

Reflective Essay

Tyler Gupton

12/2/2022

—

IDS 493

—

Sherron Gordan-Phan

In the field of cyber security, my professor once explained to me that “to understand this field you must have general knowledge that’s a mile wide but only an inch deep”. This spoke volumes to me, and it gave me a much stronger insight into what was ahead of me. This field truly is a melting pot of details both technical and general. That’s why taking interdisciplinary courses such as IDS 493 served me a great purpose in understanding this career and passion of mine. Being able to combine the knowledge I’ve gained over the years has allowed me to thrive and feel confident in the topics I discuss and troubleshoot. In This reflection essay, I’ll be going over some of the key artifacts from my portfolio that I feel best contributed to and defined my profession and educational career so far. Reflecting on these will allow both the reader and I to better map out how and why certain things have been beneficial or suppressing of my career. As well as identify key points in my story that I believe are valuable information for future job positions or employers to have during their consideration.

Classes taken:

For the last 2 ½ years I’ve been studying cybersecurity at Old Dominion University where I’ve faced and overcome numerous obstacles related to my degree. Issues that arose both in and out of the classroom needed to be addressed and handled or else my work and effort would start to dull like a worn-out knife. One of the largest obstacles that I dealt with was the dramatic blow COVID had on not just everyone’s education but their lives. The entire duration of my major has been done online and has thus created that personal gap you would typically be able to bridge in an actual classroom environment. Learning to get that exciting feeling back was one of the largest setbacks that many of us are still trying to combat. Despite being separated from people

One class that sticks out to me heavily was my CYSE 250 C++ Programming class. Taking on this class was quite the horse pill to swallow for me since learning to code is quite literally learning a new language. C++ is a coding language that is purposely less advanced and barer bone so It requires you to have a foundational understanding compared to newer coding languages. For the entirety of the semester, I was constantly pulling my hair out trying to solve little bugs that ended up teaching me many lessons. One of the biggest lessons for me was understanding technology from a different point of view. Coding caused me to gain a much better perspective on technology and the way it all communicates with one another. This helped bring the large abstract idea of cyber security into something more visual and tangible for me. This shift gave me the ability to pivot into my studies and really tackle the overwhelming concept of cyber security.

Another class that stuck out to me was my CYSE 270 Linux class. This course dove into detail about one of the most popular operating systems ever designed. Linux is one of the most effective OS due to versatility of it. It can support anything from a single PC to an entire national infrastructure. “96.3% of the world’s top one million servers run on Linux. 90% of all cloud infrastructure operates on Linux, and practically all the best cloud hosts use it” (Galov, 2022). The course covered the general usage of Linux such as how to navigate and manage it which gave me a general idea of how computers really communicate with themselves.

Bootcamp:

One of my proudest achievements is completing ODUs cyber security Bootcamp which was a 9-month extracurricular course that gave amazing coverage of the cybersecurity “lifestyle and workplace”. Taking this course taught me an incredible amount of information and exposure to the true technicality of cybersecurity. With a dying urge to start my career, I looked into it and decided to apply for consideration and was called for an interview. After passing an entry exam, I was admitted to the program where for the next month I would take an intro course. Throughout that month we would very briefly discuss the topics that we would cover. In the end, we had to pass another exam to continue or else we would be dismissed from the program. Fortunately, I had passed and for the next nine months, I would be exposed to a vast amount of information. This program is what allowed me to pivot into my career allowing me to gain a much more realistic and visual

understanding of the reality and practicality of the Cyber workforce. During this course, I maintained a full-time job, and a newborn child while also still pursuing my bachelor's. This course was certainly a humbling and trying experience, but I impressed myself by proving what I was capable of achieving even when the odds were against me. We learned great lessons about not just the technicalities of things but also the workplace environment, real descriptions of job duties, the importance of soft skills, and understanding our worth as professionals.

