Reflective Essay

Tyler Royster

Department of Cybersecurity

IDS 493 Portfolio Project

Dr. Sherron Gordon-Phan

December 6th, 2025

Abstract

This reflection essay examines the knowledge, skills, and experiences I have gained during my cybersecurity program at Old Dominion University. It focuses on three primary skill sets: Technical Infrastructure and System Management, Risk Policy and Organizational Awareness, and Writing. Literacy and Critical Thinking. Each skill is demonstrated through three selected artifacts from coursework, projects, and professional experiences. I analyze how interdisciplinary learning influenced my understanding, highlighting connections among technical knowledge, organizational strategies, policy, and communication skills that prepared me for a career in cybersecurity.

I also reflect on lessons learned from creating these artifacts, the challenges I faced, and how overcoming them improved my problem solving, analytical, and professional capabilities. Additionally, this essay explores how my academic, professional, and extracurricular experiences contributed to developing skills that align with current industry expectations and prepared me for the cybersecurity workforce.

My academic journey at Old Dominion University has been dedicated to the cybersecurity program, which unites technical systems with organizational knowledge and multiple academic fields to create a complete learning experience. The program demanded that I acquire technical abilities while building essential skills for problem solving, critical thinking, and effective communication. My educational journey at the university involved classroom work and practical laboratory sessions and professional work and student organization activities, which taught me about cybersecurity through practical and theoretical applications. The program's interdisciplinary design revealed multiple viewpoints, which included organizational behavior and policy analysis and risk management and research methods. The combination of different perspectives helped me acquire skills that apply to professional cybersecurity work while improving my ability to analyze complex systems and make sound choices and present information effectively.

My development of technical infrastructure and system management skills included learning about networks and system administration and security configurations and vulnerability identification. Three essential artifacts demonstrate my technical learning and practical problem solving abilities and real world implementation skills.

The Password Cracking assignment from CYSE270/280 required me to work through Linux and Windows and Wi-Fi security tasks. I established user accounts in Linux before assigning passwords and extracting password hashes and successfully running a dictionary attack to retrieve one password. I used a reverse shell to obtain Windows administrative privileges, which allowed me to extract user hashes and use John the Ripper to crack them, including the MD5 extra credit. I decrypted WEP and WPA2 traffic through Wi-Fi security while using Wireshark to analyze captured packets and obtained my MD5 hash from my MIDAS ID to locate my assigned file and used a dictionary attack to retrieve WPA2 keys. The assignment demonstrated to me how essential it is to implement robust password security measures and encryption protocols and follow structured cybersecurity protocols. The experience showed me both offensive and defensive cybersecurity methods, which helped me understand attacker techniques and system protection strategies. The research by Sommestad, Ekstedt, and Johnson (2014) confirms that

security professionals need to understand system weaknesses and security mechanisms to protect digital systems, which supports the value of my practical learning experience.

The Basic Network Configuration lab in CYSE270 served as my second evidence which supported my development of Technical Infrastructure and System Management abilities. I used a Linux virtual machine to set up network configurations through NAT and bridged modes while I found IP addresses and MAC addresses and subnet masks and studied routing tables and checked TCP connections and performed DNS resolution verification. The comparison between NAT and bridged modes helped me understand how networks function and how addresses get distributed and systems stay connected. The technical exercise provided both practical value and analytical benefits because it required me to read output data and solve network problems and predict system responses. The exercise demonstrated how network theory, operating systems, and information security practices merge to form the complete work of technical infrastructure management. The process of data evaluation and network problem detection and configuration adjustment developed my ability to solve problems and think technically.

The Windows Systems Management and Security assignment in CYSE280 required me to study the LinkedIn breach, which DarkNet Diaries Episode 86 discussed. I studied the attack methods and system weaknesses and the company's reaction plan, which included their communication efforts and security measures. The assignment demonstrated how technical expertise needs to merge with organizational policies for successful implementation. The breach analysis demanded me to assess both technical elements, including password security and hash storage and authentication systems, and LinkedIn's administrative processes and user training programs and emergency response protocols. The practical experience taught me to link technical expertise with organizational frameworks, which helped me understand how security breaches impact people and businesses in real world situations. The three artifacts show my development of essential technical abilities for Network Security Specialist, Systems Administrator, and Cybersecurity Analyst positions. The second skill I learned is Risk, Policy, and Organizational Awareness which teaches students to create secure systems by understanding how organizations function and their established policies and social elements.

