Reflective Essay

My Nguyen

Old Dominion University

IDS 493 – Electronic Portfolio Project

Professor Gordon-Phan

August 9, 2025

Abstract

When I began my cybersecurity degree, I imagined the field as purely technical, filled with code, encryption, and firewalls. I quickly learned it was much more than that. Every class, project, and discussion pushed me to think not only like a technician but also like a strategist, a researcher, and an ethical decision maker. Cybersecurity problems rarely have one simple solution. They require a blend of technical expertise, critical thinking, and moral judgment. Through my coursework, three skills emerged as the foundation of my professional growth: Threat Analysis, System Administration, and Ethical Analysis. Each skill is developed through hands-on projects and interdisciplinary learning, drawing from computer science, information technology, law, philosophy, and even environmental studies. In this reflection, I will explore nine artifacts, three for each skill, that demonstrate how my academic experiences shaped my abilities and prepared me for the demands of a cybersecurity career.

Portfolio Creation

When I first started collecting my work for this portfolio, I felt a bit overwhelmed. There were so many assignments and projects from different classes, and I was not sure which ones to include. As I reviewed everything, I noticed which pieces truly represented my skills and development. Narrowing it down to three skills and three projects per skill made me focus on my strengths and what employers in cybersecurity are looking for. Reflecting on each project made me think about the challenges I faced, what I learned from them, and how the different pieces connect. Some assignments were especially difficult, like tracing network traffic or analyzing ransomware incidents, but working through these helped me develop problem-solving skills and stay calm under pressure. I also realized that courses outside of pure technology, such as ethics and research methods, helped me better understand my responsibilities as a future cybersecurity professional. Organizing everything in a way that flows and tells my story was challenging but rewarding because it gave me a clear view of my progress and accomplishments.

Personal Narrative

Looking back on my experience in this program, I remember feeling nervous at first, especially when I was faced with complex projects like traffic tracing or writing scripts. There were times when I doubted whether I had the skills or knowledge to get through certain assignments, especially when technical problems seemed overwhelming. But over time, I learned to approach these challenges differently. Instead of getting stuck, I started breaking down problems into smaller steps, asking for help when I needed it, and drawing from what I'd learned in other classes, even outside of cybersecurity. For example, ethical discussions made me think about how cybersecurity isn't just about technology but about people and society, too. These

moments of growth made me more confident and helped shape the kind of professional I want to become.

Threat Analysis

Threat analysis has been one of the most challenging yet rewarding areas I have explored. The complexity of modern cyber threats means that simple technical know-how isn't enough; I had to develop a mindset that blends technical, strategic, and interdisciplinary thinking.

Artifact 1

When I first began the Traffic Tracing and Sniffing project, I was overwhelmed by the sheer amount of data flowing through networks. It was daunting to filter through and identify suspicious packets. But this challenge pushed me to improve my analytical skills and patience. Using packet capture tools taught me how crucial real-time monitoring is and how it connects theory with practice. It wasn't just about technical proficiency, I had to think like an attacker, understanding potential vulnerabilities from a human perspective. This artifact made me realize that threat analysis is a detective's job, requiring both technical tools and intuition developed through experience.

Artifact 2

Writing the Ransomware Incident Response Report was a turning point in how I view cybersecurity incidents. Instead of focusing solely on the technical fix, I had to consider the organizational impact, legal consequences, and communication with non-technical stakeholders. I learned that responding effectively requires coordination across multiple domains: legal, ethical, and operational. This interdisciplinary approach was new for me but made me appreciate how cybersecurity is as much about people and policies as it is about code. I now feel more

confident in my ability to manage incidents in real-world settings, a skill I see highlighted in many job descriptions for cybersecurity roles.

Artifact 3

The Supply Chain Attack Analysis artifact was eye-opening because it pushed me to look beyond my immediate technical environment. Understanding how vulnerabilities in third-party suppliers can jeopardize entire organizations required me to research supply chain logistics and risk management strategies, fields I had little exposure to before. This interdisciplinary perspective strengthened my ability to think systemically and anticipate threats that are not always visible on the surface. It taught me that cybersecurity professionals need to be vigilant not just internally, but in their wider ecosystem.

