CMSC 491/791 Active Cyber Defense HW 9

Name: Daniel Roh
KotH Team: Purple

Due: December 10th, 2019 at 11:59pm

Instructions

In a few sentences, answer the following questions about the King of the Hill competition.

1) **Describe what techniques you used to attack the computers on the competition network. Which ones were successful? Which ones were not?**
   The technique I used is to use netcat scan the ports of the server's ip addresses to look for the port ports and the type of service that is running on that port. From there, by using metasploit I looked for a vulnerability on the service and attempted to send a payload to exploit that service into letting me in.

   While, I was not successful in getting into a server, one of the group mates that I was with was successful using the same method, just happened to select an exploit that worked. Most of the exploits that I used to for ssh, telnet and apache was not successful, however I wonder if it is not successful due to the lack of experience I had in using metasploit to fully take advantage of those exploits.

2) **What techniques did you use to secure the computers you gained access to from the other competitors? If you did not gain access to any computers, describe what you hypothetically would have done.**
   While I did not gain access to the server, hypothetically. I would go into the system and look the username and passwords for the system and change them to make it harder for competitors to change the passwords without doing more work. Then I would go and look into finding a way to patch the open port or maybe attempt to make a custom open port which can be accessed only by my group.

3) **If you were to play KotH again, what would you have done differently?**
   - If I was to play KotH again, I would definitely do some more research into common methods to quickly gain access to the system.
   - I would also look into better understanding netcat and metasploit tools to quicker in using them. As looking up cheat sheets and examples on how to use commands did take a lot of time.

- Also, I did not have an idea on what to do once I gotten into a system. So I would look into researching into how to change the permissions and close open ports to better secure the system in the future.