sddec18-07: Software-Defined Moving Target Defense

Week 04 Bi-Weekly Report
Oct 9 – Oct 22

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

Created a complete standalone snort server within our testing network allowing us to all traffic that is being passed within the network. Started simple web penetration tests to see snort community rule alerting and starting to determine integration between snort and floodlight.

Summary of Weekly Client/Advisor Meeting

We met with our clients and gave them an update of our progress on the project. We started discussing future plans with metrics that we should define in the next week to determine what sort of testing and planning we need to do with our system to include into our research.

Pending Issues

Snort has a lot of community rules that allow to see a good amount of networking attacks but some of the networking attacks are based on certain penetration testing tools so we need to start analyzing specific attacks that we are going to do so that we can determine whether or not that snort has those rules within the community rules or if we need to create local rules. The interface still needs to be able to create rules, and it needs to be built in a way that wouldn't be difficult to edit it if the implementers wanted to add in more than one controller.

Plans for Upcoming Week

We are determining specific snort attacks and making sure that snort will be able to see those specific attacks and alert on them as well as determining our integration method with snort and floodlight. We will be planning on specific metrics for testing of our system allowing us to determine the validity of our software defined network moving target defense with testing in the next few weeks.

Individual Contributions

Team Member	Contribution	Weekly Hours	Total Hours
Andrew Thai	Uploaded load balance script to git. Figured out downloading keeps the session in load balancing as well as rotating between pages if the session is stored in the database. Worked on setting up a standalone snort machine to listen to traffic on the web network. Started using nikto to do some simple web based attacks to see what snort rules would be able to see.	10	110
Connor Ruggles	Worked more on the interface, finally figured out a consistent way to expect the controller rules to come through via an API call, scaffolded some of the other stuff out, added instructions on running and configuring the actual interface for another environment.	18	97
Emily Anderson	Continued to work on the module for nmap scans and got a test network environment set up using a mininet VM. Once the snort machine was up and running I also started looking at ways the two could be integrated and what the best next move could be	11	87
Ryan Lawrence	Continued work on the spoofing prevention module and worked on setting up a local mininet network to run tests on the module.	10	101
Corey Wright	After trying to use Snort to perform the detection for the DDoS attacks I was sending I've decided to pivot to a primarily floodlight based approach to avoid integration issues. Worked on writing the module for this and will continue to do so into the next week.	10	32