Reflection on Skills and Artifacts: Interdisciplinary Learning in Cybersecurity

Brei White
IDS 493
Dr. Tucker Steffen
April 20, 2024

Reflection on Skills and Artifacts: Interdisciplinary Learning in Cybersecurity

Introduction

As a student in cybersecurity, I've developed a range of skills that span technical expertise and interdisciplinary knowledge. Through coursework and experiences, I've gained proficiency in areas such as Unix/Linux systems, policy analysis, networking, and various other cybersecurity skills. In this reflection essay, I'll explore how nine artifacts demonstrate my growth in these areas and illustrate how interdisciplinary learning has prepared me for a career in cybersecurity. By analyzing each artifact, I'll showcase the skills I've acquired over the years.

Artifact 1: Password Cracking

Password cracking is a crucial skill in cybersecurity, enabling professionals to assess password strength and uncover vulnerabilities in authentication systems. The password cracking lab exercise provided me with hands-on experience in utilizing password cracking tools and techniques to analyze password hashes and retrieve plaintext passwords. Through this exercise, I learned to identify common password vulnerabilities, such as weak passwords and inadequate hashing algorithms, and implement measures to bolster password security. Course readings and lab exercises offered theoretical insights into cryptography and password security, while practical assignments allowed me to apply this knowledge in simulated cybersecurity scenarios.

Mastering password cracking techniques equipped me with skills in vulnerability assessment, penetration testing, and risk mitigation, essential for safeguarding sensitive information and thwarting unauthorized access attempts. Understanding the methods used by malicious actors is crucial for maintaining network and system security. By learning to crack passwords using tools like John the Ripper, I gained insights into the challenges of protecting against dictionary attacks. During the lab, I created demo users with varying password complexities and successfully cracked a password after running it through John the Ripper for 10 minutes. This experience underscored the importance of strong passwords in mitigating security risks posed by hackers.

Artifact 2: File Permission

Another Linux-based skill that I acquired is setting file permissions. To demonstrate this skill, I performed a lab where I created three groups using the groupadd command. I then assigned home directories to all users within these groups and created generic passwords for each user. Next, I established a new group and designated it as a secondary group for all three previously created demo users. Following this, I created a directory to serve as a shared space for collaboration among users. I then adjusted the file permissions to restrict access to this directory

to only members of the designated group. This exercise illustrated how to create a shared directory for collaborative purposes while implementing file permissions to enhance security. By configuring file permissions, I learned to safeguard the integrity, confidentiality, and availability of the contents within the directory, thereby ensuring secure collaboration among users.

Artifact 3: Shell Scripting

To further advance my technical skills, I engaged in a task involving shell scripting to streamline routine processes. Task A involved the creation of script code utilizing an if-else statement. The script ensured that user input was transformed into lowercase and fell within the range of 4 to 8 characters. If the input failed to meet these criteria, an error message was generated. This exercise honed my proficiency in scripting fundamentals, particularly in implementing conditional statements to enforce input validation and error handling. Task B further expanded my scripting prowess by focusing on directory manipulation. The script code facilitated the creation of new directories using an if-else statement. The script first checked for the pre-existence of the directory. If the directory already existed or if it was identified as a regular file, the script displayed the contents of the file. Conversely, if the directory did not exist, a new directory was created. This task exemplified my ability to leverage scripting for file system management and automation of routine administrative tasks. By practicing shell scripting techniques, I acquired a valuable skill set essential for automating repetitive tasks and optimizing operational efficiency in cybersecurity operations. These tasks not only solidified my understanding of scripting fundamentals but also underscored the significance of automation in streamlining cybersecurity workflows and enhancing overall productivity.

Artifact 4: Assessing Cybersecurity Policy Effectiveness

Cybersecurity professionals must also possess expertise in policy analysis and regulatory compliance. The policy analysis report on cybersecurity policy offered me an opportunity to explore the legal and regulatory frameworks governing cybersecurity and assess their implications for organizational security practices. This artifact presents a comprehensive approach to policy impact assessment, drawing insights from scholarly literature across economic, social, political, and ethical dimensions. Scholarly contributions, such as Hayes and Kotwica's evaluation of the Bring Your Own Device (BYOD) policy, offer insights that speak about productivity, the pros and cons, and the potential risks and liabilities (Hayes & Kotwica, n.d.). By integrating insights from policy analysis, risk management, and legal studies, I formulated comprehensive incident response policies to address cyber threats and data breaches. Through this process, I gained a deeper understanding of regulatory compliance, incident handling procedures, and crisis management strategies.

