Antonio Shields' ePortfolio:

Reflection Essay

Antonio Shields

Old Dominion University

IDS 493: Electronic Portfolio Project

Dr. Virginia Tucker Steffen

April 18, 2024

Abstract

The purpose of this reflection essay is to summarize the three most important skills, I feel, I have gained or enhanced during my time at Old Dominion University while pursuing my Bachelor of Science degree in Cybersecurity. Using a total of nine collected highlighted projects and assignments from a variety of courses in my curriculum, I will demonstrate how my technical skills, problem-solving & critical thinking skills, and written communication skills have been shaped so far throughout my cybersecurity journey. As a cybersecurity professional, I will continue to add to the foundational aspects displayed here in my ePortfolio as my knowledge and abilities expand concurrently with the evolution of technology and resources as my career progresses.

Antonio Shields' ePortfolio: Reflection Essay

According to Reynolds and Davis (2014), "a portfolio is a meaningful collection of selected artifacts or documents, collected over time and across interests" (p. 1). These collected artifacts should also demonstrate learning by providing the opportunity for reflection on what has been accomplished to date. An electronic portfolio or ePortfolio is a type of portfolio that takes those collected artifacts, uses the convenience and easy accessibility of technology, and allows you to exhibit and highlight areas along your learning journey in a visual fashion. Regardless of the type of portfolio method used, its intended purpose, or its focus, Reynolds and Davis (2014) mention that they all require some element of writing to provide context, description, explanation, and analysis of the included artifacts, which will be relayed throughout this reflective essay (p. 1). Reflective learning, according to Reynolds and Davis (2014), is conducting a conscious or deliberate self-assessment of the successes and any difficulties encountered throughout the production of the artifact you chose and the lessons learned that can assist you in the future (p. 2).

During my matriculation at Old Dominion University, while shorter than a traditional four-year timeframe because of being a second-degree seeking student and having prior education, my journey over the last two years towards receiving my Bachelor of Science in Cybersecurity degree has been an informative and enlightening one. In that timeframe, I have accumulated many assignments that vary in difficulty and interest. Although they are all important to the objectives of their respective courses, this ePortfolio allows me the opportunity to provide a snapshot of some of the curriculum coursework, newly acquired skills, and other skills that have been enhanced throughout my educational journey.

As a cybersecurity student and future cybersecurity professional in the industry, many skills exist that make cybersecurity professionals well-sought-after commodities and assets to any company. I

believe that the three foundational skills needed are a mixture of hard skills and soft skills. These three skills are Technical skills, Problem-solving & Critical Thinking skills, and Written Communication skills. Below I will elaborate on these three skills separately accompanied by three artifacts per skill that were accumulated throughout my degree coursework. These artifacts aim to provide proof of skill attainment, skill development, and skill reinforcement.

Technical Skills

Technical skills are qualities acquired by using and gaining expertise in performing physical or digital tasks. For a cybersecurity professional, even though there are non-technical positions available in the field, having a technical background and foundational knowledge is considered one of the core requirements to have a successful career. Over my Old Dominion University matriculation, this was my favorite skill to learn and enhance through hands-on labs and assignments as I took more advanced courses. I have utilized many software programs, operating systems, virtual machine lab environments, and network hardware that will be commonly used in the workplace. Below are a few artifacts that demonstrate some of the technical knowledge I learned and applied throughout my studies:

