Self-Reflection

Joshua Taylor

Old Dominion University

IDS 493

05 December 5, 2025

My time at Old Dominion University has been illuminating to say the least when it comes to the world of Information Technology and Cybersecurity. Before joining the cybersecurity program at Old Dominion I thought the world of cybersecurity and information technology was simply just technical skills, with little interdisciplinary interaction. Now, on the final push to completion of my degree I have realized that cybersecurity is an amalgamation of many different disciplines from the technical side such as programming, networking, server management, and more; to the more theoretical and social science side of understanding human nature, human tendencies, cybercriminal psychology, the lasting impact of these crimes and more. My time inside and out of the classroom working on cybersecurity projects and assignments, studying material about how the social sciences intertwine with cybersecurity, learning to grasp the technical skills and become proficient in them, and combining all of these concepts into a more fully realized understanding of the cybersecurity world works has been very rewarding. There are a few skills with demonstrated evidence of proficiency as well as understanding that have really stood out to me as important and integral to my learning experience throughout my program and to my potential career going forward. The courses of CYSE 201S, CYSE 270, and CYSE 301 have helped to set the foundation of what I can do, show where in the field I can end up, introduce the interdisciplinarity of the field, and encourage growth in learning about the field. Reflecting on how all of the course work and material was provided and taught to me throughout my time in the Cybersecurity program has been extremely valuable. The field is enormous and there are so many different career paths one could take within the field of cybersecurity alone. The courses I took, skills I gained, and material I learned changed what I initially thought the program would be, and what were the most important things to learn in cybersecurity may be.

One of the first eye opening courses I took that really changed the way I viewed cybersecurity was CYSE 201S: Security as a Social Science. Initially, I had thought that cybersecurity as a field was essentially just technical skills and abilities, navigating the command prompts, writing scripts, etc. This course taught me and helped me develop a broader understanding of the social aspects of cybersecurity and sharpen skills such as critical thinking, research, analysis, and other more non-technical skills per se. The social science of cybersecurity is actually a very large portion of what professionals in cybersecurity must understand to be successful. Social engineering is a "social" issue that is very prominent in cybersecurity and is something that cybersecurity professionals must understand well in order to combat. In fact, according to a journal article published in *Data & Metadata,* "Vulnerability analysis in the university community using social engineering and phishing applications" (Guana-Moya, Villacis, & Miniguano Miniguano, 2025). I bring this up because an artifact I chose to include in my portfolio is an article review I completed regarding Phishing and cybercrimes in a university student community and how the social sciences interacted with that subject. That artifact in particular I felt showcased skills that I have improved through my time at ODU and in this course such as research and analysis. Being able to read an academic journal article, analyze what is being discussed and what is pertinent and important information, and being able to then compose a digestible breakdown and analysis of that topic is a skill I have found to be more and more important as my professional and scholastic careers have progressed.

Continuing to examine what I learned and skills I gained through the course of CYSE 201S, I included an additional article review and a career paper. These reviews and analysis's enlightened me and improved my research, critical thinking, and analytical skills. The first article review I did was about deepfakes in the metaverse. This article taught me more about

cyberattacks, deepfakes, and cybercrimes against individuals. The article showed that the experts included in the article believed that women, children and the elderly are more often chose as primary targets for cybercrime in the metaverse (Stavola & Choi, 2023).I bring this up because, again this course really allowed me to showcase my research and analytical abilities through breaking down and reviewing these journal articles. The articles additionally really drove home how interdisciplinary the field of cybersecurity is and how much the social sciences are intertwined. The career paper I completed also allowed me to showcase those skills by allowing me to breakdown and analyze a career position in the cybersecurity field and how it utilizes the social sciences.

