Reflection Essay

George D Smith III

Cybersecurity, Old Dominion University

IDS 493, Electronic Portfolio Project

Dr. Gordon Phan

October 26, 2025

Introduction

Cybersecurity at Old Dominion University has been an enlightening experience that has introduced multiple technical skills. Skills involving problem solving, communicating, and rational guidelines are all ingrained within what I have learned in my classes. Classes consist of network architecture and security, penetration testing, social policy, and information systems. Courses I have taken, such as Networked Systems Security, Cyber Techniques and Operations, Ethical Hacking, and IDS 300W, have helped me understand and build both physical skills and the deeper understanding of my discipline needed for professional environments I will be a part of in my near future.

This reflection will consist of dissecting each of the skills I have learned throughout my academic career and connecting them to what I have made throughout my last three years. Each artifact will show abilities from ethical hacking, system building, system defending, and cryptography. These skills are specifically targeted towards achieving more cybersecurity job-aligned experience. I will also discuss how all my assignments have strengthened my technical understanding and soft skills, and how this has prepared me for the future.

Skills and Artifacts

One of my proudest achievements and significant areas of growth was in developing a homelab that was a simulated environment for multiple subnets. Something I worked on all summer trying to perfect and run. It took multiple rereads of my textbooks, looking up forums, reading manual pages, and even buying a new computer to get everything running how I wanted. I wanted to get more into the defensive side of cybersecurity after heavily involving myself with the offensive side. Incorporating open-source tools such as VirtualBox, OpenSense, SecurityOnion, and with OpenVPN, I was able to create my initial home lab. With my original knowledge of virtualization and Linux coming from Udemy courses, I was able to start. Of course there were some things I had forgotten, so I made sure to look back on CYSE 250: Basic Cyber Programming and Networking for basic tips on Linux systems. The course that helped me the most, though, was CYSE 301: Cyber Techniques and Operations and 270: Linux System for Cybersecurity; in modules 2 and 5, respectively, there is a whole slideshow on basic firewall tips and tricks. Combining that with my live practice with connecting my different subnets, I managed to complete my understanding of firewall basics. The next step was to incorporate an SIEM. This was introduced to my job search and my own research. I initially wanted to make a small environment with it not being too hardware heavy, but when I was inspired to move onto a more technical lab system, I realized I needed a better computer. I ran into multiple problems with the setup of SecurityOnion and even went back to rereading the networking basics course, IT 315: Intro to Network and Security. I found that I wasn’t using the right network setting on VirtualBox and had to switch my entire lab over to a host-only adapter and used OPNsense to connect all systems to the internet.

I wanted to add depth to my homelab as well, so I added Windows Server 2025 to my internal Windows machines. This allowed me to practice Active Directory hacking on something I had knowledge in. I wouldn’t have been able to know where to start, though, if I didn’t take CYSE 280: Windows Systems Management and Security the semester earlier. The class was all about Windows Server and taught me how to set up, navigate, and understand Windows Server. From adding more users for more technical depth to adding more attack surfaces and understanding the underlying setup errors that can occur.

While I focused my homelab on system defense, I had to take the opportunity to test different attacks and countermeasures using my entire lab environment on Kali Linux. This means almost all of my virtual machines are running. Machines like Windows 7-10, Windows Server 2025, Kali Linux, Kali Purple, OPNSense, and SecurityOnion are operating. While this is a huge load on my computer, I had specifically bought parts to accommodate the stress it could encounter. I would use Kali Linux in one subnet to interact with all my Windows machines in another subnet, while I had SecurityOnion monitoring the Windows machines and Kali Purple running as the base of both SecurityOnion's and OPNSense's GUIs. This could allow for rapid changes in defense through looking at SecurityOnion and interacting with OPNSense firewall rules.

Moving onto a more offensive side of cybersecurity, I initially came into college with basic hacking knowledge. I didn't start surrounding myself with the subject until my sophomore year. With my favorite class, CYSE 450: Ethical Hacking and Penetration Testing. This class taught me in-depth processes on password cracking, vulnerability scanning, steganography, and SQL injection. Homework consisting of using nmap to scan a virtual machine and exploit it was memorable and the biggest sign I wanted to go into penetration testing in my future.

Classes and Homework

While some see homework as repetitive and boring, most of my time at Old Dominion I've had fun doing homework and learning more concepts on my own. CYSE 463: Cryptography for Cybersecurity has given me inspiration to interact with multiple cryptological functions. I am fortunate to have a teacher that allowed me to spread my knowledge to areas I haven't touched in ethical hacking. For my course project I had set up a rudimentary system to encrypt files like a ransomware would do. That project took longer than I expected but led to me learning more about programming skills and coding while interacting with systems.

Writing comprehension

IDS 300W played a vital role in shaping how I approach complex problems, communicate ideas, and connect interdisciplinary research to real-world cybersecurity challenges. Writing-intensive courses such as IDS 300W and CYSE 425W have given me a look into how comprehensive and important writing is within the field. The course emphasized critical analysis, structured writing, and the importance of drawing from multiple fields when examining modern issues. Because cybersecurity is not only technical but also social, political, and ethical, the interdisciplinary mindset developed in IDS 300W directly supported my later coursework in cyber policy, network security, and ethical hacking.

One of the most valuable skills I strengthened from IDS 300W to CYSE 425W was my ability to analyze problems from multiple perspectives rather than relying solely on a technical explanation. For example, when working on my Cyber Policy Writing Project, I was tasked to analyze my policy on network security from all aspects, not just the technical aspect but from an environmental, political, and social aspect as well.

Conclusion

Overall, my cybersecurity program has given me a comprehensive, interdisciplinary foundation that integrates technical skill, communication, and critical thinking. Each course contributed to a larger understanding of cybersecurity as not only a technical field but also a human-centered discipline influenced by law, psychology, sociology, and organizational behavior.

Interdisciplinary methods were essential in helping me understand my coursework. Tools from computer science helped me solve implementation problems, while insights from psychology and social science strengthened my awareness of user behavior and social engineering. Courses like CYSE 425W and IDS 300W provided the research, writing, and source integration skills needed to analyze complex issues and present information clearly.

These combined experiences prepared me to engage in my assignments, collaborate effectively, troubleshoot issues, and apply theory to hands-on practice. It also reflects what employers expect from cybersecurity professionals: technical expertise, strong communication, ethical judgment, and the ability to understand security problems from multiple perspectives.

By reviewing my artifacts, I can see how I have developed the knowledge, adaptability, and professionalism necessary to succeed in the cybersecurity field. My interdisciplinary education has made me a more effective thinker and practitioner, ready to contribute meaningfully to future roles in the cybersecurity workforce.