

**sddec18-07: Software-Defined Moving Target Defense**

Week 07 Bi-Weekly Report

Nov 20 – Dec 3

**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 finalize the last details of our project and test it. We got packet redirection working and started to test everything. We also set up our project to use in the Cyber Defense Competition on December 1st, but due to some issues with the competition required servers, we could not actually test our system in the competition.

---

**Summary of Weekly Client/Advisor Meeting**

We met with our client and advisor to show them our final product. We demonstrated different attacks and showed them how our system handles the malicious traffic. They gave us a few final suggestions, such as adding functionality to redirect some traffic instead of blocking all of it and also adding a few more fields into the web interface.

---

**Pending Issues**

Considering that the final report is due at the same time as this status report there should be no pending issues.

---

**Plans for Upcoming Week**

This week after finishing up all of our testing and final documents, we will be preparing for our IRP presentation that is on Friday, and we will be sharing the last of our findings with our client and advisor.

## Individual Contributions

Team Member	Contribution	Weekly Hours	Total Hours
Andrew Thai	I worked on getting the machines setup for the Cyber Defense Competition, but there were issues with the competition machines when trying to setup so we ended up focusing on the process of getting everything setup from scratch. I started automating some of the testing we did with the nikto scans by having crontab entries for the scan and ping.	30	180
Connor Ruggles	Finished up the interface and got all documentation updated, very thoroughly commented the configurable parts of the interface and functions that weren't obviously named. Made sure it was a streamlined process to set up the interface and the provided backend (which won't need changed but was commented) and wrote scripts to start everything easily. Worked on the final design document, poster, and final report.	28	155
Emily Anderson	I finished making changes to the nmap scan part of the project to begin testing on it. I worked on setting up machines for the Cyber Defense Competition even though we didn't end up being able to compete. I also helped out with testing where I could and worked a lot on the final documentation.	30	152
Ryan Lawrence	Got redirection action to work for alerts to attacks and made packet redirection transparent. This means that all TCP packets can correctly flow through the honey pot server since the response still looks like it is coming from the intended target. This currently works by dynamically setting ip, mac address, and ports so that loadbalancers may be used. Produced tests for min/avg/max loads and ping loss while attacks are hitting the loadbalancer.	30	166

Corey Wright	Helped with the unsuccessful CDC server setup, worked on the final documentation that is to be submitted. Helped to test the DDoS specific portion of the code since it didn't appear to be working at first. Picked up poster, laminated, mounted it.	25	90
--------------	--	----	----