sdmay19-39: ISEAGE Traffic Generator

Week 4 Report
October 4 - October 11

Team Members

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

Summary of Progress this Report

Ethan- This week I explored using a couple Python wrappers which are advertised as being able to interact with metasploit. Both of the libraries I looked at using were not available on the Python package manager and building from source is proving hard to do in the docker configuration. I also worked to get a better environment setup through PyCharm to run tasks faster and got a lot of problems. I worked through this for awhile and may pick this up in the future, although I might switch environments because dependencies are not resolving correctly.

Pending Issues

Ethan- I'm still having trouble with my environment setup. PyCharm will not acknowledge that the docker container has all the dependencies for the current directory. Also, using a docker-compose configuration did not build before trying to run tasks. I'm also going to try and find a native Python package for pen testing because interfacing with metasploit directly has been challenging.

Dustin- Multiplatform dev should theoretically be easy with docker, but I think the version I installed with brew is behaving poorly (compose failing), I'm going to manually install the latest version and try again. Also, there isn't much online in the way of a reconfigurable sNAT, but josh is going to help me look into that this week.

Josh - I am trying to find how best to use the existing docker infrastructure to explore how we might do source address rewriting. Docker does make network configuration relatively easy, but we need to find the best combination of additional tools and docker configuration to actually accomplish our goal

---

Plans for Upcoming Reporting Period

Ethan- I will either get metasploit to work correctly or will find another library which will be easier to use in the project. By the next report I hope to have at least 1 attack correctly sent to a virtual machine.

Individual Contributions

Team Member	Contribution	Weekly Hours	Total Hours
Josh	Explored options for source address rewriting; created a sample configuration file and found a python package we can use to manipulate it	3	13.5
Dustin	Worked on configuring docker on my mac to	3	13

	implement snort task, tried to find a reconfigurable sNAT.		
Matt	Implemented brute force password cracking by generating every possible key. Created a python task to apply brute password cracking to ssh.	3	15
Ethan	Explored working with metasploit directly through python interfacing libraries	5	15

Gitlab Activity Summary

Nothing to report.