Artifact 1: Assignment 4 CYSE 270: Linux System for Cybersecurity

CYSE 270, which is the Linux System for Cybersecurity course, was taught by Professor Shobha Vatsa. The main course objectives for this class were to Introduce the basic concept and knowledge about different Linux distributions, including Ubuntu and the most popular distribution for cybersecurity, Kali Linux; Understand the ownership and permissions of the files and directories; Understand shell scripting to automate tasks; Perform essential system administration functions, such as network configuration, process and log administration, and software management; and Perform security tasks, such as footprinting, firewalls, and intrusion detection tools. As an avid Windows user, to be a successful cybersecurity professional, I knew I needed to diversify my operating system knowledge to

make myself more marketable, so this class was taken in that effort. According to Loshin & Bigelow (2021), Linux is an open-source, community-developed operating system that is supported on almost every major computer platform making it one of the most widely supported operating systems. For this course, since we were using our own respective personal computer systems, we had the option of using the Ubuntu version of Linux, which took up less disk space to operate, or Kali Linux, which took up more space but included more features to explore than Ubuntu. I went ahead and used Kali Linux because of my computer's capacity and the opportunity to explore other features during class and on my own.

In this particular artifact, the overall goal was to practice basic group and account management by completing the given tasks in the steps required. This allowed me to add new users to my network, add the users to groups, access the users' password hashes, create files and modify their group ownership permissions, and delete users upon completion. This skill is important in the workplace because employees onboard and offboard companies all the time, I will eventually be one of those employees who will need to be onboarded, so with onboarding, access accounts will need to be created for each user and given appropriate privileges based on your job. On the other end of the spectrum, when someone is being offboarded from a company, those same accesses need to be revoked and the user account deleted within the timeframe of the company's policy. As a cybersecurity professional, I could be tasked with user account and group account management or assisting in that regard to ensure correct and least privilege is properly maintained. This assignment, along with other assignments in this class, allowed me the opportunity to establish and build upon the technical concepts needed to successfully execute commands in Linux and see the results first-hand.

Artifact 2: Assignment #5 CYSE 301: Cybersecurity Techniques and Operations

CYSE 301, which is the Cybersecurity Techniques and Operations course, was taught by Professor Peng Jiang. This course focused on different tools and techniques involved in real-world cyber

operations and provided a broad range of cybersecurity concepts and essential hands-on training needed in the cybersecurity field. This class was heavily reliant on the use of a Linux system background and although not required, it was strongly recommended that CYSE 270 be taken first to establish the Linux foundation. CYSE 301 is intended to build on that established foundation, which would enable him to focus more on teaching new concepts and less on fundamentals. I originally signed up for his class before taking CYSE 270, but I heeded his advice and took CYSE 270 first, and glad I listened. Without having a solid Linux foundation, I would have been doing twice the work to succeed: learning the foundational skills on my own using outside resources while simultaneously learning the concepts he covered in class. Taking the class in the suggested order allowed me to really enjoy this course further reinforcing foundational concepts and adding more tools to my cybersecurity toolkit.

In this particular artifact, I was tasked with cracking the passwords of created user accounts and the password of the Wi-Fi based on the network traffic captured. Since the virtual lab environment used in this class was disconnected from the internet for security purposes, I was given network traffic capture files to analyze and discover the Wi-Fi password using the Aircrack wifi password cracking tool in Linux. For the user passwords, I had to create users, create passwords for the users, retrieve the hashes for the passwords, and perform a dictionary attack against them. I also created users in a Windows system and was able to use my Linux system to gain access and retrieve the hashes of the Windows users and crack the passwords using the John the Ripper tool. The Cain and Abel password cracking tool was also used to perform a brute force and a dictionary attack on the Windows system.

The concepts performed in this artifact are important because to know how to prevent attacks and security breaches, you need to know the vulnerabilities that exist in the systems you oversee and what tools are available that may be used against your system. It is said that the best offense is a good defense and knowing your system's weaknesses can assist in that regard. In the case of this artifact, picking a stronger Wi-Fi protocol and stronger passwords for both the users and the Wi-Fi can help

prevent this type of exploit. Also ensuring that all known vulnerabilities are patched timely and closing unnecessary ports will aid in preventing unauthorized access.

