sddec18-07: Software-Defined Moving Target Defense
Week 03 Bi-Weekly Report
Sept 25 – Oct 8

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 another XenServer to allow for DDOS attacks so that the server doesn't become unresponsive after every attack for testing. Setup the GIT repo for all code to be pushed to. Currently consists of the Interface and Default Floodlight controller. As people complete their individual modules, the changes will be pushed to our main controller to display all our accomplishments.

Summary of Weekly Client/Advisor Meeting

Demoed current progress to our clients and received feedback. Main points to consider going forward particularly with the load balancer is how we rotate traffic so that downloads in progress are not interrupted.

Pending Issues

As discussed in our meeting, we need to handle the case of load balancing/rotating machines while certain processes like downloads are in progress so that they are not interrupted.

Plans for Upcoming Week

Ideally, we will finalize or get close to finalizing individual parts. Once these are done and merged into our main controller, we can begin work with putting the interface on our Floodlight controller, integrating Snort into our system, and start testing.

Individual Contributions

Team Member	Contribution	Weekly Hours	Total Hours
Andrew Thai	Creating another XenServer to allow for DDos attacking. Worked on creating a script for load balancing allocation for the four web servers that are used for testing. Tested session control for downloading large files on web server via load balancing and doesn't break session.	12	100
Connor Ruggles	Worked on the interface and getting the floodlight server working with that and setting up an environment to easily develop the interface via githooks.	15	79
Emily Anderson	I am working on writing a floodlight module to control the traffic once an nmap scan is detected.	9	76
Ryan Lawrence	Worked on installing a new module to floodlight that tracks mac addresses and compares them to macs already on ports to try to detect spoofing. Additional research is being done into other components and modules of the controller to identify what can be used and what is broken and needs fixing.	10	91
Corey Wright	I currently have a working DDoS attack available and am working on analyzing the incoming traffic to our test servers and then writing a module for the floodlight controller to intercede as needed.	8	22