Reflection Essay

Stuart N. Howard III

Old Dominion University

IDS493: Electronic Portfolio Project

Professor Carin E. Andrews

22 April 2024

Introduction

As I venture deeper into the world of cybersecurity, I've encountered both challenges and opportunities for personal growth. Although I have developed some of my skills throughout my 20-plus years in the military, while attending Old Dominion University, I have been able to hone and increase my skills as well. Beyond simply acquiring technical knowledge, this journey has taught me invaluable critical skills necessary for navigating the complexities of this field. I've sharpened my technical proficiency, problem-solving abilities, communication skills, and critical thinking prowess through various courses. In this essay, I will showcase the artifacts that represent my educational journey and highlight pivotal moments that have contributed to my evolution as a cybersecurity professional. From creating Python programs to exploring password security and ethical hacking, each artifact represents a significant milestone in my pursuit of excellence in this dynamic field.

Technical Skills

My journey into cybersecurity has required me to learn technical knowledge from some of the courses I have taken. Technical proficiency is crucial in demonstrating that I can accomplish any task in my field. My journey in acquiring technical knowledge has been exemplified through various artifacts. Reflecting on these courses, I can see how challenging they were and how excited I was to take on that new change. In the CYSE250 course, I showcased my understanding of programming by creating a final project that utilized Python programming language and creates a final project. This artifact highlighted my ability to apply coding skills and underscored the importance of technical proficiency in developing cybersecurity solutions. Similarly, in the CYSE270 Password Cracking lab, I navigated the complexities of password security using Kali Linux tools, emphasizing the significance of

technical expertise in identifying vulnerabilities and implementing robust defense mechanisms. Through CYSE301, I experienced ethical hacking for the first time, and I thought it would be like the movies. Through artifacts like these, I have acquired technical knowledge and honed my problem-solving skills essential for addressing cybersecurity challenges in professional settings.

Artifact 1 CYSE250 Term Project in Python

I participated in a course that focused on cybersecurity programming and networking concepts. Throughout the course, we honed our problem-solving skills by learning programming languages and exploring the fundamentals of network protocols. At first, I found the course quite challenging because I underestimated the complexity of programming. However, I overcame this obstacle and completed the final project, which required us to develop a client-server socket that demonstrated communication between the two. This project allowed us to showcase our understanding of real-world client-server communication and how information is transmitted between our devices and servers like Google or Yahoo. One aspect of the project that I particularly enjoyed was the freedom to create whatever we wanted, whether it be games or Q&A servers. This freedom allowed us to showcase our creativity and understand the project development process.

Artifact 2 CYSE270 Password Cracking

The item I'm sharing is a lab assignment from my Linux System for Cybersecurity course. During the class, I gained an understanding of fundamental Linux operations through both graphical and command-line interfaces. I also learned about installation, configuration, file system management, shell scripts, and user authentication. The lab explored the intricacies of password cracking, using tools such as Kali Linux, MD5 hash, John the Ripper, and other

password attacks. By engaging in practical exercises, I gained valuable knowledge of the procedures for obtaining and deciphering passwords. I also learned that there are various techniques and tools at our disposal to accomplish this task, and it's crucial to determine which approach will be most effective for the specific task at hand. Furthermore, this experience underscored the significance of implementing strong password security measures to safeguard against cyber threats.

Artifact 3 CYSE301 Ethical Hacking Lab

In my Cybersecurity Techniques and Operations course, I acquired a wealth of knowledge regarding a wide range of tools and techniques for safeguarding and scrutinizing computer networks. Our curriculum delved into network mapping, advanced packet analysis, firewall configuration, intrusion detection, forensic investigation, and penetration testing. This was a pivotal experience for me, as it marked my first exposure to ethical hacking, and I was eager to learn the ins and outs of the process. Despite some difficulties along the way, I persevered and successfully completed the lab requirements. These exercises proved invaluable in refining my ability to identify and address security vulnerabilities, and I feel confident in my ability to tackle real-world cybersecurity challenges.

Communication

Effective communication is vital in cybersecurity, as it involves explaining intricate technical concepts to a diverse audience. Though I have utilized my communication skills in my military career, my courses at ODU have helped me refine them further. Communication is a soft skill trait and ability you develop throughout life (Long, 2023). I have successfully conveyed the ability to demonstrate the skill I have learned through various artifacts, such as the Penetration

Test Preparation Report. This underscores the importance of communication skills in fostering collaboration with clients and stakeholders to carry out successful cybersecurity initiatives. Moreover, my work on the Network Upgrade High School and Documentation project demonstrated my ability to communicate technical proposals effectively, highlighting the significance of clear communication in gaining support for IT projects. Finally, conducting a financial Return on Investment (ROI) Analysis is essential to determine the cost-benefit of a network system. Upon reflection, I recognize the practical application of these artifacts is similar to the reports and projects I produced while serving in the military.

Artifact 1 CYSE450 Penetration Test Preparation Report

Through my studies in Ethical Hacking and Penetration Testing, I gained a thorough understanding of the fundamentals of ethical hacking and acquired valuable tools for conducting penetration testing using Kali Linux. I was able to identify vulnerabilities in various systems and perform penetration testing on different target systems. One of my assignments, Artifact 1, involved crafting a comprehensive report that outlined the steps involved in ethical hacking procedures. This highlighted the administrative side of ethical hacking, which is often overlooked. It is essential to have a process and procedure to follow, and this assignment was the first step in letting the client know what you plan to do and identifying any legal or other issues that may arise. This underscored the importance of clear communication in conveying technical processes, a skill that is essential for collaborating with clients and stakeholders.

