E-Portfolio Reflection

Eric L.Tran
Old Dominion University
IDS 493

Introduction

My E-Portfolio serves as a reflection on the past four years of college, starting out as a Computer Science major, and now ending as a Cybersecurity major. Celeste Fowles Nguyen comments on the importance of e-portfolios "The ePortfolio serves as a living portal, whereby identity is shared with others and reimagined in narrative and conversation." Throughout these four years, I have accumulated many artifacts consisting of coding assignments, papers, labs, and various other course work. The skills I believe has helped me the most in both a university setting and at an internship setting has been critical thinking, technical skills, and writing. With all three of these skills, there will be artifacts demonstrating how I used the skill and how it shaped me as a student and eventual professional. The need for e-portfolios are increasing and as stated by Clemson University, "more than 4 in 5 employers say an electronic portfolio would be useful to them in ensuring that job applicants have the knowledge and skills they need to succeed in their company or organization."

Skill: Critical Thinking

Critical thinking to me has always meant being able to address all viewpoints effectively and be able to find a solution that can incorporate many ideas into one. Echoing Katherine Hibbs on the importance of critical thinking, "Good thinking skills are really not all that complicated, but you need a bit of knowledge and continuing practice to turn the learned skills into instinctive habits. Successful critical thinkers are judged by results that almost always involve deliberation and intuition, logic and creativity. ." With Cybersecurity, the problems facing this field is very complex and requires the combination of many disciplines. Cybersecurity is unique since it has aspects of Criminal Justice, Network Management, Political Science, and Forensics. The artifacts that will be shown for this skill demonstrates my ability to creatively find a solution, find sources relevant to the central question, and incorporate all viewpoints into one coherent idea.

CS 465 Information Assurance – Final Project

The course CS 465 taught me how to analyze the legal and ethical side of information assurance and taught me how to identify vulnerabilities and threats. I found this extremely useful during my internship at Newport News Shipbuilding (NNS) working on the Vulnerability Management Team. Regularly the team would discuss corporate regulations and policies and look at the company's overall information assurance strategy. On top of that, we had to deal with vulnerabilities that came in by the thousands daily and remediate them or put them on a remediation plan if a remediation was not recommended at the time. I was able to connect what I learned on the job to what I learned in class, especially during the policy and vulnerability modules.

For the final project, we were asked to take on the role of Chief Information Assurance Officer for a small fictional company named "QIR, LLC." The small company has been hacked, and I am tasked with creating a set of information assurance policies and procedures to reduce the risk of future attacks. To summarize what happened during the hack and how to improve the policies, I drew parallels to the 2016 DNC hack since QIR was also a political consultant company. Using social engineering the hackers were able to access thousands of emails and were able to log every keystroke of employees on the network. With all of the vulnerabilities and break down of procedures laid out, I policies and procedures backed up by sources which consisted of studies, journals, and real life events.

This final project helped reinforce the importance of policy and procedures and ensured that they are followed. Humans are the biggest vulnerability and with this assignment, I was able to develop a plan to be the first line of defense before a hacker reaches a human, as well as creating preventative measures when it does reach a human. The use of real life events and journal sources allowed me to synthesize many ideas into an effective information assurance policy for QIR. While doing this assignment, I also recalled many meetings at NNS where my team and upper management would discuss policy and how some parts needed to be edited either to be more lax or stricter.

From taking CS 465 and completing the final paper, I learned the importance of policy and procedures, and the importance analyzing small details that lead up to a cyber incident. This skill will be very helpful for my future career since policy and procedures dictate everything I am able to do and by understanding why they are there and how to improve them, I can appreciate them a lot more.

CYSE 407 Digital Forensics -Final Project

Digital Forensics was always interesting to me and for awhile it was a field I wished to go into. CYSE 407 was a very fascinating class since the class taught me about the investigation process and how physical and digital investigations were not different at all. Learning how to look at metadata and recover passwords or deleted material were some very enjoyable parts of the course. I also found learning about the different types of tools used like a Write Blocker or software like EnCase which is used to analyze and recover evidence from hard drives.

The final project asked for a creation of a mock investigation which consisted of having a description of evidence, summary of the investigation, and conclusion. I was able to be very creative in my completion of this assignment and was able to apply what I learned throughout the course into a final product. This mock case was an espionage case where the perpetrator was a high level US official caught selling information to Russia. I used resources from labs, assignments, and knowledge from my Security+ certification to explain how I extracted information from a phone, laptop, and hard drive. I was able to showcase my general knowledge of digital forensic tools in a hypothetical situation and was able to incorporate some technical data into my paper.

Having the knowledge of digital forensics and the existence of the multitude of tools available is crucial since everything is going digital. I will be able to recover data and develop an adequate investigation process if I were given the responsibility of gathering evidence after a breach or espionage case involving transmission of classified material. As pointed out in an article on DRS, which signifies the importance of digital forensics, “for the cyber security team whose role it is to protect the organization, or the investigators who are trying to establish how the business was breached, these bits of evidence are crucial. They will show how an incident happened, who was responsible, how to respond to it, and most importantly, how to stop it happening again in the future.” This assignment also demonstrated my creative abilities in developing a scenario and backing up my evidence with technical data. Along with that, I was also able to combine the knowledge of file system, operating system, and digital forensic tools to solve a central problem.

