Reflection Essay

Danny Choi

Interdisciplinary Studies, Old Dominion University

IDS 493 – IDS Electronic Portfolio Project

Dr. Sherron Gordon-Phan

December 07, 2025

Abstract

This reflection essay is a culmination of my time at Old Dominion University (ODU) and highlights three skill sets, networking skills, communication skills, and research analysis that I have acquired during my time as a Cybersecurity Major. I analyze how my experiences in certain classes like Interdisciplinary Studies and Cybersecurity shaped and molded the development of those skills. I demonstrated my development of those skills through the usage of an e-portfolio, including nine artifacts that I believe best represent my growth and challenges I faced as I draw the connections and conclusions to best determine how I would succeed in the ever-growing digital domain known as Cybersecurity.

As my time at Old Dominion University (ODU) comes to an end, and I'm reminiscing about my life here as a college student, I can't help but feel bittersweet about all the great friends, skills, and opportunities I was afforded. As much as I will cherish all the great laughs and memories here, I want to shift the focus to the part that I am most proud of, which is the skills I have acquired. As a cybersecurity major, I've acquired many skills, but the three particular skills that I've grown akin to are my technical skills, research analysis, and communication skills. All the skills I've learned have been vital in shaping me into the professional I am today, but those three particular ones are what I believe stand out above the rest. These skills were carefully crafted through the many courses I've taken in different disciplines like criminal justice, cybersecurity, and literature, while utilizing a combination of my learning of Interdisciplinary Studies as well as hands-on or real-world experiences. This essay will highlight those skill sets while referring to artifacts in my portfolio to showcase my capabilities. I will also demonstrate my personal challenges as well as any learning opportunities that came about through these times and correlate it to the cybersecurity field that I aspire to be a part of.

Cybersecurity Skill Sets

Cybersecurity is an ever-changing field that continues to grow and develop, and to be able to adapt and overcome is not a priority but a necessity. "Cybersecurity skills can be associated with the required tasks or specific sets of actions" (Alammari, Sohaib, & Younes, 2022). Cybersecurity has many skill sets that are required and are unique to each situation, but I believe the three most important to be successful are technical skills, research analysis, and communication skills. Technical skills are what I like to call the core or baseline; being able to utilize tools and software efficiently and having an overall

understanding of the subject at hand is a great foundation to build upon. Communication skill is the bridge-gapper, and it is the ability to adequately and effectively convey information clearly to a diverse audience, as well as maintaining a relationship with co-workers and customers alike. Research analysis is the growth of leadership, and it is having the ability to research, analyze, and interpret information to be able to assist or make decisions and showcase the qualities of being able to figure things out on your own. These three skill sets will be demonstrated in my e-portfolio through the usage of artifacts.

Technical Skills

Technical skills have been defined as being able to utilize and maximize efficiency in the usage of tools and having general knowledge. “Having a baseline set of knowledge, skills, and abilities can go a long way toward developing core attributes common to many work roles” (Dawson & Thomson, 2018). This affords the opportunity for professionals to utilize industry-wide tools, understand them, and stay ahead of technological progression. My proficiency in this skill set can contribute to my own personal studies as well as my various classes at ODU. Courses like CYSE 270 and CYSE 301.

Artifact 1: CompTIA Security+ Certification

This is my first artifact and was earned through my own personal study and by successfully completing and passing the CompTIA Security+ exam. In the IT industry, certifications are a baseline or a standard to highlight knowledge of a certain subject. “Research found that 94% of cybersecurity professionals believe their certifications helped them obtain employment” (Tran, Benson, & Jonassen, 2023). The primary goal for me in achieving this certification was to showcase my understanding of the foundational components of cybersecurity practices and principles and verify my technical skills in

subjects like threats and vulnerabilities, network security, access control, etc. The biggest hurdle was the exam itself, as the way these certifications phrase their questions is purposefully misleading to ensure you truly understand the subject. Through this exam, I've managed to learn how to dedicate and manage my time, as well as teaching me the importance of self-discipline and the mental gymnastics of learning new approaches to not just exam questions, but to any problem I could potentially face.

