Reflection Essay

Darren Pritchard

IDS493

Dr. Sherron Gordon-Chan

Old Dominion University

Running head: REFLECTION ESSAY

Introduction

In the digital age of education, the e-portfolio has emerged as a powerful tool for both learners and educators, providing an interactive platform to showcase one's academic journey and accomplishments. As I embarked on the endeavor of creating an e-portfolio for my university class, I found myself not only documenting my academic achievements but also delving into a process that demanded introspection, critical analysis, and a meticulous curation of my work. This reflective essay delves into the profound odyssey of constructing this digital portfolio, unraveling the intricacies and challenges encountered while crafting each of the nine artifacts that collectively narrate my academic evolution. Beyond a mere compilation of assignments, this e-portfolio became a chronicle of the trials and triumphs that have shaped my learning experience. From wrestling with intricate concepts to mastering diverse formats of expression, the journey to complete these artifacts unearthed a spectrum of obstacles that offered me unparalleled opportunities for growth. Each artifact stands as a testament not only to my academic prowess but also to the resilience and determination that accompany the pursuit of knowledge. Join me as I traverse through the labyrinth of challenges faced while constructing this e-portfolio, shedding light on the valuable insights gained through the process of overcoming these difficulties and ultimately emerging with a profound sense of accomplishment and self-discovery.

Network Security

Among the most vital skills for my professional life I’ve learned in my academic life, the exploration of "network security" emerged as a pivotal theme. As I delved into this complex realm, I grappled with deciphering the intricate layers of safeguarding digital networks against an ever-evolving landscape of cyber threats. The process of creating an artifact that encapsulated my understanding of network security unveiled a series of obstacles, from comprehending the diverse array of potential vulnerabilities to mastering the diverse range of protective measures that fortify digital infrastructures. The journey required me to navigate through technical jargon, comprehend the intricacies of encryption protocols, and engage with the ethical considerations surrounding data privacy and cybercrime. Through the lens of network security, I not only honed a technical skill set but also developed a heightened sense of responsibility in an interconnected world where the fortification of digital landscapes is an imperative. The difficulties faced in encapsulating this complex concept in a coherent and concise manner illuminated the importance of effective communication in translating technical expertise to a wider audience. The reflection on my struggle to articulate network security within my e-portfolio underscores the value of tenacity in the face of challenges and the imperative of continuously adapting to the dynamic domain of digital security.

Network Scanning

The Cybersecurity Techniques and Operations (CYSE 301) course introduced

processes required of effective network analysis and security. (Old Dominion University, 2023) Before even beginning to consider the techniques one needs to properly secure a network, a cybersecurity professional needs to use various network scanning and analysis tools in order to better understand the proper layout and topography of a network, and better understand its vulnerabilities. Understanding these vulnerabilities helps us better understand how we can better secure a network. The assignment I used for Artifact I, entitled “Sword Vs. Shield,” best represents my skills regarding this.

I began this assignment with first scanning a Windows 2008 virtual machine with a Kali Linux virtual machine to first learn the network topography and any open ports the machine has. Open ports can mean an attack vector for a potential assailant, and in this case, the kali machine was representing one such attacker. This was all monitored by the Ubuntu Virtual Machine, which can represent a potential cybersecurity professional watching over the Windows 2008 server to see who connects to it and what they do. I note the dramatic amount of traffic coming in to the Windows 2008 machine and write my responses down in the corresponding short essay.

Ethical Hacking

Artifact 2 represents the fun part of being a cybersecurity professional, in my opinion. Ethical hacking is a necessary task in network security by vexing and finding the vulnerabilities in a network, thus making sure that they aren't vulnerable to assailants. In this assignment, I start it off again in control of a Kali Linux virtual machine, which is a virtual environment meant to simulate a real-world attacker, and I am targeting a Windows XP virtual machine. I start off by scanning for vulnerable ports, and find out that port 445 is open and was the most likely avenue for attack. I then prepare the appropriate payload for this system and gain access to it. I then perform the necessary actions to prove my access to the system, namely screenshots of the desktop of this virtual machine.

