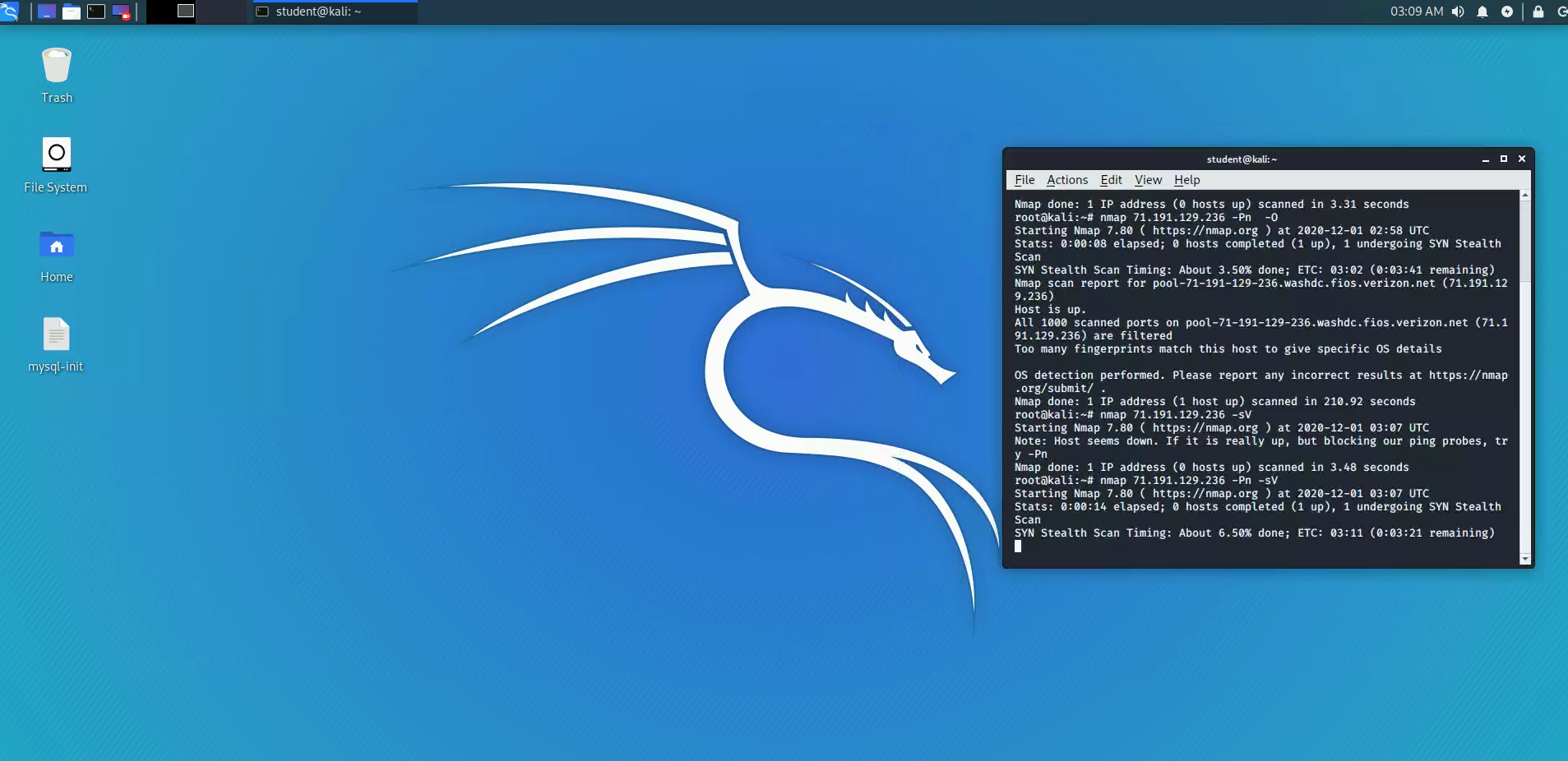
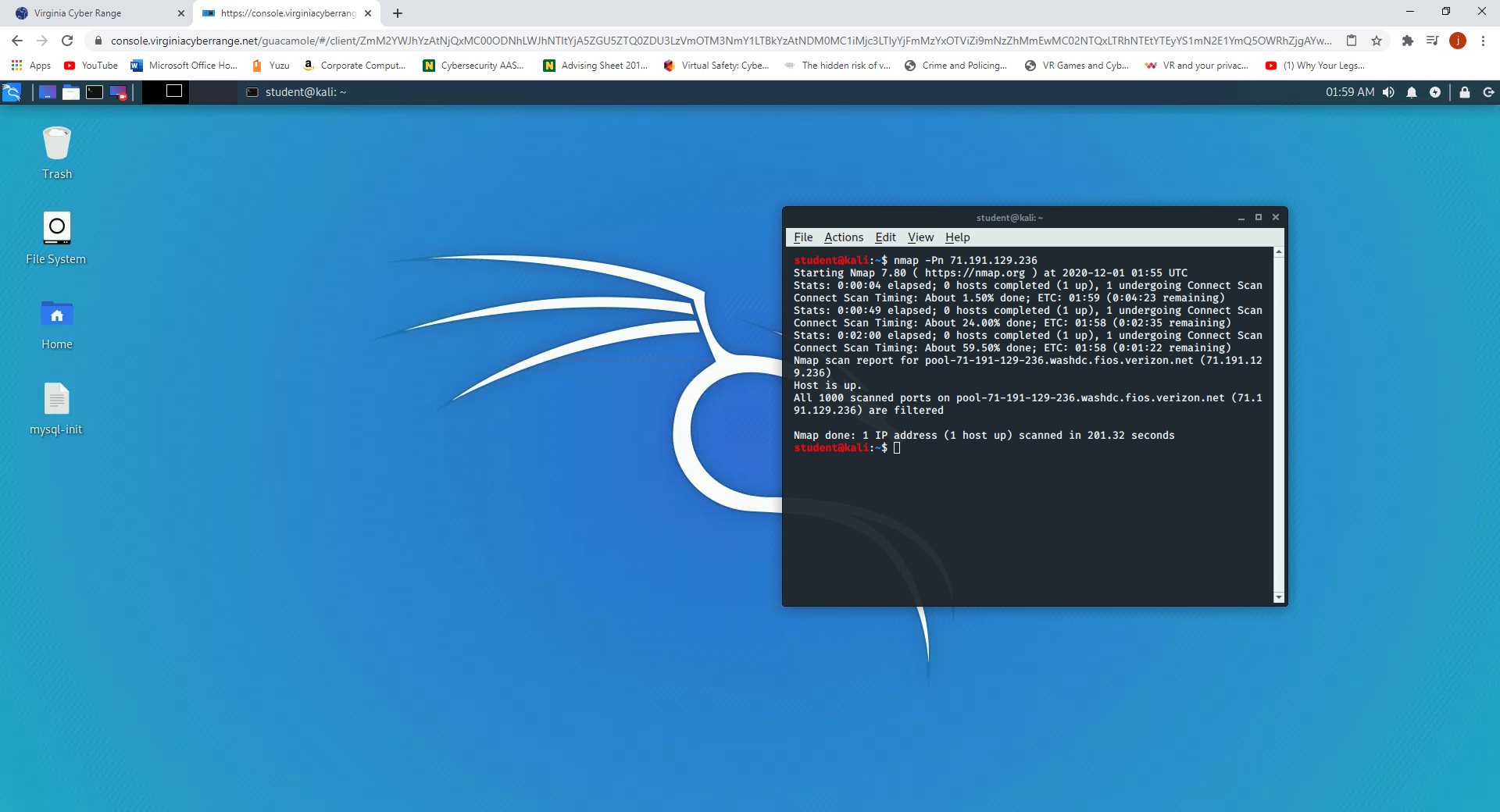
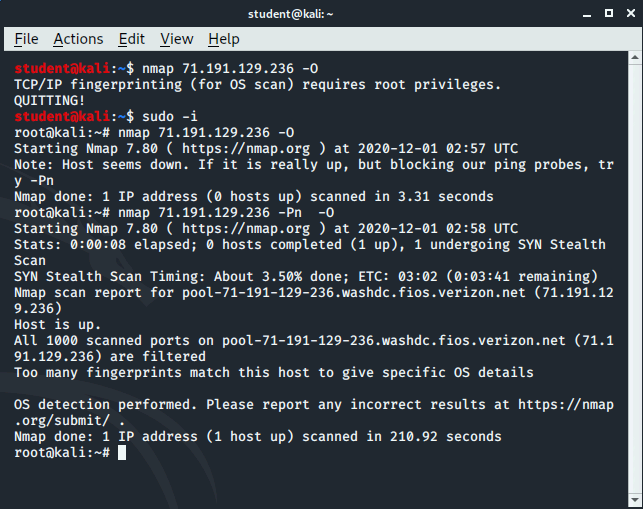
I will be using Kali linux as the attacking machine and my windows VM as the target.

