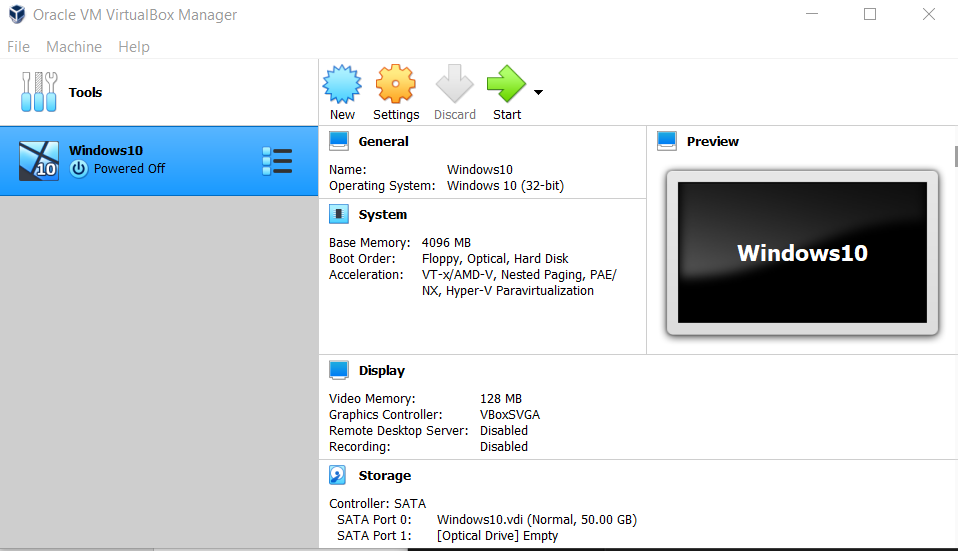
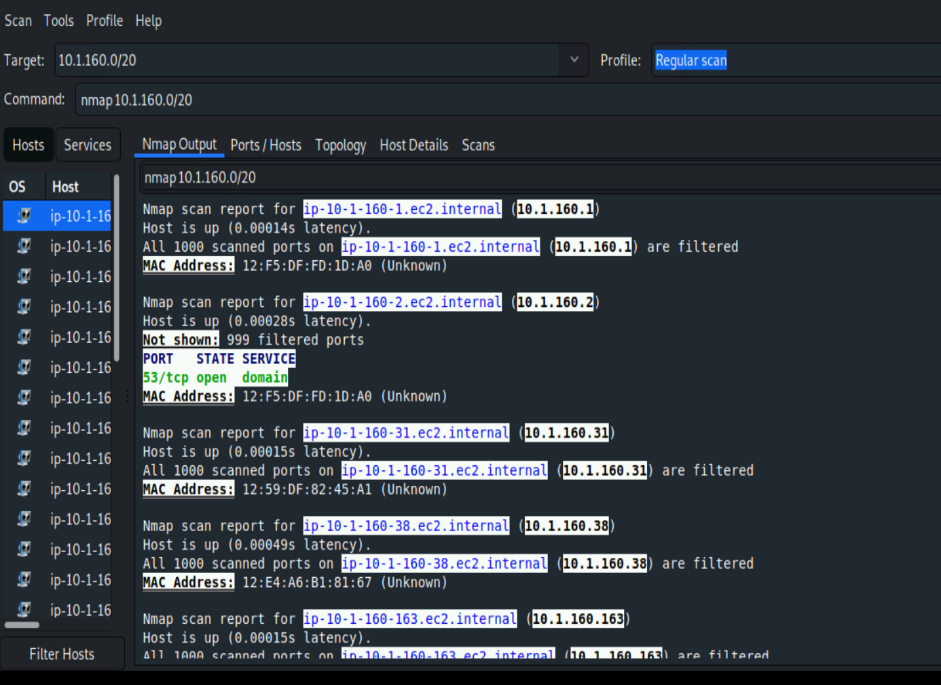
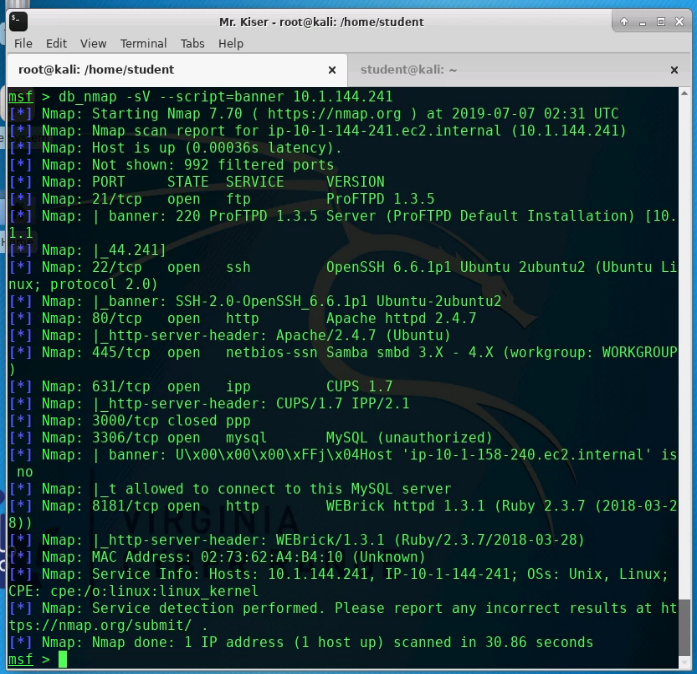
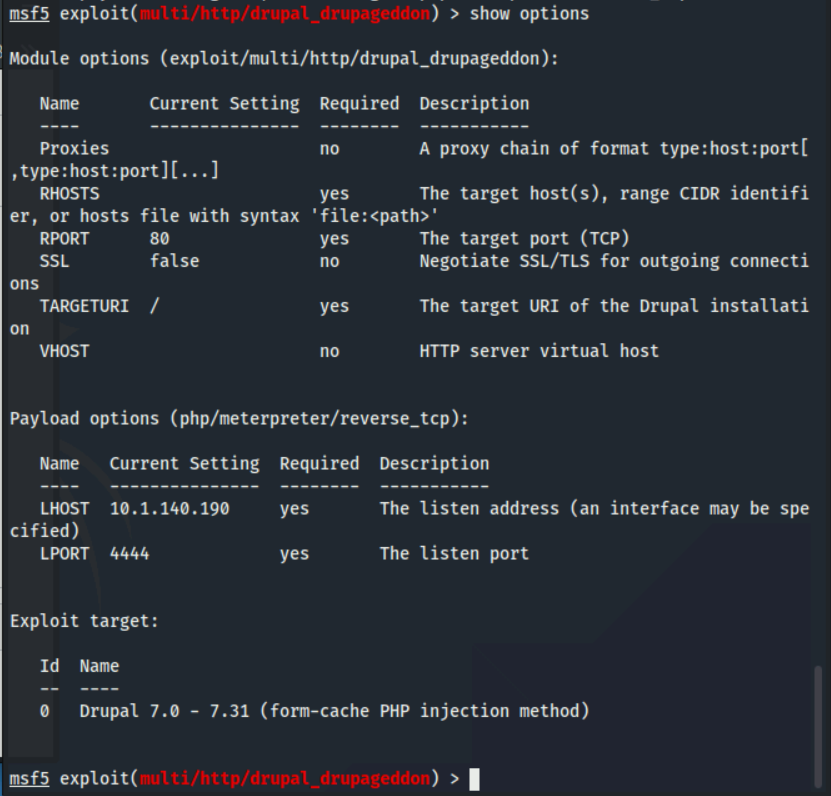
Afeefah Manzoor

