Reflection Essay

Julian Samonte

Old Dominion University

IDS 493 Electronic Portfolio Project

Professor David Prihoda

May 3, 2026

Introduction

As a senior at ODU, it is important for me to start looking into jobs that I have an interest in. This made me think about my skills and what I have to offer to a company that is looking for people in my field. I looked through a lot of the course work that I have done over the years and was able to pick three skills that stood out to me and could also stand out to possible employers. The three skills that I would like to focus on are my skills in vulnerability management, communication skills, and my skills in Linux operating systems. With that being said I think that this final project is perfect for me to look back on what I have accomplished. A benefit from doing this project and creating an ePortfolio was that it “Was an opportunity to conduct an in-depth self-evaluation and developed my skills of reflection.” (Forde, 2008).

Vulnerability Management

Vulnerability management is all about identifying security weaknesses that a system or an environment may have. The duties of vulnerability management include scanning for vulnerabilities, finding which to prioritize based on risk factor, applying patches to reduce the exposure, and knowing what to do if a vulnerability was to be taken advantage of. The goal of vulnerability management is to strengthen security and prevent attackers from being able to exploit known weaknesses. A lot of my vulnerability management comes from my experience at my internship as an IT intern. My internship experience allowed me to experience vulnerability management as I was tasked with examining their security policies to spot vulnerabilities and report them back to my supervisors.

Suspicious Email Analysis

My first artifact when it comes to vulnerability management is a document that I put together from a task I had while at my internship. The employees there reported that there was a suspicious email that was sent to a few of them and we looked into it. I was able to detect some red flags like varied IP addresses as legit bulk emails come from consistent known IP addresses. I also used file detonation to execute the suspicious link in an isolated sandbox, coming to the conclusion that it is not a safe link. My supervisor showed me a technique called advanced hunting in Microsoft Defender which showed me that I can see if anybody clicked on the malicious link. We came to the conclusion that somebody actually did click on the link. Using my knowledge I was able to come up with the plan to run an antivirus scan on their device and make them reset their password just for extra safety precaution. She stated that she did not submit any personal information, but we instructed her to follow through with the plan anyways. Thankfully there was nothing hiding in her device after the antivirus scan. This artifact shows that I have the ability to assess threats being sent to employees as well as my ability to mitigate damage that could have been caused from the phishing attempt.

Password Policy Change

My second artifact when it comes to vulnerability management is a document that I made in my internship to propose a change to their password policy. My idea was to enforce setting “Enforce Password History” to 24 or more password(s) and to set “Minimum Password Age” to 1 or more day(s). The password history change makes it so that it takes longer for employees to cycle back to passwords that they have already used after a reset. This combination of settings makes sure that employees are not

allowed to use the same passwords as this is a vulnerability that can cause a lot of problems within the environment. Leaks can happen and this can leak old passwords meaning an employee's account could be easily hacked into.

My supervisors also encouraged this change because password reuse is a major concern within organizations potentially putting them at risk. Using the same password completely defeats the purpose of resets in general. These changes would encourage employees to keep coming up with unique passwords with the first reset. Which would increase security overall.

This artifact shows that I am able to identify a common security weakness and reduce it in a structured way. I recognized that reused passwords create a vulnerability within our security and prioritized it because it affects everybody in the system. Everybody has a password making it a high impact and common vulnerability. This also shows my preventive security mindset as I am proactively trying to strengthen our defenses rather than waiting for an attack to happen and reacting. These are things that I was taught in my courses at ODU and I was happy to be able to apply them and actually come up with a change to strengthen security at my internship.

Employee Training

My third artifact is coming up with a plan for employee training to increase the strength of our human firewall. I handpicked training that I think is useful at this time. Things like phishing training, AI and deepfake training, as well as CEO scams which are all things that are very likely to happen in this day and age.

I had to come up with a plan with consideration of time employees have and the time they are willing to commit to this training. I didn’t want them to just go through the

motion and click what they needed to click to complete it. I want them to actually learn and be able to spot potential attacks that could be directed at them. This makes our security so much stronger and lets security software do its job. This artifact shows my ability to assess the vulnerability of human error and come up with a way to prevent it from exposing our system to attackers. Educating employees creates another layer of security as a lot of cyber attacks are caused by human error. It is important to mitigate human error and this artifact shows that I am able to assess this vulnerability as well as come up with a plan to mitigate it.

My work in the internship was really special to me because as I am in the field of cybersecurity, I never imagined that my input would actually be taken into consideration when fixing problems. Nguyen found that, “Students reconfigured their past in the ePortfolio, and integrated their imagined future through an ongoing process.” (Nguyen, 2013). Reading this part of *The ePortfolio as a Living Portal: A Medium for Student Learning, Identity, and Assessment* really made me think about how far I’ve come. Went from learning in the classroom as a freshman to now actually implementing my own plans to prevent and mitigate attackers online.

Communication

Communication is a very important soft skill in the world of cybersecurity. Asking any professional they will tell you that it is important for a person in the IT or cybersecurity field to be able to communicate with employees that may not know as much as them. It is important that we are able to communicate ideas and concerns that we have in the most effective way possible. It is also important that we are able to communicate and collaborate with people that are in the same field. Strong

communication skills and being on the same page is extremely important when dealing with an incident or attack. Being able to communicate and collaborate are some of the “Most in-demand soft skills sought by companies.” (Henry, 2019).

