

Reflective Essay

Tyquan Burchette

Interdisciplinary Studies Department, Old Dominion University

IDS 493: Electronic Portfolio Project

Professor Dr. Mary Ann Kozlowski

May 6th 2026

I've been able to acquire professional, analytical, and technological skills at Old Dominion University that have equipped me for a job in cybersecurity. I have taken courses in cybersecurity, criminal justice, philosophy, information technology, communications, and interdisciplinary studies. I am majoring in cybersecurity with a minor in information systems and technology. My capacity to think critically, solve technical issues, communicate clearly, and apply interdisciplinary approaches to actual cybersecurity situations has all improved because of these classes. Network systems and operations, pattern identification, and communication are the three main professional abilities I have earned during my degree program that determine my academic and job preparation. These abilities weren't acquired separately. Instead, they came about because of a combination of professional work experiences, internships, interdisciplinary theory, technical training, and collaborative learning environments. Through carefully chosen artifacts that showcase my professional and academic advancement, my ePortfolio displays these competencies. According to the National Initiative for Cybersecurity Education [NICE], 2020, cybersecurity professionals are required to have both technological proficiency and an awareness of human behavior, organizational structures, ethics, and communication. I have gained both technical proficiency and multidisciplinary knowledge from my education in classes like CYSE 301, CYSE 406,

PHIL 355E, IDS 300W, IT 315, and IT 325. This reflection explains how my academic experiences have equipped me for a profession in cybersecurity, analyzes my artifacts, and assesses my learning process.

Skill 1: Network Systems and Operations

Artifact 1: Password Cracking Using Wireshark

My password cracking homework from CYSE 301: Cyber Techniques and Operations was one of the most worthwhile technical tasks I finished. For this project, I made several user accounts with different password complexity, recorded authentication traffic, then cracked password hashes using John the Ripper and the Rock You wordlist. I also decrypted WEP and WPA2 wireless connections and examined network packets using Meterpreter and Wireshark. I now have a much better understanding of network security and authentication vulnerabilities thanks to this project. It was difficult at first to comprehend packet captures and password hash techniques. However, I was able to make the connection between basic understanding and sophisticated cybersecurity strategies by going over earlier networking principles from IT 201 and operating system concepts from CYSE 270 and CYSE 280. Patience, testing, and troubleshooting were necessary during the procedure. I had to decipher encrypted communications, recognize authentication handshakes, and closely examine packet captures. The significance of perseverance and critical thinking in cybersecurity work was reaffirmed by this study. Strong authentication procedures and password management are still crucial elements of corporate cybersecurity, according to the National Institute of Standards and Technology (2024). This expertise is closely related to my career ambitions because job ads for penetration

testers, security analysts, and incident responders often call for familiarity with packet analysis, vulnerability assessment, and password auditing.

Artifact 2: Monitoring and Sniffing Network Traffic

Using Wireshark to track real-time network traffic and mimic attacker behavior in a controlled setting was another noteworthy artifact. Identifying packet inquiries, tracking source and destination IP addresses, and intercepting login credentials were my goals. Through this project, I learned how security experts identify unusual traffic patterns and how attackers take advantage of unencrypted protocols. I was able to comprehend the wider effects of network vulnerabilities on businesses and society thanks to my study in CYSE 200, Cybersecurity Technology and Society. Because network captures can contain thousands of packets, packet analysis presented me with several difficulties. I used the filtering strategies and pattern recognition abilities I had learned in previous courses to resolve this problem. I learned how to prioritize pertinent information, spot abnormalities, and extract useful intelligence from this job. Packet analysis is still one of the most important abilities for network defenders and incident response specialists, according to SANS Institute (2023). This artifact shows that I am prepared to work in threat monitoring and security operations centers.

Artifact 3: Ethical Hacking

I had to find vulnerabilities, conduct penetration tests, and record remediation techniques in a lab setting for my ethical hacking assignment. I scanned systems, found flaws, and suggested fixes using industry techniques. PHIL 355E: Cybersecurity Ethics and CYSE 406: Cyber Law provided the foundation for this project. I learned from these

classes that cybersecurity professionals need to strike a balance between their technological skills and their ethical and legal obligations. Creativity, perseverance, and strategic thinking are necessary for penetration testing. I gained knowledge on how to approach systems from the viewpoint of an attacker while upholding moral standards. As businesses deal with more complex cyberthreats, there is a growing need for ethical hackers (International Information System Security Certification Consortium, 2024). This artifact shows my professional awareness and technical proficiency.