Artifact 2: pfSense Firewall

This artifact was completed through my CYSE 301 course and is a virtual lab exercise where I had to configure a pfSense firewall. The reason I wanted to highlight this artifact was due to how commonly used the pfSense firewall is throughout the industry. The industry utilizes many different tools, and I wanted to highlight my ability in utilizing one of the commonly used tools. In this lab, I had to configure security protocols and shape traffic flow. The biggest challenge, as someone who had never configured a firewall before, was translating security theories and practices into a real-life scenario. This practice reinforced my understanding of network security concepts, as well as giving me hands-on experience with the pfSense firewall and learning to adapt and troubleshoot in situations where it wasn't properly translating the security protocols. Troubleshooting is a critical part of any cybersecurity role.

Artifact 3: Linux

This artifact was completed through my CYSE 270 course and was another virtual lab exercise where I had to configure user account access, as well as get accustomed to the Linux software. Linux is an operating system like Windows and is viewed as a great alternative that is widely used throughout the industry. The primary goal of this lab was to

build on the foundation and fundamentals of system administration for Linux, specifically configuring user accounts, managing permission, and access. I had to create users and create accounts, adding them to their proper groups and granting access. My main challenge with this lab was understanding Linux, as well as the different command lines required. There are different software and programs, each having their own unique command lines that are similar but differ. This Linux administration lab experience is fundamental and mainstream throughout the industry.

Communication Skills

Communication skills are defined as the ability to successfully translate and receive information of varying kinds. Effective communication skills are being able to translate and convey information to a variety of audiences. Being able to translate complex information into simpler terms is an effective skill to have and is a sought-after skill in the cybersecurity industry. According to research done by Ullah et al. (2025), having great communication skills is a key contributor of success for professionals in cybersecurity, allowing for technical knowledge to be conveyed to different levels of expertise. I will be dealing with co-workers and customers with varying knowledge of IT terminology and concepts, so having the ability to successfully break it down for the target audience to understand builds camaraderie, rapport, and confidence. I was able to develop my communication skills in my courses in CRJS 315, CYSE 280, and CYSE 425W.

Artifact 4: "Black Cat" Presentation

This artifact is a presentation I had to make for my Criminal Justice course about an organization called Black Cat. This organization was infamous for conducting ransomware or cybercrimes to exploit and take advantage of people for financial reasons. This was a

Criminal Justice course that had students from varying majors. The goal of this project was to teach the class about how a cybercrime group conducted their operations, tactics, and if there were any mitigation methods. The biggest challenge was figuring out how to present technical terminology to be as simple as possible, as the class had varying levels of technical knowledge. I was able to accomplish this by practicing breaking down the jargon and using visual aids to better illustrate my point and define the implications in an understandable manner. I forced myself to tailor my speech to the audience and be highly adaptable in the case of any questions. Having strong communication skills will be vital, as conversing with customers is to be expected.

Artifact 5: Windows System Management and Security Research Paper

This artifact is a research paper I wrote for one of my classes, and it explored the various components of Windows system management and security. This paper was a bit opposite of my previous artifact, as this time I was communicating with my professor who has more technical knowledge and understanding of the subject than me, and I had to ensure that my knowledge and research were adequately covered. The biggest challenge was consolidating my research and presenting it in a clear, organized, and concise manner. In cybersecurity, I will be working with people of all different backgrounds and technical backgrounds. This paper allowed me to practice my communication skills with a more technically sound individual, which will be common in the work environment. This paper demonstrates that my communication skills are highly adjustable and can be specifically tailored to the target audience.

Artifact 6: How Effective is the NIST Cybersecurity Framework (CSF) 2.0

This artifact is about a paper I wrote on the effectiveness of the NIST CSF 2.0. This

paper was a combination of both of my previous artifacts in this section, as I had to tailor my audience to both my class as well as my professor. The primary goal for this paper was to effectively present my argument in a well-mannered and organized manner, describing the framework, including its weaknesses and strengths, and supporting my claim with evidence. A major challenge was evaluating how effective the framework is by diving into case studies, reports, and other findings to report an unbiased review of the framework. Through this paper, I was able to practice my written communication skills, as I had to articulate and effectively get my argument across, as well as honing my communication skills when catering to the diverse audience that I will face in the cybersecurity world.