Artifact 5: Incident Response Policy

In the realm of cybersecurity, the development and implementation of an effective incident response policy are important for organizations to mitigate risks and ensure operational resilience. It is important for the cybersecurity profession to understand incident response policies and even know how to create them. Developing and implementing an incident response policy has increased my skills in cybersecurity risk management and crisis response. Guided by frameworks like the National Institute of Standards and Technology (NIST) framework and the incident handling guide, I've acquired the ability to systematically address cyber threats and mitigate risks (Cockcroft, 2020; Computer Security Incident Handling Guide - NIST, n.d.). This research paper has equipped me with the proficiency to define structured incident response procedures involving containment, eradication, and recovery strategies (Darren Death & Death, 2017). By establishing network baselines and conducting pre-incident preparations, I've learned to enhance threat detection capabilities, enabling a quick response. Moreover, the implementation of containment measures and eradication efforts has refined my skills in addressing security breaches and removing malicious elements from systems (Computer Security Incident Handling Guide - NIST, n.d.).

Artifact 6: Interdisciplinary Analysis of AI in the Criminal Justice System

My exploration of AI in the criminal justice system, particularly its impact on Black Americans, underscores my awareness of cybersecurity ethics. By integrating insights from computer science, law, sociology, and critical race theory, I've criticized AI's biases and ethical implications. Ethical philosophy guided my evaluation of punishment theories' alignment with AI-driven decisions, while considerations of biological factors and neuroimaging highlighted potential racial biases. I've emphasized the importance of transparency and accountability in AI systems, advocating for regulatory frameworks to ensure fairness. The solutions that I came up with include developing bias-resistant algorithms and promoting public awareness. This artifact reflects my commitment to upholding cybersecurity ethics and safeguarding marginalized communities' rights. I've demonstrated readiness to address complex ethical issues in emerging technologies, exemplifying ethical practices in cybersecurity.

Artifact 7: Wiring Maury High School

In my wiring project, I showcased my networking skills alongside my proficiency in project budget management. I planned the network infrastructure of a 54 classroom high school. Beginning with a detailed assessment, I proposed a budget plan outlining equipment, materials, and labor costs, ensuring cost-effectiveness without compromising quality. I researched vendors to secure competitive pricing, optimizing resource utilization. I successfully implemented a robust wired network infrastructure, using industry-standard equipment and best practices. This artifact demonstrates my ability to balance technical requirements with financial considerations,

ensuring the project's success within the allocated budget. It underscores my proficiency in networking and project management, essential skills in the cybersecurity field.

Artifact 8: College Building Wiring Project

For the College Building Wiring Project, I demonstrated my networking expertise and project management skills. The plan encompassed wiring installations for both the first and second floors, strategically connecting access switches, distribution switches, and core switches to ensure seamless connectivity throughout the building. This project is similar to the one where I wired Mary High School, except in this project i also had to connect the network to the campus backbone.

Artifact 9: Router Tables

In the Router Table Configuration Project, I demonstrated my proficiency in configuring router tables, WAN ports, and LAN ports, highlighting my networking expertise. The project involved configuring router tables to optimize network performance and ensure seamless communication between Wide Area Network (WAN) and Local Area Network (LAN) devices. I analyzed the network topology and determined the most efficient routing protocols to use.

Conclusion

In conclusion, my academic journey in cybersecurity has been characterized by interdisciplinary inquiry. Through engaging with diverse disciplines and experiences, I have developed a versatile skill set essential for success in today's dynamic and multifaceted cybersecurity landscape. In classes like my interdisciplinary studies course, I was taught to look at issues through multiple lenses so that I am able to create the most optimal solutions. Each artifact presented in this reflection essay represents a unique discipline of technical expertise, critical thinking, and interdisciplinary knowledge, reflecting the depth and span of my academic and professional development. Moving forward, I am confident in my ability to use my interdisciplinary background to address complex cybersecurity challenges and make meaningful contributions to the field. As a cybersecurity professional, I am prepared to navigate evolving threats, protect critical assets, and safeguard digital ecosystems for the benefit of society and organizations alike.

References

Cockcroft, S. (2020). What is the NIST Framework? ITNow, 62(4), 48-49.

Computer Security Incident Handling Guide - NIST. (n.d.).https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Darren Death., & Death. (2017). Information Security Handbook [e-book] Develop a Threat Model and Incident
Response Strategy to Build a Strong Information Security Framework.

Fowler, B., & Maranga, K. M. (2022). Cybersecurity Public Policy. https://doi.org/10.1201/9781003259145

Hayes, B., & Kotwica, K. (2013). Bring Your Own Device (BYOD) to Work [electronic Resource] Trend Report. ProQuest Ebook Central - Reader. (n.d.).