Artifact 2 IT315 Financial ROI Analysis

In my Introduction to Networking and Security course, I gained a deep understanding of the fundamental concepts and technologies behind modern networking and data communication.

As part of my coursework, I completed Artifact 2, an assignment that required me to conduct a financial return on investment analysis to justify network upgrade investments. This experience reinforced the importance of using data-supported arguments to persuade decision-makers and secure funding for projects. Effective communication skills were vital to my success in this task, as I provided recommendations on whether to upgrade or replace a system and had to communicate my findings in a report clearly. I carefully analyzed the data and conducted a thorough cost analysis, ensuring my report was accurate and persuasive.

Artifact 3 IT315 Network Upgrade Project

As part of the Networking and Security course, I undertook a challenging project that involved upgrading a local high school based on provided building plans. My responsibility was to create a comprehensive network upgrade plan that emphasized clear communication of technical proposals. This involved budgeting for wiring, equipment, and securing network traffic. The project was particularly daunting due to the scale of the task, which included designing a network for a four-floor building and providing a detailed report of all materials and costs. Through this project, I learned the importance of articulating complex ideas concisely and understandably, which is crucial for gaining support and approval.

Critical Thinking

Throughout my academic journey, I've faced a variety of challenging courses that have pushed me to hone my critical thinking skills. Being able to analyze complex information and provide my perspective has been both rewarding and challenging. Critical thinking is especially crucial in cybersecurity, as it enables the analysis of multifaceted problems and the development of innovative solutions. In my professional experience, I've analyzed current issues and provided

recommendations for action in the Privacy and Data Protection Memo, which can be found in CYSE406. In my research paper on the IDS 300W Internet of Things Challenges, I employed interdisciplinary perspectives to tackle cybersecurity issues, highlighting the value of critical thinking in synthesizing diverse insights. Similarly, in my research on Mitigating Threats and Defending Windows Server 2019, which can be found in CYSE280, I showcased my ability to evaluate security measures and propose proactive mitigation strategies through careful analysis.

Artifact 1 CYSE406 Privacy and Data Protection Issues Memo

During my Cyber Law course, I delved deeply into the various U.S. cyberspace-related laws from both civil and criminal perspectives. The course provided an in-depth understanding of the authorities and limitations of cyber operations professionals and covered cybersecurity topics such as Federal Acquisition Requirements. The artifact I selected from this course was an assignment to argue on behalf of the people of the state. The assignment had me as an intern for the governor of Virginia. My job was to draft a memo regarding personal privacy information. The memo aimed to provide the governor with the necessary information to decide whether to create a state law or push for federal guidance. I thought this was a good assignment because it was a practical exercise that I would do if I were to work for the government or a job where you're in the position to provide input that influences the boss's decisions. There have been several times in my military career when I had to draft memos like that and send them to the bosses for his purview. Most of the time, I didn’t have a choice; I was instructed to get it done by “yesterday” for my boss, who needs it for his boss and up.

Artifact 2 IDS300W Internet of Things Challenges (IoT) research paper

In my Interdisciplinary Theory and Concepts course, I delved into the history, concepts, and practical applications of interdisciplinary studies. Through this course, I honed my ability to analyze the similarities and differences between various academic disciplines and apply interdisciplinary approaches to a specific field of study. The experience broadened my perspective on how interdisciplinary methods can be applied to cybersecurity, as well as how other disciplines intersect with it. Choosing an artifact that explored interdisciplinary perspectives on IoT challenges, incorporating cybersecurity, sociology, and legal studies, proved invaluable in developing my critical thinking skills. This approach allowed me to analyze complex issues from diverse angles and propose comprehensive solutions.

Artifact 3 CYSE280 Mitigating Threats and Defending Windows Server 2019

In the Windows System Management and Security course, I learned how to manage and secure Windows operating systems. This course covers tools for configuring, securing, and managing Windows client and server OS and their networks. It also covers malware protection, security auditing, and virtualization platform security. I selected artifact three because it was the final term paper, and it allowed me to use my critical thinking and analysis skills that formulate my thoughts on the threats to Windows Server 2019. Additionally, I took this course the semester after taking IDS300W, and that allowed me to incorporate an interdisciplinary point of view into my argument.

Conclusion

In retrospect, my journey through cybersecurity education has been a testament to perseverance, growth, and relentless pursuit of knowledge. From grappling with programming challenges to unraveling the nuances of ethical hacking, each artifact represents a chapter in my

transformation as a cybersecurity enthusiast. As I step forward into the professional realm, armed with technical expertise, refined communication skills, and sharpened critical thinking acumen, I am poised to tackle the ever-evolving landscape of cybersecurity challenges. With each artifact serving as a testament to my journey, I embrace the future with optimism, knowing that I am equipped to make meaningful contributions to cybersecurity.

References

Long, B. (2023a, July 5). *Hard skills vs. soft skills: What are they? (with examples)*. Insight Global. https://insightglobal.com/blog/hard-skills-vs-soft-skills/