E-Portfolio Reflection Essay

Cayden Bass-Hensley

Old Dominion University

IDS 493

Professor: Jessica Stanley

Introduction

My Cybersecurity Journey and Interdisciplinary Growth Introduction My name is Cayden Bass-Hensley, and I am a rising junior at Old Dominion University. I am pursuing a degree in cybersecurity, with a minor in communications. I was born and raised on the small island of Saint Kitts in the Caribbean, and I just came to the US in 2019. Cyber security is one of my strongest passions, and currently, I aim to enter into the penetration testing field of cyber security and become a penetration tester. Two skills of mine that I pride myself on are my ability to problem-solve and my adaptability to different situations and cultures. In this reflection, I will discuss several skills that I have practiced and mastered as a student, as well as the artifacts that demonstrate and showcase those skills. Ultimately, most of the artifacts discussed can relate to all the coursework I have done throughout my college career. The skills that accompany each artifact are further detailed throughout this writing. And the skills and competencies margin is how I view those particular skills I gained or practiced.

Skills and Artifacts

One of the most significant skills I have developed through my coursework and hands-on practice is technical competence in cybersecurity. This includes knowledge of network security, vulnerability assessment, penetration testing, and cybersecurity fundamentals. In my paper for CYSE 201S Research paper: PenTesting This artifact, a research paper analyzing social sciences alongside penetration testing, showcases my adaptability, writing, communication, and technical

knowledge skills. Firstly, the ability to write and communicate effectively is seen through the structure and clarity of the paper. I synthesize complex ideas and explain them concisely to the audience. Furthermore, I demonstrate technical knowledge of what penetration testing is, the process of penetration testing, and the skills needed for a PenTesting career. Secondly, the adaptation to different viewpoints and analysis of disciplines such as psychology and pen testing in unison are foundational as an interdisciplinary thinker. I am able to connect different academic concepts to synthesize my plan of action; that is present within the writing. Ultimately, my ability to understand and absorb new information, along with my writing skills, is evident within this artifact. This artifact is a reading on the National Cybersecurity Strategy. While at first, this artifact might seem like something basic. But this reading provided me with career-minded knowledge and information. As national security is a key part of any cybersecurity discipline, this reading became a reference that I will always remember. I am familiar with not just the policy itself but also the legislation and possible legal actions and knowledge associated with this policy. The knowledge gained is key for all security professions and also law professions. Furthermore, the legal and ethical knowledge associated with the NCS is relevant to other fields. But as an asset to me, the reading familiarized me with new terms and concepts in the professional governmental sector. This artifact is a module about the social sciences and their relation to the subject Itn. However, this artifact showcases the development of my reflection and analysis skills. As a student, my ability to reflect on my own performance is critical to my development. But more than my capacity to reflect, my ability to learn from those reflections is the most essential. This module gave me a chance to expand my experience in analyzing different concepts and personal reflections. Ultimately, throughout my college career at ODU, I have developed and practiced reflection and analysis skills. Such skills are crucial to the

development of an interdisciplinary thinker. And as I aim to be, an interdisciplinary thinker is something that I seek to gain. This artifact, a cybersecurity assignment based on TryHackMe, showcases my career-minded thinking and technical cybersecurity knowledge. As a cybersecurity major, I was exposed to real-life cybersecurity challenges and an overview of the knowledge and understanding needed to be a penetration tester. I am able to analyze and reflect on my experience during the TryHackMe exercise, as well as showcase my hands-on knowledge. I demonstrate real-life skills throughout this assignment that are critical to my professional future. My technical cybersecurity skills and knowledge are exposed within this artifact. I also demonstrate other disciplinary interests, such as penetration testing and possible legal challenges, while working as a cybersecurity specialist. Furthermore, as a student, I am exposed to writing, professional analysis, and critical thinking skills. I am able to expose creative analysis and critical reflection knowledge throughout my writing. Ultimately, my ability to reflect and adapt to different challenges is evident within this artifact. This artifact is an exercise based on PowerShell commands. This artifact showcases my analytical and critical thinking skills. As a student, we are asked to complete a series of tasks and questions about PowerShell commands and searching files with specific content. However, throughout this assignment, I demonstrate my skills in being able to analyze and relate data to the topic at hand. While it might be a simple catchphrase, the details and how it was achieved are key. As interdisciplinary thinkers, we encounter information from multiple disciplines daily. As we encounter such, our critical thinking and analysis skills become key to our understanding of those disciplines. Our ability to take different perspectives and think from different professions is how we achieve the interdisciplinary researcher and thinker goal.

