#### **Question 3: Penetrating & Persisting in a Network**

What steps would you take to penetrate a network, and what would you do once you've gained access?

First, an nmap scan was made to detect all IPs within the network. Once the target IP is detected we can start looking for vulnerabilities. Methods of exploitation were made to target these vulnerabilities. Once the hack has occurred, I am able to access system files.

There were three machines connected to the network. The first machine was the Kali machine which I used for my attack. The second machine was the Capstone machine which I intend to penetrate and gain access to system files. The third machine was the ELK server which was deployed to monitor the network.

When I found the target machine and its web browser, I navigated within the browser looking for possible names and directories that I could use for my infiltration. Seeing that user Ashton was the weak link and that there was a hidden “secret” directory, I updated the URI to see what was there. As I was unable to gain access, I used Hydra and the wordlist rockyou.txt to crack Ashton’s password. Once I was successful, I was able to gain information on how to access the corporate server as well as user Ryan’s hashed password. Using a simple web based hash cracker in crackstation.net, I was able to crack Ryan’s hashed password.

With user Ryan’s credentials, I was able to access the webDAV which led me to create a reverse shell and upload it to the browser. Using msfvenom to create the reverse shell, I ran msfconsole to start the listener. I used the /multi/handler exploit in this case and set the payload for the exploit. I uploaded shell.php to the target’s server and once it was activated by the target’s machine I gained shell access and immediately went to the target’s root directory. At the root directory, I was able find the flag.txt

As I did not employ any stealth techniques, my actions would be detected by the ELK server running Kibana. Also, there would be logs indicating that a shell was created. If I had missed a possible flag, I would have to re-exploit the target as I did not install a backdoor. To install a backdoor, I would have to do so during the active shell by adding a registry key to run on restart. After doing so, I would have to open ports within the target firewall that would allow for backdoor programs.