Artifact 3: Assignment 7 CYSE 450: Ethical Hacking and Penetration Testing

CYSE 450, which is Ethical Hacking and Penetration Testing, was taught by Professor Shobha Vatsa. The main course objectives for this class were to Learn basic terminology used in ethical hacking and useful penetration testing tools on the Kali Linux operating system; Learn to explore vulnerabilities in various operating systems and websites; and Operate the industry-leading tools and framework to perform penetration testing on different target systems. This class utilized the prior concepts learned in both CYSE 270 and CYSE 301 and expanded upon that knowledge through hacking and pen testing tools.

In this particular artifact, I was tasked with performing an ARP spoofing attack. ARP stands for Address Resolution Protocol. According to Graham (2021), the MAC address of a system is a unique identifier that tells who you are, the IP address identifies a system's location and these two identifiers are linked together and tracked using an ARP Table on your network (p. 20). Performing an ARP spoofing attack lets an attacker trick a victim's system into reconfiguring its ARP table to send internet traffic through the attacker's system pretending to be the router instead of the router itself. The attacker can then inspect the traffic sent first and then forward it to the actual router, ultimately becoming the man in the middle. This assignment introduced me to commands that I had not encountered to this point to extract the required information and Burp Suite, which was a tool used to intercept a website's login credentials from the victim's system. Wireshark, a familiar network traffic capture tool also used in the previous classes, was required for this assignment.

As mentioned previously, the best offense is a good defense. Knowing what vulnerabilities exist, what tools are available, and how they are used to exploit vulnerabilities will aid in patching and defending networks, websites, and systems better against attackers.

Problem-solving & Critical Thinking Skills

Problem-solving & Critical Thinking skills are imperative to have as a cybersecurity professional due to the ever-evolving landscape and the need to analyze complex situations, identify vulnerabilities, and develop practical solutions. To achieve this requires analytical thinking, creativity, and thinking outside the box. During my matriculation at Old Dominion University, I have been given many assignments and discussion posts with thought-provoking questions and scenarios that require problem-solving and the use of critical thinking. Below are a few artifacts where problem-solving and critical thinking were demonstrated:

Artifact 1: Case Analysis IT 315: Introduction to Networking and Security

IT 315, which is Introduction to Networking and Security, was taught by Dr. Vijay Kalburgi. The main course objectives for this class were to learn fundamental concepts, technologies, components, and issues related to communications and data networks. The topics discussed included different network architectures, infrastructures and configuration concepts, services provided, different protocols, different cyberattack situations, types of adversaries that exist, and some defensive tools available. Since this was an Information Technology course, it focused more on the hardware technology and infrastructure that comes along with establishing networks and ways to defend the physical equipment and wiring.

In this particular artifact, this was the final project based on a case analysis scenario. Utilizing the concepts discussed throughout the semester, I was given the task of designing a wired network for Maury High School, a local high school in Norfolk, Virginia. The requirements for this plan were that it included: two live network outlets for each classroom and office, that those outlets connect to a secure Internet connection that the whole school would share, and that the school would not have any Internet-facing servers. Other than the floor plan of the building, the rest of the implementation of the

design and the equipment used was up to me. This analysis required me to figure out the total wiring length needed for the entire building, locations needed for equipment rooms and telecomm closets, where to put these rooms and closets to provide the best equipment coverage, determine the ports needed throughout the building, network equipment to get the internet up and running, and supply an overall cost of all needed supplies with a breakdown for each item. This was a very time-consuming analysis because I had to compile all the specs for the building, determine the needed equipment, and find the price of all of those items. In a workplace environment, I imagine that this type of analysis would typically be done with more than one person, but this analysis shows it could easily be a one-man show depending on the size of the company. This type of analysis would be required in most cases because companies have budgets and the need for projects to stay within those confines. Even though for this case analysis, I was not given a budgetary restriction, I attempted to think from a business perspective and use critical thinking to achieve the goal of providing a wired network to Maury High School using efficient equipment at a reasonable cost that should be highly considered in a real-life situation.