Interdisciplinary Research and Policy Analysis

Another critical skill I have developed is the ability to conduct interdisciplinary research and analyze policy. Cybersecurity is not solely a technical field; it exists within a broader social, political, and ethical context. My papers on the social and political implications of the U.S. National Cybersecurity Strategy (2023) exemplify this skill. In CYSE 425W, I analyzed the social implications of the strategy, considering how cultural, generational, and socioeconomic factors influence the implementation and effectiveness of cybersecurity policies. I discovered that while the strategy emphasizes national resilience, it also has unintended consequences for marginalized populations who may lack technical literacy or access to secure technologies (Dunn Cavelty, Eriksen, & Scharte, 2023). This artifact taught me the value of examining cybersecurity issues through an interdisciplinary lens. I learned to integrate concepts from sociology, communications, and political science to understand the societal impact of cybersecurity policies. For example, recognizing that younger generations are more digitally literate while older populations may struggle with new security measures allowed me to think critically about how policies affect different groups. Similarly, my political analysis paper highlighted the partisan divides surrounding regulation, liability, and international cooperation in cybersecurity. Understanding these dynamics reinforced the importance of considering both technical and political factors when evaluating cybersecurity strategies (Alvarez et al. , 2023; Shankar, 2024). This suggests that my work is well researched and that I can use researched ethical evidence to support my claims. This skill reflects one of the course objectives presented in IDS 300W. According to Repko and Szostak (2021), the multidisciplinary process includes steps that help us identify and analyze relevant theories and models and perspectives and then synthesize and

critically evaluate that information to solve real-world problems. Solving the big problems requires us to integrate various disciplines and perspectives. In my case, I used this process to analyze policy solutions for cybersecurity problems. That would not be enough; many of my papers required me to learn other disciplines' concepts and use them in my writing. This suggests my work is well rounded, and it would match up with what an employer will look for.

Ethical Reasoning and Legal Awareness

My skills in ethical and legal reasoning seem to continue to improve every year. As learned in CYSE 406 Cyber Law and PHIL 355E Cybersecurity Ethics, applying ethical and legal concepts in my work will make me a well-rounded employee. Like what I did to analyze regulations in my pentesting paper. They are put in place to prevent some pentest participant from hacking the system for their own personal gain (Geer & Harthorne, 2002). That involved researching legal concepts and analyzing how to apply them to the technical discipline of pentesting. In other instances, I would be asked to analyze ethical, legal, and social dimensions of cybersecurity issues. They are disciplines that are important to the world. They show that we cannot rely on technology alone without considering how it will affect the environment and society in general. These laws and regulations make me concerned about ethical and social issues when testing a system for vulnerabilities. In addition, using principles of ethics and laws to answer such questions equipped me with the right responsibility and decision-making abilities. Inclusion of such ethical components into students' science is also agreed upon by other scholars. For example, Neil C. Rowe and Myrne Johnstone's articles imply that HST scripts and cybersecurity research should be responsible and ethical: From my experience, ethics,

thoroughness, and transparency in testing are the best predictors of social-engineering tests. success, as well as observance of legalities (Hatfield, 2019, p. 81); however, such interventions are embedded in social-technical systems that are not only technical to deal with but also demand a concern for other users in good faith (Dunn Cavelty et al., 2023, p. 19). From writing those papers and connecting them with those materials, I believe that my professionalism is evolving.

Communication and Professionalism

Another contribution of my education is learnings on communication. In cybersecurity, enhancing communication skills is as important as technical skills. This is because a huge amount of knowledge, data, and results are often exchanged between cybersecurity experts and organizations, government officials, and businesses. In my penetration testing paper, I also wrote, Good communication skills are required in various arenas throughout the process, such as communicating risks to stakeholders, writing reports, and explaining results with stakeholders, which Geer and Harthorne (2002) suggest as the primary capability a pentest expert needs. This underscored the importance of communication, that it is significant to reduce the risk of potentially harmful human parts in the process/path/systems (requiring communication skills, etc.), and that the communication results can be used to enhance that system. Also, minoring in a communication discipline allows me to improve my communication skills. Through many classes like public speaking, collaborative group work, literature writing, and science writing, my communication is enhanced. In both my social and political papers, I also practiced my communication skills, referring to political debates and controversial topics. I had to explain complicated cybersecurity laws and policies, such as cybersecurity acts and FISA, in a simple

way so that potential readers can easily understand them. This required careful attention to language, structure, and clarity. which I continue to refine through both academic and extracurricular experiences. Beyond written communication, I have developed professional skills such as leadership, teamwork, and time management through my involvement in student organizations like the Old Dominion Cyber Security Student Association and volunteer activities in my community. Managing group projects and coordinating events has improved my ability to collaborate with others, resolve conflicts, and prioritize tasks, skills that are directly transferable to professional cybersecurity work.

