Stephen Oliver

CS363

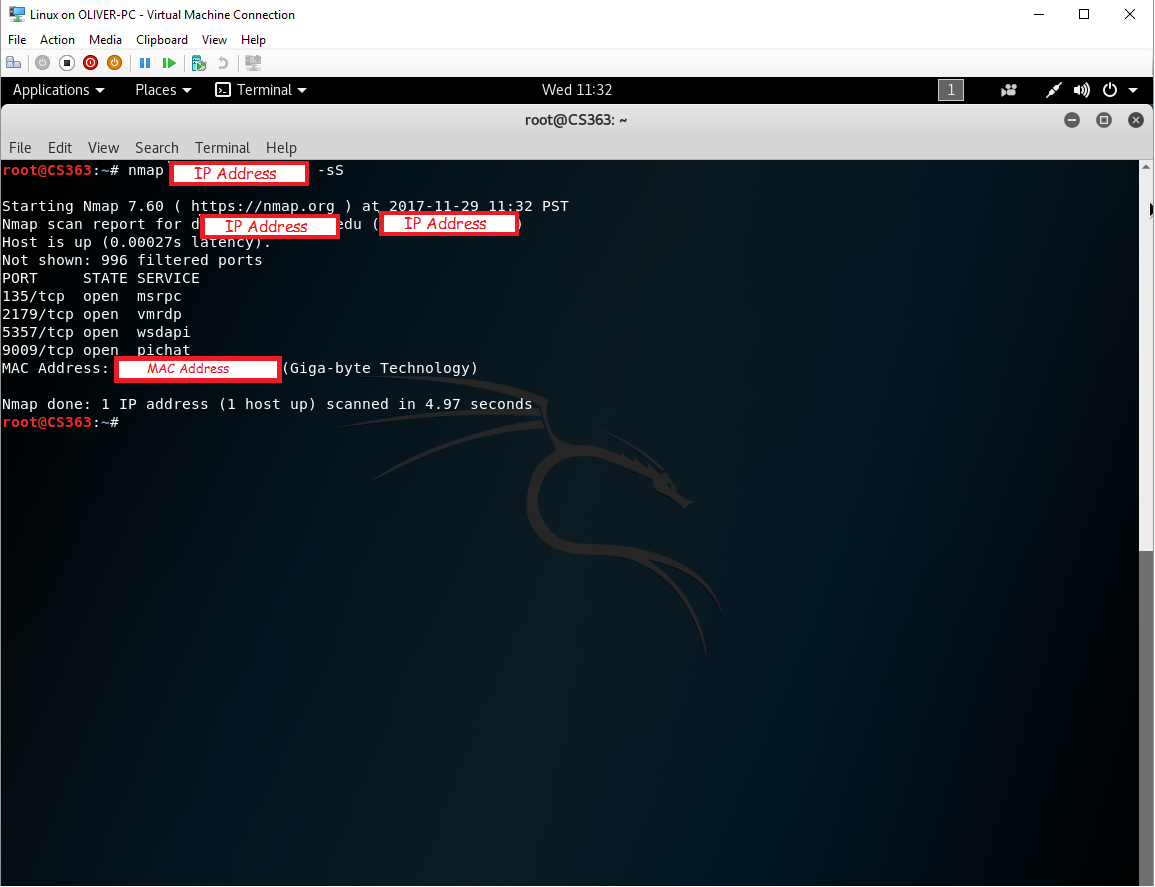
11/29/17

Lab 4: Port Scanners (NMAP)