CYSE 368 Cybersecurity Internship – Summary of the Internship

My internship with the federal government was a great opportunity, and I was able to explore many different topics during my time there. I was able to exercise my creative and critical thinking since I was placed into a fast paced environment and had to learn how to perform my duties quickly. Through technical and research, I was able to provide information to policy makers and those who were in the field.

This internship taught me about the importance of collaboration and how crucial it is to have inputs from many experts in order to report the most accurate information possible. Additionally, I also learned how to develop malware and penetrate into a network and discern what is useful and what is not useful depending on the situation. Using everything I have learned through school and certifications, I was able to apply basic knowledge and further expand my knowledge pool.

Skill: Technical Skills

Technical skills means having the ability and knowledge to perform a specific task, whether it be mechanical, scientific, or technology. These skills may be knowledge of a tool, programming knowledge or equipment. Since High School, I have been able to accumulate multiple technical skill ranging from programming languages to digital tools. Having the ability to quickly learn a technical skill is important since all industries are quickly evolving and new tools and techniques are emerging at a fast rate. Supporting the need for technical skills, particularly programming knowledge, a writer from PheonixTS states “Programming knowledge proves essential for analyzing software for vulnerabilities, identifying malicious software, and other tasks required for cyber security analysts.”

CRJS 344 Social science and crime mapping – Final Map

CRJS344 differed from most of my courses since it wasn’t about cybersecurity or programming. I have always been interested in criminal justice and ArcGIS, so when the opportunity came, I decided to take this course. Learning how to use ArcGIS was fulfilling, and I was able to demonstrate proficiency was this tool by creating maps depicting several statistics.

For the final map of the course, I was tasked with using every technique and method I have learned this far to create a map depicting problems with school placements in California in 2000. The data was exported from a government site that housed population data and school placement data. To create the map, I matched the data up and zeroed in on Riverside county. After the data was generated onto the map, I color coded the population density and generated icons for school placements which ranged from elementary to high school. During this assignment, I learned how to analyze and visualize data. With this knowledge of how powerful ArcGIS is, I was able to transfer my understanding of the capabilities to my internship and seek out those who were experts to help create visuals for me.

In the end, I showed how quickly I was able to become proficient with a digital tool and learned how to exploit data to my advantage.

CSC 205 Computer Organization – Square Assignment

CSC 205 was one of my courses I first took when I went to Tidewater Community College. This class dealt more with the hardware and operating system of computers, with most of the programming occurring in assembly language. I found this language to be very satisfying to write in and when I got the correct output, it was truly marvelous to witness.

Beginning of the course, we were given an assignment to create a program in assembly language to square any number inputted. This was one of my first assembly programs and I quickly learned the mnemonics, labels, comments, and directives. Using class notes and what I learned previously, I was able to out together a program that took a number input and produced the square result as the output.

From this assignment, I was able to visualize how a C++ program converts the code into assembly language, which then converts into machine code, which is binary. Knowing this entire process, I understood how assembly language or even machine language could be used to create viruses and how they could be exploited by hackers. The skill to understand the language of a machine is important and as stated by Ayoub Faouzi, "Assembly language is the only computer language that lets you talk to a computer in its native tongue, commanding the hardware to perform exactly as you say." This is important since vulnerabilities and hacks come in all forms, and knowing how to dissect a virus is crucial.

CYSE 301 Cyber Techniques and Operations – Kali Linux, Metasploit

Cyber Techniques and Operations provided a great sandbox to learn and test out tools that were relevant to cybersecurity and cyber operations. In this course, I learned how to crack passwords using Jack The Ripper, create stenography, and exploit vulnerabilities using Kali Linux.

The assignment has us use Metasploit to create a package that could be sent to a victim's computer. In order to deliver this package, I had to create a fake website and the victim computer had to click on a link containing the package. Once the download was complete, the attack computer had control of the victim's computer. In the process of creating the payload, I used Metasploit and msfvenom, as well as an Apache server to get everything up and running.

This assignment demonstrated how multiple tools were used to exploit a vulnerability and gain control of a computer. This lesson and experience would later be beneficial to me during my internship since I had awareness of the tools already and some experience in how they were used. As emphasized by Sandra Henry-Stocker on how important Linux is, "Linux is transparent, and that means you can learn to manipulate it in ways that are not possible with most OSes. In addition, most cybersecurity tools are written to run on Linux."

Skill: Writing

Writing has always been a skill I have enjoyed and my interests has only exploded over the past few years due to having great teachers and having opportunities to write creatively and analytically. The use of technical writing and research in cybersecurity, which was stated by Stephen Northcutt, “a technical writer must first research the topic they are writing about so strong research skills are also important.” The three artifacts in this section demonstrates my ability to analyze information and create a coherent argument for my position, while addressing other perspectives.

