Nick Marquardt

Malicious Honeypot

Senior Design Spring 2020 Self Assessment

My individual contributions to the project consisted of researching and implementing an SSH server/Honeypot, creating an email alert system, and setting up a logging system to observe activity on the server. Here are more details about my contributions: I researched what a Honeypot was and how we could set one up. I figured out how to use SSH to remotely access a Raspberry Pi while on the same network, and eventually how to access the Raspberry Pi from outside the LAN via SSH tunneling/port forwarding. Then, I set up a system to compile log files on a remote machine to keep track of users that log into the server. I used Python to create a GUI that could pull a few different log files in real time via SFTP. Next, I tested the validity of the server being found by attackers by forwarding port 22. Finally, I set up an email alert system on the server to let an administrator know that someone had accessed the server.

While working on this project I learned a number of things and built competencies with the Linux environment. I learned how to use tools like vim and Nmap proficiently and I learned how exactly attackers are able to hack into a system. I would say my biggest success was igniting a genuine interest in the field of cybersecurity. Before tackling this project, I knew nothing about cybersecurity and frankly thought it seemed boring. My successes were not without their challenges though. One of the major obstacles I faced was setting up the server. At one point I “bricked” the Raspberry Pi trying to set up a script to log server sessions automatically by writing to a read only file (/etc/profile in Linux). This was a sizable setback that led to me testing changes on a virtual machine before implementing them to the server. Another obstacle was trying to set up a vulnerable service to lure attackers. I attempted to set up a WordPress website (LAMP stack), but ran into PHP/MariaDB version issues and was unable to

get this up and running in the end. Although I could not overcome some of these obstacles, I still broadened my perspective on what can be done with a Honeypot.