Mid-Semester Self-Reflection

CMIT-450-81: Senior Seminar Project

Instructor Michael Atwood

Kyle Hathaway

10.19.2025

Introduction

The goal of my project is to create a thorough and reproducible blue team package using OSINT investigation to create detections and a demonstration with a timed incident drill in a home SOC lab. Deliverables for this project will be an OSINT intelligence brief on malvertising with IOC tables and MITRE ATT&CK mapping. A detection pack of three rules created from the brief. A SOC evidence bundle consisting of configs and dashboards. An incident response playbook and timed drill report. All of this will be presented in a GitHub repository with a reproducible README.

This class allowed me to implement a project I have been thinking about for a few years and expand upon that original idea. When I was at the Community College of Vermont, I wanted to create a lab at home to explore some of the concepts I had learned. I was never able to create that cybersecurity lab in a way that allowed me to have visibility into both the red team and blue team. This past year, I began working as a PC/Support Engineer. In my year with this company, I have been able to scavenge old networking equipment that was headed for recycling. With this hardware in hand and upon learning about what this class would be about, I thought this would be a great opportunity to follow through on this home lab.

Lab

In planning this project, I put my previous skills learned as a Chef into practice. After fleshing out the project and setting my goal, I built a timeline and schedule that I thought would be manageable and achievable. However, I may be good at managing and scheduling tasks for preparing for a big wedding, but I am not great at planning and executing a technical project just yet. I overlooked a number of things and made assumptions about the project that I should not have. What I learned was that understanding the details of each component is vital to maintaining and sticking to a project's timeline.

In the early stages of my project, I never considered the hardware requirements to run Security Onion in the way that I wanted. I was forced to scramble and piece together

machines that could handle the load. I had incorrectly assumed that, because the OS was based on Linux, it would not require much in the way of hardware. Once I met those requirements, I began installing and configuring the operating systems and environment. This was a challenging learning experience. I struggled to install all the necessary pieces and get them working together. Ingesting logs in Security Onion was another big challenge. Configuring all the VMs, the firewall, and the switch to pass logs to Security Onion took quite a while. I spent a long time reading documentation and pursuing paths that were ultimately fruitless.

The lab is now complete. The three Windows 10 VMs, two Windows 10 hosts, firewall, and switch are passing logs to Security Onion. I was excited that I was able to work through all the issues that I faced to complete the first part of this project. At the same time, I was beginning to understand that I had chosen a big project with a lot of parts to it that I didn't fully understand.

OSINT

I began the open source intelligence investigation as I was finishing the lab. The issue of understanding the details of each portion of the project became apparent from the start. Having never done an investigation like this, I didn't know how to find what I was looking for. For my initial investigation, I began using URLhaus. This was successful in providing me with Known malicious sites. I learned a lot in this initial investigation. It isn't what I set out to find, though. I would like to be able to tie the sites I find to a specific campaign.

My second OSINT investigation has been far more successful with URLScan. Once I found a few searches that are returning results that I feel are promising, I began to build a more thorough profile of each site and fill out IOC tables. I believe I can assign the malicious sites to the Nitrogen group. This is an important goal for me to reach. I didn't want to have to open up my research question to just any malicious site. I wanted to be able to attribute it to a specific group and campaign. I thought for a few days that I was going to have to rescope the research part of this project. I have decided to limit my research to just three sites rather than five.

Detection Rules and Blue Team Response

This is the part of the project that I am about to get into. This is the part of the project that I do not have any experience with. I believe this will be the most challenging part to implement. Not only will I be attempting to create detection rules, but I will be creating benign attacks to run against the lab to see if the detections work. The initial goal is to

create and test three rules. I am prepared to rescope my goal down to one successful detection.

The final part of this is to wrap it all up into a playbook hosted on GitHub for a security team to be able to implement. As I have moved through this project, I have found that organizing it in a way that makes sense to host on GitHub is confusing. Having never tried to host something on GitHub, I am not sure of the best way to structure and document everything. Here is where I am most willing to change and compromise. If I can't figure out how to create a clean and organized GitHub, I will pare it down to the bare minimum to explain my project and what I have done.

What I learned

I've learned so much at this point in my project. From creating VMs, networking, passing logs, and investigation techniques, I have been given the chance to expand my skills and knowledge in all of these areas. The biggest lesson that I have learned is that, yes, I have a lot of experience planning and executing projects, but I was competent and well-versed in cooking, planning, and executing events and weddings. There is so much that I don't know about hardware, networks, software, and research. I am not an expert, and I can't expect things to go smoothly because I just don't have the experience yet. To be successful in a project like this in the future, I need to really dig into the finer details of each part. I thought I would be able to get my lab up and running in a week. It took almost five weeks of trial and error. I have even less experience with the rest of my project, and I know it is going to take longer than I have scheduled myself for. I need to be ready to rescope and settle for not meeting my initial goals.

Conclusion

I am grateful to have this opportunity. I have been thinking about creating a home cybersecurity lab for at least two years now. This was the push I needed to realize that idea. Not only have I made it, but it is becoming far more than I had imagined. I will be able to run attacks against the environment and evaluate how they work. Then I will be able to see what a defender would see and try to remediate and defend from it. Having a view into both the attacker and the defender is really compelling to me. I think it is really valuable to try to understand how and what attackers are trying to do in order to defend against it.

I always learn best by doing. Being able to get my hands on the equipment and try to build something has been a great experience. Not only have I learned much about hardware, software, networking, and investigation, but I have also learned more about myself and the areas I need to be more aware of. Everything is in the details. Understanding all of the components is so important to seeing a successful project through to its end.