sddec18-07: Software-Defined Moving Target Defense

Week 05 Bi-Weekly Report
Oct 23 – Nov 5

Clients: Dr. Benjamin Blakely and Joshua Lyle (Argonne National Laboratory)
Faculty Advisor: Dr. Hongwei Zhang

Team Members

Andrew Thai — *Project Manager*
Connor Ruggles — *Usability Manager*
Emily Anderson — *Delivery Manager*
Ryan Lawrence — *Communication Manager*
Corey Wright — *Quality Assurance Manager*

Weekly Summary and Accomplishments

Worked on Snort integration with the Floodlight controller to detect and act on Nmaps, DDoS, and ARP spoofing attacks. Currently have a script that can push rules to the controller and have some notifications that print off correctly. Mock interface has been completed and is being upgraded to meet desired specifications. Design of tests has been discussed and approved, and the baseline control tests have been started to test the network min/max/average loads.

Summary of Weekly Client/Advisor Meeting

We met with our client on Friday, November 2nd and discussed our project as far as we have completed. We talked on the progress that we had made with the modules in the Floodlight controller and decided that it would be easier to use Snort to do the actual detecting and alerts. The Nmap scans, ARP spoofing, and DDoS will be run off that system and pushed to the controller. Conner talked about the progress he had made with the interface and is doing a good job with that. We discussed our need to meet more often both as a group and with our advisor. Plans were discussed to present our demo at the end of the month.

Pending Issues

We are currently attempting to parse the logs made from alerts in Snort and convert them into Floodlight rules. We also changed directions after discussing with our clients and decided that we were going to use Snort for detection and alerts instead of Floodlight modules. Automated testing needs to be started to generate good information.

Plans for Upcoming Week

We plan to prepare our PIRM presentation, get the python script working to send rules to our controller, and add more/edit current rules in Snort regarding nmap scans. We are also going to start preparing for the CDC on Dec 1. This will involve migrating our serve over to the ISErink servers and integrating the floodlight controller. Automated tests are also being developed so that we have enough time to generate good data.

Individual Contributions

Team Member	Contribution	Weekly Hours	Total Hours
Andrew Thai	Worked on integrating snort with floodlight. Started creating a python script that will be used the parse the logs on snort that are located at /var/log/snort/alert and grab the ip's of the src and destination machine and create a flow control rule that will block that packet. I created cron jobs that will allow for baseline timing of packets between machines and the loadbalancer so that we can start comparing to the testing when we have implemented the rules.	12	122
Connor Ruggles	Created a document to really spec out what is left to get done on the interface, set up the git repo so that it makes more sense and updated the documentation. Started working on forms to create and delete Floodlight rules.	10	107
Emily Anderson	Continued work on nmap floodlight module until we decided to use only Snort. Experimented with Snort and wrote some initial alert rules for various types of nmap scans so we can start testing.	15	102
Ryan Lawrence	Worked on snort ARP spoofing detection and notification system to match the script Andrew is working on to create rules. Setup ARP spoofers to generate tests for notifications and blocking machines.	15	116
Corey Wright	Worked on DDoS detection and alert notification using Snort. Wrote alert rules to detect the test attacks and worked on Snort syntax	13	45