Reflection Essay: Skills Gained

Ian Hagmann

Interdisciplinary Studies Program, Old Dominion University

IDS 493 Electronic Portfolio Project

Professor David Prihoda

May 1, 2026

Reflection Essay: Skills Gained

Over the course of my learning at Old Dominion University, I have gained a number of skills that should be of use in my future. In this paper I will be reflecting on five artifacts showing broad cybersecurity skill, two artifacts on the skill of self-learning, and two artifacts supporting my programming skill. Over the creation of these artifacts, I needed many resources including websites, documents, journals, textbooks, learning platforms, and lectures.

General Cybersecurity Skill

My Cybersecurity Fundamentals course had us write about a recent cybersecurity attack, focusing on how it works. This was my first time looking at the step by step detail of how an attack works on my own. One reading that stood out to me was one by Professor Messer (2014) that talked about trojan malware, which my paper topic was on a trojan, whom I remembered from my high school cybersecurity classes. My understanding of the general terms helped me understand what the malware did at a high level. Depending on what area of cybersecurity I end up working in, I might need to understand how an attack works to defend against it.

The Cybersecurity Techniques and Operations course had a number of hand-on labs where we were given access to a virtualized network of machines. The lab I chose to highlight was one on ethical hacking in which I exploited a vulnerable windows machine. I was fairly familiar with the command line already but was definitely helped by the thorough document provided to us ("Lab 3— Penetration Test on Windows", 2023). Though I know in the real world, there won't be a step-by-step document telling me how to exploit a machine. It was pretty neat being able to actually hack a machine and not just hear about attacks and vulnerabilities.

In my Windows System Management and Security course, we had a final research paper on a topic of our choosing. I chose to write about Bluetooth security, which I didn't know much

about. Researching this was a little difficult finding so many sources for the information I needed. I cited six resources, two of which really stood out. The first one (Padgette et al., 2022) was very thorough and had plenty of nice figures. The second one (Hassan et al., 2018) included quite the list of attacks on Bluetooth with explanations. I think this was my first time doing such research on such a prominent technology at such depth. Being able to research the features of a technology in depth will surely help me in my future work.

Cybersecurity Strategy and Policy was quite different from other courses I have taken and I think that my midterm was my best work that came out of the course. It was a new experience for me reading and analyzing something published by the White House (2023). I also ended up reading a law journal (Christiansen & Jarrett, 2019) for the first time. Connecting other sources for this topic was difficult when choosing one pillar to focus on. Analyzing the way the National Cybersecurity Strategy document fits into broader national policy was much harder and so I didn't write very much on that. This paper had me researching in a different area than I was used to.

The final project in my Management of Information Security course was a group project and much larger in scope than I had seen before. With such a large scope of requirements, my group decided on a time to meet in the library to plan out how we would divide the work. That took longer than I thought it would and it was difficult to spread the work evenly with the many different requirements. While writing my sections I mostly had ideas in my head and with the help of the textbook (Whitman & Mattord, 2022), I was able to finish my part. We also had to work together on finding suitable hardware from the Cisco website (*Network Switches*, n.d.), fulfilling requirements across our sections. This was a more valuable group work experience than others I have had in courses due to the scale and integration.

Self-Learning Skill

My OPNsense Firewall Blocklisting personal project was something I undertook because I was curious what it was like running a firewall with a default deny rule, preventing all traffic not specifically allowed. I had used an OPNsense firewall before in a guided lab, but not on my own. Doing so was fairly simple, though I did run into a few trouble spots. The first thing I did was download the incorrect file type for installing the OPNsense operating system. Then I had some trouble when first trying to set firewall rules on the wrong interface. I was naively trying to block incoming traffic on the WAN side instead of outgoing from the LAN side which would have made more sense if I was trying to prevent information from getting out into the greater internet. For the other configurations on the firewall itself I was mostly reading the built-in information on what everything did. From this experience, I was reminded that Linux uses HTTPS to update and how few ports would be necessary for that. I also thought of the effort it might take to add a rule to allow something which isn't working properly through by figuring out which ports it needs.

