Jordan Booker

Cybersecurity Bootcamp

09/16/2021

How to execute an offensive attack?

The virtual machines that were needed to complete project 2 were, Kali Linux, Elk servers, and the Capstone server. Kali Linux was used to be the attacker machine, Capstone was used as the victim machine, and Elk server were used to monitor the traffic and collect logs from the victim machine. Capstone servers were infiltrated with the goal to gain remote access. The tools that were used to gain access was a brute force attack where I gained the login credentials, a port scan was used identify the target and scan for its vulnerable ports, and finally, a reverse shell was used to gain remote access to the server.

The targets were identified by using netdiscover and adding an ip subnet. I then used a brute force attack to gain the users login credentials and was able to login via ssh and navigated through the directories until I found a secret directory. With access to the secret directory, I had a how-to list to access webdav with credentials found in secret folder. With access to the webdav I was able to drop in a reverse shell using msfvenom and gain remote access to the server.

I feel that the methods that were used were momentarily covert because with all the packets being sent and being analyzed in the timeframe it was easy to go unnoticed with the attacks and scans.