sddec18-07: Software-Defined Moving Target Defense

Week 02 Bi-Weekly Report
Sept 11 – Sept 24

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

Began work on prototyping our project. Research done on Nmaps, DDoS, Spoofing, Load Balancing, and what should be included in our GUI. Sketches created for a mock GUI. Worked through feedback from our first PIRM review. Got basic load balancing features to work in a small network of machines.

Summary of Weekly Client/Advisor Meeting

Ran over our breakdown of work and got some good ideas on how to implement some of our prototype. Decided that going forward everyone should have some work to present so we can receive further feedback and ideas.

Pending Issues

Load balancing between servers require a lot of background knowledge of how the network is setup and how the devices are connected to the switches so we’re researching ways to improve the balancing in a software defined network by using the REST API that is part of floodlight to gather information needed to create the balancing between similar services.

Plans for Upcoming Week

Continue the development of individual parts. Once individual parts begin to finalize, we will begin production of combining all the different elements. Work on putting the interface on the actual Floodlight controller so real testing can begin with that.

Individual Contributions

Team Member	Contribution	Weekly Hours	Total Hours
Andrew Thai	Created load balancing between servers for basic icmp, tcp, and udp traffic. Load balancing works after creating the vips, pools, and members but requires a lot of detail to setup the system for load balancing. Started researching the REST API to create a script to easily create load balancing between servers to provide a more effective moving target defense.	14	88
Connor Ruggles	Worked a lot on getting comfortable with the Floodlight API and scaffolding out a basic system for working with their API. Worked more on the interface.	8	64
Emily Anderson	I have been researching nmap scans and how to detect them and what we should do once we detect scan traffic. I have been looking into which types of nmap scans are most common and how to detect and differentiate the different types of scans	10	67
Ryan Lawrence	Started work on prevention of spoofing attacks. Taking Josh’s idea of creating a table of ip/mac addresses to check across ports for validity.	16	81
Corey Wright	I have been researching the different types of DDoS attacks and trying to figure out the breadth of these that Kali can generate and Snort can detect. I have also generally working on familiarizing myself with the system that has been set up and getting everything in an easy working order.	8	14