Stephen Oliver

CS363

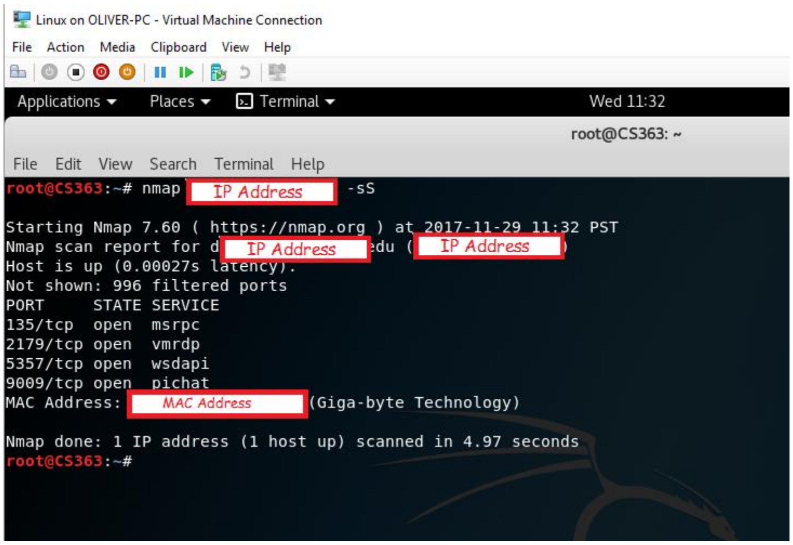
11/29/17

Lab 4: Port Scanners (NMAP)

Note: To protect the security of my machine I have obscured my IP Address and MAC Address. I choose to take this precaution because the IP of my host, due to WOU network configuration, is visible on the wider internet (i.e. outside of the private WOU network).

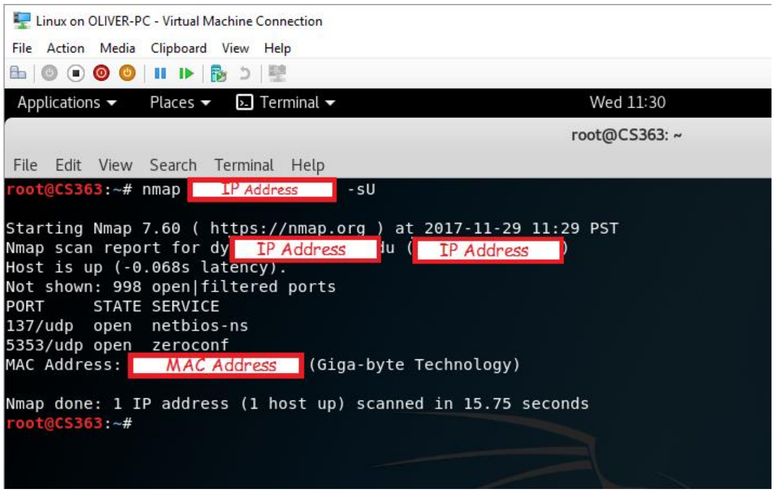
It is also important to note that my firewall prevents port scanning and connection to my VM so I had to disable it for the duration of the Lab. The ports open now may not be an accurate representation of what is normally open.

Scan 1 – TCP SYN Scan:


Linux on OLIVER-PC - Virtual Machine Connection
File Action Media Clipboard View Help
Applications ▾ Places ▾ Terminal ▾
Wed 11:32
root@CS363: ~
File Edit View Search Terminal Help

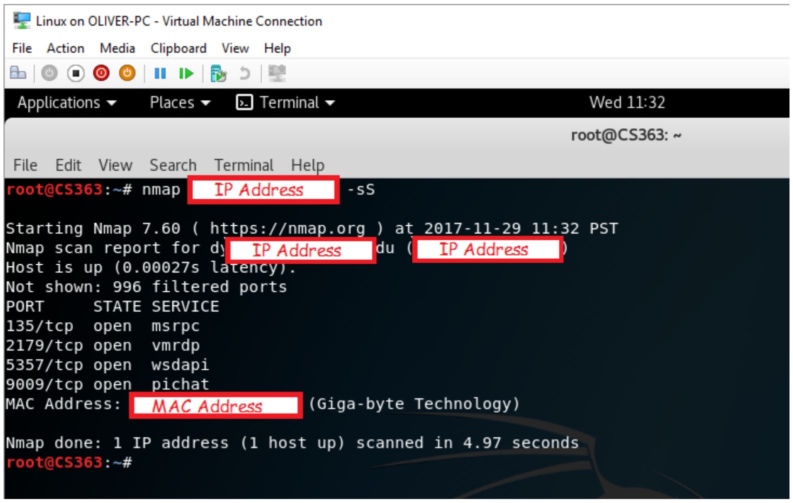
```
root@CS363:~# nmap  IP Address  -sS

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-29 11:32 PST
Nmap scan report for d IP Address edu ( IP Address )
Host is up (0.00027s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
2179/tcp open  vmrdp
5357/tcp open  wsdapi
9009/tcp open  pichat
MAC Address:  MAC Address  (Giga-byte Technology)

Nmap done: 1 IP address (1 host up) scanned in 4.97 seconds
root@CS363:~#
```

