Reflection Essay

Zyron James M. Sumulong

Old Dominion University

IDS 493: Electronic Portfolio Project

Doctor Gordon-Phan

May 5, 2026

Abstract

This essay reflects on the development of my knowledge and skills in cybersecurity that I developed over the course of my education at Old Dominion University. Specifically, this essay will focus on my knowledge and skills in three main areas: cybersecurity policy and risk management, technical security, and threat analysis. I will examine each of these areas through the lens of various pieces of artifacts such as coursework, hands-on labs, and my own personal experience. Each piece of coursework, along with many others that I am including in my ePortfolio, has demonstrated my technical growth as a cybersecurity student. This essay will discuss how I have integrated what I learned in one area into another. Furthermore, this essay will explore how Interdisciplinary Learning has allowed me to develop a wide-ranging approach to solving cybersecurity problems.

Introduction

Throughout my academic journey in cybersecurity, I have developed a strong foundation in technical, analytical, and policy-based disciplines. My background in IT, combined with my current role as a Tier II Network Engineer, has allowed me to connect classroom learning with real-world experience. This program has emphasized the importance of understanding cybersecurity from an interdisciplinary perspective, including policy, risk management, and human factors.

The three primary skills highlighted in my ePortfolio are cybersecurity policy and risk management, technical security, and threat analysis. These skills were developed through a combination of coursework, labs, and practical experience. Each artifact included in my portfolio demonstrates my growth in these areas and reflects my ability to apply cybersecurity concepts to real-world scenarios. This reflection essay analyzes those artifacts, the challenges I faced, and how these experiences have prepared me for my future career.

Cybersecurity Policy & Risk Management

The development of my understanding of cybersecurity policy and risk management has been shaped in class CYSE 280: Windows System Management and Security. One of the most impactful artifacts was my paper on the role of patch management in Windows environments. Dissanyake et al., (2020) refers to patch management as the process of applying patches to the vulnerabilities in software, systems and firmware. Through this assignment, I learned how critical it is to maintain system updates in order to reduce vulnerabilities. Initially, I underestimated how complex patch management could be in large organizations, but this assignment helped me understand the balance between security and operational stability.

Another important artifact was my security policy design paper in class CYSE 300: Introduction to Cybersecurity. In this assignment, I was required to develop a policy for protecting sensitive systems, including database servers. This assignment forced me to expand upon technical configurations and to take into consideration organizational objectives, compliance requirements and risk mitigation strategies. I had to apply knowledge from multiple courses, including networking and cybersecurity fundamentals, to create a comprehensive solution. This experience reinforced the importance of structured policies in protecting systems.

Additionally, the risk management paper I wrote in IDS 300W: Interdisciplinary Theory and Concepts, focused on analyzing the organizational, technical, and human factors that shape effective cybersecurity risk management. Through this assignment, I learned how interdisciplinary approaches are essential to identifying and mitigating risk. I explored how technical controls, governance structures, and human behavior intersect to influence decision-making and security outcomes. This artifact allowed me to connect academic theory to practical risk assessment, reinforcing my understanding of policy implementation and operational readiness.

Technical Security

My technical skills have been developed primarily through hands-on labs and projects. One of the most impactful experiences was the Linux password cracking lab in class CYSE 270: Linux System for Cybersecurity. In this assignment, I created multiple user accounts with varying password complexities and used John the Ripper to test their strength. This lab provided insight into how hash crackers can be utilized by security analysts and criminals to discover vulnerabilities in passwords (Marchetti & Bodily, 2022). It also introduced me to offensive security concepts, which are essential for understanding how to defend systems.

One of my strongest technical artifacts is the secure client-server application I developed in class CYSE 250: Basic Cybersecurity Programming and Networking. This project involved implementing authentication, password hashing, and basic encryption using Python. Through this assignment, I learned how to design secure systems and protect user data. It also reinforced concepts such as data integrity, confidentiality, and secure communication. The project received top recognition within the class for its design and implementation, highlighting both my technical skill and my ability to apply cybersecurity concepts effectively.

Another key artifact was my Windows penetration testing lab in class CYSE 301: Cyber Techniques and Operations. This assignment allowed me to explore system vulnerabilities and understand how attackers exploit weaknesses. I performed privilege escalation, created administrative accounts, and extracted password hashes. Scarfone et al. (2008) describe that the post-exploitation phase of penetration testing includes gaining elevated privileges, creating persistent accounts, and collecting credentials to simulate how attackers maintain access to compromised systems, which mirrors the activities I conducted during the lab.

An additional artifact that demonstrates my technical knowledge is my CompTIA Security+ certification, which can be found in my About Me section. This certification demonstrates my foundational knowledge in cybersecurity principles, including network security, threat detection, and risk management. Knapp et al. (2017) states that professional certifications serve as recognized measures of competency that validate these skills. The lab exercises I completed, such as the Linux password cracking and Windows penetration testing labs, were reinforced by the concepts covered in Security+, showing how practical application complements theoretical knowledge. Overall, this artifact strengthens both my technical competence and my professional preparedness for cybersecurity roles.