ENG 111 – Tablets Vs. Laptops

One of my first few classes during the early years of college was ENG 111 at Tidewater Community College. For this assignment, I had to write an argumentative paper about two topics and address both sides with credible sources. I decided to go with a topic I have never done before, and chose to write about whether or not tablets or laptops should be used in a classroom setting. I pointed out health issues, multitasking issues, and economic issues related to each side of the argument and provided statistics from studies. This paper refined y writing style and corrected a lot of bad habits I had. The improvements I made to my writing and additions to my style are still used even now, and I hope to improve further since writing will always be used everywhere. Writing is another form of communication and the work I did on this paper not only demonstrated my abilities to write, but demonstrated my abilities to view different sides of an argument and form an inclusive conclusion.

ART 101 – Art Analysis

Art 101, similar to Social Crime Mapping was a course I never expected to take, but quickly enjoyed every aspect of it. This class taught me how to look at the small details and how art, or anything in life can be interpreted in multiple ways.

The final assignment asked me to go to a museum to choose several paintings to analyze. The paintings could be of anything, be any style, and could be mounted on anything. I decided to choose paintings that made me feel warm, made me feel nostalgic and had a spring time feeling. I chose more than twelve paintings and had to analyze each one describing the how it was painted, the material is was painted on, the story behind it, how it made me feel, what was symbolic about it, etc. This assignment taught be the importance of details and careful analysis of method. Depending on the stroke and intensity of the strokes, or even the color pallet, it can tell a deeper story than what is painted in the painting. I also gained experience in analytical writing and learned how to express what I felt on paper, while backing it up with sound evidence.

IDS 300W – How Has Cyber Operations Impacted American Society?

IDS 300W was one of the first classes I took after switching from Computer Science. This class taught me the importance of multidisciplinary studies and how cybersecurity can be approached from many disciplines since the problems cybersecurity presents are complex.

For the final paper, I decided to have a central question on “How has cyber operations impacted American society?” The three disciplines I chose to answer this question were economics, political

science (national security), and psychology (cognitive). Using journal sources, I backed up each discipline and described how each one could create common ground to answer this question. Overall, this assignment exercised my ability to interweave different perspectives and analyze each discipline to find out how they could fit into the bigger picture. I believe this ability is important because there will be times when a problem will occur and no one discipline will be able to resolve it. Having the ability to convey the perspectives and find common ground is crucial when trying to unify ideas in order to answer a pressing situation.

Conclusion

Critical thinking, technical skills, and writing are skills that I have been able to refine and adapt throughout my educational and early professional years. My e-portfolio demonstrates my skills and as Christine Forde has stated, “A professional portfolio provides a space in which you can plan and reflect in depth on your practice, helping you identify y our strengths and find ways of building on these.” Through coursework, I exercised each skill and gained a better understanding as to how they will play a part in my future career. Interdisciplinary studies was brand new to me a few months ago when I switched over from Computer Science, but I now know why it is so important. Having knowledge and expertise from many different schools of studies allows an extensive analysis of a problem. Cybersecurity is an issue that can impact everything from economics to psychology, and now that I know how important interdisciplinary is, I can apply it to other areas of my life since nothing is ever black or white. The courses I have taken thus far has helped me as I worked at my internships and has given me a leg up in terms of base knowledge to work from. The knowledge gained from the Cybersecurity program will help me as I transition into my career after graduation and with an interdisciplinary viewpoint, I am more open to other disciplines and I now know the importance of seeking out other expertise to help with a complex issue.

References

Deon. (2020, February 24). The importance of digital forensics in cyber security. Retrieved April 18, 2020, from https://www.drs.co.za/the-importance-of-digital-forensics-in-cyber-security/

Does a Cyber Security Career Require Programming Skills? (2020, January 21). Retrieved April 18, 2020, from https://phoenixts.com/blog/do-you-need-programming-skills-for-a-cyber-security-career/

Faouzi, A. (2013, February 14). x86 Assembly Language, Part 1. Retrieved April 18, 2020, from https://resources.infosecinstitute.com/x86-assembly-language-part-1/#gref

Forde, C., McMahon, M. & Reeves, J. (2009). What is a portfolio?. In *Putting together professional portfolios* (pp. 1-11). London: SAGE Publications Ltd doi: 10.4135/9781446216149.n1

Henry-Stocker, S. (2019, January 12). First step to becoming a cybersecurity pro: Linux. Retrieved April 18, 2020, from https://www.networkworld.com/article/3331930/first-step-to-becoming-a-hacker-linux.html

Nguyen, C.F. (2013). The ePortfolio as a Living Portal: A Medium for Student Learning, Identity, and Assessment.

Pherson, K. H. (2017, March 8). Key Critical Thinking Skills For Security Professionals. Retrieved April 18, 2020, from https://www.securityinformed.com/insights/key-critical-thinking-skills-security-professionals-co-14642-ga.22310.html

The What, Why, and How of ePortfolios. (n.d.). Retrieved April 18, 2020, from https://www.clemson.edu/academics/programs/eportfolio/information.html