sddec18-07: Software-Defined Moving Target Defense

Week 06 Bi-Weekly Report
Nov 6 – Nov 19

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

We were able to create the connection between the snort alerting to the floodlight controller by using a python script. The script allows us to create floodlight rules that block the source traffic so that it stops any types of scanning that may be happening against our network or machine. The script grabs all the alerts that snort generates and handles the web scanning (nikto), nmap scanning, and ddos attacks and temporarily blocks to the traffic for 240 seconds after the alert is created in hopes of the scan to time out.

Summary of Weekly Client/Advisor Meeting

We met with our client and demonstrated to them what we have been working on. We each showed them examples of running our attacks, which then would generate Snort alerts and Floodlight rules, then traffic would be blocked. We discussed how to move forward to work on rerouting some of the malicious traffic to a Honeypot server instead of just plain blocking it like we are doing now. Discussion was also made about how to handle arp spoofing when detected.

Pending Issues

We want to start preparing for the Cyber Defense Competition on December 1st, but we have not yet heard from the coordinators. They said it would be okay for us to compete and that they would get things set up for us, so we can start getting our stuff set up, but that has not happened yet. We are a little worried we won’t have as much time as we wanted for that.

Plans for Upcoming Week

We plan to work on our system by creating a honeypot server and creating rules that will redirect the traffic to the honeypot server instead of blocking it out completely, unless it is a ddos attack which will just be shut out. We will also be working on creating the demo for the Cyber Defense Competition that is happening on Dec 1.

Individual Contributions

Team Member	Contribution	Weekly Hours	Total Hours
Andrew Thai	Created a python script for connecting the snort alerting to the floodlight rules modules. This allowed for rules to be created once the alert appeared in the snort and we were able to effectively block it. This script runs every 30 seconds and checks to snort alerts and parses through the alerts and then creates the POST request to the controller that creates the rules for 240 seconds to allow for any type of scans to time out.	28	150
Connor Ruggles	Worked a bunch on trying to resolve a CORS issue with the new interface, and got a workaround figured out. Will be implementing that and also worked on the layout of the pages of the new interface, as the logic itself is for the most part done.	20	127
Emily Anderson	Got snort alerts working the way we want them to for four different types of nmap scans. Once they had basic functionality, I worked on testing different variations of the rules in snort and am still working on customizing them a little more to make things easier.	20	122
Ryan Lawrence	Got alerts to output to snort for arp spoofing. Did research on how to handle the alert since arp spoofing needs to be handled different than blocking the source.	20	136
Corey Wright	Finalized the ddos alerts and test that I am using to make sure the snort machine is working. I managed to not break anything on the server this week, which is really nice. I also checked the alerts and made sure that only one alert is generated per attack.	20	65