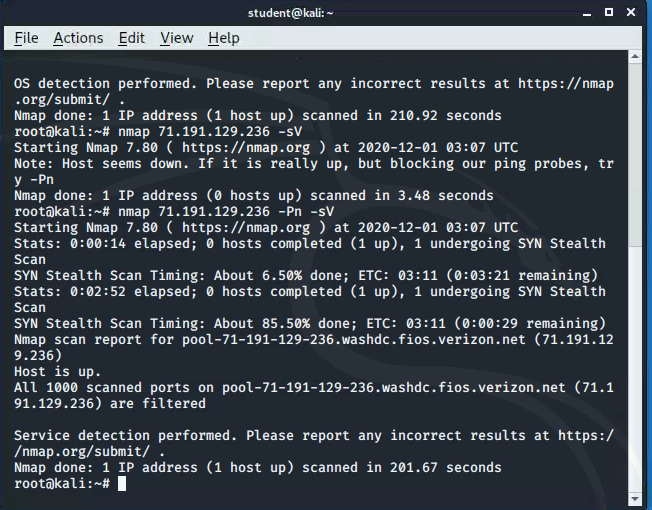




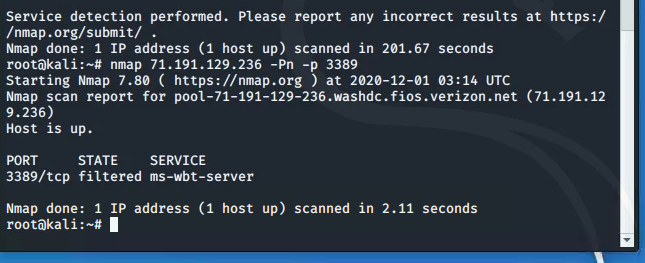
Here I run a nmap scan on my target (71.191.129.236) I had to use the Pn command because the first scan using just nmap said the host was down, after using the PN command I was able to ping the IP.



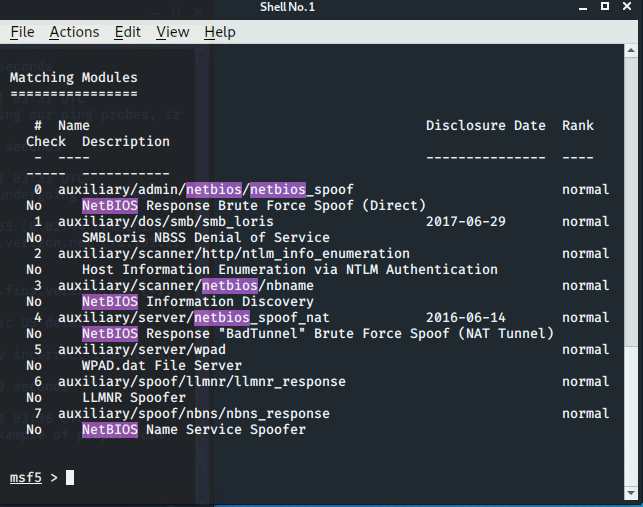
Here I used Remote OS detection using TCP/IP stack fingerprinting and the results weren’t what I was looking for since it said “too many fingerprints match this host”



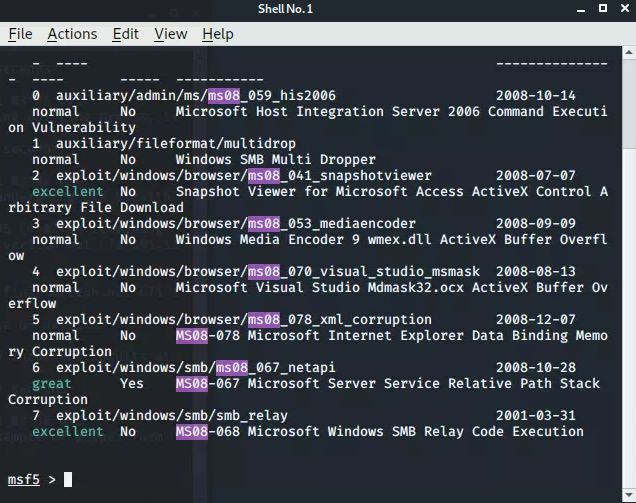
Here I use the –sV command above to try another way to get the OS or ports but it didn’t really work out.



