EE/CprE/SE 491 Weekly Report 1

Report Coverage: 02/04/2019
Project Title: Security Orchestration Platform
Client: “The Company”
Advisor: Doug Jacobson
Team Members:

- Adam Crosser (Implant and EDR Testing Developer)
- Logan Kinneer (Implant and EDR Testing Developer)
- Daniel Limanowski (Frontend Lead)
- Vijay Uniyal (Frontend Developer)
- Justin Roepsch (Frontend Developer)
- Paul Chihak (Implant and EDR Testing Lead)

Weekly Summary

This week our team continued research and development on the project.

Past Week Accomplishments

Group Accomplishments

- Communicating with project stakeholders

Individual Accomplishments

- **Adam Crosser:** Continued reviewing existing source code. Research Amazon Cloudfront and DevSecops. Researched best practices for programming in C# and reviewed Microsoft documentation on writing code which communicates using the HTTP protocol using Microsoft libraries. **BLOCKED:** I need to implement domain fronting using Amazon CloudFront, but cannot do this until the client providers funding for AWS resources. They have agreed to the requested amount of resources and are simply waiting for the proper forms to be completed, etc.
- **Daniel Limanowski:** I worked with my team and our clients to formulate appropriate meeting times for the semester. The client is restricting us to a maximum frequency of bi-monthly meetings. We have a set time every two weeks to meet, and this week was our first time. I also have been helping my sub team fix problems with their development environments. Finally, I am in the process of adding user authentication to the web application.

- **Vijay Uniyal:** Met with C2 Dev team to review and assign jobs to each team member. Started work on encrypted API using HTTPS comms. Currently researching into utilizing Rest API's and Django framework. Ran into multiple obstacles with API calling but slowly making progress. Troubleshooted development environment problems that had been an obstacle for awhile.
- **Logan Kinneer:** Performed researched how virtual environments in Linux work. Installed cuckoo in a virtual environment in a fresh install of Ubuntu 18.04.1 LTS. Researched how to integrate Cuckoo's Django web application with our web application.
- **Paul Chihak:** Worked with cuckoo to get it to function within Proxmox despite not being supported. However due to limitations this means that could not use the built in volatility memory dump option so switched to nested virtualization with virtualbox.
- **Justin Roepsch:** Implemented dockerization of app for production deployment on dockerization branch. It still needs to be further tested, documented, and cleaned, but it is functional and can be ran with one script.

Individual Contributions

Brief summary of individual team contributions given below.

Name	Individual Contributions	Hours this week	Hours cumulative (for second semester)
Adam Crosser	Researched Amazon Web Services. Learned about Amazon CloudFront and domain fronting. Read relevant parts of HTTP protocol specification. Learned about various request types such as GET, POST, etc and required headers in an HTTP request such as the HOST header.	6	6
Daniel Limanowski	Set up meeting dates for client and advisor,	6	6

	helped teammates set up dev environment, writing code to enable user authentication for the C2.		
Vijay Uniyal	Researching Rest API and Django framework so I can work on encrypted API calls. Overcame various obstacles in development environment.	6	6
Logan Kinneer	Installed Cuckoo and researched how to integrate it into our web application	6	6
Paul Chihak	Worked with cuckoo virtualization	6	6
Justin Roepsch	Implemented rough version of dockerization	8	8

Plan for the Upcoming Week

- **Adam Crosser:** Waiting for client to purchase resources I need to implement domain fronting using Amazon CloudFront. Will continue to research best practices for software development using C#. Going to read published research on implants used by various APt groups as this will help to make the implant realistic by emulating actual adversaries.
- **Daniel Limanowski:** I will continue to work on user authentication as it is a crucial feature for the web app. I will also be writing tests and documentation for this code.
- **Vijay Uniyal:** Continue to research into Rest API and Django framework and getting a working example that utilizes both so I can slowly begin development on encrypted API.
- **Logan Kinneer:** Begin implementing integration between Cuckoo and the our web application.

- **Paul Chihak:** Should be able to finish up cuckoo and start working with its Web interface.
- **Justin Roepsch:** Clean up the dockerization code, improve it's messages to the user, gather input from others on it's functionality, and merge into main branch.