Reflective Essay

Anthony Gomez-Reyes

Old Dominion University

IDS 493

Dr. Phan

Introduction

As I look back on my academic journey, I can clearly see how each class, assignment, and project helped shape the skills and confidence I now have as a developing cybersecurity professional. When I first entered this program, I knew I was interested in technology, but I did not fully understand how many different fields contribute to cybersecurity. Through writing assignments, cybercrime research, database work, team leadership, and hands-on security exercises, I learned that cybersecurity requires technical knowledge, strong communication skills, ethical awareness, and the ability to analyze problems from many different angles. Klein (2020) explains that interdisciplinary learning helps students integrate ideas across fields to solve complex issues. This idea represents my experience very well. The artifacts in my portfolio show how different subjects allowed me to build a stronger and more complete understanding of cybersecurity. This reflection essay discusses the skills I developed, the artifacts that demonstrate those skills, and how my academic experiences contributed to my career readiness. The more I worked on these assignments, the more I realized that cybersecurity is not just about technology. It is about people, ethics, communication, and lifelong learning. This reflection helps me better understand the kind of professional I want to become and the direction I want to take in my career.

Interdisciplinary Learning in Cybersecurity

One of the biggest lessons I learned throughout this program is that cybersecurity is naturally interdisciplinary. Every assignment I worked on showed me that you cannot understand cybersecurity by focusing only on computers or technical processes. You also have to understand human behavior, laws, communication, business needs, and even psychology. Kshetri (2023) explains that cybersecurity requires a combination of social science, technology, and policy knowledge. I found this to be true in many of my assignments.

For example, when I completed my research paper on cybertrespass, I learned that unauthorized access to systems is not only a technical issue. It is also a legal and ethical concern. Understanding cybercrime required me to think like someone studying criminal justice. I needed to analyze laws, understand how courts define digital intrusion, and consider the real consequences of violating privacy. This showed me that cybersecurity professionals must think beyond technical actions. They must understand how their decisions impact people, society, and organizations. Another example comes from my work in writing courses. When I wrote essays or reflections, I developed strong communication skills that I now know are essential in cybersecurity. Peltier (2016) states that the ability to clearly explain security issues is a key part of the job, especially when working with non-technical audiences. My writing experiences taught me how to organize my thoughts, explain concepts clearly, and reflect on what I have learned. These skills will help me write incident reports, document findings, and communicate risks in a professional setting. I also learned about databases in a completely different course, and surprisingly, that work helped me develop technical skills that are important in cybersecurity. Understanding how data is stored, organized, and protected allowed me to make connections between data structures and security responsibilities. Connolly and Begg (2021) emphasize that database literacy is a major part of many IT and security roles. Working on this project taught me to create tables, build relationships, and think about how data can be exposed or protected. These examples show how each discipline added new skills to my toolkit. Instead of learning in separate boxes, my classes worked together to help me grow into someone who can think from multiple perspectives.

Skill Development Through Course Artifacts

1. Log Analysis Skills

One of the most practical skills I developed was the ability to analyze logs. I completed a log analysis practice exercise where I had to look at system entries and identify suspicious behavior. At first, reading logs felt confusing, but over time I got better at recognizing patterns such as repeated failed login attempts, unusual access times, and unfamiliar user accounts. Stallings and Brown (2021) explain that logs are one of the most important sources for detecting intrusions. Working through this assignment taught me how much information is hidden in plain sight. This artifact improved my attention to detail. It also taught me how to think like a security analyst. I learned that not every unusual entry is an attack, but every suspicious entry requires attention. I also improved my ability to write clearly because I had to explain my findings in simple language. This exercise made me feel more confident in my technical abilities and helped me imagine what it would be like to work in a real Security Operations Center.

2. Cybercrime and Ethical Awareness

My expanded cybertrespass research paper was one of the most eye-opening assignments I worked on. I went into the project thinking it would be a basic research paper, but it ended up teaching me so much about human behavior, criminal intent, and the importance of ethics. I had to analyze malware, entry techniques, and real cases involving unauthorized access. This required me to think about both the technology and the people behind the crimes. Whitman and Mattord (2021) argue that cybersecurity professionals must be grounded in ethics because they often have access to sensitive information. This assignment made me reflect on what it means to act responsibly in the digital world. Researching this topic also strengthened my academic writing and APA citation skills. It pushed me to look at different perspectives and evaluate the impact of cybercrime on individuals and organizations.