Password Cracking

Secure passwords are the bedrock of a successful network security policy and it is vital that each password is sufficiently secure. Passwords are able to be targeted by brute force attacks, and as such, are always under threat when they're not strong enough. A vital part of password security is understanding the mechanics by which you make a sufficiently strong password, which is by increasing its length, and thus, its entropy. The amount of entropy a password has, the more difficult it is to crack. Artifact III is an assignment in which I, again as an attacker, successfully attempt to crack a number of vulnerable passwords on a vulnerable network, which leads to me gaining access to it. I do this by first analyzing the results of a packet capture file, which contains instances of someone logging into this network, from which I can take the encrypted password and crack the encryption, descrambling the correct password for the network.

Research

In the realm of cybersecurity, research is a vital skill that serves as a strong defense against evolving threats. Creating an e-portfolio artifact about the importance of research in cybersecurity highlighted the need to stay ahead by exploring vulnerabilities, understanding new risks, and anticipating potential attacks. Navigating through complex research papers and incident reports showcased the value of being proactive in this field. Summarizing intricate research findings also emphasized the skill of translating technical details for different audiences. Ultimately, this artifact underscored how research acts as a powerful tool, equipping us with the knowledge needed to effectively safeguard digital landscapes.

Machine Learning in Intrusion Detection Sytems

In the landscape of cybersecurity, the effective fortification of networks hinges upon the integration of advanced technologies. In my research article, I delved into the realm of intrusion detection systems, with a specific focus on the transformative role of machine learning. Just as secure passwords form the foundation of a robust network security policy, the strategic deployment of machine learning algorithms stands as a critical shield against modern cyber threats. By analyzing vast streams of data, these algorithms have the capacity to discern anomalous patterns, swiftly identifying potential breaches before they escalate. Just as the mechanics of constructing a strong password rely on increasing its entropy, the potency of machine learning-powered intrusion detection systems lies in their ability to process and comprehend complex data sets. Through meticulous analysis and evaluation, my research article sheds light on how the amalgamation of machine learning and intrusion detection not only bolsters the resilience of digital landscapes but also exemplifies the dynamic synergy between cutting-edge technology and proactive cybersecurity strategies. In Artifact IV, I wrote about how these machine learning algorithms are being used in modern intrusion detection systems.

Risks and Vulnerabilities of AI in Financial Systems

In the intricate realm of modern finance, the adoption of Artificial Intelligence (AI) introduces a paradigm shift that demands meticulous scrutiny of risks and vulnerabilities. In my essay, I meticulously dissect the potential threats AI poses to financial institutions, akin to the vulnerability of passwords to brute force attacks. Just as secure passwords are essential to thwart cyber intrusions, comprehending the multifaceted risks of AI is crucial to safeguard the integrity of financial systems. By harnessing AI's prowess, financial institutions can automate processes, optimize investments, and enhance customer experiences. However, akin to the complexity of deciphering encrypted passwords, the intricate algorithms of AI can become susceptible to manipulation, leading to unintended consequences. My essay delves into these intricacies, illustrating how the dynamic interplay between AI's innovation and the vulnerabilities it presents forms a narrative akin to the art of intrusion detection. By thoroughly dissecting these potential pitfalls, my research underscores the paramount importance of a balanced approach, where the potential rewards of AI in finance are maximized while actively mitigating the associated risks, thus resonating with the essence of a robust cybersecurity strategy. In artifact V, I wrote about such risks and vulnerabilities after an extended research period.

Security Policy for an Information System

In Artifact VI, I wrote a security policy for a small theoretical information system. In the ever-evolving landscape of information systems, the establishment of a robust security policy serves as the linchpin for safeguarding digital assets. My essay delves into the intricate process of crafting a viable security policy, drawing parallels to the meticulous construction of impregnable passwords. Just as secure passwords are pivotal to fortifying network security, a comprehensive security policy forms the cornerstone of an information system's resilience. By defining access controls, encryption protocols, and incident response plans, such policies emulate the complexity of password mechanics that enhance their strength. However, akin to the task of creating a secure password, devising a practical and effective security policy necessitates a delicate balance. My essay navigates through the nuances of aligning policy stringency with operational efficiency, much like the careful calibration of a password's complexity to rememberability. By intricately dissecting the elements of policy formulation, my research underscores the imperative of a holistic approach that harmonizes stringent security measures with the flexible functionalities an information system requires, mirroring the essence of orchestrating robust cybersecurity strategies.