Artifact 2: Assignment 2 CYSE 301: Cybersecurity Techniques and Operations

Again I am selecting an assignment from CYSE 301, Cybersecurity Techniques and Operations, taught by Professor Peng Jiang. In this particular artifact, performing network traffic capture and sniffing techniques was the goal of this assignment. The primary tool used for the assignment was Wireshark. According to Hanna (2024), Wireshark is one of the popular open-source network analyzers that can capture and display real-time details of the traffic going through a network, and depending on the protocol used, the read traffic can be viewed in plaintext or ciphertext. This assignment was conducted in the virtual lab environment that used three devices, a Kali Linux system that was configured to be outside the network, an internal Kali Linux system, and an Ubuntu Linux system. The goal of the assignment was for the External Kali to gain access and monitor the traffic between the Internal Kali and

the Ubuntu Linux using Wireshark. This network traffic capture was performed in steps and provided many real-time results. The reason this artifact was chosen is because it demonstrated a few instances where problem-solving and critical thinking came into play: First, I had to obtain all the network traffic information by following steps to get the correct results needed; Secondly, I had to analyze all the traffic received through Wireshark, to determine what was there and how it was useful. In using Wireshark, the information is not always in plain sight, requiring some navigating and deep-diving to find the information you seek. This can also require some interpretation to understand what is occurring.

In the workplace, a cybersecurity professional could be tasked with monitoring network traffic either manually or by reviewing the logs of an automated process. Critical Thinking comes into play when analyzing the traffic to determine what is coming into and leaving out of a network. Problem-solving comes into play when you discover an issue within the traffic and have to act on that discovery and determine what next steps need to be performed to mitigate the issue. For example, discovering an open port that should be closed because of unsecured protocols or unauthorized data leaving a company's network.

Artifact 3: Midterm Case Scenario CYSE 407: Digital Forensics

CYSE 407, which is the Digital Forensics course, was taught by Professor Bryan Bechard. The objective of this course was to learn the basic concepts of digital forensics through the use of fundamental techniques and the use of collection, processing, and preservation tools for digital evidence. Those techniques and tools are commonly used on computers, mobile devices, networks, and cloud computing environments. To display understanding, I was responsible for engaging in oral and written communications to report digital forensic findings and prepare court presentation materials.

According to the Department of Defense Directive 5505.13E (2010), Digital Forensics is, "in its strictest connotation, the application of computer science and investigative procedures involving the

examination of digital evidence - following proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possibly expert testimony" (p. 14). For this particular artifact, I was given the task, in a case scenario, of creating and running a brand new digital forensics lab for a mid-size police department that is sustainable for the next three years. This assignment required the designing of a lab with a physical layout and floor plan that contained: an evidence storage room that could hold up to 20 cases, two analysis computers, the use of physical security measures of my choice, and any other hardware or software needs discussed in class up to that point in the semester. Other requirements for this assignment were a lab accreditation plan, lab maintenance plan, and lab staff job descriptions. For the accreditation plan, I had to figure out what entity was responsible for digital forensic labs in the US and that was the ANSI-ASQ National Accreditation Board (ANAB). After finding out what entity, I needed to make sure that the lab I was creating would contain all the requirements to obtain that accreditation. Once the requirements were known, I could design the lab. How I designed the lab was my choosing, as long as the accreditation and assignment requirements were met. This assignment required the use of problem-solving and critical thinking through creating the entire case scenario but primarily designing a forensic lab from scratch. Even though in a real-world situation, I would be given a space to utilize in an established mid-size police department and go from there, in this case, I was not. In making this design concept, I had to think about the physical security aspect, how many rooms were needed, what equipment was needed, where it would go, open floor concept vs. privacy concerns, the number of entrances needed in case of a fire, and the need of fire alarms and where they should be placed. To successfully design this digital forensic lab, I had to remember the basic importance of evidence collection and preservation and that evidence needs to have a chain of custody, be secured at all times, and remain unaltered to be deemed admissible in court. Remembering this assisted greatly in configuring my lab design.

