To briefly talk about my capstone I will break it up week by week and summarize the week and talk about what well that week and what didn't

Week 10: This week was about learning how to properly recover virtual machines from snapshots so this week was for building the foundation for the entire project. I had some struggles with getting the file eraser script for windows to work so I decided to make a file spammer script instead. The linux file eraser worked as expected so I recovered that virtual machine from the snapshot

Week 11: This week had to do with creating a winlocker and executing it. This week overall went really well. I learned a lot about how malware and malicious functions worked. I learned how to use the win32 api using ctypes in python.

Week 12: This week was about keyloggers. I created a simple keylogger in python that tracked every single keystroke of the user which was then sent to a .txt file. This week overall went really well. I ended up using a program from intro to programming and put it on top of the keylogger to make it look more normal when the user clicked on the program.

Week 13: This week was originally about making an ssh worm, however I decided to create a SSH bruteforce program instead because I thought it would be more interesting. I tested this with a wordlist against my raspberry pi making that the target that week. I cracked my Raspberry pi's password multiple times proving this ssh brute force program to be simple and effective. This week taught me to change my password and that I'm not truly secure as I think

Week 14: This week was about phishing and setting up a fake cyber security company called ruzensec. I created a program that allowed me to send emails one at a time and a version that took a for loop to spam emails to a selected target. I created two fake employees that I sent phishing emails to that contained a malicious domain. I also set up two more phishing emails with the url of a http server that was running off my raspberry pi to simulate an attacker setting up a phishing email that would redirect victims to their c2 server.

Week 15: This week was about researching, developing and testing ransomware. I had a lot of struggles with the encryption function but managed to figure it out later on. I did significant amounts of testing on virtual machines and even bare metal with this program which I wouldn't recommend. The ransomware would lock the user out, lock user input, encrypt the selected file paths listed within the program, and then display a ransom page displaying a fake bitcoin address demanding you to pay or else your encrypted files would be deleted.

Week 16: This week was based as a continuation of week 15. I looked over the source code of the ransomware program and changed some things. The biggest issue I had was once I transferred the .py to a .exe it didn't work as intended because the ransom page doesn't display in the .exe version. Looking past the ransom page problem the script still executed and locked the user out, locked user input, as well as encrypting all the listed folder paths.