Old Dominion University

Reflection Essay

Noah Salafranca
IDS 493
Dr. Tucker
October 6, 2024

Introduction

An ePortfolio is a valuable tool for furthering students' futures. ePortfolios allow students to integrate their knowledge, skills, and experiences gained through their coursework, internships, and extracurriculars. As Celeste Fowles Nguyen argues the importance of ePortfolios, she states, "The ePortfolio gives students a way to create a narrative applicable to academic, professional, or personal aspects of their lives" (Nguyen, 2013, p. 139). Throughout the IDS 493 course and creating my ePortfolio, I learned that an ePortfolio is more than a collection of works; it's the signs of my progress and the highlights representing my best qualities.

Throughout college, I have been developing fundamental skills for a cybersecurity major: technical, communication, and critical thinking skills. These skills are vital to my professional goal of becoming a cybersecurity specialist. A technical skill set is fundamental to the abilities of a cybersecurity professional. Also, cybersecurity professionals must communicate these technical cybersecurity topics to colleagues, clients, law enforcement, forensics teams, and more. Furthermore, professionals must demonstrate critical thinking when developing strategies and analyzing and mitigating threats. My ePortfolio will not only display the artifacts I've compiled to display these skills, but it will also showcase my path to cybersecurity through Dan McAdam's idea of causal coherence in which "one event caused, led to, transformed, or in some other way is meaningfully related to other events in one's life" (McAdams, p. 105).

Technical Skills

Technical skills are crucial in cybersecurity as they provide the framework for effectively detecting, examining, and mitigating cybersecurity threats. Cybersecurity has various technical aspects, like operating systems, network security, encryption, programming, and more. With

knowledge of these aspects, cybersecurity specialists can perform tasks like penetration testing or firewall configuration. As a cybersecurity major learning about this content, it is clear that "students need good technical skills coupled with a desire for further knowledge and understanding of protective security measures" (Payne et al., 2021, p. 9). To showcase my fundamental knowledge and technical skills gained from coursework, my ePortfolio will include the following artifacts:

Active Reconnaissance & Vulnerability Scanning

In my Ethical Hacking and Penetration class, I learned to explore vulnerabilities and worked with tools and software in the cybersecurity industry. I completed a lab focused on active reconnaissance and vulnerability scanning in this class. In the lab, I executed Linux commands *host* and *dig* to determine the host's IP address and live status. Furthermore, I investigated the host's zone transfer capabilities by conducting DNS enumeration, which looks into the host's DNS records. Through this class and lab, I also gained more hands-on experience with Nmap, a network mapper. In Nmap, I scanned for vulnerabilities, running services, and open ports by performing ICMP and TCP sweeps and using NSE scripts. Additionally, I got to perform HTTP and FTP brute force attacks on the target host. The skills learned in this lab are essential in understanding network environments, detecting vulnerabilities, and testing security systems.

Sword vs. Shield

In my Cybersecurity Techniques and Operations class, I was introduced to diagnostic software tools for network exploration and mapping. In this lab, called Sword vs. Shield, I assumed the roles of attacker and defender. I worked on two crucial technical skills: network scanning and firewall configuration. As an attacker, I first scanned a local area network (LAN) using Nmap from an external virtual Kali machine and identified open ports, operating systems,

and running services. As a defender, I configured pfSense firewall rules to prohibit certain kinds of traffic between the LAN and the Kali VM. In this specific lab, I blocked ICMP and allowed FTP traffic. The skills I learned in this lab are essential in network security.

Password Cracking

Once again, in my Cybersecurity Operations and Techniques class, I worked on technical skills in password cracking and wireless network security. In Linux, I learned how to generate passwords and hash functions to understand the significance of password strength in security systems. I learned how to extract passwords from hashes through hash dumps and reverse shell connections in Windows. I was also introduced to tools like John the Ripper and Cain and Abel to crack passwords through brute force or dictionary attacks. With Wi-Fi, I also gained experience decrypting WEP and WPA/WPA2-protected traffic. These technical skills in hashing and encryption are essential in understanding password vulnerabilities.

Communication Skills

> According to Haney and Lutters:
>
> "Cybersecurity education is viewed through a technical lens, with little to no mention of 'soft skills' such as communication, teamwork, and relationship building. These skills are critical to the work of cybersecurity advocates who have a social and organizational focus and impact" (Haney et al., 2017, p. 1).

To discuss cybersecurity knowledge with audiences of various levels of technical ability, cybersecurity professionals must have strong communication skills and writing abilities. For example, concise communication is crucial in incident response, where mitigation must be quick to action. Additionally, strong writing abilities will help create security policies and raise

awareness. To display my communication capabilities, my ePortfolio will include the following artifacts:

Cybersecurity Fundamentals Blog

In my Cybersecurity Fundamentals class, I completed a written assignment that honed my communication skills to convey cybersecurity topics. As a term project, I was tasked to write a blog that researched and explained a recent cybersecurity incident. This blog focused on the attacks' vulnerabilities, technologies, and social implications. I analyzed the Target data breach of 2013, showing how hackers used malware and phishing tactics to exploit network and authentication vulnerabilities. With this blog, I demonstrated my communication skills by explaining the attack, the circumstances of the attack, specific vulnerabilities, and effects in a way that the average reader can understand the situation. I touched on the technical concepts of the attack, like encryption, RAM scraper malware, and network segmentation. This combination of communication and writing skills is needed when reporting cybersecurity incidents and bringing about awareness.

