5/5/2026

Reflection Essay

IDS 493 – Electronic Portfolio Project

AKPOVI, DANIEL
School of Cybersecurity - Old Dominion University

Abstract

In this reflection essay, I discuss how creating my ePortfolio helped me reflect on how my coursework has contributed to my development as a cybersecurity student. I focus on three main skills: scripting and technical skills, analytical thinking, and writing and communication. I explain how my work on Linux systems, ethical hacking, my internship, cybersecurity ethics, Windows patch management, policy analysis, research writing, cyber law, and literature journals helped me prepare for a career in cybersecurity. These artifacts made me see cybersecurity beyond the technical aspects, and this reflection shows how my coursework has influenced my professional development and how my degree is a preparation for my career.

Reflection Essay

As I work on this portfolio, I look differently at my degree. I used to see most assignments as not related. I did one course, then another, and hardly paused to think about how they were related. But creating this portfolio helped me to see those connections through the skills they have given me. The three most notable areas of skill I gained are scripting and technical skills, analytical thinking, and writing and communication ability. I selected them as they align with what I have done, the cybersecurity job I desire, and what employers are looking for. The U.S. Bureau of Labor Statistics estimates information security analyst jobs will grow by 29 percent between 2024 and 2034, and the National Association of Colleges and Employers (NACE) lists communication, analytical thinking, and technology as some of the career-readiness skills of college graduates should possess (NACE Education, 2025; U.S. Bureau of Labor Statistics, 2025). Creating this portfolio helped me understand the point of my degree. Cybersecurity does not just fall within one field, as many security decision impact different sectors. I noticed that during my coursework, where some courses taught me how to set up and monitor systems, how to read logs and identify vulnerabilities, and others encouraged me to consider ethics, risk, and policy, along with the impact of security decisions. This portfolio helped me put this together. I do not view my coursework as individual tasks anymore because they are connected in preparing for my cybersecurity career.

Scripting and Other Technical Skills

Artifact 1: Shell Scripting

Linux System for Cybersecurity (CYSE 270) provides one of the strongest technical foundations in my portfolio. This course focused on Linux in a cybersecurity setting.

Specifically, we covered the installation, configuration, networking, scripting, file systems, and firewalls on a Linux operating system. The Shell Scripting Artifact assignment provided an opportunity for me to create and run bash shell scripts. This was done by writing the scripts in vi, making them executable with "chmod +x" command, verifying permissions for each script, listing the contents of each script file, and running the scripts through the terminal. As part of this assignment, I needed to be very careful about the syntax, permissions, and file paths as one incorrect item would cause the entire script to fail. This experience allowed me to understand that scripting is a skill to possess in system administration. Nyarko-Boateng et al. (2024), describe how bash has an advantage when combined with other command line tools and utilities. They note that Bash provides great ability for automated administrative activities within a Linux environment. That statement can apply to this artifact since the lab showed me how scripting aids in performing efficient system administration and daily cybersecurity operations.

Artifact 2: Ethical Hacking

The artifact from CYSE 301 (Cyber Techniques and Operation) displays a different side of technical skill. This class specifically dealt with ethical hacking, cyber operations, hands-on attack and defense work. The project presented here used Nmap to perform a scan of a target system. Metasploit was used to exploit the SMB and EternalBlue vulnerabilities on the target system. Using meterpreter, the following tasks were performed: creating a Windows 7 payload, uploading files to the target system, and escalating privileges to gain more access to the target machine. The sequence of these steps, from gathering information, choosing the exploit, setting the listener, verifying access, and recording what happened, was necessary to complete the task correctly. If I missed any steps in the proper order, the entire task would fall apart. Beyond the coursework itself, this project allowed me to think about information security in the same way

that O*NET describes information security analysts: as individuals who identify the vulnerabilities in a system and who create suggestions or solutions to those identified weaknesses (O*NET OnLine, 2026).

