COSC 4010
Cyberforce

Name: Andey Tuttle

Final Reflection

December 9, 2020

Last year during Cyberforce, Rafer and I had teamed up to look at putting together an Intrusion Detection System and other attack recovery mechanisms; I wrote several system backup scripts and a reverse shell detection script. Last year I was afraid to go in and touch any of our active services for fear of breaking them, but this year had me thrown into the metaphorical deep end of the pool after the competition began and I had to get up to speed on securing several systems in just a few months. As a result of the timeline for the competition, I'll reflect on what happened before selected for the competition, after selections were announced, and after the competition was over.

Before being selected for the competition, I focussed my time on two projects. First, developing the webscraper and data collection mechanisms for Ishihara, and secondly, developing a NetLogo kernel for the Jupyter notebook ecosystem. Ishihara began the year as mostly an idea without any of the web scraping tech necessary to collect the data that is at the core of its research question. I had to learn a decent amount about websraping something as gated as Instagram; in the past I had only ever scraped totally acessible data, often from Wikipedia or other fully open sources, and never had to deal with scraping information on as large a scale as this project required. The NetLogo kernel has been a beast in an entirely different way, before that project, the most complex piece of software I had ever put together was a simple front-end/back-end web application, but this project required integrating several moving parts that I was entirely unfamiliar with. It's been eye opening to see how much time it takes to put together these complex projects, and after spending dozens of hours trying to get the Java Virtual Machine to properly interface with CMake libraries and native C code, I've had to return to the drawing board to try to find another way to integrate those pieces.

During the preparation for the competition, I learned several tools for network analysis and vulnerability detection. I learned how to use Nessus, Metasploit, and Armitage all to track down open vulnerabilities on the systems provided to us. I learned a lot about what the normal behavior of Apache, POP3, SMTP, FTP, and ModBus protocols look like so that I would hopefully be able to recognize malicious activity under the new, "Assumed Breach" model of scoring used this year during the competition.