Cryptography Project Paper

Through my completion of this assignment and cryptography class, not only did I gain technical skills in encryption, but I also gained communication and written skills vital to cybersecurity. The focus of my project paper was the security of cryptocurrency wallets and the vulnerabilities and technologies behind them. Explaining blockchain technology, cryptocurrency wallet vulnerabilities, and cryptographic techniques in a comprehensive and structured report helped me develop my communication and writing skills for a dense subject like encryption and cryptocurrencies. Additionally, researching cybersecurity incidents and crypto technologies has helped develop my analytical skills.

Cyber Law Memorandum

In this assignment, I further developed my communication skills, which are helpful in cybersecurity. Writing this memorandum helped me improve my ability to communicate disputed cybersecurity topics like privacy and data protection. Furthermore, I focused on writing a clear explanation of topics surrounding personally identifiable information (PII) and biometric data while explaining relevant legislation and policies like the the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and Texas Data Privacy and Security Act (TDPSA) to call for data protection in Virginia. This strengthens my ability to communicate cybersecurity concerns to decision-makers, ensuring they know the significance of data privacy.

Critical Thinking Skills

In this ever-evolving digital world, cybersecurity professionals must anticipate more advanced threats. Critical thinking skills are essential in cybersecurity because they allow professionals to evaluate complex security risks and develop solutions. Dr. Ileana Hamburg states, "Critical thinking is the process which occurs when a person analyzes, evaluates, and interprets information and then applies it corresponding; it is an ability which is beyond memorization" (Hamburg, 2022, p. 9). To display my critical thinking skills, my ePortfolio will include the following artifacts:

Windows System Management and Security Research Paper

In my Windows System Management and Security class, I had the chance to sharpen my critical thinking skills by completing aresearch paper on mitigating phishing attacks in Microsoft programs. In this research paper, I had to assess several phishing techniques and examine how they exploit technological weaknesses and human behavior. I had to think critically when evaluating the effectiveness of security measures like multifactor authentication. In identifying

vulnerabilities in Microsoft programs like OneDrive, Outlook, and Teams, I had to discern what technological solutions would fit my proposed security practices.

Critical Analysis of Parasite

In Film Appreciation class, my analysis of the 2019 Bong Joon-ho film Parasite sharpened my critical thinking skills when exploring how the film's visual elements, sound design, and narrative provide social and economic commentary. I connected different aspects of the film, like mise-en-scène, editing, symbolism, and genre shifts, to deeper meanings of socioeconomic inequalities. Although this analysis doesn't relate to cybersecurity, my critical thinking in the film is similar to how one would identify hidden flaws and patterns in cybersecurity. Cybersecurity involves analyzing technological environments and user behaviors to detect threats, just like how I film elements to detect deeper socioeconomic meanings.

Corporate Information Security Policy

In this assignment, I develop my critical thinking skills by anakyzing and integrating information security concepts to develop a corporate security policy. To create a comprehensive security policy, I had to assess possible risks and consider security factors like data classification, access control, and incident response. Furthermore, I had to strategize a plan that included human measures, like cyber awareness training, and technical measures, like encryption and multifactor authentication. These critical thinking skills are vital in cybersecurity. Cybersecurity professionals must use critical thinking to assess network layouts, identify risks, and respond to incidents, just as I examined the corporate system to create a security policy.

Conclusion

In conclusion, building my ePortfolio has been a worthwhile experience that showcases the skills and knowledge I have acquired through college as a cybersecurity major. Compiling

and analyzing these artifacts has strengthened my grasp of cybersecurity, from strengthening my critical thinking and communication skills to gaining proficiency in penetration testing and network security. In addition to showing my development, my ePortfolio demonstrates my preparedness for the cybersecurity industry, where these skills are crucial. With the combination of courses, technological projects, and written assignments, I have developed a narrative in my ePortfolio demonstrating my development and enthusiasm for cybersecurity.

References

Hamburg, I. (2022, June). EP4-USING INTERDISCIPLINARY PROBLEM-BASED LEARNING AND CRITICAL THINKING IN CYBER TRAINING. In ERACON Congress & CAREER-EU Conference (p. 5).

Haney, J. M., & Lutters, W. G. (2017, July). Skills and Characteristics of Successful Cybersecurity Advocates. In SOUPS.

McAdams, D. P. (2001). The Psychology of Life Stories. Review of General Psychology, 5(2), 100–122. https://doi.org/10.1037/1089-2680.5.2.100

Nguyen, C. F. (2013). The ePortfolio as a Living Portal: A Medium for Student Learning, Identity, and Assessment. International Journal of ePortfolio, 3(2), 135-148.

Payne, B. K., Cross, B., & Vandecar-Burdin, T. (2022). Faculty and Advisor Advice for Cybersecurity Students: Liberal Arts, Interdisciplinarity, Experience, Lifelong Learning, Technical Skills, and Hard Work. Journal of Cybersecurity Education, Research & Practice, 2021(2). https://doi.org/10.62915/2472-2707.1095