Reflections on Developing Core Cybersecurity Skills

Neriah Alcantara

Old Dominion University

IDS493: Electronic Portfolio Project

Professor Prihoda

4/27/2025

Introduction

My academic journey has been transformative, significantly shaping my understanding and approach to various disciplines. During my cybersecurity coursework, I cultivated a multifaceted perspective, integrated technical knowledge, and applied attention to detail in personal and academic contexts. Specifically, I have developed skills in detailed analytical thinking, technical cybersecurity operations, and comprehensive risk assessment.

Key artifacts such as interdisciplinary research presentations, ethical hacking exercises, and a comprehensive cyber risk assessment project demonstrate these competencies. Reflecting on these experiences has highlighted the importance of adaptability, interdisciplinary thinking, and rigorous technical practice in Cybersecurity. Through these developments, I have strengthened my academic foundation and prepared myself for future professional challenges, where continuous learning and flexible problem-solving are essential.

Building Detail-Oriented Thinking through Interdisciplinary Research

With my first skill on the list, detail orientation is indispensable across many fields, especially Cybersecurity, where meticulous attention is needed to identify vulnerabilities and anomalies. The first course that helped me broaden my horizons would be Interdisciplinary Theory and Concepts, also identified as IDS 300W. This class helped me develop a more holistic definition of Cybersecurity as an interdisciplinary activity, consciously stepping back from the predominant technical view by integrating multiple perspectives from adjacent fields or fields that encompass my perspective of Cybersecurity.

This course introduced me to approaching it from a multi-dimensional perspective. An extra artifact to back this claim would be the PowerPoint presentation on the Interdisciplinary Research Process I had created for one of my assignments during class. Making this PowerPoint of Repko and Szostak's book helps me break down the process into simpler components, such as selecting a topic, identifying relevant disciplines, researching, and providing insights. Making it easier to remember with the addition of hand drawing the diagram and illustrations to make the assignment uniquely personalized (Repko, A. F., & Szostak, 2023).

However, the second yet major assignment that impacted me was my final essay, *Biometrics or Machine as The Shield*, taking everything I've learned during my past semester into a final essay on a topic the professor approved. My essay explored authentication and authorization with the growing need for secure protocols and measures through the IoT (Internet of Things). The process was challenging, requiring a deep dive into any three adjacent fields that intersected my chosen topic. However, looking back on this assignment, this essay was the first time I could dive deeper into my major. Despite uncertainty about choosing the right adjacent fields, the assignment ultimately boosted my confidence in tackling complex cybersecurity topics without feeling overwhelmed by their multidisciplinary nature.

The essay was an interdisciplinary activity before I had any experience with other cybersecurity-related courses. This start helps me think systemically whilst broadening my

horizons and approaching future assignments and challenges with an open mind. While connecting detail orientation with interdisciplinary studies doesn't seem intuitive, the thorough exploration of diverse academic fields and the problem breakdown helped me become more aware of the finer details in different areas.

Developing Technical Proficiency with Linux and Metasploit

The second skill I wanted to highlight would be understanding Linux-based systems and Metasploit. The class on Cybersecurity Techniques and Operations, CYSE301, provided the opportunity to delve into the intricacies of using Linux as a pen-testing environment without information being convoluted. Assignments for this class were in-depth as they immediately asked for the knowledge that the professor had taught us and applied what we learned to practical exercises.

An artifact to back this up would be my fourth assignment, which is about ethical hacking through Metasploit with Kali Linux on a virtual box. It involved using Metasploit for penetration testing and vulnerability exploitation, which enhanced my comprehension of cybersecurity operations. *Assignment Four: Ethical Hacking* required me to do basic reconnaissance of a target system using tools like Nmap to identify open ports and running services, followed by using well-known CVE vulnerabilities to find exploits that could be used to gain access to a machine. During this week, Professor Peng Jiang walked us through the assignment process. At first, navigating Metasploit felt overwhelming due to the vast array of commands and options. However, the professor's clear explanations helped demystify the tool for me. I feel more confident experimenting with new security tools independently, which will be critical in my future career as technology evolves (P. Jiang, personal communication, March 23, 2023).