Research Analysis

Research analysis is the thorough investigation and exploration of different materials on a certain subject. Once the research is completed, you will have to apply proper analytical techniques to interpret and draw conclusions to come to a sound decision. There was a study and that "study has identified five key initiatives that organizations have implemented to improve their security culture to influence and change employees' behaviors" (Alshaikh et al., 2020), showcasing that good research can be favorable even guiding organizations to make changes to their cybersecurity strategies. In cybersecurity, being able to interpret and understand materials like tickets and emails will not only improve security but can support decision-making. Drawing conclusions based on sound evidence to come to a well-documented decision will be critical not only in the specialist role, but in the team lead role down the road. Having good analysis skills allows for proactivity in assessing and identifying any exploitations or vulnerabilities. I was able to get practice and hone my skills in my CYSE 280, IDS 300W, and IDS 425W courses.

Artifact 7: Compare and Contrast Windows Server

This artifact is a little different, as I wanted to include something that highlighted my creativity. The goal of this project was to create a form of visual that differentiates and highlights similarities between the different iterations of Windows Server. Essentially a history lesson, with our choice of how we wanted to present our research. The way I presented my work was by creating a flow chart that was to resemble a server. Then I included a bubble chart to show the differences. This was challenging, as Windows Server has been around forever, so there were a lot of conflicting reports and sources. This project not only improved my knowledge of Windows Server but allowed me to step out of my typical writing space and create a different format. Comparing and contrasting is a great tool to understand and help differentiate the differences, no matter how minuscule. In cybersecurity, it will be common for software and other platforms to have updates or changes, so being able to practice recognizing key differences and similarities and sometimes organizing conflicting information into an analysis was a great skill to showcase.

Artifact 8: Political Implications of the NIST Cybersecurity Framework (CSF) 2.0

This artifact was, like the title states, a deep dive into the political implications of the NIST CSF 2.0. The primary goal for this paper was to analyze CSF 2.0 in the political realm. Certain ideas like how adoption rates are influenced by the political landscape or how different stakeholders, i.e., government and private entities, create influence and a power dynamic in the cybersecurity landscape. This paper was challenging, as I had to navigate the political aspect of cybersecurity and gain a better understanding of an aspect that I had no idea about, nor did I really care for. I had to organize and consolidate conflicting reports

from different agencies into a concise, unbiased, and balanced analysis. This paper allowed me to practice understanding and researching cybersecurity in landscapes outside of the IT world, allowing me to expand my horizon on perspective.

Artifact 9: Aiming for the Stars: An Interdisciplinary Study

This artifact was one of my favorite papers to write, albeit challenging, as it was on a topic not pertaining to cybersecurity. The goal of this paper was to pick three disciplines and pick a topic to write about. This paper was challenging, as Interdisciplinary Studies is a concept that I'm unfamiliar with. My topic for the paper was the colonization of Mars. I had to research topics that I was unknowledgeable about and present my concise argument that it is feasible to colonize Mars. In cybersecurity, as much as it would be fun to understand just the security aspect of the network, understanding the network and other aspects will allow for a better perspective to ultimately support decision-making. Completing this research project allowed me to improve my analytical and critical thinking skills and break down seemingly complex arguments into simpler, more manageable ones.

Conclusion

In summary, my time at ODU has allowed me to take a multitude of classes that have equipped me with skill sets to improve in my desired field of cybersecurity. These technical skills, communication skills, and research analysis are key components in being successful and adapting and being at the forefront of the ever-changing digital landscape. Through my nine artifacts present in my e-portfolio, I have been able to demonstrate how these classes have shaped and ultimately molded me into the professional I am today. I will continue to grow and develop upon the foundation that ODU has set as I continue this journey down the cybersecurity path.

References

Alammari, A., Sohaib, O., & Younes, S. (2022). *Developing and evaluating cybersecurity competencies for students in computing programs.* PeerJ Computer Science, 8, e827. https://doi.org/10.7717/peerj-cs.827

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: Five initiatives from three Australian organizations. *Computers & Security, 100*, Article 102003. https://doi.org/10.1016/j.cose.2020.102003

Dawson, J., & Thomson, R. (2018). *The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. Frontiers in Psychology, 9*, 744. https://doi.org/10.3389/fpsyg.2018.00744

Tran, B., Benson, K. C., & Jonassen, L. (2023). *Integrating certifications into the cybersecurity college curriculum*. Journal of Cybersecurity Education, Research and Practice. https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=1138&context=jcerp

Ullah, F., Ye, X., Fatima, U., Akhtar, Z., Wu, Y., & Ahmad, H. (2025). *What skills do cyber security professionals need?* arXiv preprint arXiv:2502.13658. https://doi.org/10.48550/arXiv.2502.13658