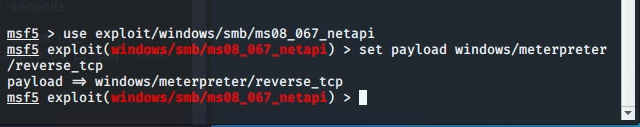
Here I check for port 3389 if it is open to figure out if the target is running windows, which it is. Above picture



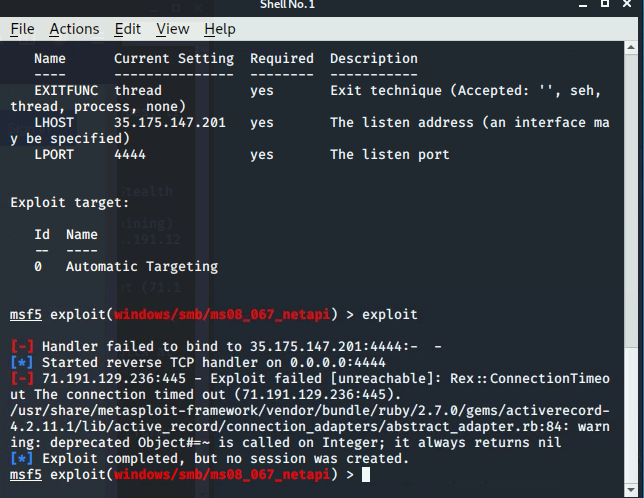
Here im looking at metasploit commands I can use to get access to the target, but I do not use netbios.



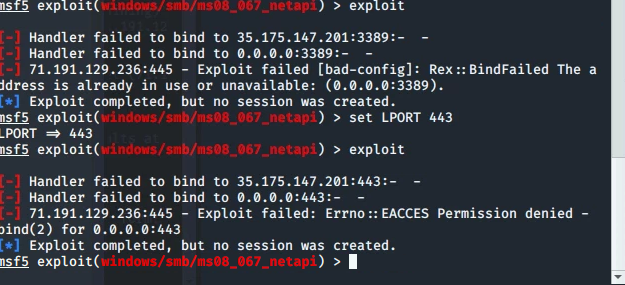
Here I chose my exploit which was netapi, **ms08\_067\_netapi** is one of the most popular remote exploits against Microsoft Windows. It is considered a reliable exploit and allows you to gain access as SYSTEM - the highest Windows privilege.



Meterpreter is an advanced, dynamically extensible payload that uses in-memory DLL injection stagers and is extended over the network at runtime. It communicates over the stager socket and provides a comprehensive client-side Ruby API. It features command history, tab completion, channels, and more. Here I just do the auto payload since I don’t need to do it manually and will let Metasploit do it for me.



So the exploit I was trying to do was get remote access on the hacked system using only the IP address. It didn’t work as it failed to bind.



I tried another port but I seem to not be able to create a session.

What I learned in this project that I will be going over in my write up is: Kali Linux, Nmap, Nessus, Metasploit and their functionalities and how crucial they are to gaining access to someone's system.

Kali Linux is a Debian-based Linux distribution and is targeted at sophisticated penetration testing and security auditing. Kali Linux includes several hundred resources, such as Penetration Testing, Vulnerability Analysis, Digital Forensics and Reverse Engineering, targeted towards different information security activities. While using Kali Linux I saw many tools like John, Autopsy. Sqlmap, Wireshark, Aircrack-ng, Nmap and so many more. I’ve used all these tools in previous labs so they were helpful in terms of doing the project and understanding what I am doing. Using Kali VM was fairly easy and I ran into zero issues, there's nothing I would've changed in terms of using a different machine as an attacker because I think Kali Linux is the best. Kali Linux has so many tools which can help the hacker do their job efficiently. You have full customization of Kali ISOs, Kali Linux live USB with LUKS encrypted persistence and multiple persistence stores and Kali Linux metapackages. The list goes on. I digress, Kali was efficient for me doing this project and I had fun doing it. The only challenge I really encountered was trying to download Nessus onto the Kali machine, which I was unable to after several hours of trying different methods. I could not figure out why I could not get Nessus.

