Slide 2:

As for the technical background, I chose this topic because I am interested in blue teaming, but more specifically the Cybersecurity Analyst route.

I have applied various concepts from what we learned in class to this project, such as Networking, Pentesting, and SIEMs.

To proceed with this project, I had to go through some prior steps. First, I downloaded "virtual box," which allows users and administrators to easily run multiple guest operating systems on a single host. I then installed two different VMs on virtual box, which required the integration of a DHCP server between them for their internal network, and, by definition, a DHCP Server is a network device that automatically assigns IP addresses and other network settings to endpoints. It took me some extra learning to understand how to set up my virtual machine environment to complete the upcoming tasks, and this is where I give my thanks to the cyber security Youtuber "Network Chuck" and his video "how to build a HACKING lab to become a hacker."

Then, I went into the victim machine and manually opened port 22 by opening the /etc/ssh/sshd_config file and removing the comment sign that is next to the line "port 22." It is important to note that for this to work, you must first restart the sshd service, with the command "service sshd restart".

I then created a new user named "Benjamin" on my victim machine for the attacker to run their brute force against, and I also gave him a very complex password because I did not want the attacker to accidentally find his password credentials during his brute force attack for project purposes.

To then demonstrate my actual project, I pretended that the hacker found critical company credentials online, which includes a victim's user, and an IP address. I then ran a scan against the victim machine's IP using "nmap -sS –sV <victim IP>" which allowed discovery of an open port 22. Then I applied the newly discovered username to the tool "hydra" to run the attack; hydra is an open-source login cracker that allows us to perform various kinds of brute force or dictionary attacks using wordlists. It is also important to note that the wordlist that I used in this attack is called "rockyou.txt" which contains a list of just over 14 million passwords that were previously leaked in data breaches. It is also important to note that this attack will only work if there is a password listed on this wordlist that matches the username provided; however, for the sake of the project, I made the password as complex

as possible because I did not want to breach the account, I only wanted a handful of logs to be produced from this attack.

I then collected the logs on the victim machine, uploaded the logs to Splunk, analyzed the logs, and created an alert.

Slide 3:

Reference to DHCP server

Slide 4:

Reference to SSH Config file

Slide 5:

Screenshot of nmap command

Slide 6:

Screenshot of hydra command

Slide 7:

In the following video demonstration, I will act as the script kiddie portraying his journey in the attack, from network scan to brute force attack. I will then act as the company's cybersecurity analyst by taking the logs and uploading them to Splunk for further analysis and creating an alert from them.

Slide 8:

****Video****

Slide 9:

In summary, I simulated a very loud brute force attack, I collected the authentication logs, I uploaded the logs to Splunk, I analyzed the logs, and I then created an alert.

Slide 10:

To mitigate this kind of attack, you should close port 22, you could use SSH keys, you should make sure all passwords are strong, you shouldn't leave credentials online, and you could even allow Splunk to manually monitor logs.