This assignment overall was very enjoyable to complete as I was the sole person creating an elaborate digital forensic lab concept. In reality, as a cybersecurity professional, I would probably be minimally involved in creating something like this, so it did require some out-of-the-box thinking on my part to provide a successful solution.

Written Communications Skills

Since the COVID-19 pandemic, we have become more reliant on communicating electronically than ever before. Written communication is still utilized heavily to aid in understanding. Cybersecurity professionals must be able to effectively communicate complex technical information through written reports, documentation, and emails, ensuring accuracy and attention to detail in written communication. Below are a few artifacts that demonstrate the use of effective written communication concerning important topics in the cybersecurity field:

Artifact 1: Analytical Paper CYSE 200T: Cybersecurity, Technology, and Society

CYSE 200T, which is Cybersecurity, Technology, and Society was taught by Professor Christopher Bowman. The main course objective of this class was to explore how technology relates to cybersecurity from an interdisciplinary perspective with an emphasis on the way technologically-driven cybersecurity issues are connected to cultural, political, legal, ethical, and business domains.

In this particular artifact, I was tasked with producing an analysis of the social meaning and impact of cybersecurity-related technical systems. This paper was unique because I was required to use two to three discussion posts previously done in the class and relate them together to create the analysis paper. The topic that I settled upon to analyze was Cyber Harassment and Cyber Stalking. Harassment and Stalking have been crimes for a long time that would traditionally be conducted in person, by mail, or by phone, and usually in local proximity. However, with the increase in technology availability and easier access to most people online, the reach to commit these crimes now spans

globally. This paper discusses what the crimes are, how the committing of these crimes through technology has increased, how jurisdictional issues and anonymization of these crimes make it difficult to pursue legal action, and ways forward to slow down this growing problem. In completing this assignment, I liked the concept of combining three discussion posts that I did not realize at the time which ones I would use or that they would be used later for that purpose. It took some creativity to intertwine the different discussion topics written at various times into a single paper that flowed throughout, but it turned out very well in my opinion.

Artifact 2: Final Paper for IDS 300W: Introduction to Interdisciplinary Theory and Concepts

IDS 300W, which is Introduction to Interdisciplinary Theory and Concepts, was taught by Dr. MaryAnn Kozlowski. The course objective of this writing-intensive class was to examine issues related to interdisciplinary perspectives by studying the differences and similarities among academic disciplines and applying an interdisciplinary approach to a specific topic of study.

In this particular artifact, I selected my final assignment, which was a paper on the topic of Cyberbullying. Throughout the course, the paper was created in steps. The steps used in the paper creation were the 10 steps of the interdisciplinary research process. According to Repko, Newell, & Szostak (2012), Repko proposed the following 10 steps: “Define the problem or state the focus question, Justify using an interdisciplinary approach, Identify relevant disciplines, Conduct a literature search, Develop adequacy in each relevant discipline, Analyze the problem and evaluate each insight into it, Identify conflicts between insights and their sources, Create or discover common ground, Integrate insights, and Produce an interdisciplinary understanding of the problem and test it” (p. 9). I wanted to pick a topic that was cybersecurity-related and after recently, at the time, completing my CYSE 200T paper on cyber harassment and cyberstalking, I decided to dive deeper into the social issues in technology, more specifically, cyberbullying amongst adolescents. Cyberbullying in my paper looked at

the interdisciplinary approach between the Psychology, Criminal Law, and Information Technology disciplines. Psychology focused on creating cyberbullying prevention programs that brought awareness and re-education of the subject to the aggressors and bystanders while also providing psychological and emotional support for the victims. Criminal Law focused on, as previously mentioned in my CYSE 200T paper, the constraints that exist in pursuing legal action due to jurisdictional issues and the lack of an overarching law in place. Information Technology focused on social media platforms and their obligation to assist with preventing cyberbullying through their platforms and whether they hold any responsibility.