Written Communication

Writing accurate articles that correctly document and report on relevant information is a vital part of cybersecurity and is required almost every day. In the intricate realm of cybersecurity, where the smallest oversight can lead to significant breaches, the importance of accurate written communications stands as an unwavering pillar. Much like the precision required to code intricate algorithms, the art of conveying information with exactness is critical to effective cybersecurity practices. Whether it's documenting security protocols, crafting incident reports, or articulating policy guidelines, the clarity and accuracy of written communications serve as a shield against misunderstandings that could lead to vulnerabilities. Just as a single line of code can impact an entire system, a poorly communicated directive can compromise an organization's security posture. Myriad challenges in cybersecurity stem from misinterpreted instructions or unclear documentation, underscoring how the meticulousness of accurate written communications parallels the exactitude demanded by securing digital landscapes. As my exploration of this facet within my e-portfolio demonstrates, the potency of precision in communication resonates throughout the domain of cybersecurity, forming a linchpin that fortifies defenses against the ever-evolving landscape of cyber threats.

The SolarWinds Hack: How, Why, and What Could’ve Prevented it

Artifact VII deals with an essay I wrote on the SolarWinds hack. The SolarWinds hack emerged as a watershed event, reshaping the paradigm of cybersecurity on a global scale. My essay dissects the multifaceted implications of the SolarWinds hack, akin to a deep analysis of a sophisticated attack vector. Much like studying the mechanics of a breach, my exploration delves into the methods used to infiltrate SolarWinds' software supply chain, illustrating how vulnerabilities in one node can reverberate through an entire network. As I navigated through the intricacies of this attack within my essay, parallels emerged between the SolarWinds hack and the intricate process of identifying weaknesses in complex systems. The breach highlighted the strategic interplay of tactics such as lateral movement, stealthy data exfiltration, and evasive techniques, reflecting the complexity akin to solving a cryptic puzzle. By examining the aftermath, response strategies, and the broader lessons for cybersecurity, my essay not only underscored the interconnected nature of digital vulnerabilities but also emphasized the necessity of proactive defense mechanisms. Just as dissecting the SolarWinds hack unveils the intricate web of cyber espionage, my exploration illuminated the pivotal role of continuous adaptation and vigilance in safeguarding digital landscapes against evolving threats.

Ethical Reflections on Google Street View: A Deontological Analysis

Artifact VIII is an essay I’ve written on the ethical problems regarding Google Street View and its implementation. This was argued from the standpoint of deontology, which is a philosophical school founded by philosopher Emanuel Kant, and showcases the interdisciplinary aspects of cybersecurity. In a landscape shaped by rapid technological advancements, my essay scrutinizes the ethical intricacies surrounding the implementation of Google Street View, approaching the issue through the lens of deontological ethics. Much like dissecting a complex algorithm, my exploration delves into the fundamental principles and duties that underpin this technological innovation. From the standpoint of deontological ethics, concerns arise not only about the invasion of privacy and the potential for unintended data collection but also about the broader ethical obligations that underlie such implementations. Just as evaluating a program's code requires a deep understanding of its functions, my essay delves into the underlying motivations and consequences of Google Street View. The analysis echoes the meticulous process of ethical reflection, spotlighting the tension between technological progress and the preservation of individual rights. As my exploration illustrates, the ethical implications surrounding Google Street View unfold as a nuanced discourse that prompts a deeper inquiry into the moral obligations inherent in the application of advanced technologies in our interconnected society.

Effectiveness of Diceware Passwords: A Security Review

Artifact IX delves into the ingenious application of the Diceware method for generating passwords. Much like unraveling the mechanics of an intricate code, my exploration sheds light on how this technique, characterized by its straightforwardness, evolves into a powerful tool for bolstering online safety. By dissecting the essence of Diceware, my essay elucidates how it involves generating strong passwords by selecting random words from a list created through dice rolls. This process draws parallels with the meticulous assembly of cryptographic components, underscoring the significance of unpredictability and variety. Additionally, my investigation delves into the art of crafting passphrases, revealing their resilience against diverse password cracking tactics. Just as comprehending the architecture of a security system is pivotal, my research accentuates how the Diceware method withstands brute force attacks and augments overall password security. In essence, my essay underscores how Diceware encapsulates the sophistication of robust security practices, exemplifying the potential of uncomplicated yet potent approaches in reinforcing digital safeguards.

References

Old Dominion University. (2022). *Cybersecurity Courses.* School of Cybersecurity. Retrieved August 5th, 2023, from https://catalog.odu.edu/undergraduate/schoolofcybersecurity/