EE/CprE/SE 491 Weekly Report 2

Report Coverage: 09/10/2018 - 09/14/2018
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 met and formally assigned project roles. We have two teams: an implant development team and a web frontend development team. We continued to research technical aspects and feasibility of project plan. We sent initial brainstorming ideas to “The Company.”

Past Week Accomplishments

Group Accomplishments

- Discussed required project functionality with the client
- Began creation of a timeline for the project
- Met with team and formally assigned roles
- Conducted research into technical aspects of project

Individual Accomplishments

- **Adam Crosser:** Continued to research domain fronting and how it can be used with Amazon CloudFront as a covert C2 channel. Researched into C# and the .NET framework as this is what we will be using for the implant.
- **Daniel Limanowski:** Researched javascript and React (the frontend framework we will be using for the command and control server) as well as Django (the backend framework) and its corresponding language - Python. I pushed existing code to our Gitlab and coordinated meetings.

- **Vijay Uniyal:** Continued research into react. Encountered problems when properly setting up on Windows environment but was able to troubleshoot. Making progress in learning how to create an app in React.
- **Logan Kinneer:** Researched the Microsoft COM. Learned more about C# by watching tutorials and writing simple code. Began to study the pre existing code for the application.
- **Paul Chihak:** Re-Affiliated myself with the existing codebase for the application. Continued looking into different strategies for automating EDR testing. Also found a few possible exploits that we could add for privilege escalation (requires powershell) and process injection.
- **Justin Roepsch:** Set up React on laptop and ran and modified a few simple apps. Pulled existing code from repo, and got through most of cnc setup for development.

Pending Issues

We are currently not facing any issues since we have just started on the project our primary focus has been research.

Individual Contributions

Brief summary of individual red team contributions given below.

Name	Individual Contributions	Hours this week	HOURS cumulative
Adam Crosser	Researched technical aspects of what I will be working on and planned project features.	6	14
Daniel Limanowski	Researched technologies to be used for web application	7	13
Vijay Uniyal	Researched React more and properly setup environment despite obstacles	6	11

Logan Kinneer	Researched the Microsoft COM. Learned some C#. Studied the existing code for the application.	7	11
Paul Chihak	Found different strategies for EDR testing automation and possible privilege escalation using powershell.	6	11
Justin Roepsch	Set up and ran React on laptop. Started setup and exploration of existing project.	6	11

Plan for the Upcoming Week

- **Group:** Work on project schedule and timeline and continue discussions with client on features and requirements.
- **Adam Crosser:** Continue to research on C# and the .NET framework. Learning more about windows Component Object Model (COM) and how in-process and out-of-process COM servers work. Looking into file format for how .NET CLR binaries are packaged.
- **Daniel Limanowski:** I will continue to research advanced web application development and user experience protocols. I will ensure that everyone can meet in person next week and demo the existing code.
- **Vijay Uniyal:** Continuing research into React, hopefully will be able to better learn the fundamentals of this new code and be able to understand our existing code better after researching more.
- **Logan Kinneer:** Work with the team to learn more about how the codebase works. Investigate ways to automate malware scanning.
- **Paul Chihak:** Going to execute the power pool vulnerability to see if it is realistic privilege escalation feature as well as continue finding ways to automate EDR testing.
- **Justin Roepsch:** Finish exploration and setup of existing project after group discussion on the topic. Continue relearning React. May also setup React on Desktop.