EE/CprE/SE 492 Weekly Report 3

Report Coverage: 02/18/2019
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. Met with professor to discuss our progress thus far on the project.

Individual Accomplishments

- **Adam Crosser:** Researched new payload delivery mechanism including XLM 4.0 macro payloads (i.e. https://outflank.nl/blog/2018/10/06/old-school-evil-excel-4-0-macros-xlm/) and other delivery mechanisms (i.e. https://www.cybrary.it/channelcontent/squiblydoo-attack-with-com-scriptlets/). Researched more into how to use Docker and Kubernetes in various cloud environments. Learned that AWS does not appear to natively support Kubernetes like other cloud providers. **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:** Began testing with new user authentication APIs. This is one step of many to ensure secure and proper user access control within the C2 portion of the project. I wrote python code and unit tests for the APIs to ensure proper functionality.
- **Vijay Uniyal:** Gained a much better understanding of DRF framework and how to integrate that into the encrypted API communication I'm currently coding. Still in early forms of testing but getting a good framework/foundation.
- **Logan Kinneer:** Worked on integrating Cuckoo's web interface with our application's web interface. Researched how to automate the setup of Virtualenv.
- **Paul Chihak:** Researched methods of creating the in-app malware builder. Currently looking at options using an XML document that can be parsed and have different parameters modified depending on what each implant requires. Also finished creating the Cuckoo Sandbox virtual machine and will create an OVA so the rest of the team doesn't have to go through all the steps to set it up.
- **Justin Roepsch:** Worked with others to make sure they knew how to use docker-compose script that I created. Started work on task of logging user actions using Django logging system. I'm not currently able to get very far in it, as users must be added first, but they should be done by next week, so I will be able to continue.

Individual Contributions

Brief summary of individual team contributions given below.

Name	Individual Contributions	Hours this week	Hours cumulative (for second semester)
Adam Crosser	Continued research of new payload techniques and technologies that allow development of cloud native applications	5	15

Daniel Limanowski	Wrote code to make Django's backend work with the React frontend with respect to user login.	6	18
Vijay Uniyal	Gained a better understanding of DRF framework and working on prototype/testing.	5	17
Logan Kinneer	Worked on integrating Cuckoo's web interface with our application's web	5	16
	interface, and researched Virtualenv		
Paul Chihak	Research malware builder options. Finish setting up Cuckoo.	5	16
Justin Roepsch	Started work on logging actions	4	18

Plan for the Upcoming Week

- **Adam Crosser:** Continuing to research new payload techniques and implement domain fronting when I obtain access to AWS resources that are required to implement it.
- **Daniel Limanowski:** Have the user authentication functional by the end of next week so that other team members are not blocked or waiting on my requirements.
- **Vijay Uniyal:** Solidify the foundation/framework I have and try to bring it all together to start working towards a prototype for the API communication.
- **Logan Kinneer:** Continue to work on Integrating Cuckoo with the frontend.

- **Paul Chihak:** Need to create an OVA for the Cuckoo Sandbox out of my Proxmox VM so that way the rest of the team doesn't have to go through the arduous process of setting it up.
- **Justin Roepsch:** Work on logging actions of actual users after Daniel creates them.