EE/CprE/SE 491 Weekly Report 10

Report Coverage: 11/05/2018 - 11/09/2018
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 to research and worked on development of early prototypes.

Past Week Accomplishments

Group Accomplishments

- Our group presented to the class on our challenges and gave a demo of our frontend. We continued to research and expand on prototypes.

Individual Accomplishments

- **Adam Crosser:** Researched AWS deployment architecture and method of deploying our infrastructure using container-based microservices. Researched the possibility of including Mac OS X payloads outside of the C# code that we have been developing. Conducted research to see how difficult it would be to port functionality implemented on windows to another platform. Conducted research into the Mac OSX sandbox and documented sandbox escape techniques (https://www.mdsec.co.uk/2018/08/escaping-the-sandbox-microsoft-office-on-macos/)
- **Daniel Limanowski:** Researched Ansible and its capabilities for deploying our solution as a way to automate the process of setting up our offensive orchestration environment. Wrote a playbook to deploy an existing solution on a RHEL 7.5 server.
- **Vijay Uniyal:** Gained stronger understanding of Unidirectional data flow for my Internal state in the App component. Explored bindings in java script to better utilize React ES6

components. Explorable functionalities became slightly wider due to my understanding of these topics.

- **Logan Kinneer:** Researched techniques for building web applications with Django. Figured out how to create another page within the application. Explored methods of integrating feedback from Cuckoo with the application.
- **Paul Chihak:** Deployed Cuckoo Sandbox in a virtual machine to view what data will be received and how useful its web application will be. Practiced analyzing several different payloads against the sandbox to ensure that it will work across multiple different use cases.
- **Justin Roepsch:** Researched and tested sockets in Python, for use in the bi-directional communication requirement. We will want to use the default TCP for transmission, because of it's greater reliability over UDP.

Individual Contributions

Brief summary of individual team contributions given below.

Name	Individual Contributions	Hours this week	Hours cumulative
Adam Crosser	Researched new deployment architectures and services we could use on AWS to make our lives easier. Expanded research to focus on platforms outside of windows and how existing red team techniques, tactics, and procedures can be ported to other platform. See above section on individual accomplishments for more information.	5	59

Daniel Limanowski	Researched Ansible and the concept behind playbooks and wrote a playbook to deploy existing solution.	7	62
Vijay Uniyal	Researched event handler and explored interactions with forms and events	7	56
Logan Kinneer	Learned more about the Django framework and how to integrate Cuckoo into the project.	6	57
Paul Chihak	Setup Cuckoo Sandbox in a virtual machine and tested several payloads against it.	5	53
Justin Roepsch	Researched and tested Python sockets	5	55

Plan for the Upcoming Week

- **Adam Crosser:** Continue to conduct research into how our client conducts red team operations and writing test code.
- **Daniel Limanowski:** I plan to work with the bot team to create a playbook for their Cuckoo sandbox deployment such that our entire solution is automated.
- **Vijay Uniyal:** Researching Event Handler and exploring interactions with Forms and Events. Will proceed to work with Daniel to implement Cuckoo Sandbox.
- **Logan Kinneer:** Will continue to work on integrated Cuckoo into the web app, and continue research on other features that need to be added to the application.
- **Paul Chihak:** Work with Daniel to create a ansible playbook to help automate Cuckoo Sandbox deployment. Also continue discussing ways to implement the Cuckoo Sandbox web application so that our client can easily access it from our web front end.

- **Justin Roepsch:** Examine and test different ways to enforce correct levels of authorization.