I found through my time in this program that I enjoyed more thoroughly the technical aspects of cybersecurity and the IT field. A course I found that let me develop and showcase new skills was CYSE 270: Linux Systems for Cybersecurity. CYSE 270 was my first real foray into the Linux operating system. I had heard of Linux but had no real practical experience with the operating system. One important thing this course taught me was just how valuable being proficient in utilizing the command prompt is in navigating, managing, protecting, automating, and altering things in the Linux world. That is why I felt the desire to showcase of skills and abilities I gained through the completion of the course and studying the material presented.

The artifacts I chose to include in this portfolio are primarily based around utilizing the Linux command prompt and completing tasks through manipulation of the command prompt. The assignments and artifacts I included are basic and advanced networking configurations, and user and group account management. These assignments showed me and allowed me to demonstrate proficiency in creating, managing, deleting, and protecting group and user accounts. Additionally, it taught me and showcases basic network troubleshooting skills such as verifying

internet and DNS connectivity, checking TCP connections and routing tables, changing filenames, setting up firewalls, set up IP forwarding, and a few other skills; all from the command prompt. An additional skill this set of artifacts taught me was how to set up a virtual machine using Oracles Virtual Machine software. These skills are the skills that I had initially joined the program looking to learn and the course itself was instrumental in developing the skills I needed to succeed when using various Linux OS's.

Another course I found to be important to my growth in the field of cybersecurity was CYSE 301: Cybersecurity Techniques and Operations. This course included teaching skills in command prompts, but also how to use third-part software such as Wireshark to sniff network traffic, how to attack and defend cyberattacks, and password cracking. I chose to include this course and these three artifacts in my portfolio because they demonstrated skills that are more attuned to the cybersecurity field as opposed to simply just IT skills. These skills and abilities I learned here are technical and are what I found I thoroughly enjoyed learning about and developing for use in the professional world. Learning how to scan and sniff network traffic showed the importance of proper firewall setup and encryption. Again, developing skills in network management and firewall creation. While my "Sword vs. Shield" and Password cracking artifacts showed the skills I learned to attack as a red team member or defend as a blue team member which are skills useful for cyber defense careers and fortifying personal systems as well. While the password cracking artifact showed me just how easy passwords are to crack, the importance of complex passwords, and the skills to ensure the companies I work for are properly defended by enforcing strong password policies to defend against cyber-attacks.

Reflecting on the coursework, skills, abilities, and information I have learned and gained from this program has been rewarding and enjoyable. When I first began the program, I was only

focused on the technical side of the field with little to no thought on the interdisciplinary side of cybersecurity. Having now completed courses that demonstrate the interdisciplinary level of the field, I have a new appreciation for the field as a whole and where I could end up. What those courses that were not heavy in the technical side of things taught me were the skills to properly research, analyze, and compile reports and breakdowns of sometimes complex and difficult subjects to a digestible format. Those skills are valuable because the laymen may not be familiar with the terminology and the field of cybersecurity. Part of being a cybersecurity professional is being able to teach and show everyone better cyber practices no matter their skill level, and the skills shown in the courses I have taken have helped instill that ability. The technical side of this cybersecurity program has really helped me become confident in my IT and cybersecurity abilities and has given me many skills. Troubleshooting both basic and advanced issues for users, groups, and networks in the command prompts of Linux and Windows; skills in network and system security and defense by configuring and utilizing firewalls, network security requirements, third-party software like Oracle VM and Wireshark, and teaching me skills in password manipulation and password cracking. These technical skills are vitally important to being an effective and efficient cybersecurity professional, and through my artifacts, I believe I have demonstrated the skills gained through this program. I enjoyed this program and believe I have achieved what my desired learning outcomes were for this program as a whole while also expanding my knowledge base and expanding my overall understanding of cybersecurity as a whole.

References

Guana-Moya, J., Villacis, S., & Miniguano Miniguano, D. (2025). Vulnerability analysis in the university community using social engineering and phishing applications. *Data & Metadata*.

Stavola, J., & Choi, K.-S. (2023). Victimization by Deepfake In the Metaverse: Building a Practical Management Framework. *International Journal of Cybersecurity Intelligence & Cybercrime*, 1-20.