Basic Security Controls

My first artifact is a document that I composed to inform the employees at my internship of basic security controls. I put this together in order to help them identify and understand these controls. I turned this document into multiple knowledge-based documents for employees. They are able to read up on these things and gain a better understanding of things we are doing. This artifact demonstrates my ability to communicate with employees who are less familiar with the cyber world. Being able to explain and give them an idea of what I deal with is important in helping people to understand and prevent problems on their own in the future. Being able to explain issues and security controls in simple language for them to understand clears up confusion and overall makes it easier to solve issues that will eventually happen.

Milestone Project

My second artifact is a project that I did my senior year that I had to collaborate with a person in the same major to complete. As stated before, being able to collaborate with other people in the same field is another aspect of communication. This project was worth a lot of our overall grade and we were able to collaborate and get it done, getting a good grade for it. I remember it being a little bit of a struggle to collaborate with this person as our schedules were almost completely opposite. However, I was able to actively communicate with him and we were able to find times to meet up and work on this project. This artifact demonstrates that I will be able to communicate effectively with

future coworkers and I am also able to collaborate well on projects to get them done to the best of our ability. Communication is key when it comes to partner work and my communication skills were proficient in finding a good time for me and my partner to be able to create something great.

Info Literacy Group Project

My third artifact is another project that I had, but this one was completed my senior year. It was a group project between four people including myself. My last artifact showed I can work with a partner, this artifact shows that I can work with multiple people. I was able to communicate my thoughts and ideas in a way that my group could easily understand. I was also able to be an active listener trying to understand other people's ideas and asking them questions when I needed clarification. Our effective communication skills helped us to avoid any misunderstandings and made sure that everybody has input. This artifact also shows that I will be good with teamwork in the future as I will most likely be working with a team and other staff in security.

Linux Operating Systems

Linux operating systems are widely used when it comes to IT and cybersecurity. Many critical infrastructures such as servers, websites, cloud systems, data bases, and even cybersecurity tools use Linux operating systems. It’s important to be able to navigate these systems and be able to perform troubleshooting and analysis on what could be going on in these infrastructures. The knowledge that I have in Linux provides a strong base for working in real world security tasks like monitoring and investigating systems.

Password Cracking

My first artifact for Linux is an assignment that I completed in my CYSE270 course here at ODU. It demonstrated my ability to crack simple passwords. Using my skills I am able to see which passwords are too weak and which are able to withstand the password cracking that I was able to do. In the future this will help me to form a plan for password requirements when analyzing a system's password policies. As I did for my internship.

File Permissions

My second artifact is an assignment I did in the same class that shows my ability to manipulate file permissions within Linux. I am able to change who can read,write, and execute a file. If this permission is set incorrectly this will lead to unauthorized access to what could be confidential information. This is critical in cybersecurity as access control is a big deal making sure only authorized users can see certain information. I show in my artifact that I know how to change permissions making sure each user or group can only have access to things I want them to. Whether that be reading, writing, executing, or no permissions at all.

Network Analysis and Firewall Configuration

My third artifact is an assignment I had in my CYSE301 class. This assignment shows that I am able to analyze traffic in Wireshark that comes from Linux systems. It also demonstrates my ability to analyze a firewall and make rules to either block or allow traffic from certain IP addresses. Being able to analyze traffic is an important skill, I know how to see exactly what is happening on a network in real time and being able to detect threats. This relates to being able to manipulate the firewall as I am able to block

these threats from being able to send harmful packets. I also feel that it was smart to include an artifact of the past and an artifact that was created recently. I showed that I am able to develop in this field. “Eportfolios have emerged as a way for students to begin to capture…context-spefic complexities of knowledge growth in teaching.” (Parkes et al., 2013). I feel that adding this artifact along with the other two have shown my knowledge growth well. This will be useful in the future as I will be able to stop bad actors as soon as they make their move on any systems I work with.

Conclusion

My four years at ODU have been very helpful at giving me the necessary skills in order to succeed in my near future. I am hoping that with my new knowledge and skills in ePortfolios I can show my skills. As I know, “College graduates need to be prepared to demonstrate that they have acquired skills, competencies, and knowledge for the global workplace’s demands.” (Holtzman, 2022). School has given me the opportunity to really sharpen my skills in vulnerability management, communication, and Linux operating systems. I think that these skills that I have listed, as well as others I didn’t mention, will set me up nicely for a career that I will have. I think that with these skills and the new skills I learned in this class, I will be able to stand out nicely to employers in my field.

Works Cited

Forde, C. (2008). *What is a portfolio?* SAGE Publications. https://us2.sagepub.com/sites/default/files/upm-binaries/24497_01_Forde_Ch_01.pdf

Henry, H. (2019, July 23). *Top soft skills in the 21st century workplace*. Junior Achievement of South Florida. https://jasouthflorida.org/top-soft-skills-in-the-21st-century-workplace/

Holtzman, D. M., Kraft, E. M., & Small, E. (2022). *Use of ePortfolios for making hiring decisions: A comparison of the results from representatives of large and small businesses*. Journal of Work-Applied Management, 14(1), 18–34. https://doi.org/10.1108/JWAM-01-2021-0001

Nguyen, C. F. (2013). *The ePortfolio as a living portal: A medium for student learning, identity, and assessment*. Stanford University. https://files.eric.ed.gov/fulltext/EJ1107805.pdf

Parkes, K. A., Dredger, K. S., & Hicks, D. (2013). *ePortfolio as a measure of reflective practice*. *International Journal of ePortfolio, 3*(2), 99–115. https://www.theijep.com/pdf/IJEP110.pdf