Jalen Powell

05/02/2023

COMP 5830

Cyber Security Final

First Flag

This is the first flag that I found by looking around Alice's user on the virtual machine and found a familiar file. The step on the MITRE attack framework is reconnaissance as I gathered information. The IP address I found this on was 172.31.54.91.

Second Flag

Looking at the hint above, it says that bob uses weak passwords because they will be hashed. I was passwords guessing until one worked. This MITRE attack framework step was 'persistence' as I continued to try different passwords until I gained access. The IP was 172.31.54.91.

Third Flag

Seeing the hint above, I began looking at ways that Bob could take me to his next host Ip address. I ssh into the new host and found the file. The MITRE Attack framework step here was Lateral movement as I was moving from host to host inside the virtual machine. The IP address was 172.31.58.234.

Fourth Flag

Finding the next flag required me to investigate the bash history of Bob helping Charlie. I found Charlie's password(eHJXxSL5lHE8jcAF) and used it to access his user and found the fourth flag. The MITRE step was Credential Access. The Ip was 172.31.58.106.

Fifth Flag

We needed to ssh to a new host which was 172.31.61.234. I had to find Charlie's ssh key and use the same command as Alice and Bob's needed. I needed to enter an open ftp server to extract that fifth flag. The step was Collection and Impact. The IP address is 172.31.61.234.

Final Flag

The final flag was in a var directory and all that was needed to view was the 'cat' command and it said it was the FINAL FLAG. The step was Impact as well. The IP address is 172.31.61.234.