Patrick Bays

CYSE 368

ODU Spring 2026

Professor Teresa Duvall/TA Joshua Russell

ANVIL Systems Group, Inc.

Reflection #1

03/01/2026

Internship Reflection Paper

50 Hours

Working as a network/field engineer for 50 hours has given me knowledge into the remediation steps involved in the aftermath of a blue team investigation. A blue team contracted by the DoD ran an investigation on our operations network and discovered several significant vulnerabilities. The part of the remediation process that I'm assigned to is to ensure that all our devices on the network, across multiple sites, adhere to the DoD Security Technical Implementation Guide (STIG). This process includes running an ansible script using the latest published DISA (Defense Information Systems Agency) STIG ansible role to alter vulnerable system files, process configurations, and to ensure that only approved software runs on those machines. Most of the time, this process includes debugging the script when it fails out, or skipping certain checks or changes due to different configurations of each computer, to be completed manually later. After a successful run of the script, I have to login to our Tenable Security Center instance and run a credentialed scan using a scan policy delivered to us by the customer for their individual STIG configurations, sorted by OS version. Once the compliance scan is finished, I have to go through every HIGH risk level finding and

investigate them on the host, either remediating them or marking them as a false positive. False positives are recast as LOW risk findings, and any finding that needs to exist due to specific circumstances surrounding each machine are marked as Acceptable Risk and documented. Lastly, I run a final scan on the host to ensure that any remediated vulnerabilities don't still exist. I was also assigned a more specific POA&M (Plan of Action and Milestones) to disable zone drifting on select hosts, a simple firewall configuration change.

The value of maintaining secure configurations and regular blue team investigations are the most important things I've learned. The whole point of STIG'ing our systems is to minimize attack surfaces, where every active port, unpatched service, or weak password is an open door to malicious actors. Hardening these systems in this way forces attackers to find much more complex and sometimes more easily detectable routes. I previously had no experience with blue team investigations, but through this experience, and seeing what results they had for my company, I learned that they are essential for properly maintaining an effective security posture. Not only do they utilize tools that real hackers use to test networks against an extensive database of attacks, but they also detect common vulnerabilities like expired certificates for HTTPS encryption and weak PKI (Public Key Infrastructure). The combination of the two serves to create Defense-in-Depth, where even if one layer fails, the other is designed to catch anomalies and minimize data theft.

In addition to work… I kept up with the 4 other courses I'm doing this semester, my software engineering course and my digital forensics course taking up the vast majority of my extra time. I also setup a home theater PC that hosts a NAS (Network Attached Storage) system to provide my partner and I 10TB of network storage space in RAID 1. Currently, It's a repository for our movies and special pictures that we share, to avoid data loss if one of our

computers gets corrupted or one of our drives fail. I have a hope that it will end up as a universal share when I have a proper home lab set up, with maybe a thin-client hypervisor pulling from it or something like that. When we move into our apartment in April, it will run our main TV for playing games and watching movies with friends, as well has running that local file server in the background.

Overall, the first 50 hours have been a pretty intense experience. I only recently got my TS/SCI clearance, which enables me to work on our higher-value networks, and I really got thrust into the thick of it with being assigned hands-on remediation of hosts on our main operations network. It's one thing to read about Defense-in-Depth in the classes I've taken, but it's a totally different experience actually going through and applying those principles, especially to sensitive machines that handle vital data every day. To be honest, it was pretty nerve-wracking to know that, if I irreversibly messed up on a remediation step, that we would have to send an employee out to that site to fix it in-person - especially operating as a 3-person network team, including myself. I've also had limited experience with ansible, so there was a little bit of a learning curve there as well in personally debugging those STIG scripts. Seeing firsthand how important blue team investigations are for keeping systems secure has certainly enhanced my perspective, especially when operating in a secure environment like we do at ANVIL. A lot of my day-to-day was just running scans and remediating things that were found to be out of compliance, but it's work that needs to be done to both protect the security of the company and national security. It definitely gives me more of a sense of purpose in that way. Juggling my work with the large amount of classes I've decided to take this semester is also quite the challenge, but I'm learning tons of extra stuff by virtue of my work that helps my classes and extracurricular home projects go more smoothly as well.