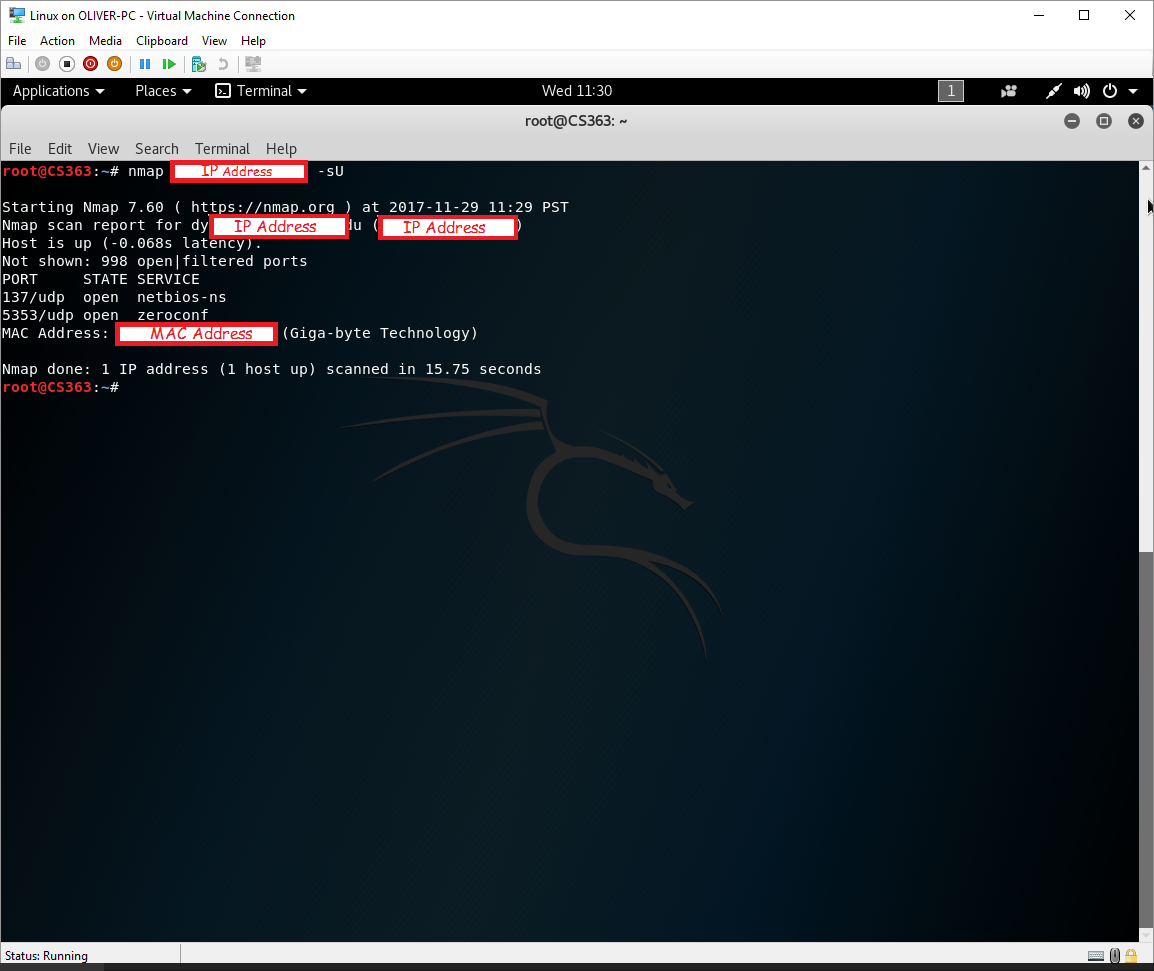
Note: To protect the security of my machine I have obscured my IP Address and MAC Address. I choose to take this precaution because the IP of my host, due to WOU network configuration, is visible on the wider internet (i.e. outside of the private WOU network).

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.