3. Database Development and Technical Proficiency

My database project is an important artifact because it marks the moment when I realized how interconnected cybersecurity and information systems are. I created multiple tables, designed relationships, wrote insert statements, and enforced constraints. The project required accuracy and logic. Even though it was not a cybersecurity class, the technical skills I learned directly relate to protecting data in real environments. Connolly and Begg (2021) explain that databases store the most valuable information in organizations, so understanding how they work is crucial for protecting them. This assignment strengthened my problem solving abilities and helped me understand how data flows through systems. It also taught me that even small errors in structure can lead to major vulnerabilities.

4. Written Communication and Reflection Skills

My writing assignments throughout the program helped me grow in ways that go beyond technical skills. I learned how to express myself clearly, reflect on my learning, and communicate complex ideas in a way that regular audiences can understand. This is incredibly important in cybersecurity. Peltier (2016) notes that being able to communicate risks is just as important as identifying them. Writing reflections and essays helped me better understand my own learning. I discovered patterns in the way I work, the challenges I faced, and the improvements I made along the way. These writing tasks helped me build confidence and gave me the tools to speak professionally about my experiences and goals.

5. Leadership and Team Collaboration

A final artifact that reflects my growth is my team contribution report as a team leader. Leading a team taught me how important communication, clarity, and responsibility are in collaborative environments. Cybersecurity professionals rarely work alone. Morgan (2022) explains that teamwork is essential for incident response and threat monitoring.

As a team leader, I had to keep my group organized, communicate expectations, and make sure everyone was supported. This experience helped me develop patience, organization, and leadership qualities that I will need in my future career. It also taught me how to manage workloads and understand different working styles.

Career Readiness and Professional Growth

When I look at the skills and artifacts in my portfolio, I can see how much they contributed to my career readiness. Each assignment challenged me in a different way, but together, they formed a strong foundation for entering the cybersecurity field. I developed the technical skills to analyze threats, understand data structures, and research attacks. I also developed the analytical skills to interpret information and think critically. Equally important, I improved my communication abilities and leadership skills. Klein (2020) explains that interdisciplinary education prepares students for complex careers by teaching them how to integrate knowledge from different fields. This is exactly what happened for me. Cybersecurity is constantly changing, and my ability to learn from many disciplines will help me stay adaptable in the workforce. My portfolio shows that I can analyze problems, communicate clearly, and make decisions based on ethical reasoning and solid research.

Conclusion

This reflection essay highlights the skills, experiences, and interdisciplinary learning that shaped my growth throughout this program. Each artifact in my portfolio represents a different part of my development as a cybersecurity student. From log analysis to research on cybertrespass to database design and leadership work, I built a wide range of competencies that I will carry into my future career. I learned that cybersecurity is not only about technology. It is about communication, ethics, research, teamwork, and lifelong learning. The assignments I completed pushed me to think from different perspectives and to reflect on my goals as a cybersecurity professional. As I move forward in my career, I feel prepared and confident in my ability to contribute meaningfully to the field. This program helped me discover my strengths and shaped the direction I want to take in my future.

References

Connolly, T., & Begg, C. (2021). *Database systems: A practical approach to design, implementation, and management* (7th ed.). Pearson.

Klein, J. T. (2020). *Interdisciplining digital humanities: Boundary work in an emerging field*. University of Michigan Press.

Kshetri, N. (2023). *Introduction to cybersecurity*. MIT Press.

Morgan, S. (2022). *Cybersecurity workforce study*. Cybersecurity Ventures.

Peltier, T. R. (2016). *Information security policies, procedures, and standards: Guidelines for effective information security management*. Auerbach Publications.

Stallings, W., & Brown, L. (2021). *Computer security: Principles and practice* (5th ed.). Pearson.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security* (7th ed.). Cengage Learning.