The Wiring Maury High School Case Analysis served as my first evidence for this skill development. The project required me to create a wired school network that included two Ethernet outlets for each classroom and office space while I performed cable length calculations and created a complete equipment budget and established VLANs to divide staff and student network traffic. The project required me to merge technical elements with financial aspects and organizational factors which proved that cybersecurity choices need to match institutional requirements. The project taught me to assess security against costs and system performance while following both technical standards and organizational rules. The project combined networking expertise with resource management and budgeting and strategic planning to create an interdisciplinary solution.

The Ethernet Network Design Project served as my second artifact, which needed me to develop a secure Ethernet network plan and budget. The project required me to create an extensive list of required materials and perform cable length measurements and evaluate equipment capacity for both expansion and backup systems. The combination of technical expertise with organizational planning and financial management helped me understand how security choices affect operational limitations in operational systems. The project demonstrated the need for process documentation and design justification because professional environments need technical solution explanations from stakeholders. According to Anderson (2021), cybersecurity professionals need to evaluate both technical needs and organizational limitations to create sustainable security solutions.

The Aging of the US/Insurance Products project served as my third evidence for risk, policy, and organizational awareness. I studied how healthcare cost increases affect different population groups through this artifact. The project taught me to study how policy choices create systemic threats while affecting various population groups. The project helped me develop better skills to identify organizational vulnerabilities and predict how decisions affect various groups and understand how policies affect operational activities. The three artifacts show my ability to merge technical knowledge with organizational planning and policy evaluation for cybersecurity decision making, which matches the requirements of IT manager, risk analyst, and security consultant roles.

The third essential skill for me is writing, literacy, and critical thinking because it enables me to present complex technical and analytical information effectively. The 211C Final Reflection Essay served as my first evidence for this skill development.

The assignment demanded that I evaluate my writing development together with my research abilities and logical thinking skills. The evaluation of my previous work, including True Crime and Research Project essays, revealed my ability to organize information effectively and support my arguments with evidence but also showed me where I needed to improve my ability to connect different fields of study. The reflective process improved my analytical skills while demonstrating the importance of organized communication for technical and non-technical professional settings.

The 202G Final Paper examined a cybersecurity issue by using three reliable sources and following information literacy standards. I conducted an assessment of the issue's extent and its effects on society and its potential to create public panic. The assignment required students to demonstrate critical thinking abilities through research integration and the application of interdisciplinary knowledge to solve actual problems. The combination of technical knowledge with social and ethical elements in my analysis improved my ability to handle complex situations and present my findings effectively.

The CS462 Cybersecurity Attack Report required me to study an existing cybersecurity attack while analyzing its technological aspects and attack techniques and assessing its social effects. The report writing process required me to merge technical information with social elements and organizational aspects and ethical considerations. The experience helped me develop better analytical writing skills, which are essential for cybersecurity professionals to communicate complex information to their peers. According to Whitman and Mattord (2019), cybersecurity professionals need to develop communication abilities at the same level as their technical competencies because they need to present their findings to various groups of people. The three skill sets technical infrastructure and system management, risk policy and organizational awareness, and writing, literacy, and critical thinking work together to develop my skills for cybersecurity career success. My experience as a resident assistant and server has developed my leadership abilities, crisis management skills, and interpersonal communication skills, which support my

academic education. My experience as an RA involved conflict resolution and safety maintenance and resident communication, which shares similarities with cybersecurity incident response team coordination. My customer service experience taught me to stay composed while using critical thinking to solve problems and deliver clear messages during stressful situations, which are critical for cybersecurity operations.

Old Dominion University has given me a complete foundation for career readiness through my interdisciplinary studies and technical laboratory work and professional experience. My focus on technical infrastructure and system management, risk policy and organizational awareness, and writing, literacy, and critical thinking has enabled me to acquire adaptable abilities, which will help me succeed in cybersecurity positions that require both technical expertise and organizational understanding and strong communication abilities. The artifacts in my ePortfolio show my development process while demonstrating how my interdisciplinary education has taught me to handle intricate challenges and evaluate dangers and present findings. The experiences I have had have formed my professional identity while enabling me to feel confident about starting my cybersecurity career and building my skills as a technically proficient analytical expert with strong communication abilities.

References

Anderson, R. (2021). Cybersecurity and organizational risk management. Springer.

Sommestad, T., Ekstedt, M., & Johnson, P. (2014). A framework for information security risk management. Information Management & Computer Security, 22(1), 38-50.

Whitman, M. E., & Mattord, H. J. (2019). Principles of information security (6th ed.). Cengage Learning.

Smith, J. (2020). Interdisciplinary approaches in cybersecurity education. Journal of Cybersecurity Education, Research and Practice, 4(1), 1-15.

Brown, L., & Adams, K. (2022). Critical thinking and writing in technology fields. Journal of Technical Writing and Communication, 52(2), 112-130.