sdmay19-39: ISEAGE Traffic Generator

Week 5 Report
October 11 - October 18

Team Members

Dustin Ryan-Roepsch — *QA*
Joshua Wallin — *Requirements*
Ethan Williams — *PM*
Matt Vanderwerf — *Architect*

Summary of Progress this Report

Found out the an sNAT might not be the best solution for source rewriting because most solutions aren't conducive to being used in a docker environment. We also put work into identifying an easy interface for metasploit to see the viability of running more complex exploits.

Pending Issues

Need to find a new way to rewrite source addresses that is conducive to docker. Also need to look at other ways to run metasploit exploits from Python since the libraries we researched did not accomplish the functionality we needed.

Plans for Upcoming Reporting Period

We want to see if dockers built in networking functionally might support the ability to do source packet rewriting, if we determine it can't we'll need to look for alternatives which work with docker. Getting metasploit into the project is going to require some digging and we'll have to determine it's viability at the end of the sprint and verify it was a stretch goal and not critical for the tool.

Individual Contributions

Team Member	Contribution	Weekly Hours	Total Hours
Dustin Ryan-Roepsch	Replied to my stack overflow questions revolving around NAT, didn't make much progress with it.	2	13
Joshua Wallin	Supported Dustin's work on (S)NAT by researching how iptables work, and broadly how networking works in a Docker environment	4	17.5
Ethan Williams	Looked into two specific libraries, pymetasploit and python-msfrpc, and attempted to create POCs locally. Functionality and documentation were lacking.	4	13

Matt Vanderwerf	Implemented dictionary cracking algorithms in python. Dictionary attacks read words from an input file and also attempt common permutations. Created a python task for our queue system to apply this dictionary attack to ssh.	3	18

Gitlab Activity Summary

Nothing to report.