Cyber Squad of Boone inc.
June 21st, 2022

Team 4
Derrick - Threat Assessment Center
Dylan - Local Incident Management Team
Gavin - Regional Incident Management Team
Ty - Damage Assessment Team

Target: Team 2 - Lauren, Ryan, Zack, Patrick

Summary
Red Team performed a red team engagement on Team2.

The engagement performed by the red team employed real-world adversary techniques to target the systems under test. The sequence of activities in this approach involves open source intelligence collection, enumeration, exploitation, and attack in order to perform specific operational impacts. It was our goal to penetrate Team 2's system and identify any vulnerabilities.

Our goal was focused on security weaknesses, but these positive observations were made.
.

- Their systems were up to date.
- While they had ports open, we were unable to utilize these open ports to gain access.

Users	IP
ostrowskilm	152.10.223.202
Ryan	152.10.195.213
zackery	152.10.219.216
turnerpj	152.10.215.214
server	152.10.214.101

Metasploit exploit command found a backdoor that we focused on as our vector of attack. Using nmap on the IPs we found that ports 22, 53, 80, and 443 were all open, 22 and 80 being open on all users. Using metasploit we attempted to employ a phpmyadmin backdoor exploit that needs port 80 to be open to no avail, this was attempted on each user. We discovered that port 21 was open as well which opened the possibility of TCP attacks. Wireshark packet sniffing was attempted during this time. We did the entire suite of metasploit payload attempts for potential apache vulnerabilities and potential TCP vulnerabilities. None of these payload attempts were successful. We also tried accessing their server using ftp with Sina's username. We were able to successfully enter port 21 on their server using ftp and Sina's username. After entering the server, we were able to find a password file that was used when simulating "John the Ripper" from earlier in the semester. The passwords were hashed for the users and we did not have the necessary privileges to crack these passwords.

Red Team - Attack on Team 2 Steps

- Couldn't connect to port 22 on their server
- Tried Metasploit backdoor exploit
- Nmap to find open ports 22, 53, 80, 443
    - nmap (IP) -sT
- All of their users have port 22 and port 80 open
- Phpmyadmin backdoor exploit specifically port 80. Tried this on each user
- Port 21 is open on their server
- Wireshark packet sniffing attempt
- Tried changing Metasploit payload payload/cmd/unix/interact
- Metasploit apache payload attempt
- Multiple TCP exploit attempts
- Multiple apache payload attempts
- Successfully used ftp sina@<server IP>
- Accessed password file on server