Matt Kinderman 05/5/23

For flag 1, I started by just signing in using ssh to Alice's account on the IP address 172.31.63.53. Once in, I tried using **ls** but no files showed up. Then, I used cd to navigate backwards in the file system until I saw the threats-and-countermeasures.txt file. This is part of the Initial access phase of the MITRE ATT&CK framework because I was working on getting ssh'd into the system to have my initial connection.

For flag 2, I continued with my discovery phase in the ip address 172.31.63.53 and learned more about the file system. Eventually, I came across /etc/shadow.bak which allowed me to open it. This backup gave me access to Bob's password hash which allowed me to discover the password "password123" offline using John the Ripper and the command `sudo john /home/matt/shadow.bak --format=crypt`. This is part of the Credential Access phase of the MITRE ATT&CK framework since I was using John the Ripper to test a file which contained a lot of common passwords to find Bob's password. Once I obtained the password, I had to simply switch users with su from Alice to Bob.

For flag 3, I had to move to the new host, 172.31.56.129 in order to find the next one. To do this, I had to find a ssh key for Bob so that I could get in since his password wasn't working for the new IP address because I needed a private key. Through more discovery, I searched through Bob's file system to find a .ssh which commonly contains private keys to sing in with and there was a file in there called ed25519.key. I used this private key to ssh into the new IP address under Bob's account with the command `ssh -i ~/.ssh/ed25519.key bob@172.31.56.129`. From here I could find the next flag in the file system. This begins as the Credential Access phase of MITRE ATT&CK framework because I am starting by searching for a private key to use for access to another system. The next phase is Lateral Movement which is where I move from the first IP address to 172.31.56.129.

For flag 4, I needed to get into Charlie's file system, but did not have his private key. I stayed on the same IP address, 172.31.56.129 for this flag. Since the hint said that Bob would help Charlie when he was busy, I looked into Bob's bash history. Using `cat ~/.bash_history` I was able to see the command `echo oJvyEjXnwq0/MwtY | su - charlie -c /var/do-charlie-task.sh`. When running this line, it returned "this is doing something". This meant that I could use echo given that encrypted string to remotely execute file search commands. I modified this command to be `echo oJvyEjXnwq0/MwtY | su - charlie -c 'cat /home/charlie/flag.txt'` which allowed me to find the new string. This is part of the Execute phase of the MITRE ATT&CK framework because I was executing remote code to find the fourth flag in Charlie's file system.

For flag 5, I had to first get into the new IP address, 172.31.63.225 to find the next flag. I was able to use echo again to find the private key for Charlie and saved a copy of it to my local machine and used the command `ssh -i /home/matt/charlie.key charlie@172.31.63.225`. After this, I just used find to look for files with the word flag in the name. This is where I found flag 5. This is part of the Discovery phase of the MITRE ATT&CK framework because I was using find to find files within the file system.

For flag 6, I used a similar technique as I used to find flag 5 in the IP address 172.31.63.225 as well. Through using `find / -name '*flag*' 2> /dev/null` I could see the location of final-flag. This is also part of the Discovery phase of the MITRE ATT&CK framework since I was looking through the file system to come across the file I was searching for.