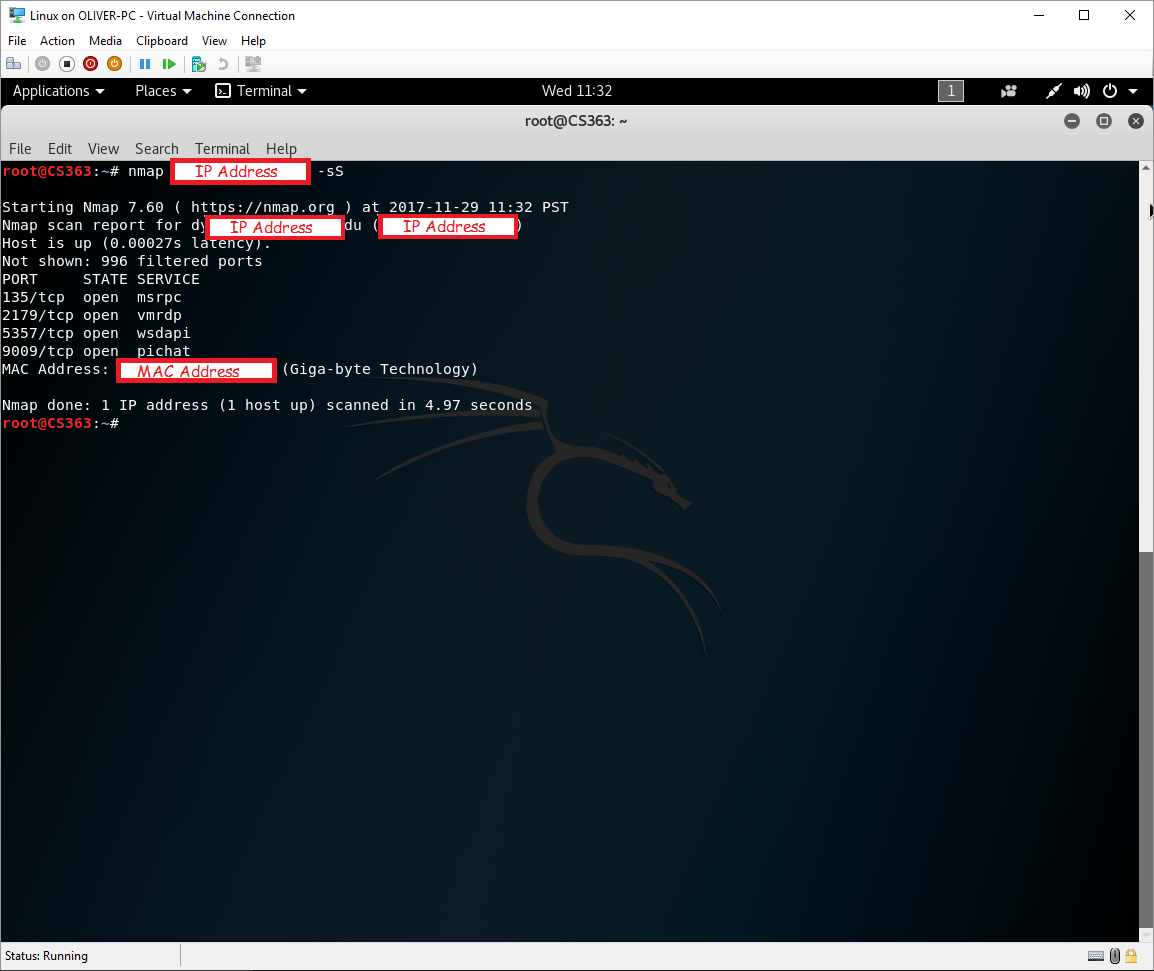
**Scan 1 – TCP SYN Scan:**

****

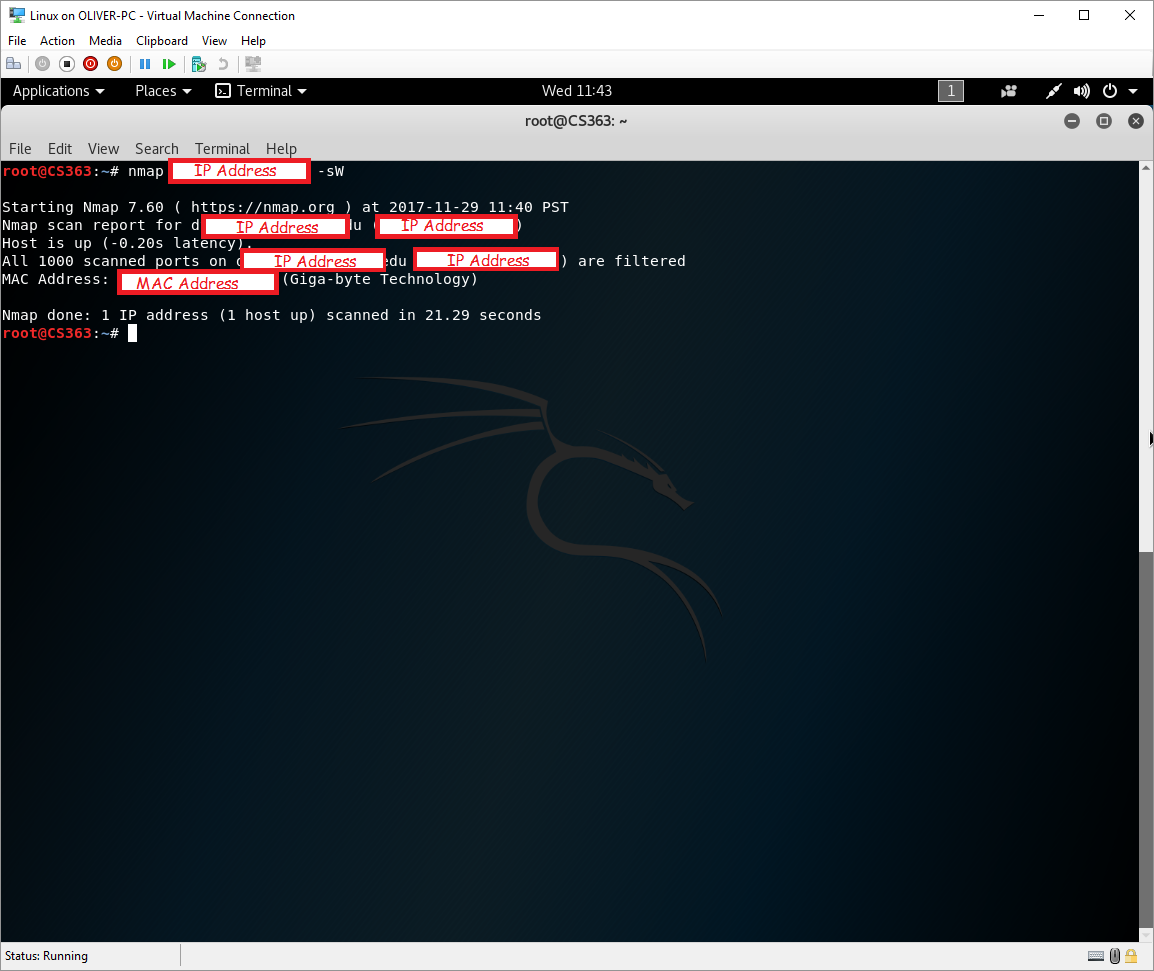
**Scan 2 – UDP Scan:**

