Reflection

Diana Y. Solorzano

Department of Cybersecurity, Old Dominion University

IDS 493: Electronic Portfolio Project

Dr. Sherron Gordon-Phan

August 03, 2024

IDS 493 Reflection

Abstract

This reflection paper analyzes the growth and development of my skills and experiences in my professional and academic career. The artifacts used to support my skills will be pulled from different courses taken while completing my bachelor's degree in cybersecurity. Analyzing in depth the different artifacts will allow me to demonstrate how I have refined my technical skills, analysis skills, and critical thinking skills.

Introduction

Over the years I have had the opportunity to gains valuable skills and experiences in my personal and professional life. Mastering my troubleshooting skills as an aircraft mechanic, leadership skills in being a supervisor, and even communication skills when planning and coordinating volunteering events. During my time at Old Dominion University pursuing my bachelor's degree in Cybersecurity, I have had the opportunity to refine and gain more skills and experiences. Many of my classes focus on learning technical skills and understanding how to analyze policies. Three skills that I have mastered during my academic year have been a variety of technical skills, critical thinking, and analysis. These skills stand out to me because they are vital skill as move forward into advancing my professional career. A career in cybersecurity requires its professionals to have a fundamental understanding of how IT infrastructure works, analyze new policies and procedures, and be able to critically think to resolve issues. I will explain how each artifact listed showcases the skills I have learned throughout my academic career.

Technical

IDS 493 Reflection

Technical skills are extremely valuable in any position within the cybersecurity field. Some may say even required. Cybersecurity professionals at a minimum need to have a fundamental understanding of the IT infrastructure. Old Dominion University's cybersecurity program includes plenty of courses that focus on teaching valuable and relevant technical skills needed to pursue a career in cybersecurity. Throughout my courses, I have had the opportunity to learn how to code in Python, network security, and Kali Linux. Not only was I able to learn these skills, but I was also able to apply them to projects in order to demonstrate that I am also able to apply what I have learned to real situations.

My first technical artifact listed is a project assignment for my CYSE 450 Ethical Hacking and Penetration Testing course. This assignment was aimed at completing a successful SQL Injection using Metasploitable2. Being able to understand how malicious attacks are executed is a valuable skills for professionals wanting to go into the cybersecurity field. This assignment required me to use a secondary Kali Linux VM in order to create an account using command lines. I was able to successfully execute an SQL Injection using sqlmap. This malicious code allowed me to get usernames and passwords from the website's database. It also taught me what some vulnerabilities organizations need to have when creating websites.

My second artifact listed is another project assignment from my CYSE 450 Ethical Hacking and Penetration Testing course. This assignment was aimed at completing a successful automated SQL Injection using Cross Site Scripting (XSS). This assignment is built on precious ones with the addition of automation. Professionals need to not only know how to execute malicious attacks but also do it in an effective manner to prevent realistic attacks. I was able to use different hacking tools in order to successfully execute this attack.

My third artifact listed is a final project from my CYSE 250 Cybersecurity Programming and Networking course. This course not only taught me technical skills in network security by Python coding as well. The goal of this project was to create a database server that communicated with a client in order for users to play a music trivia game. This project forced to so search for outside sources. I had a fundamental understanding of how to program using this language but was struggling to apply the knowledge to being able to create a game that worked. In the end, I was able to program an interactive game that successfully had the client and server communicate with one another.

Critical Thinking

As a cybersecurity professional, being able to critically think about situations will be needed in order to resolve solutions in the most effective way possible. While there are many ways to resolve IT issues, some resolutions are better than others. This is where being able to critically analyze situations will become vital. During my time at Old Dominion University, I had the opportunity to take CYSE 425W Cyber Strategy and Policy. This course forced me to analyze different policies and their strategies in order to understand how they came to what. Analyzing different factors that contributed to these policies was vital to understanding why and how these policies came to be. Throughout this course, I choose to focus on the Online Age Verification Policy. Not just what the policy itself was, but also who it affected and what contributed to its creation.

My first artifact listed is my Policy Analysis Paper 1 from my CYE 425W Cyber Strategy and Policy course. This paper was focused on analyzing a cyber policy and understanding why it had been implemented. I researched the Incident Response Plan / Policy and was able to get a better understanding of not only what it was but also how it can be used. After this paper

analysis, I decided to change my policy moving forward since it was more of a best practice rather than a cyber policy that affects the general public.

My second artifact listed is my Policy Analysis Paper 2 from my CYE 425W Cyber Strategy and Policy course. For this paper, I decided to change directions in the policy I was analyzing and decided to further research the Online Age Verification Policy. While completing this assignment, I was able to understand that the origin of this policy came about as a form of protecting minors. While the policy had good intentions, I discovered that there were some ethical issues that conflicted with individual rights. Throughout this paper I had to analyze and explain whether or not the claims were true and how could this policy have been affected by those who sponsored it.

My third artifact listed is my Policy Analysis Paper 4 from my CYSE 425W Cyber Strategy and Policy course. For this paper, I decided to further investigate the Online Age Verification Policy to understand how different policymakers had an influence on the policies and the changes they had the further they moved up. During this research, I looked into the policymakers and the general idea of what they supported in order to understand their influence on the policy I was analyzing. After the completion of this assignment, I was able to understand that even for technical policies many outside factors play a role in how these policies are shaped. Each assignment forced me to think more critically about the policy in place.

Analysis

Being able to analyze situations and trends is vital in a career field that is constantly changing. Throughout different courses at Old Dominion University, I was asked to write a paper analyzing a specific topic and the effects it had, all related to cybersecurity. The three artifacts

that I have chosen to showcase my analysis skills are CYSE 280 Windows Systems Management and Security, CYSE 425W Cyber Strategy and Policy, and CYSE 495 Human Factors and Policy in Cybersecurity. Each one of these classes forced me to analyze a topic or policy in order to have a strong understanding of not only what it was but also how it came to be. I was then asked to make the correlation of how the specific topic analyzed had affected the cyber security world. These research papers were focused around the evolution of Microsoft Malware, the evolution and effect of cyber policies, and how organizations are affected by social engineering attacks. Each assignment refined my ability to analyze concepts to a deeper understanding.

My first artifact listed is my Final Research Paper from my CYSE 280 Windows Systems Management and Security course. This final paper was focused on analyzing the evolution of Microsoft malware and its impact on cyber-attacks. I began by analyzing and researching the different types of Microsoft products and how they became a powerhouse in the IT world. In then looked into different malware that used some type of Microsoft product in their malware deployments and how they have developed over time. Finally, I analyzed the impact these types of malware attacks have had on Microsoft as a company as a whole.

My second artifact listed is my Midterm assignment for my CYSE 425W Cyber Strategy and Policy, and CYSE 495 Human Factors and Policy in Cybersecurity course. In this paper, I took a deeper look at understanding how the National Cybersecurity Strategy worked and why it existed. I was able to understand the goals intended by our government as well. Finally, I was forced to analyze whether or not the goals listed were achievable in current times.

My third artifact listed is my Final paper for my CYSE 495 Human Factors and Policy in Cybersecurity course. For this final paper, I decided to research and further analyze what social engineering was and how it had developed over the years. I was able to learn about the different

techniques used to execute these types of attacks and just how evolved they had become just within the last 5 years. This paper wasn't just about researching social engineering attacks, it also required me to understand and explain the impact these types of attacks had on organizations and finally provide effective ways to prevent these attacks.