Scan 2 – UDP Scan:


Linux on OLIVER-PC - Virtual Machine Connection
File Action Media Clipboard View Help
Applications ▾ Places ▾ Terminal ▾
Wed 11:30
root@CS363: ~
File Edit View Search Terminal Help

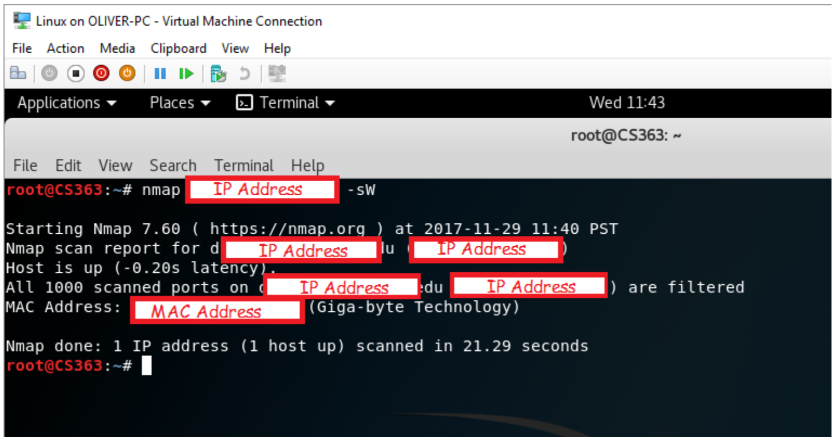
```
root@CS363:~# nmap  IP Address  -sU

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-29 11:29 PST
Nmap scan report for dy IP Address u ( IP Address )
Host is up (-0.068s latency).
Not shown: 998 open|filtered ports
PORT     STATE SERVICE
137/udp  open  netbios-ns
5353/udp open  zeroconf
MAC Address:  MAC Address  (Giga-byte Technology)

Nmap done: 1 IP address (1 host up) scanned in 15.75 seconds
root@CS363:~#
```

Scan 3 – TCP ACK Scan


Linux on OLIVER-PC - Virtual Machine Connection
File Action Media Clipboard View Help
Applications ▾ Places ▾ Terminal ▾ Wed 11:32
root@CS363: ~
File Edit View Search Terminal Help

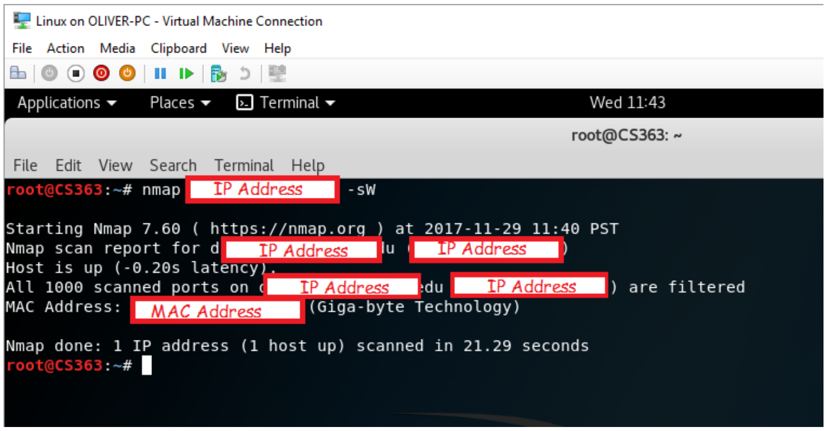
```
root@CS363:~# nmap  IP Address  -sS

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-29 11:32 PST
Nmap scan report for dy IP Address du ( IP Address )
Host is up (0.00027s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
2179/tcp open  vmrdp
5357/tcp open  wsdapi
9009/tcp open  pichat
MAC Address:  MAC Address  (Giga-byte Technology)

Nmap done: 1 IP address (1 host up) scanned in 4.97 seconds
root@CS363:~#
```