I received my Intel NUC as a gift and wanted to find something to do with it. I decided to install Arch Linux as the operating system because of its difficulty and how minimal it is as the Intel NUC is a mini PC. When I installed Arch, they had just started including a guided install, but I wanted to try the old manual way with the help of the installation guide on the wiki (*Installation Guide - ArchWiki*, n.d.). It was fairly difficult, but I managed to successfully install Arch Linux and moved onto making my NUC easier to access. I had heard of using keys as a way to authenticate an SSH connection instead of a password, so I figured that out with some search engine queries. Next, as my main desktop has a wireless NIC, I wanted to get the NUC to broadcast a wireless network upon booting. That was quite difficult to find what I could use to do

that and how to configure it. I ended up using NetworkManager and needed to set up Kea DHCP for a DHCP server so that I wouldn't have to manually set my IP. Then I wanted to try hosting a Minecraft game server, which wasn't too hard with some web searches. I also found a Python script that I could modify slightly to broadcast the server in a strange way. Lastly, I wanted to host the Damn Vulnerable Web App as I previously messed around with it in the Cyber Security Student Association. Overall, I was glad I could make use of my gift and learned a lot about Arch Linux and running services/servers.

Programming Skill

In my Basic Cybersecurity Programming and Networking course, we had a final project to encompass our learning of Python and networking concepts. I had some Python knowledge from before this class but did learn more like working with files and networking sockets. It seems most of what I learned came from MindTap (*MindTap - the Leading Digital Learning Tool*, 2019), Cengage's learning platform, which I no longer have access to. Programming has always been easy for me, so I had no trouble writing my final project code. I made sure when putting it together to have the leaderboards and timing done on the server side to prevent some forms of cheating. Having a server side and client side program made me think about the design choices of where to put what logic. I am even using what I learned about working with files and socket programming in my courses this semester.

The final project in my other programming course, Introduction to Object Oriented Programming, was the culmination of our Java learning. This one was different in having to make a program following specifications from a written document. It was also made easier by having a previous problem that was very similar. Before this class I did have some Java learning in high school, so a lot of the course was review. Most of my learning for this project probably

came from the textbook (Deitel & Deitel, 2014) with some further clarifications in the lectures (Kalburgi, 2024). Coding classes and their necessary functions from the written specifications was new to me, but not too difficult.

Conclusion

My time attending Old Dominion University had me creating artifacts that demonstrate general cybersecurity skill, self-learning, and programming. I had some previous experience, but my skills were definitely expanded upon by these courses. The many resources along the way helped me create and accomplish what I set out to do. These courses were spread over a couple of years during my time here at Old Dominion University teaching me many things and furthering my skills. I hope that these skills will aid me in my future out in the working world.

References

Christiansen, N. B., & Jarrett, J. E. (2019). Forfeiting cryptocurrency: decrypting the challenges of modern asset. *Department of Justice Journal of Federal Law and Practice, 67(3)*, 155-180. https://heinonline.org/HOL/PrintRequest?handle=hein.journals/usab67&collection=journals&div=49&id=639&print=section&sction=49

Deitel, P. J., & Deitel, H. M. (2014). *Java How to Program: Early Objects*. Prentice Hall.

Hassan, S. S., Bibon, S. D., Hossain, M. S., & Atiquzzaman, M. (2018). Security threats in Bluetooth technology. *Computers & Security*, *74*, 308–322. https://doi.org/10.1016/j.cose.2017.03.008

Installation guide - ArchWiki. (n.d.). Wiki.archlinux.org. https://wiki.archlinux.org/title/Installation_guide

Kalburgi, V. (2024). 202410_IT_205_15592_IT 205 (10). Old Dominion University, Introduction to Object Oriented Programming. Canvas: https://canvas.odu.edu

Lab 3— Penetration Test on Windows. (2023). In P. Jiang (Ed.), *CYSE 301: Cybersecurity Techniques and Operations.* Old Dominion University.

Messer, P. (2014, September 7). *Trojans and Backdoors - CompTIA Security+ SY0-401: 3.1*. Professor Messer IT Certification Training Courses. https://www.professormesser.com/security-plus/sy0-401/trojans-and-backdoors-2/

MindTap - The leading digital learning tool. (2019). Cengage.com. https://www.cengage.com/mindtap/

Network Switches. (n.d.). Cisco. https://www.cisco.com/site/us/en/products/networking/switches/index.html

Padgette, J., Bahr, J., Batra, M., Holtmann, M., Smithbey, R., Chen, L., & Scarfone, K. (2022). Guide to Bluetooth Security. *NIST*. https://doi.org/10.6028/nist.sp.800-121r2-upd1

The White House. (2023). *NATIONAL CYBERSECURITY STRATEGY*. https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Whitman, M. E., & Mattord, H. J. (2022). *Principles of Information Security* (7th ed.). Cengage Learning.