Reflection Essay

Owin Ifill

Interdisciplinary Studies: Old Dominion University

IDS 493: Electronic Portfolio

5, December 2025

Introduction

Throughout my interdisciplinary degree program, I learned a wide range of skills that helped shape me into a more prepared and well-rounded cybersecurity professional. Because the program draws from different subjects including cybersecurity, networking, policy studies, writing, and basic computer science. I had to learn how to think and work in many different ways. Instead of only focusing on one skill set, I learned to combine technical knowledge with critical thinking, communication, and ethical decision-making. After reviewing the work I completed over the past few years, three skills clearly stand out as my strongest: Linux skills, problem-solving and analytical thinking, and network security and networking fundamentals. Each of these skills is represented by artifacts I created during my coursework, and each artifact reflects real learning, growth, and preparation for the cybersecurity field. In this essay, I explain how these artifacts demonstrate the development of my skills and how my academic experiences have prepared me for career readiness in cybersecurity.

Linux Skills

Artifact 1: Penetration Testing (Ethical Hacking)

Artifact 2: Linux Commands Lab

Artifact 3: Sword vs. Shield Firewall Project

Linux is one of the most important tools in cybersecurity, and throughout my program I spent a lot of time learning how to use it. My first artifact, the Penetration Testing assignment, shows how I learned to use Linux-based tools to test systems ethically. In this assignment, I used penetration testing methods to explore vulnerabilities and understand how attackers might try to break into a system. This wasn't just about running commands, it required learning the ethical

responsibilities behind cybersecurity work. I had to understand what it means to test a system safely, legally, and responsibly. This assignment also showed me how powerful Linux tools can be when used correctly.

My second artifact, the Linux Commands Lab, represents my ability to work confidently in a Linux environment. In this lab, I practiced using basic but essential Linux commands, such as navigating through directories, checking file permissions, examining logs, and managing system processes. At first, working in a command line environment can feel intimidating. But this lab gave me the chance to practice step-by-step, and over time the commands became more natural. This hands-on experience helped me build the foundation necessary for more advanced cybersecurity tasks. Linux experience is something almost every cybersecurity job post mentions, and this lab helped me gain the confidence to work with it.

The third artifact, the Sword vs. Shield Project, shows a deeper level of Linux skill configuring a firewall. In this assignment, I had to create a firewall in Linux and understand how to filter and manage network traffic. This required not only technical skill but also an understanding of how attackers think and how defenders protect systems. This project helped me see the difference between offensive and defensive cybersecurity and how both sides require strong Linux knowledge. By working through this assignment, I learned how firewalls contribute to system hardening, how to block certain types of traffic, and how to create a more secure environment.

Together, these three artifacts show my growth with Linux from basic command line work to ethical hacking, to building defensive tools. These skills directly connect to real job requirements in cybersecurity, making me more prepared and confident as I move into my career.

Problem-Solving and Analytical Thinking

Artifact 1: Case Analysis (Budget, Networking, Security Planning)

Artifact 2: Policy Analysis (Foreign Cybersecurity Policy)

Artifact 3: Analysis Paper (Social Impact of Cybersecurity)

Problem-solving and analytical thinking are at the heart of cybersecurity. My Case Analysis artifact shows this skill especially well. In this project, I had to design a networking plan, create a budget for equipment, and develop a security plan all while staying within strict financial limits. This meant looking at multiple factors at once: cost, performance, and practicality. It forced me to think realistically and use knowledge from different subjects. Business classes helped me understand budgeting and cost justification, while IT and cybersecurity courses helped me decide which devices and protections were necessary.

My Policy Analysis artifact shows analytical thinking in a different context. Instead of focusing on equipment or networks, this assignment required me to analyze a foreign cybersecurity policy and evaluate whether it was effective. I had to read policy documents, think about government strategies, and use evidence to support my argument. This helped me understand that cybersecurity is not just technical, it also affects national security, international relations, and global stability. The assignment required critical thinking, research skills, and the ability to explain how policies shape the cybersecurity landscape.

The third artifact, my Analysis Paper on the Social Impact of Cybersecurity, pushed me to look at cybersecurity through a social and ethical lens. I explored how cybersecurity affects

people, institutions, and society as a whole. Writing this paper helped me learn how to communicate complex ideas in a way that others can understand. Cybersecurity professionals often work with people who are not technical, so being able to explain the social impact of technology is an important skill. This assignment also showed me how cybersecurity issues like privacy, surveillance, and digital safety affect everyday life.

These three artifacts show that I can solve problems from multiple angles technical, financial, political, and social. This is important because cybersecurity professionals are often required to make decisions that balance all of these areas. Strong analytical thinking helps in roles such as risk analysis, security planning, consulting, and incident response.

Network Security / Networking Fundamentals

Artifact 1: Wireshark Traffic Tracing and Sniffing

Artifact 2: Hands-On #3 (Networking Plan for Two-Floor Building)

Artifact 3: Hands-On #6 (Networking Communication Letter)

Networking is the foundation of cybersecurity, and my artifacts show the technical and communication skills I gained in this area. The Traffic Tracing and Sniffing assignment shows my ability to use Wireshark to analyze network data. I learned how to follow packet flows, filter traffic, identify patterns, and recognize unusual behavior. Understanding how network traffic works is essential for detecting attacks, troubleshooting issues, and securing systems.

In Hands-On #3, I created a full networking plan for a two-floor building. This meant deciding where to place networking devices, planning cable routes, choosing equipment, and staying within a budget. This project helped me connect theory to real-world applications. It also

taught me how to think ahead, plan carefully, and justify decisions based on costs and needs. This type of project is very similar to what network technicians and cybersecurity analysts do in real organizations.

The third artifact, Hands-On #6, may not seem as technical, but it highlights an equally important skill communication. In this assignment, I wrote a professional letter explaining the budget and materials for a networking project. This taught me the importance of clear communication in cybersecurity. Even the best technical plan is useless if no one understands it. Cybersecurity professionals must be able to communicate with managers, clients, and team members who may not have technical backgrounds.

Taken together, these artifacts show that I understand networking from both a technical and communicative perspective. Networking fundamentals are a big part of almost every cybersecurity job, and these assignments helped me develop confidence in this area.

Conclusion

Looking back at my program as a whole, I can clearly see how the interdisciplinary approach helped me grow in multiple ways. I learned not only technical skills like Linux, penetration testing, and networking but also broader skills like communication, critical thinking, and ethical awareness. The combination of different subjects helped me understand cybersecurity as more than just technology. It is connected to people, laws, budgets, communication, and global issues.

My strongest skills Linux proficiency, analytical thinking, and networking fundamentals came together through hands-on assignments that challenged me to think across disciplines. These skills match what employers look for and prepare me for real responsibilities in the

cybersecurity field. The interdisciplinary approach taught me to be adaptable, thoughtful, and ready to solve complex problems from different angles. Overall, my academic journey has prepared me to enter the cybersecurity field with the knowledge, confidence, and mindset needed to succeed.