Chris Evans ePortfolio:

Reflective Essay

Chris Evans

Old Dominion University

IDS 493: Electronic Portfolio Project Course

Dr. Sherron J. Gordon-Phan

Aug 1st, 2023

Abstract

This portfolio is an accumulation of collected artifacts and experiences documenting the academic career or a cybersecurity student at Old Dominion University. In the following work I will cover the technical skills, communication skills, and research skills gained and how they contribute to a deeper understanding and learning of cybersecurity. This portfolio is both to serve as evidence for others to review and as a learning journey for review for myself, the student.

Introduction

As a student at Old Dominion University, I have been exposed to a tremendous amount of new information, topics, people, and ways of thinking. Over the course of my learning, I have taken many classes that have covered different subjects ranging from technical computer concepts to broad interdisciplinary studies. All of these courses have caused me to grow as a person and student and changed how I look at the world and tackle problems. Soon I will be graduating Old Dominion University with a Bachelors in Cybersecurity and it is time to reflect and compile a portfolio of the skills I have gained and how my time at ODU has benefited me.

Portfolios are critical tools for students to self-reflect on what they have learned and how much progress they have made in learning. This portfolio will have the main purpose of being an evidence showcase of the various artifacts of my education and how they demonstrate understanding of the concepts studied to others.   The second purpose of this portfolio will be to me the student, to serve as a journal that chronicles accomplishments in an attempt to provide motivation and to be reviewable (Forde.)

Skills Overview

Being a cybersecurity student has given me a broad overview of many different technologies and fields. Cybersecurity professionals similarly need to be competent and understand a multitude of various technologies in order to do their job effectively. The demand for cybersecurity service and professionals will only grow in the coming years (Aiyer.) ODU has provided me with many skills, but I will go over and outline a few in particular that have been central as I have grown and become a cybersecurity professional. Below I will go over the technical skills, writing and communication skills, and the research skills I have gained at ODU as well as list three separate pieces of coursework that are artifacts of my learning efforts. The combination of these skills and artifacts will stand as evidence for my maturation as a student.

Technical Skills

Technical skills are the basis of cybersecurity professionals tool kit. Understanding of how computers function, how they communicate, and how those technologies can break or become attacked is absolutely the heart of the discipline. Through many classes at ODU I have learned how computers function, how they communicate over networks and how I can attack and defend them. Courses such as Cyber Techniques and Operations CYSE 301 or Digital Forensics CYSE 407 have provided me with understanding of different technologies through hands on projects.

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

CYSE 270 Linux System for Cybersecurity was a class that taught me how to navigate the Linux command line and to carry out the responsibilities of a junior Linux system administrator. The course was very technical as we learned how to write commands to the Linux operation system as well as how to navigate the file structure. We learned further technical aspects like scheduling Chron Jobs.

The artifact presented is Assignment 4 where we input commands to manage new users and groups and configure their file and access permissions. This is a critical role as a user given the wrong permissions can limit organizational effectiveness or expose critical data and networks to unauthorized users. In the assignment I utilized the command line effectively structuring commands and carried out a common activity of a Linux system administrator.

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

CYSE 301 Cybersecurity Techniques and Operations was a class that introduced tools and techniques used to secure and analyze large computer networked systems. We configured firewall rule tables to modify and monitor traffic, performed advanced packet analysis on transmitted data, and most exciting of all preformed penetration testing techniques. This class was tremendously exciting as we got to get hands on and implement the theory of cybersecurity with actual tools.

Assignment 2 covered the configuration of a firewall rule table for a pfSense firewall in order to block a specific type of network traffic to a specific host IP address on a network. This is useful for a multitude of reasons and a common task for a system administrator and helps protect host systems from unwanted probing attacks or malicious packets. Before being able to configure this traffic we had to establish a virtual local private network or VLAN in linking multiple virtual machine hosts together. The assignment was helpful for students to understand how they can connect hosts, communicate, and block traffic.

Artifact 3: Final Paper for CYSE 407 Digital Forensics.

CYSE 407 Digital Forensics covered the foundational techniques and tools to collect, process and preserve digital evidence on various computing devices. We gained an understanding of how to use various tools and software, as well as how to handle it responsibly so that if we are called to cooperate with law enforcement or testify in a court of law, then our findings will be presentable materials. This course was exciting as we again got hands on with various software and used the tools to extract data or find information.

The final paper assignment for this course was to combine all the topics we had learned and to create a report of our findings for a fictitious investigation. We outlined what items we were performing digital forensic investigations on, how we handled the investigations and tools and techniques we used, as well as prepared our findings in a way that would be appropriate for a professional or courtroom setting.

Communication and Writing Skills

Old Dominion has a strong emphasis on communication and writing skills and even has students complete interdisciplinary writing intensive courses as part of their degree programs. Throughout my studies I have had to communicate effectively with classmates and professors as well as write effectively to convey technical ideas. This constant practice has strengthened my skillset in conveying information and in choosing how to best communicate in different environments and with different purposes or people.