Scan 4 – TCP Window Scan:


Linux on OLIVER-PC - Virtual Machine Connection
File Action Media Clipboard View Help
Applications ▾ Places ▾ Terminal ▾ Wed 11:43
root@CS363: ~
File Edit View Search Terminal Help

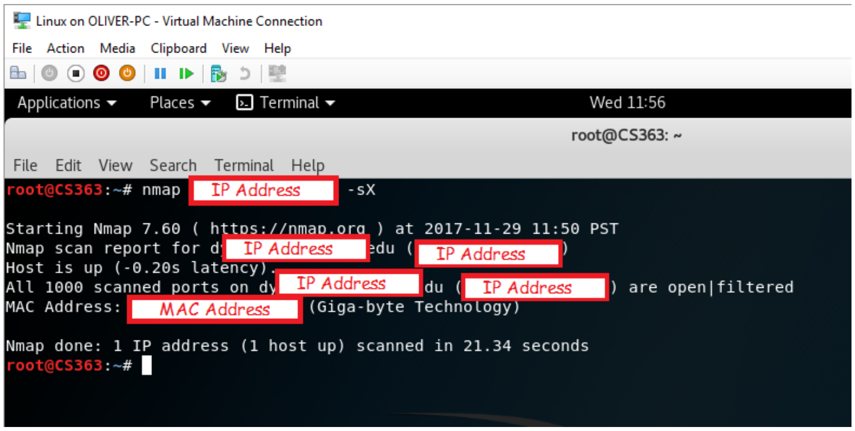
```
root@CS363:~# nmap  IP Address  -sW

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-29 11:40 PST
Nmap scan report for d IP Address lu ( IP Address )
Host is up (-0.20s latency).
All 1000 scanned ports on ( IP Address du  IP Address ) are filtered
MAC Address:  MAC Address  (Giga-byte Technology)

Nmap done: 1 IP address (1 host up) scanned in 21.29 seconds
root@CS363:~#
```

Scan 5 – FIN Scan:


Linux on OLIVER-PC - Virtual Machine Connection
File Action Media Clipboard View Help
Applications ▾ Places ▾ Terminal ▾ Wed 11:43
root@CS363: ~
File Edit View Search Terminal Help

```
root@CS363:~# nmap  IP Address  -sW

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-29 11:40 PST
Nmap scan report for d IP Address lu ( IP Address )
Host is up (-0.20s latency).
All 1000 scanned ports on ( IP Address du  IP Address ) are filtered
MAC Address:  MAC Address  (Giga-byte Technology)

Nmap done: 1 IP address (1 host up) scanned in 21.29 seconds
root@CS363:~#
```

Scan 6 – Other Scans (Xmas):

