# Project Proposal

## Logan Flecke

### Overview

I will be setting up a Network Intrustion Detection System for the Cyber Lab in Hailstones 15. This NIDS will integrate with automated threat intelligence feeds and automated malware analysis. After configuring the environment, I will perform attacks on either VMs or host machines using malware found in the wild and base my attack methodology on the tactics, techniques, and procedures (TTPs) of threat actors relevant to that malware.

I believe I will be able to complete this project with confidence. I have been experimenting with Security Onion and Wazuh for over a month to familiarize myself with the setup, use cases, and limitations. Last summer, I was an intern for a Cyber Threat Intelligence team where I studied threat actors and their threat to the organization. I also took action against indicators of compromise (IOCs like IPs and URLs) and am familiar with those functions. The pentesting class will help guide me as I test configurations and perform the attack simulations. Lastly, the malware analysis class will benefit my use of the automated malware analysis reports generated.

The results from this project will expand my knowledge while giving back to the Xavier Computer Science Department. It fills the gap of the Intrusion Detection Systems class that my class missed out on and I will learn what attackers’ actions look like on defenders’ infrastructure. The use of malware found in the wild transforms this from a low-level learning environment to one that is seen in the real world. Finally, the NIDS that I build can be used by the department for years to come.

### 

### References to Resources

Deep has provided me with access to the server in Hailstones and a folder to store virtual machines. Each of the following open-source components require their own machine.

Security Onion

Network Intrusion Detection System

Captures all traffic associated with security ruleset

This is the main component

IntelMQ

Automated threat intelligence feeds

Collects IOCs from intelligence feeds (MISP, AlienVault) to be sent to Security Onion

Security Onion will engage IntelMQ when specific security rules are triggered

Cuckoo

Automated Malware Analysis

Performs behavioral analysis and reports information needed for hunting and detections

Security Onion can forward a file to Cuckoo for behavioral analysis

osTicket

Ticketing system

Assigns tasks to users based on incidents that were created from correlated events

Requires a web server and receives alerts from Security Onion via email

### 

### Division of Likely Tasks

Setup Security Onion on the Cyber Lab server in Hailstones 15.

Integrate IntelMQ and Cuckoo into Security Onion.

Identify possible threat actor TTPs to emulate.

Perform threat actor simulation to test detection, intelligence, and analysis.

Refine detections and intelligence efficiency and visibility

Optional: build a ticketing system to correlate events into incidents and recommend remediation.

### 

### Realistic Timeline

Considering a timeline of 13 weeks, starting next week and ending the week before it is due, this is my ideal timeline with Monday, Sept. 11 starting the first week:

Week 1:

* Setup Security Onion on the Cyber Lab server

Week 2:

* Setup IntelMQ for automated intelligence into Security Onion

Week 3:

* Setup Cuckoo for automated malware analysis into Security Onion

Week 4:

* Buffer time to complete setup and refine configurations

Week 5:

* Identify threat actors and relevant malware to emulate on this environment

Week 6:

* Plan attack methodologies

Week 7:

* Perform multiple attacks on the VMs and/or host machines in the lab

Week 8:

* Analyze the results and identify gaps in detection or other areas of improvement

Week 9:

* Buffer time to finish attack, analysis, and additional IDS enhancements

Week 10:

* Setup web server to host osTicket (hosted on the network, not public-facing)

Week 11:

* Correlate events more accurately into incidents in Security Onion

Week 12:

* Configure osTicket to receive incidents correlated

Week 13:

* Refine the project to be presentable and well organized