A Reflective Analysis on My Cybersecurity Competence and Interdisciplinary Growth

Donte Staves

School of Interdisciplinary Studies, Old Dominion University

IDS 493: Electronic Portfolio Project

Dr. Sherron Gordon-Phan

December 9, 2025

Abstract

This reflective essay examines the development of technical and problem-solving skills, communication skills, and critical thinking skills throughout my time in the cybersecurity program at Old Dominion University. Through nine artifacts which include lab report assignments, policy papers, a case study presentation, and a job-ad analyses, I demonstrate how interdisciplinary methods enhanced my ability to approach complex cybersecurity problems. Technical assignments like network traffic analysis, password cracking, and firewall evaluation, strengthened my hands-on problem-solving capabilities. Policy papers and job-ad analyses strengthened my communication skills, while research papers and case studies developed my critical thinking in ethical and policy-related contexts. By integrating scholarly research, professional job expectations, and interdisciplinary theories, this essay highlights the connection between academic experiences and career readiness in cybersecurity. Ultimately, this reflection illustrates how combining technical knowledge, ethical reasoning, and effective communication prepares me for a professional career in the cybersecurity field.

Introduction

Throughout my time in the cybersecurity program at Old Dominion University, I have developed a range of skills that combine technical knowledge, ethical awareness, policy understanding, and critical thinking. The program puts an emphasis on interdisciplinary learning which requires students to integrate concepts from multiple fields to address complex cybersecurity challenges. For my e-portfolio, I have chosen to focus on three skills, and they are technical and problem-solving skills, communication skills, and critical thinking skills. Each skill is demonstrated through three artifacts, including lab report assignments, policy papers, research projects, and job-ad analyses. These artifacts highlight my growth and illustrate how the integration of interdisciplinary methods has enhanced my understanding of cybersecurity. This reflective essay examines how my coursework and professional experiences developed these skills and prepared me for future career opportunities in the field.

Technical and Problem-Solving Skills

Through my coursework in CYSE 301: Cybersecurity Techniques and Operations, I gained essential technical and problem-solving skills that directly support my development as a future cybersecurity professional. This course required me to work extensively in virtual environments to analyze networks, identify vulnerabilities, and develop strategies to protect systems from potential threats. Assignments like network traffic tracing and sniffing challenged me to use diagnostic tools like Wireshark to monitor flows and identify anomalies in real time, which taught me to interpret complex datasets and make informed security decisions (Saxena & Sharma, 2017). Another assignment, the Sword vs. Shield analysis, allowed me to examine

offensive and defensive cybersecurity techniques, giving me a hands-on understanding of the strategic balance between attackers and defenders in a networked environment. Additionally, the password cracking assignment pushed me to think critically about password policies, encryption strength, and user behavior, which strengthened my understanding of authentication vulnerabilities and mitigation strategies (Ji et al., 2015).

Each of these assignments required a systematic approach to problem-solving, as I had to analyze the scenario, select appropriate tools, execute tests in a controlled environment, and produce comprehensive reports that articulated my methodology and conclusions. These experiences not only improved my technical proficiency but also enhanced my ability to troubleshoot and adapt to new challenges quickly, a skill that is vital for any cybersecurity professional. Furthermore, these assignments emphasized the importance of attention to detail. As small errors in analysis or configuration could lead to critical gaps in security, highlighting how precise problem-solving and methodical thinking are integral to the field. Collectively, these hands-on experiences helped shape my confidence and capability in handling real-world cybersecurity challenges.

Communication Skills

Communication is a critical skill in cybersecurity, as technical knowledge must often be translated for a non-technical audience, stakeholders, or collaborative teams. I strengthened this skill through coursework that involved writing policy papers and conducting job analyses, where I had to present complex technical concepts in a structured, professional format. For example, my policy paper on the Political Implications of Cybersecurity Incident Response Policy required me to examine how political considerations affect cybersecurity strategies and clearly communicate findings and recommendations to a professional audience. Similarly, the Network

Security Policy: Foundation of Cybersecurity Strategy paper asked me to analyze organizational approaches to protecting data and networks while presenting my analysis in an accessible, logical, and evidence-based manner. Completing a job-ad analysis for a cybersecurity analyst position at Bridge Core further allowed me to translate industry expectations into actionable insights which taught me how to interpret and summarize real-world requirements in a clear and organized way (Graham & Lu, 2023). These assignments developed my ability to construct persuasive arguments, structure my writing logically, and cite evidence from multiple sources while following certain formats like APA. Beyond written communication, the assignments reinforced the value of clarity and precision conveying technical and strategic information, skills that are crucial when collaborating with colleagues, presenting to leadership, and consulting with clients. Through repeated practice, I learned to balance technical detail with readability, ensuring that my work can be understood and acted upon diverse audiences while maintaining technical precision. This skill was developed systematically through coursework and is essential for career readiness and professional effectiveness in the cybersecurity field.

Critical Thinking Skills

Critical thinking is fundamental to understanding and addressing the complex challenges present in cybersecurity. I honed this skill through assignments that required analysis from multiple disciplinary perspectives which include technology, ethics, law, and policy. My interdisciplinary research paper required me to answer a problem using multiple disciplines and synthesizing information from various academic sources, challenging me to create my own research question, find a solution to the question using multiple disciplines, evaluate sources to integrate into my paper, and draw a well-reasoned conclusion. In the cybercrime case study, I analyzed a ransomware group named Blackcat, where I examined the affidavit of the group, the

key participants, how the crime was investigated, and the outcome of the court proceedings. Finally, my policy research paper on the ethical implications of data security policies prompted me to consider privacy, regulatory compliance, and the moral responsibilities of organizing and managing sensitive information (Shwartz, 2011; Bashir & Khalique, 2016).