Artifact 3: Final Internship Paper

My internship (CYSE 368) also gave me an insight into the technical side of the industry. In the final internship paper, I discussed the various tasks that I performed such as monitoring devices with SolarWinds, reviewing firewall entry requests with Siphon, checking VLAN and ACL segmentation of the network, reviewing and documenting tickets, and even building my own lab at home with pfSense and Nessus Essentials. While these tasks might not necessarily be the flashiest tasks for the cybersecurity field, they are certainly some of the most useful. Much of the work required patience and focus. Furthermore, security decisions on a device do not affect only that device, so any change to any devices in the network require a specific reason and a boundary for the change. Building my lab also helped to fill in the gaps in my knowledge regarding firewall settings. For instance, I was able to play with the firewall rules, configure NAT and port forwarding settings, review the logs created by these devices, and perform vulnerability scans on the systems after making changes. The skills I learned here are directly applicable to current job postings for system administrators (Leidos, n.d.).

Analytical Thinking Skills

Artifact 1: Case Analysis: Cyberwar – Fair Fight or Digital Fallout

Cybersecurity Ethics (PHIL 355E) challenged me to consider beyond the technical aspects of cybersecurity. Until then, I tended to focus on whether a system was safe or not, whether a control was successful or unsuccessful, whether a defense was able to prevent an attack. A different set of questions was introduced by this course. Boylan, Taddeo and

contractarianism were some of the tools I applied in the artifact I use here to explore cyberwar. I argued that most cyber wars cannot pass a fairness test since civilians are co-users of digital infrastructure, digital harm does not require actual physical destruction to be significant, and no one behind a veil of ignorance would desire to accept rules that put common people at risk of unseen cyber damage. What made this artifact analytical and distinguished it from merely being a reflection is the process of evaluating both sides of an issue and comparing each argument to a specific frame of reference. Therefore, instead of just determining if a cyber action worked; I determined who took the risk for the cyber action; who did not agree to it; and is there enough reason to support the decision made to complete the cyber action that would pass ethical review? The type of analysis I used aligns well with the NIST's guidance for workplace skills that connects cybersecurity work to competencies such communication, problem-solving and good judgment (NICE Framework Resource Center, 2024).

Artifact 2: Impact of Windows Patch Management on Cybersecurity

The Windows System Management and Security (CYSE 280) research paper improved my analytical skills because it required me to consider a technical issue from an evidence, process and consequences perspective, rather than just a configuration perspective. I examined Windows patch management and its impact on security in this project. It was not enough to explain the functions of patches. I needed to also explore why and when patching can be delayed, the challenge associated with maintaining security while maintaining operational stability, the use of frameworks and automation in managing patches, and the greater exposure to threats when known vulnerabilities are left unpatched. This approach allowed me to view system management as a series of decision points as opposed to a checklist. Dissanayake et al. (2021), identified through a systematic literature review of 72 studies that patch management is

influenced by both technical and socio-technical issues, and that many commonly known problems have been only partially solved by existing solutions. This finding correlates with this artifact as my paper was required to address patching as both a technical and an organizational and risk-based problem simultaneously.

Artifact 3: Policy Analysis Paper

I furthered my ability to think analytically through CYSE 425W (Cyber Strategy and Policy) by examining cybersecurity policy beyond its superficial understanding. This class covered cyber strategy and policy which included planning principals, risk management, political and ethical ramifications, institutional relations, and national security concerns. In the policy paper I used in this artifact, I utilized concepts like contextual integrity, privacy self-management, chilling effects and unequal harm across communities to examine policies that protect the privacy of consumers. More importantly in this project, it forced me to view privacy as more than simply an individual setting issue. It is also about whether data flows are appropriately situated within their context; whether individuals have sufficient safety to engage in digital activities; and whether disparate groups experience equal levels of exposure to risk. To accomplish this kind of work, it is required to do beyond a simple summary. I was compelled to define the connection between policy, public trust and behavior, and provide examples of how security mechanisms may influence who feel protected and who feels watched. According to the World Economic Forum (2025), analytical thinking is among the most skills employers appreciate, whereas networks and cybersecurity are the two fastest expanding skills areas, which is why I closely associate this artifact with the work I hope to do.

Writing and Communication Skills

Artifact 1: AI, Privacy, and Data Security

ENGL 211C (Writing, Rhetoric and Research) provided me with the writing foundation that supports much of the rest of my college experience. My AI, privacy, and data security research argument served not as a one-off task to complete. It taught me to make a purpose in writing a paper. In this assignment, I had to clarify the important terms, narrow the topic, structure the research, and show the reader the argument without losing the main point. It may seem easy until you attempt to do it well. This course has made me realize that there is a difference between information gathering and case making. Such a difference is important when it comes to cybersecurity. The value of a report or a recommendation is quickly lost when the writing is loose, diffused or lost in detail without purpose. Communication is one of the fundamental career-readiness competencies as NACE (2025) defined; and that is quite well-suited to the field since security professionals may need to provide an explanation of technical risk to non-technical people.