While the creation of the artifact was not tricky, courtesy of the professor, the assignment was only possible because of his hands-on guidance and instruction, which cleared my doubts and allowed me to grasp the nuances of Metasploit and Kali Linux. Due to the relatively light nature of the course, I became more eager to tackle extra credit assignments to challenge myself, exploring other security topics such as *SQL Injection* due to my interest at the time. The practical knowledge gained from CYSE 301 has equipped me with essential tools for various cybersecurity roles and helped me build up more nuanced courses such as MSIM 470 and Foundations of Cyber Security whilst maintaining rigorous attention to detail throughout future assignments.

Strengthening Core Cybersecurity Foundations through Practical Application

The last skill I want to highlight is an in-depth understanding of cybersecurity concepts. I brought attention to this coursework as the curriculum introduced me to multiple topics within my cybersecurity major. My experience with this class may be one of the most challenging subjects in my semester due to the number of topics and trying to comprehend Cybersecurity as a whole. However, it is the most impactful due to the understanding I gained.

The Foundations of Cybersecurity course delved deeper than CYSE301 introduced; it expounds more on different types of attacks and security-related topics with heavy reliance on Dieter's *Computer Security* textbook (Gollmann, 2011, p. 17). One of the major assignments during this class was the *Cyber Risk Assessment Project*. This project required me with a team to conduct a comprehensive cyber risk assessment for the VM pool on Move, using Metasploit on multiple systems to conduct exploits. This project required a team to discover security holes and vulnerabilities within the target environment and gather all the necessary information into comprehensive documentation for the semester.

Initially, I felt apprehensive about the reliance on teamwork due to my assumed inadequacies of putting my knowledge onto the report, fearing that what I research will not be enough compared to the rest of my teammate's expertise and skill. However, teamwork was essential in completing the assessment, similar to real-world situations where it is rare for an individual to work alone, especially in professional cases such as cybersecurity. Considering the project's breadth and depth, collaborative teamwork was beneficial and an indispensable learning experience compared to the solo work assignments I used to do. And soon enough, I felt more comfortable after completing this artifact.

During the project's culmination, this project stood out as the creation of the deliverable was difficult before and during its process due to the need for meticulous analysis, which is required for the report. This project emphasized the importance of continuous learning and adaptation in my chosen field by synthesizing theoretical concepts and practical applications.

Conclusion: Integrating Academic Learning with Future Practice

The reflection on my skills and experiences highlighted the evolution of my growth throughout each class. It has allowed me to bridge the gap between my academic journey and lay a path towards my professional aspirations. Each explanation of how my skills came to be through my artifacts has helped me reinforce my understanding of theoretical knowledge and practical applications with the interdisciplinary nature of Cybersecurity. Despite its disjointed nature, looking back at how each applied knowledge reinforces all my aforementioned assignments in a way that creates a narrative that weaves all these skills and learning experiences into a tapestry of continuous growth and adaptability. (McAdams, 2001, p. 100; Nguyen, 2013, p. 135).

Moving forward, I intend to integrate the lessons from my coursework and experiences into my future endeavors, approaching challenges with a comprehensive and adaptable mindset. In particular, I plan to continue strengthening my interdisciplinary research abilities and hands-on technical skills, ensuring I can effectively bridge theoretical knowledge with evolving industry practices.

Citations

Gollmann, D. (2011). Computer Security (3rd ed.). Wiley. Retrieved from https://www.perlego.com/book/3865766/computer-security-pdf (Original work published 2011)

McAdams, D. P. (2001). The Psychology of Life Stories. Review of General Psychology, 5(2), 100–122. https://doi.org/10.1037/1089-2680.5.2.100

Nguyen, C. F. (2013). The ePortfolio as a Living Portal: A Medium for Student Learning, Identity, and Assessment. *International Journal of ePortfolio*, *3*(2), 135-.

Repko, A. F., & Szostak, R. (2020). Interdisciplinary research: Process and theory (4th ed.). SAGE Publications