Skill 2: Pattern Recognition

Artifact 1: Job Advertisement Analysis

I examined several cybersecurity job postings as part of IDS 493 to find common credentials, certifications, and skill requirements. I was able to identify trends in the cybersecurity employment market thanks to this assignment. I discovered recurrent prerequisites including proficiency with Linux, scripting, network security, risk management, and effective communication. Certifications like CEH, CISSP, and Security+ were also widely used. The interdisciplinary research techniques covered in IDS 300W were directly related to this project. I gained knowledge about themes, information synthesis, and data evaluation from various sources in that course. I was able to gain a better understanding of company expectations by applying those same techniques to job postings. Information security analyst jobs are expected to increase dramatically during the next ten years, according to the U.S. Bureau of Labor Statistics (2025). I was able to match market demand with my academic preparation because to this artifact.

Artifact 2: Vulnerability Scanning Report

I used programs like Nmap and OWASP ZAP to do vulnerability checks during my internship in web development at Old Dominion University. My ability to spot trends in security flaws, such as unsecured ports, shoddy setups, and exposed services, has improved because of this experience. At first, the amount of technical information in scan results was too much to handle. I used systems analysis concepts from IT 363 and analytical frameworks from CYSE courses to get around this obstacle. In cybersecurity, pattern recognition is essential since attackers frequently take advantage of recurrent vulnerabilities. I improved my ability to prioritize risks and suggest solutions by learning to recognize these patterns. Vulnerability management is one of the fundamental skills of contemporary cybersecurity experts, according to the Open Worldwide Application Security Project (2024).

Artifact 3: Writing Scripts and Commands

I had to use Bash scripts and command-line tools to automate system functions for my Linux scripting project in CYSE 270. Scripting was challenging at first since scripts frequently failed due to syntactic issues. However, I was able to approach scripting logically thanks to my programming knowledge from IT 205. I gained knowledge about automating procedures and methodically debugging scripts. The use of pattern recognition to command-line contexts was illustrated in this assignment. I gained the ability to recognize and effectively automate repetitive administrative duties. Cybersecurity operations are becoming more dependent on automation (Scarfone & Mell, 2023). This item is directly related to my career aspirations because many job

advertisements for system administrators and security analysts require scripting knowledge.

Skill 3: Communication

Artifact 1: Customer Service Experience

My communication abilities were greatly enhanced while I worked in Walmart's electronics department. I frequently gave consumers technical product explanations, addressed their inquiries, and made suggestions depending on their requirements. I learned how to translate technical knowledge into a language that non-technical people can comprehend from this experience. Professionals in cybersecurity need to communicate with management, staff, and clients about technical threats. My confidence in professional communication was greatly enhanced by my COMM 101: Public Speaking class. One of the most important soft skills for technology workers is still communication, according to Katz (2022).

Artifact 2: Desk Reception at Old Dominion University

I manage policy enforcement, emergency situations, and conflict resolution in my role as a desk receptionist at Old Dominion University. I've learned how to speak effectively, remain composed under pressure, and make snap decisions thanks to this work. These abilities are directly relevant to cybersecurity incident response, where experts need to take prompt action in the event of a security breach. My understanding of human behavior and dispute resolution was enhanced by my criminal justice education, especially CRJS 215, which increased my efficacy in this position.

Artifact 3: Esports Code Switch

My involvement in competitive esports events via Code Switch improved my ability to collaborate with others and communicate in stressful online settings. Real-time cooperation, strategic preparation, and flexibility are necessary for competitive gaming. Members of the team must be able to communicate effectively, spot trends, and act quickly. These encounters are like cybersecurity operations centers, where groups work together under pressure to identify and address threats. According to research by Dede (2021), collaborative digital environments can greatly enhance communication and problem-solving abilities.

When I reflect on my academic career, I see how both technical training and interdisciplinary learning have influenced my growth as a cybersecurity expert. My education in cybersecurity, information technology, philosophy, criminal justice, communications, and interdisciplinary studies has given me a broad viewpoint that improves my capacity to tackle challenging issues. I learned how to combine theories, assess evidence, and approach problems from several angles in classes like IDS 300W, which made them very beneficial. These interdisciplinary approaches helped me combine technical knowledge with ethical, legal, organizational, and human concerns while preparing me for advanced cybersecurity education. My chosen skills, communication, pattern recognition, and network systems and operations form the cornerstone of my professional identity. I showed my technical expertise, analytical thinking, and professional communication through my artifacts. These skills set me up for success in positions like security analyst, penetration tester, digital forensic investigator, or cybersecurity consultant and closely match the requirements stated in cybersecurity job postings. Understanding technology, people, organizations, and society is just as

important to cybersecurity as safeguarding systems. I can handle security concerns with adaptability, inventiveness, and ethical responsibility since I am an interdisciplinary thinker. I am certain that the abilities I acquired during my degree program will help me succeed in my long-term career as I continue my education and professional growth.

References:

Dede, C. (2021). Digital collaboration and professional skill development.

Katz, R. L. (2022). Skills of an effective administrator.

National Initiative for Cybersecurity Education. (2020). *Cybersecurity workforce framework*.

<https://www.nist.gov/>

<https://owasp.org/>

<https://www.bls.gov/>

<https://www.isc2.org/>