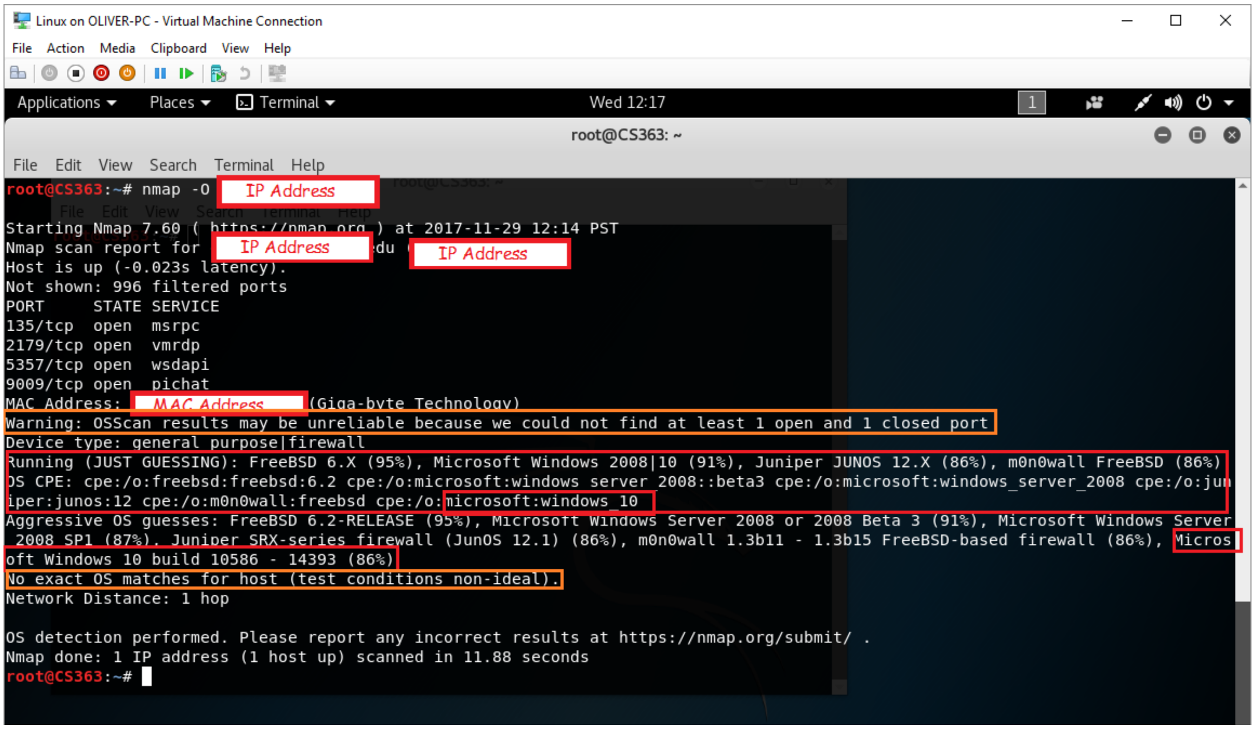

Linux on OLIVER-PC - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Wed 11:56
root@CS363: ~
File Edit View Search Terminal Help

```
root@CS363:~# nmap  IP Address  -sX

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-29 11:50 PST
Nmap scan report for d IP Address edu ( IP Address )
Host is up (-0.20s latency).
All 1000 scanned ports on dy IP Address du ( IP Address ) are open|filtered
MAC Address:  MAC Address  (Giga-byte Technology)

Nmap done: 1 IP address (1 host up) scanned in 21.34 seconds
root@CS363:~#
```

Questions:

1) 1 Host is running (My Home Desktop) and the IP address is xxx.xxx.xxx.192. NOTE: I have obscured my IP address to preserve the security of my machine as noted above.
2) Msrp, vmrdp, wsdapi, pichat, netbios-ns, and zeroconf
3) Yes, but it requires the scan to find one open and one closed port to be releliable. It could not find this for the host(s) that I scanned so it tried to guess the running OS; one of the guess was correct but it also guess many others that were not, I run Windows 10 and it came up with the following from the NMAP OS detection command.

   Command: nmap -O <ip address>


Linux on OLIVER-PC - Virtual Machine Connection
File Action Media Clipboard View Help
Applications
Places
Terminal
Wed 12:17
1
root@CS363: ~
File Edit View Search Terminal Help

```
root@CS363:~# nmap -O  IP Address

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-29 12:14 PST
Nmap scan report for  IP Address  du  IP Address
Host is up (-0.023s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
2179/tcp open  vmrdp
5357/tcp open  wsdapi
9009/tcp open  pichat
MAC Address:  MAC Address  (Giga-byte Technology)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|firewall
Running (JUST GUESSING): FreeBSD 6.X (95%), Microsoft Windows 2008|10 (91%), Juniper JUNOS 12.X (86%), m0n0wall FreeBSD (86%)
OS CPE: cpe:/o:freebsd:freebsd:6.2 cpe:/o:microsoft:windows_server_2008::beta3 cpe:/o:microsoft:windows_server_2008 cpe:/o:juniper:junos:12 cpe:/o:m0n0wall:freebsd cpe:/o:microsoft:windows_10
Aggressive OS guesses: FreeBSD 6.2-RELEASE (95%), Microsoft Windows Server 2008 or 2008 Beta 3 (91%), Microsoft Windows Server 2008 SP1 (87%), Juniper SRX-series firewall (JunOS 12.1) (86%), m0n0wall 1.3b11 - 1.3b15 FreeBSD-based firewall (86%), Microsoft Windows 10 build 10586 - 14393 (86%)
No exact OS matches for host (test conditions non-ideal).
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 11.88 seconds
root@CS363:~#
```