sdmay19-39: ISEAGE Traffic Generator

Week 8 Report
November 22 - November 28

Team Members

Dustin Ryan-Roepsch — *Quality Assurance*
Matthew Vanderwerf — *Architect*
John Wallin — *Requirements*
Ethan Williams — *Product Manager*

Summary of Progress this Report

This week we further refactored the architecture to implement a second test subnet and queue. We also created a script to rewrite iptables rules which will become necessary later to allow our consumers to spoof their source. Additionally, we further improved our snort and wget tasks which will later be ran against our test networks.

Pending Issues

We all have our proof of concepts done but they’re not integrated into the task architecture and are not pointed to go to the ISEAGE environment. We discussed with our client and advisor about getting these machines setup and are planning on working on getting proof of concepts put together after winter break.

Plans for Upcoming Reporting Period

Snort: I will continue investigating my snort packet generator, I need to hand craft examples that trigger snort and compare my generated packets with them.
Architecture: In the upcoming period I will test tasks within the new two subnet architecture.
Source Address Translation: Create a scripted version of the SNAT technique, to establish rewrite rules for a given set of IPs and perform a basic dictionary attack across these addresses, such that no recipient can determine the originating point of the packets. Two-way communication should also be possible (to simulate the ISEAGE environment)

Individual Contributions

Team Member	Contribution	Weekly Hours	Total Hours
Dustin Ryan-Roepsch	I worked on verifying my Snort task. Some of packets I’m creating aren’t formed according to the rule files exactly, but others are.	1	20
Matthew Vanderwerf	This week I continued the refactor of our architectural design. I refactored the design to include an additional package for bash scripts that are necessary to our deployment. After this I updated the docker-compose.yml to spin up two consumers (to test two CDC subnets). Then I updated RabbitMQ to have	5	31

	two separate queues to enqueue traffic generation tasks, one for each test subnet.		
John Wallin	I expanded my existing example of using a script to automatically rewrite IP table rules from a simple configuration file, and successfully ‘attacked’ these IPs from the same container; I struggled to get the packets rerouted correctly to facilitate two-way communication, but this should improve with the ISEAGE environment and additional exploration of the Docker and iptables documentation	3	28.5
Ethan Williams	I built out a wget tool that parses a config file of targets with options and runs wget against all of them. I am dumping the output to console right now but am looking into if there are any benefits to parsing it.	3	23

Gitlab Activity Summary

Nothing to report.