These assignments taught me to question assumptions, weigh competing priorities, and approach problems systematically. I also learned to integrate theoretical knowledge with practical applications while using reasoning and logic to propose solutions that are both effective and ethically responsible. The ability to think critically enables me to anticipate potential risks, evaluate the consequences of security decisions, and develop strategies that balance technical requirements with ethical and legal considerations. Furthermore, by reflecting on these assignments, I recognize how knowledge from multiple domains like law, ethics, computer science, and organizational policy interacts to shape informed decision-making in cybersecurity (Nikitina, 2006). This skill is essential for addressing the complex and dynamic challenges that cybersecurity professionals face today.

Interdisciplinary Learning and Degree Outcomes

An interdisciplinary approach has been central to my development as a cybersecurity professional. Courses like IDS 300W emphasized strategies contextualizing, conceptualizing, and problem-centered learning, which provided a framework for integrating knowledge across multiple disciplines (Nikitina, 2006). By combining technical labs, policy analysis, and ethical research, I learned to address cybersecurity challenges from various perspectives, considering technical feasibility, ethical responsibility, and policy implications simultaneously. Artifacts like firewall evaluation reports, password cracking analyses, and policy papers illustrate the application of interdisciplinary knowledge in practical contexts (Saxena & Sharma, 2017; Ji et

al., 2015; Khari, Gaur, and Tuteja, 2013). This integration of disciplines has enhanced my ability to approach problems systematically and creatively and bridging the gap between academic learning and professional practice.

Additionally, interdisciplinary learning has been instrumental in developing my professional identity. Engaging with ethical frameworks, industry research, and technical labs allowed me to reflect broader implications of cybersecurity work. For example, analyzing ethical considerations in data security policies (Shwartz, 2011; Bashir & Khalique, 2016) informed my understanding of responsible cybersecurity practices, emphasizing that technical competence alone is insufficient for professional success. By combining these insights, I am better equipped to navigate complex challenges and communicate solutions effectively within a professional environment. Overall, my degree outcomes demonstrate that interdisciplinary methods are not just valuable academically but are also critical for career readiness and professional growth.

Conclusion

Reflecting on my academic journey, it is clear that the combination of technical and problem-solving skills, communication skills, and critical thinking skills has shaped both my identity as a cybersecurity student and my readiness to enter the professional field. Each artifact in my portfolio demonstrates not only the knowledge I acquired but also the interdisciplinary approach that guided my learning throughout the program. By integrating technical assignments, policy papers, and analytical projects, I developed a well-rounded understanding of cybersecurity that extends beyond computers and networks. Instead, my experiences highlight cybersecurity as a discipline that also relies on ethics, communication, law, psychology, and strategic planning. This broader perspective has allowed me to approach cybersecurity challenges with depth and adaptability which are qualities that employers seek in today's evolving digital landscape.

The interdisciplinary methods emphasized in my program were crucial to how I interpreted and completed my assignments. Courses like IDS 300W taught me to analyze issues through multiple lenses and integrate theories from different disciplines into my work. This approach became particularly important when completing policy-related assignments or evaluating ethical considerations, where I had to balance technical accuracy with social responsibility and organizational limitations. Additionally, working with virtual lab environments in CYSE 301 helped me translate conceptual knowledge into practical application, reinforcing the importance of understanding both theory and practice. The merging of these perspectives strengthened my ability to learn independently, adapt to new challenges, and make informed, balanced decisions.

As I prepare to transition from academics into my cybersecurity career, the skills I developed through my coursework and artifacts provide a strong foundation for professional growth. Interdisciplinary thinking will continue to guide how I analyze problems, communicate with colleagues or stakeholders, and evaluate the broader impact of cybersecurity decisions. This mindset is essential in a field where technical solutions must be aligned with ethical standards, legal requirements, and organizational goals. By completing this ePortfolio, I demonstrated my competencies and gained a deeper understanding of how each experience shaped my development. Ultimately, this reflection confirms my education has prepared me to contribute meaningfully to the cybersecurity field and continue growing as a learner and a professional.

References

Bashir, B., & Khalique, A. (2016). A review on security versus ethics. *International Journal of Computer Applications*, *151*(11), 13-17.

Graham, C. M., & Lu, Y. (2023). Skills expectations in cybersecurity: semantic network analysis of job advertisements. *Journal of Computer Information Systems*, *63*(4), 937-949.

Ji, S., Yang, S., Hu, X., Han, W., Li, Z., & Beyah, R. (2015). Zero-sum password cracking game: A large-scale empirical study on the crackability, correlation, and security of passwords. *IEEE transactions on dependable and secure computing*, *14*(5), 550-564.

Khari, M., Gaur, M., & Tuteja, Y. (2013). Meticulous study of firewall using security detection tools. *International Journal of Computer Applications & Information Technology*, *2*(I), 2278-7720.

Nikitina, S. (2006). Three strategies for interdisciplinary teaching: contextualizing, conceptualizing, and problem-centring. *Journal of curriculum studies*, *38*(3), 251-271.

Saber, V. A. (2025). Exploring the Correlation Between Vulnerability Scanning and Nmap. *International Journal of Intelligent Computing and Information Sciences*, *25*(1), 41-50.

Saxena, P., & Sharma, S. K. (2017). Analysis of network traffic by using packet sniffing tool: Wireshark. *International Journal of Advance Research, Ideas and Innovations in Technology*, *3*(6), 804-808.

Schwartz, P. M. (2011). Privacy, ethics, and analytics. *IEEE security & privacy*, *9*(3), 66-69.