Application to Career Readiness

All of these skills, technical competence, interdisciplinary research, ethical reasoning, and communication, converge to prepare me for a career as a penetration tester. Penetration testing requires not only the ability to identify and exploit vulnerabilities but also an understanding of human behavior, organizational culture, and legal frameworks. By integrating insights from social sciences, communications, and policy analysis, I can approach cybersecurity challenges with a holistic perspective. For instance, my understanding of social engineering, cultural influences, and policy implications allows me to anticipate how users and organizations might respond to security measures. Similarly, my technical skills enable me to conduct thorough assessments and generate actionable reports. The combination of these skills reflects the interdisciplinary approach emphasized in IDS 300W and aligns with best practices in professional cybersecurity. Research suggests that successful cybersecurity practitioners are those who can bridge technical expertise with strategic thinking, ethical judgment, and effective

communication (Nielsen & Scarfone, 2020; Von Solms & Van Niekerk, 2013). Also, these assignments (TryHackMe, Cyber Fast Track, and the Coastal Virginia Cybersecurity Student Association) have allowed me to practice what I have been learning not only from this class but have also given me confidence that I know basic skills to solve real-world scenarios, along with providing a portfolio of artifacts that I can show future employers my capabilities.

Conclusion

In conclusion, I have developed several critical skills throughout my college education as a student. I have practiced and mastered different skills and analysis, through the several exercises and assignments I have completed. Also, I am aware that I still need to practice and work on different disciplines as well as my own critical thinking. But as I am a student, my ability to self-reflect on and improve my work, is something that I look forward to and enjoy doing. Furthermore, my goal to become an interdisciplinary thinker is on the right path and moving forth towards progress. All in all, improvement is a goal for the future and being able to analyze my own ideas is a valuable skill that all students should possess. First and foremost, I developed technical skills related to cybersecurity and computing throughout my classes and various practices. I learned to use skills such as network vulnerability assessment and penetration testing of systems which are crucial on network security. For instance, I learned some of the knowledge through writing CYSE 201S paper that title is Cybersecurity Career: Penetration Tester in which I applied the knowledge of social engineering to the career of Penetration Tester. While writing this paper, I have used some psychological concepts I learned such as cognitive bias and how those concepts influenced the society; for example, 7 principles, a few of them are

likability bias, and reciprocity. I used the structure of the concepts on one project scenario that committed cybercrime in the introduction of the memo. Since I was not a psychology major, I did not know how those strategies are immensely used maliciously in the world. This paper made me recognize how my planned career is significant to this world as a gatekeeper but more importantly, how I can enhance my ability based on technical knowledge with social science knowledge as the author mentions this is strategic advantage [penetration testing] helps organizations identify both technological and human vulnerabilities that could cause a security breach (Hatfield, 2018). For me, this is why gaining technical knowledge and skills through various classworks such as CS 462 Cybersecurity Fundamentals, and IT 315 Networks & Security is truly important as the responsibility of the Penetration Tester. These two classes taught me various topics such as malware, virus, cyber forensic, Linux and Unix operation, firewalls for cyber security, and so on. Those learning experiences truly helped me when I did the TryHackMe mission for the application process and during Cyber Fast Track; hence, lots of fundamental networking knowledge is required for the missions that guide students on how hackers attack certain systems. In this journey, I learned that TryHackMe and Cyber Fast Track are the places where we should explore attacks on computer and network systems without compromising ethical principles while strengthening both attacking and defending points of view skills simultaneously. These experiences demonstrated that technical competence in cybersecurity is not only about learning specific tools or protocols but also about developing a mindset that anticipates, analyzes, and mitigates threats effectively.

References

Alvarez, D., Jehl, L., Chanin, N., & Putnam, A. (2023). The U.S. National Cybersecurity Strategy: Key Takeaways. Willkie Farr & Gallagher.

Dunn Cavelty, M., Eriksen, C., & Scharte, B. (2023). Making cyber security more resilient: Adding social considerations to technological fixes. *Journal of Risk Research, 26*(7), 801-814.

Geer, D., & Harthorne, J. (2002, December). Penetration testing: A duet. In *18th Annual Computer Security Applications Conference* (pp. 185–195). IEEE.

Hatfield, J. M. (2019). Virtuous human hacking: The ethics of social engineering in penetration-testing. *Computers & Security, 83*, 354–366.

Nielsen, L., & Scarfone, K. (2020). *Cybersecurity workforce development: A competency-based approach*. National Institute of Standards and Technology.

Repko, A., & Szostak, R. (2021). *Interdisciplinary research: Process and theory*. Sage Publications.

Shankar, N. (2024). The Biden Administration's National Cybersecurity Strategy: Opportunities and Challenges. *Middle East Institute*.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97–102.