One module that stuck out to me during the entire course was my networking module. In this module, we broke down the barer bone parts of how data is transferred from one place to another location. We covered topics such as "hardening network devices, firewall setup, TACACS+ and RADIUS protocol for AAA, VPN set up for Enterprises, and disabling insecure and legacy network protocols" (2) This was yet another moment where I began to actually visualize how things worked and with that change In perspective, I was able to understand the foundations of security and start to connect the technicalities to something tangible. This gave me an extremely competitive edge over students who are only in their 4-year degree. Within one month of the boot camp, I had already surpassed the value of knowledge id advanced in the year and a half id been studying prior. It also was an amazing opportunity for me to network and get to know other people in the same field as me. Just a reminder that covid hit as soon as I changed my major and because of so I had a much more reduced social interaction with peers and professors. Because of the boot camp I now have a few good buddies where we share information and look out for each other with possible job opportunities. As well as professors and other individuals who are professionals and even CEOs of their companies. I gained a strong feeling and understanding of what the social and technical environment was like before I had even started a position anywhere.

Certifications:

During my boot camp, I was given a strong push to drive toward certifications since I already had a vast amount of knowledge and support at my disposal. Although certifications come with their pros and cons. A popular term that gets thrown around is the idea of "Cert Hunting" which is when an individual gets caught up in the misconception that a "got to have them all" mentality is an effective way to start your career. It was important to be strategic with not only which ones I take but when. Mostly due to the fact that I had an incredibly busy schedule at the time and studying for this test would certainly require a good portion of that. I ended up shooting for my Network+ certification first since the module that covered networking in my boot camp was literally designed around the basics of the test. The course covered a decent portion of what was expected to be on the test but once I began studying the exams objectives, I realized I was in over my head. I took nearly a week off work to study and followed along with exam prep courses and eventually would end up taking the test and passing my first try! It was very technical and was definitely intimidated by the exam but in the end, I was extremely proud of that achievement. With that drive, I knew Security+ was going to be the next one up. I ended up taking that one a few months later with the same process but this time the exam was much more managerial shaped versus highly technical like the network+

Internship:

Following this tide of commitment to the field I decided that now that I have my certifications, I should begin applying for internships as soon as possible. I polished my resume and applied to 30+ positions but only received a call back from one, Ferguson. I would then accept the full-time internship as a cyber threat responder in which I worked alongside the incident response team here at Ferguson. We are the first responders to over 30,000 endpoint devices deployed across the world and it's our responsibility to mitigate issues as they arise and bring in any other teams that we may have here at Ferguson. I was immediately exposed to an enterprise environment which allowed me to understand how very large concepts and objectives

are tackled by corporations. I was also fortunate enough to work with numerous teams such as the networking and vulnerability teams. Below I've added some points that I've referenced from my resume.

- Incident Response: Experience with investigations, combatting compromised accounts, Threat hunting malware, EDRs, sandbox analysis, email security, certification management, Active Directory.
- Vulnerability Management: Familiarity with Configuring APIs, Automation, Github, and Cloud storage. Tracking down log4j vulnerability across 400+ services & 3rd parties. Tracking and patching severe vulnerabilities such as BlueKeep, Eternal blue, and Log4j across the enterprise.
- Service Desk: Helping users remove malware / PUPs and troubleshooting other security-related technical issues.

This allowed me to walk away with very beneficial information that I could apply to future positions. And allowed me to gain an incredible amount of exposure as an intern.

Conclusion:

As I previously mentioned at the beginning of my essay, cyber security really is a melting pot of information that's considered one topic. Having an understanding of a mile wide and an inch deep its certainly one of the best ways that I can describe what I've learned so far. These courses and my internship have helped sharpen my professionalism and given me a much stronger understanding of the technicalities of the field I'm in. Interdisciplinary courses such as IDS 493 have helped me compartmentalize and map all these accomplishments into a presentational form that you're currently reading. Fortunately, I've been blessed to pursue my career and pivot into what I've accomplished so far. Taking these courses/internship have truly set me up for success in my future career and I feel confident saying I'm a cybersecurity professional.

References:

- 1.) Galov, N. (2022, November 18). 111+ linux statistics and facts-linux rocke hard in 2022. WebTribunal. Retrieved December 2, 2022, from <https://webtribunal.net/blog/linux-statistics/#:~:text=are%20using%20Linux,-,96.3%25%20of%20the%20world's%20top%20one%20million%20servers%20run%20on,are%20the%20most%20popular%20ones>.
- 2.) Secure, shareable credentials. Secure, Shareable Credentials. (n.d.). Retrieved December 2, 2022, from <https://app.digit.ink/view-credential/820eb645-2102-4409-a74a-d107f8bf43c6>