

Reflective Essay

Dj Smith

IDS 493 Portfolio Project

Dr. Sherron Gordon-Phan

December 9th, 2025

Abstract

This essay reflects on my academic, professional, and personal growth throughout my time at Old Dominion University as a cybersecurity student. By revisiting the work I completed through, technical labs, research papers, policy analyses, cyber law studies, and leadership. I explore how each learning experience contributed to the development of my skills, confidence, and readiness to enter the cybersecurity field. This paper highlights the accomplishments, lessons, and realizations that defined my time at ODU and prepared me to begin a career as a Cybersecurity Analyst.

When I think back on my time at Old Dominion University, it doesn't feel like just a list of classes or assignments, it feels like a journey of figuring out how I learn, how I work, and who I want to be professionally. Coming into the cybersecurity program, I knew I was interested in technology, but I honestly didn't realize how much the field would challenge me to grow in areas beyond computers. I quickly learned that cybersecurity requires strong writing, patience, communication, leadership, and the ability to think from multiple angles. As I reflect on my coursework and the work I produced, I can see how each experience prepared me for the real world and shaped the mindset I'll carry into my career.

One of the first moments where cybersecurity felt real to me was during the password-cracking assignment. This was my first time actually doing anything that I thought was related to cybersecurity. Once I had completed the program, "password security" was just a phrase everyone repeated, but running John the Ripper and seeing weak passwords get cracked instantly changed my perspective. At the time, I remember being surprised at how fast everything

happened. Now, looking back, I realize that assignment was the beginning of me learning how attackers think and how easy it is for organizations to overlook simple risks. It taught me to never underestimate how small mistakes can open the door to major vulnerabilities. More importantly, it gave me a sense of responsibility. If I'm going to protect systems one day, I have to think like someone trying to break them. That mindset continues to guide me as I prepare for a SOC analyst role. It was a great learning experience that I will continue to look back on till this day.

Another major moment in my development came from my Wireshark labs. I still remember how confused I was the first time I opened the tool and saw hundreds of packets flying across the screen. It felt overwhelming, but as I learned to filter packets, identify ICMP and DNS traffic, and follow communication between devices, something clicked. I started to understand what "normal" traffic looks like. That skill is huge in cybersecurity because analysts need to be able to spot abnormalities quickly. Looking back now, I can see how those early labs helped me build confidence in reading network behavior. They also taught me patience and understanding network data doesn't happen overnight, and it took practice to become comfortable interpreting what I was seeing. The work I did in those labs laid the foundation for the analytical skills I'll use every day in the cybersecurity field. One thing that I really took away from this experience would be the fundamentals are the framework of cyber security but also i needed to work harder than i had to before to get an understanding in the networks.

While the technical assignments pushed me to improve my hands on skills, my work with cybersecurity policy and organizational research opened my eyes to how complex the field really is. Cybersecurity isn't just about protecting systems. It's also about understanding how businesses operate, how risks affect decision making, and how people interact with technology.

When I researched companies like Dollar Tree, Enterprise Mobility, ABNB Federal Credit Union, and Amwins, I learned how leadership, budgeting, staffing, customer demands, and digital transformation all play a role in how secure a company is. At the time, I didn't fully realize how important this perspective was, but looking back on it now, I see how much it shaped my understanding of organizational risk. It taught me to think beyond the computer screen and consider the human and business elements of cybersecurity. It also showed me a new career path I might want to pursue once I get some more experience in the cyber field. The job I was thinking of is a management position. I realized I like policy and even though I might not be the fastest and strongest in the technical side of the field. I would say one of my strong suits is talking and being a people person so policy resonated with me and made me think about different paths I could take in the cyber field.

