Reflective Essay

Tyler Walker

Department of Cybersecurity, Old Dominion University

IDS493: Electronic Portfolio Project

Professor Carin Andrews

December 5, 2025

Introduction

Throughout my cybersecurity degree program I have grown in ways that I did not expect when I first began. I entered the field with a basic interest in technology, but over time I discovered how many different disciplines come together to create a well rounded cybersecurity professional. As I progressed through each course and each assignment I was able to grow in my thinking as well as my problem-solving abilities as a result of the use of both technical knowledge and analytical/creative thinking in combination with effective communication. The interdisciplinary nature of the program has been one of its biggest strengths because it taught me how to draw from computer science, information systems, policy studies, writing, and even elements of psychology. These learning experiences shaped my three most marketable skills. They are my proficiency with Kali Linux, my programming ability in Python, and my growing expertise in network security. Each of these skills is supported by artifacts that represent my best work and demonstrate how my coursework prepared me for real responsibilities in the cybersecurity field.

Kali Linux

My first major skill is my ability to use Kali Linux for ethical hacking and system analysis. This skill has become a core part of my cybersecurity foundation because it gives me real, hands on insight into how attackers think and how defenders need to react. The first artifact I chose for this skill comes from Lab Assignment 3, where I used tools like John the Ripper, Aircrack ng, and Wireshark to explore password cracking and wireless security. Working through this lab showed me just how weak a system becomes when it relies on poor passwords or outdated encryption. It also helped me realize that technology alone cannot protect a network. Strong security depends on users and administrators making smart, informed choices.

My second artifact for this skill is Lab Assignment 5. This assignment continued to build my familiarity with wireless security by having me capture handshakes, crack WEP and WPA2 keys, and analyze decrypted network traffic. At first, the idea of breaking into a wireless network felt complicated, but once I began working through the steps I saw how attackers approach these scenarios. I learned how to interpret packet captures, identify browsing activity, and connect network behavior to possible risks. The interdisciplinary nature of the course also helped me here because my prior experience with data analysis and communication studies made it easier to explain my findings and understand why certain traffic patterns matter.

The final artifact for this skill is Lab Assignment 4, which involved using Metasploit to exploit vulnerabilities in a controlled environment. This was one of the most challenging and rewarding labs because it required both technical accuracy and critical thinking. I had to identify a vulnerability, research how it could be exploited, and then run the appropriate module. Completing this assignment strengthened my ability to troubleshoot, document processes, and think like an adversary. These three artifacts show my progression from basic tool usage to deeper understanding of offensive security methods, which directly supports many job postings that ask for experience with penetration testing tools and vulnerability analysis.

Python Programming

My second major skill is Python programming. Python is used everywhere in cybersecurity and information technology for automation, scripting, data processing, and security testing. My first artifact for this skill is my Python and socket programming project, where I built a small task management system that communicates over a network. I created both the server and the client, designed a simple encryption feature, and stored user tasks in a JSON file. This project taught me how to structure a multi file program and how data moves across a network. It also

opened my eyes to the importance of secure communication, even in simple applications. I learned problem solving techniques that I now use in other coding situations, especially when something does not work the first time and I need to troubleshoot methodically.

My second artifact is the Q3 script, which had me read input, process names, and print them in a new format. It was a pretty small assignment, but it ended up teaching me a lot about how Python handles strings, lists, and user input. These might seem like simple concepts, but they're really the foundation for building anything bigger in programming. What surprised me was how much my other coursework influenced the way I approached it. Classes centered on writing and communication helped me keep my code clean, organized, and easy to follow; almost like writing a short, clear paragraph that someone else could understand without needing me to explain it.

My third artifact is the Q1 script, which reads a text file and creates a new one with duplicated lines. This assignment strengthened my understanding of file handling and showed me how Python can automate tasks that would take forever if done manually. Since many cybersecurity jobs involve reviewing logs, parsing data, or running automated processes, these skills translate directly into real world expectations. Together, these artifacts show that I can write functional, organized, and well structured Python programs, which is something that appears in almost every cybersecurity job description.

Network Security

My third major skill is network security, which is really at the heart of modern cybersecurity. The first artifact I chose for this skill is Lab Assignment 6, where I used steganography tools to hide and extract secret messages inside image files. Before this lab, I never realized how much data can be tucked away in places you wouldn't normally think to look.

It showed me that cyber threats aren't always loud or obvious; they're sometimes quiet, hidden, and easy to miss unless you know what to look for. Working through the assignment gave me valuable hands on experience and helped me build an investigative mindset, something that will be incredibly important in any future security role.

My second artifact is my General Review of the National Cybersecurity Strategy. This paper helped me see cybersecurity from a national and policy based perspective rather than only a technical one. I learned how government strategies shape the direction of the field, including how the United States plans to defend critical infrastructure, support public and private partnerships, and disrupt threat actors. Writing this paper pushed me to connect what I learned in my hands on labs with the bigger picture of national security. It also helped me practice the type of analytical writing that many cybersecurity careers require.

The third artifact is my SCADA Systems paper. This assignment focused on industrial control systems and the unique vulnerabilities that come with them. I learned how fragile critical infrastructure can be if it is not properly protected and how cyberattacks in this area can have real physical consequences. This paper challenged me to think beyond traditional computing environments and consider how cybersecurity connects to engineering, public safety, and risk management. These three artifacts demonstrate that I can understand cybersecurity not only at the technical level but also at the policy and infrastructure level. This interdisciplinary understanding is something employers value highly.

Conclusion

Looking back at my coursework, I can really see how each lesson and assignment shaped me into an interdisciplinary thinker. The technical labs gave me real, hands on experience, my programming assignments taught me how to approach problems creatively, and my research

papers helped me understand the bigger picture behind cybersecurity issues. Courses like Interdisciplinary Research, Process, and Theory also made a huge difference. They taught me how to communicate my ideas more clearly, stay organized, and see how different fields connect and support one another. Being an interdisciplinary thinker is incredibly important in cybersecurity because no single field has all the answers. Technology, policy, human behavior, and communication all have to work together. Everything I have learned in this program has prepared me to step into the cybersecurity world with confidence, curiosity, and a strong foundation that I know I will keep building on.