Artifact 4: Report Project for CS 465 Information Assurance

CS 465 Information Assurance is a course that covers the more organizational side of cybersecurity. Course topics include planning and deployment, verification and evaluation, incident response, policy language, enforcement, and legal, ethical, and social concerns. The course largely covers how senior leadership would attempt to structure their organization to provide coherent cybersecurity solutions.

The report project assignment tasked students with creating a report about a fictitious breach of a fictitious company and what effects it had and how it was responded to. To be successful in this assignment, I needed to communicate the most important who, what, where, and when. Further, I had to communicate relevant information to relevant parties at their level of understanding, while covering technical material such as vulnerability assessments.

Artifact 5: Midterm for CYSE407 Digital Forensics

This artifact is the Midterm assignment for my Digital Forensics course. This assignment tasked the student with creating a blueprint for the operation and development of a digital forensic laboratory in a fictional police department. The goal is that the document be a guide for the function and operation of the forensics lab. This assignment required me to communicate technical ideas to a reader that may not be technical, such as the administration of a police department, and outline the specific hardware needed, the personal needed, as well as the industry standards that the digital forensic lab will be striving to be in compliance with. Using lists and a diagram I am able to communicate roles and responsibilities as well as outline operation of the lab.

Artifact 6: Background Research Memo for CYSE 406 Cyber Law

CYSE 406 Cyber Law covered various law topic as they related to cybersecurity. We learned what laws impact cybersecurity practitioners and how the law is structured and administrated. We also covered how authorities operate and their limitation legally and online.

The background research memo was a fictitious memo for a fictitious politician attempting to educate that politician on the relevant facts of a Cybersecurity bill currently stalled in congress. The Representative did not need to have the entire bill told to him in the memo. I attempted to communicate succinctly the relevant information that the Representative needed as well as what information he should express to his constituents. This was a case where I was careful to try to be clear, not use technical jargon, and be as brief as I could while covering relevant points. Should the Representative want further clarification I included links for further reading.

Research Skills

While studying I often had to write papers that were long and required citation. Even more so, as an online student I often had to rely on myself when I faced a learning block or needed answers to a question I had. Those conditions have caused me to become skilled at researching any question or concern I have and learning where I can turn to for valid and credible answers. Luckily my professors at ODU have provided students with understanding of the major regulatory bodies and industry leaders in cybersecurity, groups like the Cybersecurity and Infrastructure Security Agency CISA, Information Systems Audit and Control Association ISACA, and the MITRE Corporation's with their Critical Vulnerabilities and Exploits CVE list help cybersecurity professionals research for reliable information.

Artifact 7: Preventing Bank Fraud Research Paper for IDS 300W Interdisciplinary Studies

IDS 300W was a writing intensive course that covered combining different disciplines in an attempt to gain new insight and knowledge. For this course we had a research paper that required seeking new perspectives and multiple sources to discuss the interdisciplinary problem of cybercrime, in particular how to prevent online bank fraud.   I spent many hours seeking out the relevant sources of information for this paper and it was very helpful to my own path as I learned so much.

Artifact 8: Analysis of National Cyber Security Strategy for CYSE 425W Cyber Strategy and Policy

CYSE 425W was another writing intensive course that attempted to cover policy, planning, strategy and development and implementation of cybersecurity at all levels of public and private organizations. We covered various topics, like initiatives and planning and risk management. This assignment was an analysis of the United States National Cybersecurity Strategy for 2023 under the Biden administration. The strategy was a departure from past administrations as it outlined a more aggressive role for the federal government than previous administrations had pursued. This was great as I researched multiple government documents and saw how they evolved over time.

Artifact 9: Controversy Over Pegasus Spyware for CS462 Cyber Security Fundamentals

CS 462 Cyber security fundamentals covered basic networking and cyber threats and defenses. This class required me to research a tremendous amount of information on my own as I attempted to master the subjects presented. I relied heavily on my ability to seek true information from industry leaders and apply it to the course. The research paper was on Pegasus Spyware used by an Israeli firm that was a particularly strong hacking tool, and how it had been used by oppressive governments against dissidents or in crime. The research for this paper took about a month of scouring international sources and overseas journals. Assembling a coherent picture of the issues at had was difficult but attainable.

Conclusion

As my time completes at Old Dominion University, I am excited to continue using my technical skills to solve problems in cyberspace, my communication skills to work together with stakeholders, and my research skills to continue learning everyday so that I can be a better cybersecurity professional. The time I have spent at Old Dominion University has been incalculably valuable in my progression to a cybersecurity career.

Citations

Aiyer, Bharath. 2022. New Survey reveals $2 trillion market opportunity for cybersecurity technology and service providers. *McKinsey & Company.* https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers

Forde, C., McMahon, M., & Reeves, J. (2009). Putting together professional portfolios. SAGE Publications Ltd, https://doi.org/10.4135/9781446216149