Artifact 2: Overview of the IoT Cybersecurity Improvement Act of 2020

The English writing I did in CYSE 406 (Cyber Law) was quite different from the one in ENG 211C, but it was also crucial. This legislative research aide memo assignment requested that I break down the IoT Cybersecurity Improvement Act of 2020, provide an overview of what the law does, identify the shortcomings of the law, and offer some potential improvements in a way that would make sense in a letter to the constituents. The audience is a non-cybersecurity population. I could not conceal myself behind jargon or presume a common background. There was a need to ensure that the issue was readable and useful. Such writing is important in the workplace, where security tasks frequently involve policy, compliance, and communicating with the public. Among the activities that O*NET (2026) records as related to the work of information

security analysts are documenting security issues and writing reports; reason why this artifact is more than a class exercise to me.

Artifact 3: Journal Entries

WCS 100L (Introduction to World Literatures & Cultures) is one of the less obvious artifacts in this portfolio, but I believe it fits in. The journal entries of this course helped me become better at writing with context, voice, and perspective. On one occasion, I noted the message of Chimamanda Adichie about the harmfulness of single story and how repetition of narratives reduces people and places into one image. Other entries were on migration, race, state violence, and culture expectation. Those subjects helped me be more attentive to the how we frame people and how we value opinion. This is more important in cybersecurity than I initially thought. Users, colleagues and clients are never abstract entities. Security work occurs in an environment that is defined by trust, fear, culture and different experiences. Equity and inclusion are listed as one of the competencies of career readiness by NACE (2025); moreover, this artifact allowed me to develop this aspect by writing and reflecting instead of only focusing on technical works.

Conclusion

Looking across this portfolio, I see how each of these projects connects to the others. While they may indicate different skills and knowledge, they collectively form a picture of the type of cybersecurity professional that I am becoming. The technical projects have allowed me to learn about the necessary skills in the field, such as my ability to assess systems' security and my capacity to identify types of threats that can exist within a network. The analytical thinking artifacts show a different kind of growth. They required me to examine cybersecurity questions through ethics, system management, patching practices, risk, and policy rather than stopping at

the technical surface. The writing courses have helped me to develop further as a student because I now have a better understanding of how to convey my knowledge of cybersecurity to others. The current ePortfolio proves that what I am prepared to step into the cybersecurity field with real skills, and a wider perspective. At this stage in the process, I no longer view my degree as a collection of assignments. I see it as the foundation of my professional identity.

References

Dissanayake, N., Jayatilaka, A., Zahedi, M., & Babar, M. A. (2021). Software security patch management - A systematic literature review of challenges, approaches, tools and practices. *Information and Software Technology*, *144*(0950-5849), 106771. https://doi.org/10.1016/j.infsof.2021.106771

Leidos. (2026). *Mid-level system administrator*. Leidos Careers. https://careers.leidos.com/jobs/17501842-mid-level-system-administrator

NACE (2025). *Competencies for a career-ready workforce career readiness competencies*. https://www.naceweb.org/docs/default-source/default-document-library/2025/career-readiness/competencies/nace-career-readiness-competencies-december-2025.pdf

NICE Framework Resource Center. (2024, May 16). *Workplace skills and the NICE framework | NIST*. NIST. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/workplace-skills-and-nice-framework

O*Net OnLine. (2026, April 14). *Information security analysts*. O*Net OnLine. https://www.onetonline.org/link/summary/15-1212.00

Owusu Nyarko-Boateng, Nti, I. K., Mensah, A. A., & Gyamfi, E. K. (2024). Controlling user access with scripting to mitigate cyber-attacks. *Scientific African*, *26*, e02355–e02355. https://doi.org/10.1016/j.sciaf.2024.e02355

U.S. Bureau of Labor Statistics. (2024, August 29). *Information security analysts: Occupational outlook handbook: U.S. bureau of labor statistics*. Bls.gov; U.S. Bureau of Labor Statistics. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

World Economic Forum. (2025, January 7). *The future of jobs report 2025*. World Economic Forum. https://www.weforum.org/publications/the-future-of-jobs-report-2025/digest/