Investigation of some aspect of Cyber Defense

Suggested due date: 18 October, 2021 (Submission instructions are here)

1. There will not be a traditional paper midterm exam this semester. Instead, students will identify, create, and complete some project or get some results related to vulnerability assessment. Students can choose to do anything that is exciting to them. This is intended to be an opportunity for students to bring out their creative energy that has been hiding for years. The more creativity displayed the higher the grade. Some suggested paths to a project/results are listed below.

2. This may be done in a group of two or three. However, in that case the result/project should be significantly more ambitious than that expected for a single person.

3. Scoring of the project/results will be out of 30 points.

4. There is no strict due date but students are encouraged to pace themselves so they do not try to cram a submission into that last week of the semester. I suggest aim to submit by October 18.

Suggestions

You like to destroy things

1. Develop some malware that aims to destroy my laptop. Create a means to deploy the malware on my laptop. Be merciful - limit the damage so I will not have to spend more than 2 hours to restore everything to normal. Copying someone else's malware is not going to get you a high grade. I will be especially interested in the way you are able to get the malware on the laptop - perhaps via a vulnerability.

You want to be a RAT

1. Develop a stealth communication mechanism for sending messages between computers. It should be impossible or at least extremely difficult for a system administrator to check whether such messages are actually communicated - either while a message is being sent or that a message had been sent earlier. It is OK to use steganography or IP headers to hide messages but 1) I will be impressed with another approach that has not reached popularity 2) remember that I do not care what the messages actually are - I only care about detecting the existence of a message - so checking header values and traffic levels should create a challenge for both those approaches 3) I will be really impressed if you use an OS or application vulnerability to create the covert channel.

You like to play games

1. Create an interactive multiplayer game where players shoot vulnerable code at each other
and hope that the targets execute the code. The game must support very devious and clever ways to get the vulnerable code to the target. Once vulnerable code is set, some exploit on that code will be attempted. This will likely require the target to unwittingly cooperate with the exploit. Vulnerable code could be designed to allow some players to gang up on other players.

2. Create an I-Wars game where players acquire wealth, then build armies, then have wars. The result of wars is that the winners lose some of their wealth but are able to plunder some of the loser's wealth. The game ends when one player has all the wealth. Rules should be carefully designed to encourage declarations of war (i.e. players cannot possibly win the game with declaring some wars).

**You want to work for the NSA**

1. Develop a mechanism that can detect dormant command-and-control covert channels.
2. Break the encryption on smartphone voice messages
3. Analyze cell traffic to determine who is communicating with whom