Max Wilson
Professor Akbas
CS 490 - Group 6
9/13/21

Engineering Notes

9/13/21:

We discussed the overall project plans with Boeing and had team introductions. The scrum master assigned for this project is Anthony Johnson, with me as a backup. At this first meeting, we also discussed the breakdown for our project and how we were going to set up our goals for this semester. I was assigned as part of the red team, which means I work as a penetration tester to infiltrate and test the aircraft network we are creating. We discussed our strengths and weaknesses, especially how we all know little about aircraft networks but are excited to take on the challenge.

9/15/21:

At the second official scrum meeting, I was assigned cybersecurity expert as my role, to help facilitate a more streamlined tasking for the project. I learned that the aircraft control domain is similar to how a car's computer is accessed via a tool called the "canbus." I am interested to learn more about how one could physically gain access to the cockpit in a situation and connect a canbus tool to the network to infiltrate it. I hope to expound upon this at a later point in the semester.

9/16/21:

Not much time has passed since the last scrum meeting but we officially discussed our plans with Professor Akbas and Professor Chang. We discussed how we were going to set up the network via a virtual machine software called QEMU. It was determined that we would all separately work on parts of the network on our own devices and merge them at a later date due to not having access to a central computer that can be converted as a server at this time. I worked on the backlog with Anthony, created a Github repository for the project, as well as a shared Google Drive network to facilitate ease of access for documents throughout the project.

9/20/21:

Due to still being in the design and set up phase of the project, we met again to go over the status of the aircraft domain network. We set up a weekly meeting time with Boeing for 5:30 pm and received a presentation in depth of how aircraft networks are usually connected. I also just thought of how a black box could be modified by malware or a similar attack and how that could affect the network in a real-world scenario. I will make sure to ask next meeting to see if this could be a test to complete on our network.

10/7/21:

I have been working on setting up the TFTP server via QEMU on the network for the past week so far. I also went over with the team how we should set up our penetration testing toolkit now that we have moved onto sprint two. I suggested ParrotSec in a VirtualBox due to it having a large degree of customization and tools meant for testing networks. This evening we also talked to Boeing and I learned that the TFTP server is a common issue in the network due to it not being as secure. This will definitely have to be a part of the testing for either this or the next sprint.

10/14/21:

We had our next sprint meeting and went over with professor Akbas how we would like to use funds to purchase a specified Linux computer to act as a server for the project. I sent multiple penetration testing guides and tutorials through the Discord group that we set up in the previous sprint. The TFTP server at this point has been set up and can be added to the overall network in the future. I also downloaded ParrotSec and put it on my VirtualBox on my laptop so that I am prepared for future testing.

10/21/21:

I worked on the SRS and SDD which are due for sprint two soon. I added in the work and plan so far for the penetration testing portion of the project, as well as my contribution to the TFTP server. I hope to start working on one of the first scripts for penetration testing at the start of sprint three too.

10/31/21:

I am currently working on a packet sniffer in Python with Anthony, Charles, and Maxwell. I hope to be able to submit it for sprint two so that we can present it at our upcoming demo two this coming week. The python script is based on code within a book called “Black Hat Python” which teaches how to implement basic python scripts for penetration testing. The meeting was successful this weekend and the script should be tested in time for the demo.

11/4/21:

It is now the start of sprint three, and the packet sniffer was implemented and tested correctly for the previous sprint too. I am excited going into sprint three, as it means the capture the flag (CTF) against Prescott will be coming up soon. For this sprint, I was assigned with continuing to work on the pentesting scripts.

11/11/21:

Due to projects ramping up this semester, not much progress has occurred for sprint three so far. I am planning on modifying a man-in-the-middle script I have been working on in python though which hopefully can be tested before thanksgiving. Anthony plans to troubleshoot it as well with me next week.

11/18/21:
Progress on the MITM script is going well and I have also focused on using a RAT to possibly get it onto the network. The trojan would be a good baseline for how secure the network is at this point so far.

11/25/21: Thanksgiving Break

11/28/21:
Although the MITM code has not been successful, I have found a RAT called "technowhorse" which is a very versatile trojan that can penetrate a network, even deactivating antimalware software in the process. We set up a time to present with Boeing for December 6th. I plan to test the RAT tomorrow and send the code to Anthony to test against the GAP part of the network.

11/29/21:
I worked on the final versions of the SDD and SRS, adding in the progress I have had this sprint on the scripts for the toolkit. I downloaded the RAT and tested its functionality on my ParrotSec network, isolated from my main network. I uploaded the RAT documentation to Discord for Anthony to test it. Lastly, I modified the demo for presentation three so that it included the progress on the RAT and our final plans this semester.