I do not engage in cyberbullying, but I use social media where I see online comments and read stories on this issue all the time. Cyberbullying is a growing problem and has a psychological effect on the victims that if not properly mitigated, could elevate to physical harm to either themselves or someone else. Law and Technology must assist in making a safe place free of that activity and have laws in place to deter or punish those who choose to partake in it. This class was very thought-provoking and finding a topic that not only showed relevance to my major but was also interrelated to other social science disciplines was not the easiest to achieve, but I like the result of the paper created thanks to the 10-step approach to interdisciplinary research that was used.

Artifact 3: Policy Analysis Paper 1: CYSE 425W: Cybersecurity Strategy and Policy

CYSE 425W, which is Cybersecurity Strategy and Policy was taught by Professor Lora Pitman. The course objective of this class was to explore cybersecurity policy-making and strategy development. This includes planning principles in cyber strategy; risk management; connections between cybersecurity policies, businesses, and governmental institutions; the knowledge, skills, and abilities needed to develop and implement cybersecurity policy; the social, political, and ethical implications that arise in cybersecurity policies and strategies; and the ties between national security and cybersecurity policy.

Over the semester I was given the task of analyzing an existing cybersecurity policy from three different perspectives on three separate papers. In this particular artifact, I chose the first analysis paper that I wrote about the Data Breach Notification Law. The first paper established the foundation for the other two papers by explaining what the Data Breach Notification Law is, why the law was developed and implemented, and the different variations in the United States, Europe, and Australia.

This topic was important to me because since joining the military in 2015, I have been the victim of many data breaches of many companies, including the Office of Personnel Management. This common occurrence of data breaches from different companies made me interested in the notification process and how it works. While researching the topic, I became more knowledgeable about the European Union's General Data Protection Regulation (GDPR) and the European Union's approach to the law. I also discovered that the United States lacks an overarching federal law regarding Data Breaches because each State is in charge of making its laws regarding data breaches, further complicating jurisdictional issues.

This assignment allowed me to become more knowledgeable on the subject of Data Breaches. Also, in writing the different analysis papers mentioned previously, I was able to display and communicate my findings and thoughts in a comprehensible way.

Conclusion

My time at Old Dominion University pursuing my cybersecurity degree has provided me with a structured environment to learn foundational concepts and techniques in the field of Cybersecurity. I have also learned skills that not only apply to cybersecurity but span across multiple disciplines. The resources acquired from different courses and through online research will prove to be beneficial now and in the future. As I begin to transition from the classroom to becoming a cybersecurity professional in the workforce, I will be able to rely upon my current knowledge and use the learning methods I have

been taught to continue to obtain information. As a cybersecurity professional in a constantly updated environment, I will be a lifelong learner who will have to stay current with technology and information to stay relevant in defensive strategies. Having the technical skills, the problem-solving & critical thinking abilities to adapt to new situations, and written communication skills to properly relay information to peers and other non-cybersecurity individuals will serve me and any company I work for well in my future endeavors. As I navigate through my cybersecurity journey, I hope that I continue to represent Old Dominion University, my department, my instructors, myself, my family, and my community in the best light.

References

Graham, D. G. (2021). *Ethical Hacking: A Hands-on Introduction to Breaking In*. No Starch Press.

Hanna, K. T. (2024, January 10). *What is Wireshark?*. TechTarget WhatIs. https://www.techtarget.com/whatis/definition/Wireshark

Loshin, P., & Bigelow, S. J. (2021, October 6). *What is the Linux operating system?*. TechTarget Data Center. https://www.techtarget.com/searchdatacenter/definition/Linux-operating-system

Lynn, W. J. (2010, March 10). DoDD 5505.13E, March 1, 2010. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/550513Ep.pdf?ver=2019-06-06-103505-737

Repko, A. F., Newell, W. H., & Szostak, R. (2012). *Case studies in interdisciplinary research*. SAGE Publications, Inc.

Reynolds, N., & Davis, E. (2014). *Portfolio Keeping: A Guide for Students* (3rd ed.). Bedford/St. Martin's.