COSC 4010
Cyberforce

Name: Andey Robins

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 mesh those pieces together into a cohesive product.

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. I also learned a ton about Azure as a platform. Previously, my limited experiences in cloud hosting was strictly in AWS; however, after this class I've gained a strong background in Azure, and I'm confident that I could stand up a network of similar complexity to the Cyberforce networks in a week or two to satisfy the requirements of some small IT organization. As I reflect on what I got out of this semester, a number of less technical skills also spring to mind. I'm far

more comfortable presenting information about the security of a system, and would be able to offer recommendations for security changes that should be undertaken to ensure the security of a system. Being forced to personally pull together the security of a system made me far more comfortable with diving into the weeds and starting to pick off security vulnerabilities one by one. Whereas last year during this same competition, I was afraid to make any changes to the system for fear of breaking everything; this year I was far more comfortable with approaching the system one problem at a time. I wasn't able to fix every vulnerability before the competition, but under the new assumed breach scoring methodology, this was less of a concern than being able to respond to active intrusion and kick attackers out of the systems.

After the competition was over, I returned primarily to working on Ishihara, secondarily on the NetLogo kernel, using some of the time I had previously dedicated to Cyberforce to help get ready for the GRE and applying for graduate school, and polishing up a couple other pieces for CEDAR that Shaya had asked me to fix up. Ishihara has progressed to the point where, even with rate limiting, our scrapers are being denied for viewing too many pages. Instagram presents us with a login page, and we then need to login if we want to continue. Shaya, Jessa, and I have been regularly meeting to try to brainstorm ways to get around this (I rewrote the scraper to use a lighter, less demanding scraping API) or to figure out another way to get the data that we need. Another thing I worked on was a maze generator in the Pac-Man repo. Mason helped teach me some best practices for writing Go code as I rebuilt the incomplete code I had started years ago.

Overall, this class allowed me to learn a lot of things in a wide variety of fields, increasing the breadth of my knowledge as opposed to increasing depth like many traditional classes do. It's given me a lot more experience in the domain of working in a sys-admin and network security role, something that will certainly be applicable in future competitions that I'm able to compete in on behalf of CEDAR. In the time when I wasn't preparing for Cyberforce itself, I learned a ton about how research moves from idea through the phases of code, data, paper, and publication through the work we did on Ishihara, and I got to experience the hair-pulling struggle of trying to develop software that gets two things talking that were never designed to work together.