Nick Marquardt

Summary of Hours Report

In the Fall semester, the first 3 or 4 weeks were a lot of brainstorming projects that our team might be interested in. At first, I was really interested in creating a music robot that could download and parse MIDI files from the internet and play them in real time. The other group members did not seem too interested in the idea, so we kept brainstorming. Eventually John came to the table with the Malicious Honeypot idea. It seemed interesting, and like something that would get us out of our comfort zones. We spent a lot of time learning about the concepts behind Honeypots. These concepts include what a honeypot is, how a honeypot is used, what kinds of honeypots there are, and what level of intereactibility they can be. I owned a Raspberry Pi and had a little bit of experience using a Linux terminal, so we decided to host a server on my Raspberry Pi. Most of my semester was spent researching topics related to cybersecurity, planning the project, and trying to get more familiar with working in an SSH terminal and Linux in general.

In the Spring Semester, it was time to start implementing the features we had planned. I did a lot of setup on the server. This setup includes figuring out how to use SSH remotely, getting email alerts working, and creating a system to read logs from the server. This semester was a lot of trial and error. At one point I bricked the server by writing a faulty script to a read only file on the server. On top of that, I had to learn how to create and program a GUI in Python's tkinter which I had not done before. Once the logger was a little more operational, I needed to know that an attacker could actually find our system. I took a risk and forwarded port 22 on the server and recorded the activity overnight to see failed login attempts from nearly 100

IP addresses. I also tried (and failed) to set up a LAMP stack to run a vulnerable service (WordPress) on the server for a more subtle way of luring an attacker.