sdmay19-39: ISEAGE Traffic Generator

Week 6 Report
October 18 - October 25

Team Members

Dustin — *QA*
Josh — *Requirements*
Ethan — *PM*
Matt — *Architect*

Summary of Progress this Report

We ruled out the Metasploit developer library as a candidate in our project. This is because it depends on python 2 while our project depends on python 3. We initially chose python 3 to enable us to use multithreading in the language if necessary. Additionally, the Metasploit developer library has very minimal documentation to the point that we do not believe we would be able to reverse engineer it and determine how to use it.

Pending Issues

We need to determine if iptables are a reasonable solution to rewriting source addresses in the packets we are sending. We also need to investigate other libraries to use for exploitation and possibly investigate creating some of our own exploits.

Plans for Upcoming Reporting Period

We plan to perform additional research into iptables in order to determine if we will be able to use it to successfully rewrite the source address of packets. We also will look into additional frameworks for exploitation or investigate how our architecture might be extended to support some exploitation functionality.

Dustin:
I will create a proof of concept snort rule scanner, that takes a rule file and generates tcp and udp packets according to the rules, to be able to send packets that trigger default snort configuration alarms

Josh:
I will create a proof of concept for editing iptables across multiple Docker containers, so that we can generate spoofed traffic originating from a single source to many recipients

---

Individual Contributions

Team Member	Contribution	Weekly Hours	Total Hours
Dustin	This week I read about IP tables, and also learned how snort rule configuration files are structured.	3	16
Josh	This week I worked on studying iptables; I also looked back at existing python libraries for handling configuration files	2	19.5

Ethan	After doing a little more testing into the libraries, I gave up and looked for alternative approaches. The best I found is a framework released by the devs to write exploits in Python. I determined this would be an unnecessary amount of work to rewrite the exploits the tool has, so we're leaving it out of the project for the time being.	5	18
Matt	Investigated design tradeoffs of queue architectures. Began working on initial scheduling algorithm to accurately enqueue traffic generation tasks at realistic intervals.	4	22

Gitlab Activity Summary

Nothing to report.