Individual Capstone Assessment
Senior Design
Robert Deal
September 9, 2023

Senior Design Project

For my senior design, I plan on creating a framework that can send and manage connections to different devices that serve as an example for threats from a bad actor. I intend to craft a short list of exploits that I can perform on my own hardware as if I was an outside actor. The goal is mostly to cement my theoretical knowledge on security through practical examples from the opposing side's perspective. I will be alone on this, and thus it will serve as a perfect opportunity to pour focus into this practical aspect. I could do a million ctf's and likely never encounter the sorts of problems that would result from this near-as-possible real world example. I'm excited at the opportunity presented.

In my official instruction at UC, I have learned the important features of what make computer systems work. I haven't had much chance, except in the later years of instruction, to get genuine cyber security training. Most of my courses have been very general to the computer science course, but have nonetheless taught the important topics that are critical for cyber security. Network administration, low level programming, and network systems are some of the things that were taught that are critical to a project like this one, and I would struggle to find better sources to learn it than a genuine course. I'm currently taking classes like Cyber Defense Overview, which I hope will help with this project. I hope that next semester I find some more courses that could assist in my knowledge relating to this project as well.

During my co-op experience, I have learned much about the field of offensive cyber. I spent 4 semesters at ICR Inc. where I learned much about reverse engineering on Ghidra, scanning ports with various bash commands, exploit framework usage with a company tool, and experience with many more critical tools like git or wireshark. I got genuine practical experience with how their systems worked, but I felt that I didn't have much of a chance to piece all the bits together. I mostly was made to jump around to different tasks, and wasn't able to develop something in its totality. Hopefully, this project will allow me to put together an example in a whole package. During my co-op experience, I became well acquainted with git, even submitting a patch to the linux kernel team with it and their mailing list. I hope that these practical experiences will really help out in the project to come.

Even before going to UC, I have been excited about cyber security. It has been a topic that as a child has always sounded interesting to me, and this project is a perfect chance to really test and develop my knowledge on the subject as a whole. My plan for this project relies on experience I gained on my co-ops. They used a tool, not dissimilar to something like metasploit, to construct, send, and manage exploits to test security of different systems. I intend to follow in that vein and construct a tool that can be used in the command line to simply and easily send and manage exploits to example devices. The tool will be constructed from the perspective of a bad actor.

The easy part is programming the framework tool, as that will consist of some relatively simple high level programming that will manage and handle the different exploits. The harder part will be discovering vulnerabilities and implementing exploits to different devices, while also doing it in a way that would be considered "stealthy" to any imagined administrators that would be managing the devices. The ideal end goal is to produce a package that could, with simple commands, attack various devices and produce a result that a bad actor would be aiming for, like sending sensitive information back to a host, or allowing for a level of control from the host. My current idea of what would be a “complete” project would be at least 3-5 different exploits that would display a variety of different techniques. The number will most likely change, but the goal would be to display features that would be considered “valuable” to a bad actor on at least 3 real world devices. I will likely not know when I am completely “done”, as that would be hard to put a solid finish point to, but I will likely consider it done when it can reliably demonstrate enough functionality to sufficiently scare myself. I hope that accurately informs my intentions on the project’s functionality.