
Not shown: 1706 closed ports
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
53/tcp   open|filtered domain
80/tcp   open|filtered http
513/tcp  open|filtered login
514/tcp  open|filtered shell
3128/tcp open|filtered squid-http
MAC Address: 08:00:27:A6:95:06 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 1.493 seconds
```

Exhibit 14: Xmas (-sX) scan



```
msfadmin@metasploitable:~$ sudo nmap -sX 10.0.2.13

Starting Nmap 4.53 ( http://insecure.org ) at 2021-01-14 17:50 EST
Interesting ports on 10.0.2.13:
Not shown: 1706 closed ports
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
53/tcp   open|filtered domain
80/tcp   open|filtered http
513/tcp  open|filtered login
514/tcp  open|filtered shell
3128/tcp open|filtered squid-http
MAC Address: 08:00:27:A6:95:06 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 1.655 seconds
```