EE/CprE/SE 492 Weekly Report 2

Report Coverage: 02/11/2019
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:** Researched common antivirus evasion techniques such as XOR encryption, code obfuscation, and anti-emulation. Researched how sandbox evasion can be used evade email security appliances and other preventative controls **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:** This week, at Justin’s request, I peer-reviewed and tested his Docker code. I ensured that the Dockerization operated as expected and that the documentation was clear on how to make it work. Additionally, I continued work on creating users and groups within Django, to eventually allow for user authentication and the different level of groups that the client needs.
- **Vijay Uniyal:** Got a foothold into Rest API and now working on Django tutorial. Learned how to properly pull/modify API requests and integrate them into testing. Now exploring intricacies of Django and slowly getting a hand of it.

- **Logan Kinneer:** Ran into dependency issues while trying to get the project to run on an Arch machine. Researched Docker and Django in preparation of integrating feedback from Cuckoo into the web app.
- **Paul Chihak:** Cuckoo is now functional within virtualbox. Got the nested virtualization figured out after a decent amount of research however it does limit performance. Probably not going to use Proxmox as our virtualization manager due to the limited performance and lack of benefits. However if I can find a way to get Cuckoo to play nice with Proxmox that would be preferred.
- **Justin Roepsch:** Completed documentation and cleaning of code for dockerization of production application. Ensured that it worked on more than just my environment, and that it worked without the use of previously generated artifacts. Discussed it’s performance with Daniel, the Frontend lead, and came to the conclusion that the dockerization itself is complete until we later implement postgres for the database instead of SQLite. Merged to master.

Individual Contributions

Brief summary of individual team contributions given below.

Name	Individual Contributions	Hours this week	Hours cumulative (for second semester)
Adam Crosser	Researched common antivirus evasion techniques such as XOR encryption, code obfuscation, and anti-emulation. Researched how sandbox evasion can be used evade email security appliances and other preventative controls. BLOCKED: Until I get access to Amazon AWS	4	10
Daniel Limanowski	Peer-reviewed code, wrote code to allow for user authentication, group assignments, and permissions.	6	12

Vijay Uniyal	Researched into API requests and modifications for the HTTPS comms that needs to be implemented. Now working on Django tutorial.	6	12
Logan Kinneer	Researched Docker and Django	5	11
Paul Chihak	Figured out nested virtualization however this limits performance so going to research Cuckoo with Proxmox to bypass.	5	11
Justin Roepsch	Completed dockerization for current version of the application and ensured its success.	6	14

Plan for the Upcoming Week

- **Adam Crosser:** Continue previous week's research. Continue to dig into Amazon AWS, Kubernetes, and Container based deployment models. Read up on unit testing and continuous integration using Jenkins and how it can be applied to development being done by the implant team. Hopefully I will get AWS access so I can start on implementing domain fronting.
- **Daniel Limanowski:** I will continue on implementing user authentication. I will create the various groups we need within the application (C2). Finally, I will start research on permissions within Django, to see what existing support is out there (or if we have to build out something proprietary for this).
- **Vijay Uniyal:** Further researching and exploring Django tutorial. Planning to get a hang of it this week so I can start implementing API with it and then move on to learning DRF.
- **Logan Kinneer:** work on integrating the feedback from Cuckoo into the web application.
- **Paul Chihak:** Research how to make Cuckoo play nice with Proxmox so that way I don’t have to deal with nested virtualization. Otherwise can just use Virtualbox on top of Windows which would work but I already have Proxmox setup and would prefer to use that.

- **Justin Roepsch:** Start working on logging and understanding how user accounts are being set up by Daniel.