Cyber Squad of Boone inc.
Team 4 - Derrick, Dylan, Gavin, Ty
June 22nd, 2022

Summary
Blue Team response to engagement from Team2.

Vulnerabilities
- Low level user accounts have read access to important system files. They also have access to file creation and system navigation. Through social espionage, red team gained access to this account and used it to access important files and create new files that compromised the system.
- User1 (low level user account) had a very weak password with no further account protection. Red team was able to gain access to this low level account because of the use of a weak password.
- Slowloris file contains potential DoS vulnerability. Red team was able to scan this file for vulnerabilities after connecting to the system through metasploit.

Remediation
Since our main issue was the user1 account on a couple of the systems most of our remediation focused around these accounts. Some of the steps we could take to secure these accounts were:
- *Deleting unused accounts* - Since none of the accounts were actually in use they honestly did not need to be on the systems anymore. To prevent our "dummy" accounts from being used as an entry point for our system we opted to just delete all of them.
- *Using a stronger password* - The password for these accounts was "banana" which did not even require John the Ripper to crack, they simply just guessed it. To reduce further possibilities of entry to our system via an insider threat we ensured that the remaining accounts have passwords with a viable length and multiple types of characters.
- *Changing account permissions* - In Team 2's report they mentioned being able to access important files and logs such as the /etc/hosts file. To fix these we had to go through and think of all of the files that only super users should have access to and use the chmod command to change permissions for them.
- *Deleting malicious file* - During their penetration test the Red Team was able to access our system and run a looping file. To locate this and remove it we referred to the log files provided by Linux in the /var/log directory and then subsequently used rm to remove it.

Retest
After using the methods described above in the remediation section, we conducted tests that the red team used against us. After completing the retest, we were not able to access our system and every aspect of it that was seems to be secure.

Updating Documentation
Due to the lack of prior documentation, we decided to use this as a base to start and further penetration tests will contribute to this documentation