Threat Analysis

The development of my threat analysis skills has been influenced by both technical labs and research-based assignments. The Wireshark traffic analysis lab in CYSE 301 was one of the most valuable experiences in this area. Through this lab, I learned how to capture and analyze network traffic between virtual machines using Wireshark, identify patterns, and detect anomalies. This skill is directly applicable to real-world cybersecurity roles, particularly in network monitoring and incident detection.

In CS 462: Cybersecurity Fundamentals and CYSE 300 , I analyzed real-world cyberattacks such as the Change Healthcare breach and the Target data breach. These assignments helped me understand how vulnerabilities are exploited and the impact of security failures on organizations and individuals. I learned that cybersecurity is not only a technical issue, but also involves human factors, organizational decisions, and risk management.

These artifacts helped me develop a more comprehensive understanding of incident response. Instead of focusing solely on detection, I began to understand the importance of prevention, response planning, and recovery. This shift in perspective is critical for a career in cybersecurity, where professionals must anticipate and respond to evolving threats.

Interdisciplinary Learning

One of the most valuable aspects of my academic program has been its interdisciplinary approach. Cybersecurity is not limited to technical skills; it also involves policy, management, and human behavior. Courses such as IDS 300W: Interdisciplinary Theory and Concepts helped me understand how different disciplines contribute to problem-solving and decision-making. The

authors describe cybersecurity as a field that overlaps data, systems, and human behavior, emphasizing that effective cybersecurity research and practice requires integrating knowledge from technical, organizational, and social perspectives. For example, my policy-related assignments required me to consider legal and organizational factors, while my technical labs focused on system-level implementation. Suryotrisongko and Musashi (2019) state that human behavior is a critical factor in cybersecurity outcomes, demonstrating that technical solutions alone are insufficient to address real-world threats. Combining these perspectives has allowed me to approach cybersecurity challenges more effectively. Additionally, reflecting on projects where I initially struggled taught me the importance of adaptability and continuous learning. This interdisciplinary mindset is essential in the field, as real-world problems rarely fall into a single category. Engaging with multiple perspectives not only enhanced my analytical skills but also strengthened my ability to communicate and collaborate with diverse teams, a competency critical for professional cybersecurity practice.

Career Readiness

The skills and experiences I have developed throughout my program align closely with the requirements of a Cyber Network Defense Systems Analyst role. My technical background in networking, combined with my experience in system administration and security analysis, provides a strong foundation for this position. Additionally, my exposure to real-world cyberattacks and incident response concepts has prepared me to analyze and respond to security threats. Reflecting on these experiences, I recognize the value of continuous professional development, including certifications like Security+ and TS/SCI clearance, in complementing academic knowledge. These artifacts and experiences collectively demonstrate my readiness to

apply theoretical knowledge in operational environments, think critically under pressure, and collaborate effectively.

My current role as a Tier II Network Engineer has also contributed to my readiness. Through this position, I have gained experience in monitoring network performance, troubleshooting issues, and working in operational environments. These experiences have strengthened my ability to think critically and respond to problems under pressure, which are essential skills in cybersecurity.

Conclusion

Overall, my academic journey has provided me with a comprehensive understanding of cybersecurity. Through a combination of policy, technical, and analytical skills, I have developed the ability to approach cybersecurity challenges from multiple perspectives. The artifacts included in my ePortfolio reflect my growth and demonstrate my readiness to transition into a cybersecurity role.

The interdisciplinary approach taken by this program has been especially helpful in allowing me to combine knowledge from diverse sources and apply that knowledge towards resolving real-world scenarios. Upon entering this new career path I intend to build upon these foundations through certifications and hands on experience. Ultimately this program has prepared me not only to begin working in the field of cybersecurity; however also grow in an environment that continues to evolve rapidly.

References

Dissanayake, N., Jayatilaka, A., Zahedi, M., & Babar, M. A. (2021). Software security patch management—A systematic literature review of challenges, approaches, tools and practices. *Information and Software Technology*, *144*(0950-5849), 106771. https://doi.org/10.1016/j.infsof.2021.106771

Knapp, K. J., Maurer, C., & Miloslava Plachkinova. (2017). *Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance*. AIS Electronic Library (AISeL). https://aisel.aisnet.org/jise/vol28/iss2/4/

Marchetti, K., & Bodily, P. (2022, May 1). *John the Ripper: An Examination and Analysis of the Popular Hash Cracking Algorithm*. IEEE Xplore. https://doi.org/10.1109/IETC54973.2022.9796671

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008, September 30). *Technical Guide to Information Security Testing and Assessment*. Csrc.nist.gov. https://csrc.nist.gov/pubs/sp/800/115/final

Suryotrisongko, H., & Musashi, Y. (2019). Review of Cybersecurity Research Topics, Taxonomy and Challenges: Interdisciplinary Perspective. *2019 IEEE 12th Conference on Service-Oriented Computing and Applications (SOCA)*. https://doi.org/10.1109/soca.2019.00031