Melvin Moreno
COMP5830
Dr. Springall
2 May 2023

Final Assignment

***Bold** indicates main Framework Technique used

Flag 1:

- Offensive Technique: Obtained access and searched around using ls -a and cd.
- MITRE ATTACK Framework Technique: Reconnaissance, Resource Development, and **Discovery**
- IP Address which Flag was obtained: 172.31.54.97

Flag 2:

- Offensive Technique: Found the shadow.bak file to get the hashed passwords and used john to brute force the password: “password123"
- MITRE ATTACK Framework Technique: Initial Access and **Credential Access**
- IP Address which Flag was obtained: 172.31.54.97

Flag 3:

- Offensive Technique: Found the ~/.ssh directory to get the authorized key to move IP’s. “bob@ip-172-31-54-97:~/.ssh$ ssh -i ~/.ssh/ed25519.key bob@172.31.63.214”
- MITRE ATTACK Framework Technique: Discovery and **Privilege Escalation**
- IP Address which Flag was obtained: 172.31.63.214

Flag 4:

- Offensive Technique: Looked through the .bash_history file to find charlie’s password.
- MITRE ATTACK Framework Technique: Discovery, **Lateral Movement**, and Privilege Escalation
- IP Address which Flag was obtained: 172.31.63.214

Flag 5:

- Offensive Technique: Used anonymous login on ftp server to find flag.5.txt and then get command.
- MITRE ATTACK Framework Technique: **Collection**
- IP Address which Flag was obtained: 172.31.58.112

Flag 6:

- Offensive Technique: Looked at other services running on the device, found it in /var path.
- MITRE ATTACK Framework Technique: **Discovery**
- IP Address which Flag was obtained: 172.31.58.112