ITN 261

Text

Description automatically generatedProject



Graphical user interface, website

Description automatically generated

In ITN 261- Network Attacks, Computing Crime and Hacking- I have gotten a lot more hands on experience than I had ever experienced in any other class that I have attended at Northern Virginia Community College. I feel like that I have learned a lot more and will retain a lot more information than I have in any other class I have taken-besides ITN 277-Forensics two.

I was able to experience a lot more hand on experience with Linux as well as using Network Miner and WireShark. I personally was a little familiar with both but after this semester I feel like I am a lot more competent to look through PCAP files as well as using Linux. I learned more practical and quicker ways to look through PCAP files by using both Network Miner and WireShark and using their unique layout to my advantage. With investigating PCAP files, I can easily figure out the of different devices’ IP addresses, MAC addresses, hosts name, websites visited, and OS information on Network Miner than on Wireshark. It is also a lot clearer to see images and any messages sent can be seen on Network Miner a lot faster than on WireShark. With that information, I can easily follow the content on WireShark and follow the TCP or HTTP stream than I can on Network Miner.

I unfortunately could not get Nessus activated on my machine even after resetting my Kali machine, so I was not able to play around with it and learn from the labs with Nessus Tenable. Even with the other labs that we performed on the Kali Linux machine; I was able to get a little more comfortable with using a Linux system different Linux commands. The NMAP tools that we used on Linux system seemed a little different and a little more difficult for me to use, since I am not used to using Linux commands like this. I did find it much clearer to read and examine than with the PCAP files that we had to look throughout in class though.

In Kali I learned a lot more about Metaspoitable than I did in my ITN 266- Network Security Layers-class and was able to get some hands-on practice with it. The best way I learned to maintain access after hacking into the system is through finding a backdoor on the machine, which we can do with a payload of Meterpreter. After that we can observe the machine, do privilege escalation, steal information, or many other things within the system that we were able to hack into.

Overall, I was able to learn and execute what I learned in the class with hands on labs, without blindly following along to directions and creating a deeper understanding of the material that we were learning, such as examining PCAP files on Network Miner and WireShark, overall Linux commands, finding backdoors and maintaining access in the system and the theory behind these attacks and how they are possible.