****

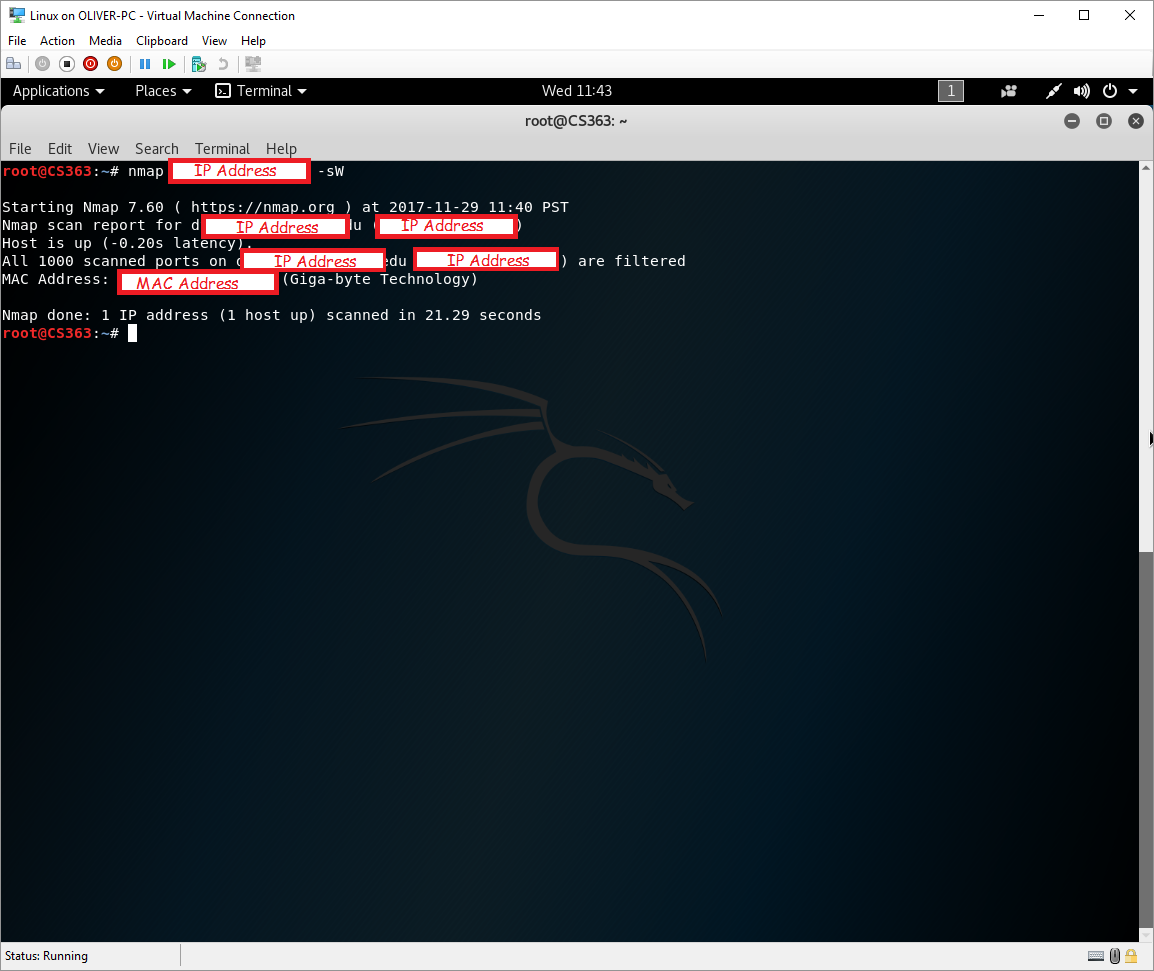
**Scan 3 – TCP ACK Scan**

****

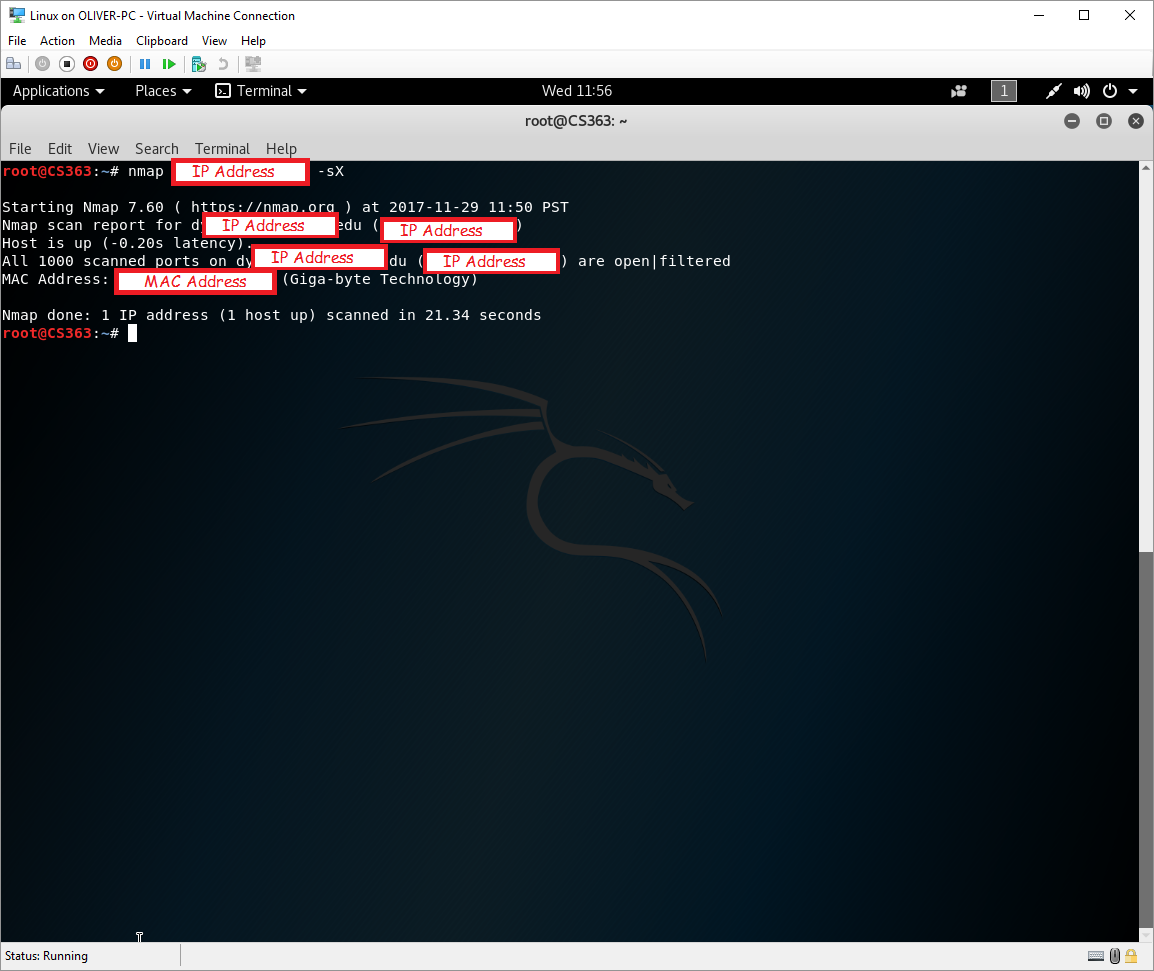
**Scan 4 – TCP Window Scan:**

****

**Scan 5 – FIN Scan:**

****

**Scan 6 – Other Scans (Xmas):**

****

**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>

