EE/CprE/SE 491 Weekly Report 3

Report Coverage: 09/17/2018 - 09/21/2018
Project Title: Security Orchestration Platform
Client: “The Company”
Advisor: Doug Jacobson
Team Members:

- Adam Crosser
- Logan Kinneer
- Daniel Limanowski
- Vijay Uniyal
- Justin Roepsch
- Paul Chihak

Weekly Summary

This week we had the opportunity to meet with our point of contact in-person and attend a presentation where we learned more about their organization and the types of things they typically do on a red team at PwC. Outside of this we continued to research the technical feasibility of our project as well as work to develop the project plan and requirements.

Past Week Accomplishments

Group Accomplishments

- Attended presentation given by PwC at IASG Security Club
- Conducted individual project research

Individual Accomplishments

- **Adam Crosser:** Learned about techniques PwC will typically use on a red team engagement such as the Kerberoasting attack which can be used to conduct a known plaintext attack by exploiting the kerberos protocol to retrieve credential material.
- **Daniel Limanowski:** Researched design thinking processes, especially that of the testing stage. I gained an understanding of the different stages and levels of proper software testing like unit tests, integration tests, and end-to-end tests.
- **Vijay Uniyal:** Researched further into React, realized that although I set it up in a Windows VM it would be hard to follow previous steps that got us the source code. Re-configured and set it up in a linux VM for easier coding down the line.

- **Logan Kinneer:** Researched and installed Malice. Learned more about how the current application works. Learned more C#.
- **Paul Chihak:** Found a few frameworks that we can potentially leverage to aid us in distributing payloads across EDR solutions. One of them, cuckoo sandbox, seems to have great potential and we might be able to find a way to get it to coordinate with our web application without needing to manually go through and find a way to send results. Also discovered gitkraken which just got added to the github student pack and seemed like a good way to coordinate responsibilities.
- **Justin Roepsch:** Followed Daniels advice to use a virtual environment to finish setting up the project, and was successful in doing so. I am now able to make changes to the project code, and can see those changes when it is deployed. Watched Daniels Demo of the project, and further explored parts of the project as they were mentioned. Continued getting used to React.

Pending Issues

We are currently not facing any issues and are focusing on research.

Individual Contributions

Brief summary of individual red team contributions given below.

Name	Individual Contributions	Hours this week	HOURS cumulative
Adam Crosser	Researched kerberoasting attack and how we could integrate it into the implant possibly	7	21
Daniel Limanowski	Researched code testing and how it can help our team identify bugs	5	18
Vijay Uniyal	Re-configured entire setup due to realizing Windows would cause future problems	6	17
Logan Kinneer	Installed Malice, learned more about	6	17

	how the current application works, and learned more C#.		
Paul Chihak		6	17
Justin Roepsch	Finished setup of project, more learning about the project and React.	6	17

Plan for the Upcoming Week

- **Group:** Continue to work on project plan
- **Adam Crosser:** Conduct further research into red team TTPs (techniques tactics and procedures) as well as research Microsoft COM and other windows technologies
- **Daniel Limanowski:** I will conduct research on web sockets for realtime data transfer with APIs as this is a much-needed feature for the web application to make it more user-friendly and responsive.
- **Vijay Uniyal:** Delve further into Research for react and use it to understand current source code. Will learn more about ReactDOM and complex Javascript in JSX.
- **Logan Kinneer:** Will experiment more with malice and talk with the team about other EDR solutions. Will also talk about how these solutions should be integrated into the current project.
- **Paul Chihak:** Want to setup cuckoo sandbox and see what the capabilities of the product is and whether or not it will be able to help us in any way. I also want to dig into how it is doing malware analysis and whether or not we can pull results from EDR solutions with it or if we will need to write that ourselves.
- **Justin Roepsch:** I will research what the dockerization of the app would entail. I'll also take a shallower dive into some other things on the list of responsibilities for the web app.