REFLECTIVE ESSAY

BY: BRYANT WATKINS

IDS 493

Professor Carin Andrews, MBA, MAcc, CPA

8/9/2025

Introduction

My time here at Old Dominion University has seemingly flown by. I started my coursework in the Fall of 2019, and it has taken me six long years to finally get to this point. I have taken many courses during my time, but throughout these courses I have been able to pinpoint three of the top skills that will be at the forefront of my career in cybersecurity. These skills include – computer programming, ethical hacking/penetration testing, and Linux systems. These skills will provide me with the adequate foundation necessary for a lengthy and successful career ahead.

Computer Programming

Computer Programming was one of the very first information technology courses I had ever taken. My experience in this skill dates back to my days in high school. During my sophomore year I took Computer Programming, and then my senior year I took a higher-level Advanced Placement Computer Programming course. I quickly found my footing in these courses and excelled greatly in my assignments. Computer programming was something that I immediately found a fondness for. These courses would provide me with two years of programming with Java before I ever made it to college.

My coursework at Old Dominion University in computer programming was more extensive and advanced. Computer programming at Old Dominion University gave me my first experiences with the Python programming language. My first cybersecurity major course was Basic Cyber Programming and Networking (CYSE 250). During my enrollment in this course, we completed multiple assignments that allowed me to acquire additional computer knowledge and skills.

One supporting artifact from my coursework would be the *for loop* assignments. These assignments provided me with an opportunity to craft *for loop* programs with varying outputs. Another supporting artifact were *String* assignments. The *String* assignments allowed me to create programs that would produce varying outputs based on user string inputs. The other supporting artifact of note was the file assignments. Those assignments had me creating programs that could manipulate relevant text files.

In solving many of these assignments, I was able to draw back to the relevant module course materials that provided in-depth instruction and guidance. My previous coursework dating back to high school was also an incredible aid, while the programming language was Java instead of Python, the material and structure was still very similar. This course taught me the skills, techniques, and operations necessary to craft elaborate computer programs as a well-rounded programmer. Computer programming can be an incredibly integral function to successful cybersecurity operations, many positions that I will be aspiring to will require some level of programming expertise.

Ethical Hacking/Penetration Testing

There were multiple courses that I enrolled in while completing coursework at Old Dominion University. I took Cyber Techniques and Operations (CYSE 301) in the Spring of 2024, and I also took Ethical Hacking and Penetration Testing (CYSE 450) in the Spring of 2025. These courses would prove to be monumental in providing me with great experience in the field of ethical hacking and penetration testing. This was a field that I have great interest in and believe is an incredibly valuable skill set to develop for my career in cybersecurity.

The first major supporting artifact from these courses was the ethical hacking assignment from CYSE 301. This assignment had me use a virtual machine environment to mirror a “victim” desktop screen, and it provided me with my very first ethical hacking experience. Another major supporting artifact stemmed from the malware analysis assignment in CYSE 450. This assignment included systematic analysis of potential malware through the Bazaar platform, and I was provided with valuable experience in cybersecurity analysis. The final supporting artifact of note was the hashing assignment in CYSE 450. The hashing assignment allowed me to create and manipulate hashes – giving me extensive experience in hashing.

The process for completing these assignments was admittedly arduous, but I was able to lean on the lectures and lab guidance documents provided. Taking CYSE 301 certainly proved beneficial in providing me with prior ethical hacking experience, such experience aided me in the process of completing CYSE 450 assignments. Overall, these courses taught me the fundamentals of ethical hacking and penetration testing. Ethical hacking and penetration testing is certainly a major pillar of cybersecurity; my dream job is to be a professional penetration tester. These courses also have inspired me to pursue a CompTIA PenTest+ certification during my cybersecurity career.

Linux Systems

Linux is an important platform that I was able to learn about from multiple courses at Old Dominion University. I enrolled in Linux System for Cybersecurity (CYSE 270) in the Fall of 2024, and the previously mentioned Cyber Techniques and Operations (CYSE 301) also provided me with experience in the Linux system. These two courses provided me with my foundation of knowledge in the Linux system. During my enrollment in these courses; there were numerous assignments that would supply me with major supporting artifacts.

The first supporting artifact was the Basic Linux Commands assignment in CYSE 301. This assignment entailed completing common commands that provide a foundational level of knowledge on how to operate the Linux system. Another supporting artifact was the Shell Scripting assignment from CYSE 270. This assignment involved crafting shell scripts on Linux that would produce a plethora of desired outputs. The final supporting artifact of note was the Automation assignment from CYSE 270. That assignment gave me my first experience in creating scripts in Linux that would conduct certain desired tasks per an automated schedule.

Figuring out the process for these assignments relied on lecture materials as well as trial-and-error practicing. CYSE 301 certainly proved incredibly beneficial in my CYSE 270 assignments, as the prior Linux system experience from CYSE 301 significantly aided my understanding of Linux operations for CYSE 270. These courses in tandem taught me many important commands and operations necessary to successfully be capable of utilizing the Linux system. Linux is undoubtedly vital to many professional cybersecurity functions; the experience and knowledge I gained in Linux will provide me with additional tools necessary to a successful cybersecurity career.

Conclusion

Interdisciplinary methods and theories were important to my understanding of my coursework because it gave me a road map to connecting multiple disciplines together. Information technology, cybersecurity, and law/ethics are all disciplines that constituted my cybersecurity major coursework at Old Dominion University. Comprehending my lecture material required me to be capable of tying together concepts and skills from across multiple disciplines. Interdisciplinary Studies (IDS 300W) certainly proved pivotal in my cybersecurity coursework.

During my coursework I quickly learned to never value certain areas of knowledge over others. Learning that aided in my ability to later draw upon previous knowledge from earlier courses that would tie into future courses. All previous knowledge gained would prove incredibly relevant to future coursework. Many assignments completed required me to rely on concepts and skills previously obtained. The interconnectedness of all my courses was something I found to be incredibly intriguing and beneficial.

It is very important to be an interdisciplinary thinker in cybersecurity because cybersecurity has many moving parts that all work together ultimately. Cybersecurity employers are certainly looking for well-rounded and versatile candidates that possess expertise and experience across numerous disciplines. The experience I have received from my earlier interdisciplinary coursework has been immensely valuable. I now possess the ability to reach across multiple sectors of cybersecurity to create a comprehensive and complete foundation of cybersecurity knowledge and skills needed for a professional cybersecurity career.