My policy and risk assessment assignments were also turning points in my learning. Understanding how cybersecurity affects government systems, elections, and national security helped me see the field from a larger perspective. It showed me that cybersecurity professionals have a responsibility beyond protecting data. We also help maintain stability, trust, and safety in society. These assignments taught me the importance of communication. Explaining risks to leaders who don't have technical backgrounds requires clarity and confidence. Looking back, these projects helped improve my writing, push me to think critically, and prepare me for the type of communication analysts must do when reporting incidents or presenting findings. This and my professor made me open up and think of a career in the government or FBI to be exact. The thing I found out they get to do, left me interested and researching another path with the government. Cyber security is very broad but in a good way because you can do some much with the degree even though I might get overwhelmed since you can't just stick with one thing, by

having multiple options also make this degree worth it cause there are a plethora of jobs you can get with it.

One of the most impactful areas of my interdisciplinary learning came from studying cyber law. The cyber law case analysis challenged me to think about how laws like the CFAA apply to real situations. Understanding how warrants work and how digital evidence is evaluated helped me see cybersecurity from a legal standpoint. This knowledge is extremely important for analysts because legal consequences are tied to many decisions made in security investigations. Looking back, I can see how this assignment taught me to be more intentional with documentation and aware of the ethical responsibilities that come with handling sensitive information.

My leadership reflection was another meaningful part of my growth. Before that assignment, I had never taken the time to think deeply about the kind of leader I am or want to be. Connecting leadership theories to my real life experiences helped me recognize the strengths. I naturally bring such things as staying calm, being supportive, and communicating clearly. These are skills I will use throughout my career because cybersecurity is a team oriented field. Incidents happen fast, and teams need to rely on each other. When I recall this assignment now, I can see how understanding leadership concepts strengthened the way I see myself professionally. It helped me realize that who I am as a person matters just as much as what I know technically.

Overall, my time at ODU helped me grow in so many ways. Courses like IDS 300W improved my writing and pushed me to analyze information more deeply. My CYSE labs helped me develop confidence with tools and real-world security scenarios. Policy based assignments taught me to think about the big picture. The law and leadership assignments helped me understand the human side of the field. When I put all of these experiences together, I can see how

interdisciplinary my education truly was, and how necessary that is for a cybersecurity professional.

I am proud of the work I completed at ODU because I can see the progress in every stage. I entered the program unsure of what to expect, and I'm leaving with a stronger understanding of cybersecurity, a better sense of who I am, and a clear vision of the career I want to pursue. I feel prepared to step into the role of a Cybersecurity Analyst because ODU taught me not only how to handle technical challenges, but how to think critically, adapt to new situations, communicate clearly, and understand the bigger picture.

As I close this chapter, I look back at the freshman I was, scared about changing my major and not hoping I would get a sign that I'm doing the right thing. I will always be grateful for the challenges, the late nights, the assignments that confused me at first. Also want to say that I'm glad that I took the chance and switched my major to something that genuinely challenged me and the accomplishments that showed me I was improving. Looking back at everything I've done, I know that my time at ODU shaped me into someone who is ready to take the next step in the cybersecurity world with confidence, discipline, and purpose.

Reference

Smith, D. (2025). *Password Cracking Assignment* (Unpublished student assignment). Old Dominion University, Department of Cybersecurity.

Smith, D. (2025). *File Permissions Assignment* (Unpublished student assignment). Old Dominion University, Department of Cybersecurity.

Smith, D. (2025). *Network Traffic Tracing & Sniffing Lab* (Unpublished student assignment). Old Dominion University, Department of Cybersecurity.

Smith, D. (2025). *Company Research & Organizational Risk Review* (Unpublished student assignment). Old Dominion University, Interdisciplinary Studies Program.

Smith, D. (2025). *Cybersecurity Policy & Risk Assessment Analysis* (Unpublished student assignment). Old Dominion University, Interdisciplinary Studies Program.

Smith, D. (2025). *Economic Impact of Cybersecurity Policies Paper* (Unpublished student assignment). Old Dominion University, Interdisciplinary Studies Program.

Smith, D. (2025). *Cyber Law Case Analysis* (Unpublished student assignment). Old Dominion University, Department of Cybersecurity.

Smith, D. (2025). *Windows System Security Research Project* (Unpublished student assignment). Old Dominion University, Department of Cybersecurity.

Smith, D. (2025). *Leadership Reflection & Theory Application Paper* (Unpublished student assignment). Old Dominion University, Interdisciplinary Studies Program.