



Identify the 3 most intellectually interesting things you learned in this course. Why did you choose these 3?

1. Using RE tools like Ghidra and IDA: It was interesting to practicably be able to see how malware is created and the tactics used to make it difficult to identify. Also being able to solve crackmes by solving each component of the requirements was challenging but very satisfying.
2. Actual deployment of a RAT: It was very insightful to be able to see how real-world malware overtakes a system. Using tools like RegShot to see the changes made to the registries and using FakeNet to simulate a network and analyze the malware's communication request was extremely informative.
3. Setting up the lab environment: It was very beneficial to learn how to set up environments that ensure malware isolation from the host machine and the network. It was great practice to be able to use virtual machines and being able to gain the experience that could translate to real-world applications.

Identify the 3 most professionally useful things you learned in this course. Why did you choose these 3?

1. Development of virus removal program (RAT): It was great practice to understand how the malware attaches itself to the windows system to ensure persistence and then being able to develop a program to identify the presence of the RAT and then being able to remove the registries and processes to rid the machine of the virus. This is great knowledge to have as a cybersecurity professional and having this experience will look good on a resume.
2. Creating reports on projects: Having the practice to develop an insightful report on the weekly projects that gives details on the processes, the methods, and the applications used is valuable and I think this will translate into an applicable skill in the professional realm. Also having the GitHub repo that demonstrates the practice and knowledge acquired from the projects will be beneficial in demonstrating to potential employers the experience gained from the projects.
3. Learning extensively on computer organization and memory: Being able to utilize the concepts learned in previous courses and apply them to hands on projects to manipulate and leverage program memory to overtake a program was satisfying and important in demonstrating why these concepts are necessary for an aspiring cybersecurity professional.