System Administration

My system administration skills grew through hands-on projects that combined coding, automation, and emerging technology research. Each artifact in this category challenged me to expand both my technical capabilities and strategic thinking.

Artifact 1

This was my first time using Python to develop a security-focused application. I had to learn how encryption works, implement secure protocols, and ensure the transfer was reliable. The iterative nature of programming pushed me to adopt a growth mindset, and accepting failure as part of learning. More than just coding, this project taught me how to design security solutions from the ground up, blending software development with system security principles. It was a tangible example of how interdisciplinary knowledge: programming, cybersecurity, and systems thinking that comes together in practical work.

Artifact 2

Automating system tasks through shell scripting was both empowering and frustrating. Initially, I struggled with syntax and logic, but as I progressed, I began to appreciate how scripting can save time and reduce errors. This artifact connected the dots between operating system theory and real-world system maintenance, highlighting the importance of precision and efficiency in cybersecurity. The experience helped me internalize that good system administration requires both deep technical knowledge and an ability to think about long-term system health.

Artifact 3

Researching AI's role in cybersecurity expanded my horizon about the future of the field. I was fascinated by how machine learning algorithms can identify patterns and predict attacks, but I also grappled with ethical questions surrounding AI. This interdisciplinary research paper gave me a taste of emerging technologies and the responsibility that comes with them. It encouraged me to think critically about balancing innovation with ethical safeguards, an ongoing challenge in cybersecurity.

Ethical Analysis

Ethics in cybersecurity is often overlooked, but it forms the backbone of trustworthy and responsible practice. My ethical analysis artifacts deepened my understanding of the human and societal dimensions of technology.

Artifact 1

This paper forced me to confront difficult questions about privacy, accountability, and the limits of surveillance. I reflected on situations where ethical lines blur, such as monitoring employees or handling user data, and realized that there are no easy answers. Engaging with

ethical frameworks from philosophy and law helped me develop a thoughtful approach to dilemmas I expect to face in my career. This artifact reminded me that cybersecurity professionals must uphold values that protect society while navigating complex technological challenges.

Artifact 2

The CIA triad is often taught as a technical concept, but my analysis showed me its deeper ethical implications. For example, ensuring confidentiality is not just about encryption; it's about respecting people's rights. Integrity and availability carry similar moral weight. This artifact was a synthesis of technical knowledge and ethical reflection, illustrating the inseparability of these domains in practice. It also reinforced why ethical thinking should be integrated into every stage of cybersecurity work.

Artifact 3

This artifact was unexpected but highly enriching. Exploring how remote work affects cybersecurity, environmental sustainability, and urban planning required me to step outside traditional cybersecurity boundaries. I examined sociological and environmental research, understanding how technological shifts influence broader societal systems. This broadened my perspective and showed me that cybersecurity's impact extends far beyond technology, it's a social and environmental issue as well. Being able to consider these wider contexts will make me a more responsible and effective professional.

Finishing the Portfolio

Completing this portfolio was the moment everything came together. I wanted it to look professional but still show my personality and how I work. Including my reflection essay directly in the portfolio was important because it connects all the projects and shows how they are part of

my learning journey. Adding my updated resume was the final step, showing that I am prepared to move forward into the job market. Designing the portfolio made me think carefully about how I want to present myself to future employers. I aimed for a clean and organized look that is easy to navigate. This process gave me a chance to appreciate how far I have come and made me more confident about my career path. Looking at this portfolio, I can see my growth from a beginner to someone ready to take on real-world cybersecurity challenges.

Conclusion

Reflecting on my entire program, I realize it taught me much more than technical skills. It challenged me to think critically, consider ethical questions, and understand how different disciplines connect within cybersecurity. The interdisciplinary approach made learning more engaging and gave me tools to solve problems from various perspectives. Courses like IDS 300W strengthened my research and writing skills, which made other courses easier and more meaningful. I now understand that being able to think across fields is a major advantage in a fast changing industry like cybersecurity. This portfolio is more than just a collection of my work. It is proof of my growth and a clear sign of where I am headed next. I have learned that cybersecurity is not just about fighting hackers or programming; it is about understanding people, systems, and ethics all at once. I feel prepared to face new challenges because my skills go beyond technology. I am excited to continue learning and growing in a field that is vital to today’s world.