sdmay19-39: ISEAGE Traffic Generator

Week 7 Report
November 15 - November 21

Team Members

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

Summary of Progress this Report

This week we created a tool to parse Snort rule definitions, improved the architecture of our task queue, and continued to develop our proof of concept for IP table manipulation / source address manipulation and started drafting what a configuration file could look like for a wget task. These are all key milestones in progressing towards a minimum viable prototype of the program.

Pending Issues

Now that we are relatively convinced that IP tables will be a good solution for our packet rewriting purposes, we need to focus on integrating our separate pieces together, and ensuring everything still works as expected in an actual iseage environment.

Plans for Upcoming Reporting Period

Dustin: I will setup a demo instance of Snort and send test packets to it to verify the work I have done this week was successful
Ethan: I need to build out a tool to take targets from a configuration file and run wget against them
Matt: I will utilize the new refactor to incorporate a second subnet and consumer into our current architecture demo.
Josh: I will expand my example use of SNAT for an attack on multiple victim IPs from multiple source address to be more automated, as a proof of concept

Individual Contributions

Team Member	Contribution	Weekly Hours	Total Hours
Dustin Ryan-Roepsch	I created a tool that read a Snort rule definition and use the scapy python library to generate packets that will alarm snort.	3	19
Matthew Vanderwerf	This week I refactored my architectural design of the solution. The design now contains separate modules for Tasks and Configurations. This reduces coupling and creates a better design.	4	26

Josh Wallin	I cleaned my existing proof of concept given commentary from Professors Rursch and Jacobson, and expanded it slightly to show scalability across multiple docker containers	3.5	25.5
Ethan Williams	I did research into Python configuration files for use in my wget proof of concept. Josh has also done research on configuration files but I’m researching with regards to my wget automation task. We’ll have to collaborate in the future to build a configuration that fits both of our needs.	2	20

Gitlab Activity Summary

Nothing to report.