Nmap is an awesome tool and I had zero problems using it. I’ve used it in previous labs and it is really fun to use and toy around with. Nmap is very straight forward and I think anyone trying to use it, even beginners can easily understand what they are doing and what information they are gaining by looking at all the commands and figuring out which each one does. Using Nmap gives you so much information on your target. Nmap can be detected, usually only scan types that establish full TCP connections are logged. SYN stealth scans can sneak through but intrusive scans using Nmap version detection, can be detected if the administrator is reading the system logs regularly. The only way you could avoid this is possibly proxy chaining but proxy chaining and using Nmap will be quite difficult because the support for proxy on Nmap is very limited because you cannot use UDP scans, SYN stealth or OS detection scans so it might hurt your scouting ability. Overall Nmap was crucial to this project because it gives you ports, whether the host is up and what kind of distribution the target is running.

I was unable to download Nessus and I understand that it will make me lose points on the project and I understand that it is needed in this project. However, I will talk a little bit about Nessus from what I have learned on the internet and YouTube videos. Nessus is a remote protection monitoring application that checks a device and raises an alarm if any bugs or vulnerabilities that might be exploited by malicious hackers to reach any computer that you have linked to a network are found. Nessus is a security detector for networks. To handle vulnerability checks, it uses plug-ins, which are different directories. This makes adding plug-ins and seeing which plug-ins are installed simple to make sure the plug-ins are present. A server-client architecture is used by Nessus. It would need to develop the main server on a supported Unix-like operating system. For Unix, Linux and Windows, the client is open. The server is not an alternative because it "carries out security checks". Nessus is free which is awesome and it is open source and many people work on Nessus and keep it up to date.

Metasploit is a computer security platform that provides information on program bugs, the creation of IDS signatures, and facilitates penetration testing. This tool can be used against a remote target computer for executing and creating exploit code. The Metasploit Framework is a forum for scalable open-source penetration testing used to target applications to test for security vulnerabilities. It is one of the most widely used methods for penetration testing and is compatible with Kali Linux. Metasploit consists of modules and a datastore. Using Metaplsoit was really fun and versatile in terms of figuring out which is the best method to exploit your target. I gave several examples of the exploits I could use but I ended up going with remote access through IP. I feel like maybe I was missing somethings that I could not figure out myself or properly research and it led to my error of not being able to get access. I am honestly not too sure how I could’ve done anything really different unless I had someone critique me on the way and correct my mistakes or point to a better method. Metaplsoit and Nmap were crucial to this project. Especially trying to execute the exploit I wanted to do. Metasploit is awesome for exploiting weaknesses in the target system and gain entry, based on the target blueprint we received from the information collection and enumeration process. Access to this target system means leveraging one or more of the bugs identified during previous phases and likely bypassing the security measures introduced in the target system (such as antivirus, firewall, IDS, and IPS). Exploiting a flaw on the target allows limited access to the system. We will however, want full root/administrator level access to the target to get the best out of our mission. This can be done using multiple approaches to improve the new user's rights. Once completed, with the highest rights, we will have complete leverage over the system and can probably penetrate further into the target. Maintaining Access is crucial as well. That’s why we would run meterpreter – run persistence. You would want a backdoor or something in case the administrator restarts their computer which will defeat all the work you have done. When administrative access is gained, most penetration testers get carried away, because if the device is later patched, then they no longer have access to it. Persistent backdoors allow us to enter a device in the past that we have successfully breached.

As I stated before, I did not run into many challenges at all honestly, except for downloading Nessus and creating a session to get remote access. There is so much information in this class from the labs, which I revisit and do because they are fun and I enjoy them and learn something new every time and you have Google. I felt like I was prepared for this project by the curriculum. As I didn’t really have to use google that much. Overall, this project was fun and I learned a lot about the programs I was using and what they are used for and how much power they have. I understand I was not able to complete some of the steps, downloading Nessus and actually penetrating the system. I hope you could tell me what I could've done differently professor or done better. I want to review any comments or advice you give and apply it and hopefully penetrate the system. I felt like maybe it’s the ports I was using but I'm not entirely sure. But I enjoyed this class a lot and I would take it again. Thank you again for teaching this course professor.