E-Portfolio Reflection

Esther Lawal

IDS 493

12/2/2025

Cybersecurity Portfolio Reflection: From Technical Skills to Professional Readiness

Introduction

When I initially started to study cybersecurity as a degree, my perception was that the job of the security person was all technical: find vulnerabilities, fix systems, and apply controls. IDS 300 W changed this perception. During that course, I was introduced to theory and the so-called narrative identity, meaning a project portfolio is not a mere set of projects but rather a story that it narrates about your future career. My portfolio has a particular narrative: I began with basic technical skills, found out what was missing in my knowledge base, and made a conscious decision to acquire additional skills, which are policy, leadership, and organizational thinking. This story proves that contemporary cybersecurity experts should combine both technical skills with policy knowledge, human factor knowledge, and communication capabilities. This integration can be seen in my artifacts. They demonstrate that cybersecurity is not a matter of tools and code only, it is about how technical decisions impact organizations, teams and people.

Network Security

Vulnerability scanning with Nmap and Nessus was presented to me in my Network Security. I evaluated the actual network infrastructure, traced the security vulnerabilities and provided remedies. However, the true learning was received through the realization of WHY this work is important.

The problem was to relate technical discoveries to business effects. In the IT 315 course, my professor has stressed that it is not important to have a vulnerability unless it compromises the mission of the organization. This statement stuck with me. I needed to understand to inquire: What are the most vulnerable areas? How much money would it cost to fix them compared to the

cost of being attacked? It was the first big lesson that I was able to make: cybersecurity is not only technical.

I also enrolled in CS 425 (Cyber strategy and policy) at the same time, which compelled me to consider such compliance guidelines as NIST 800-53. Then, it happened that my scan results were not simply the data points anymore, but the evidence of the policy violations. This was not easy to integrate at the beginning. I had a hard time striking a balance between technical accuracy and policy requirements. However, the revelation occurred when I understood that they are not conflicting goals; they are one and the same, but different perspectives of the same goal.

This intuition was confirmed by Ramezan (2023): operations roles (32.8 percent of cybersecurity engineering) need technical expertise and policy knowledge. My project proved that I was able to provide both.

Penetration Testing: Identifying Knowledge Gaps (CS 301)

CS 301 shifted me out of passive scanning into active exploitation. I applied Metasploit and Burp Suite to attack intentionally vulnerable applications. This was thrilling, yet there was a major gap-I could not code. My professor stated that 67.6 percent of the jobs involving penetration testing involve programming. I was aware that I possessed technical knowledge in the field, yet I was deficient in depth in programming. This was a painful but valuable lesson, I must confess. I attended class day in and day out with some Computer Science majors who were aware of how-to code. I did not. I had to understand that this was a weakness and I had to correct it.

The legal factor was equally significant. As Jacob et al. (2020) observe, cybersecurity education needs a grasp of the computer crime statutes- knowing what is legitimate testing and unlawful hacking. My CS 201S policy background was beneficial, yet in CS 450, I also realized

that, in many ways, penetration testers are legally liable. All tests should be approved. All findings should be defensively recorded. It has changed my views about security work-it is not only a question of identifying vulnerabilities, but a question of identifying them legally and morally. The other thing this project taught me is that it is important to recognize gaps in knowledge. The initial stage of learning is to acknowledge that you do not know.

Linux system (CS 270) shell script and security policy, password cracking and task automation. The technical process was simple: set up rules, test alerts, and document processes. The valuable learning was the learning of the purpose of these rules.

According to Abrahams et al. (2024), knowledge of the key performance indicators (KPIs) is needed in order to quantify the effectiveness of security operations. In CS 270, I struggled with this? How long is a satisfactory response time? They are not technical questions, but organizational questions. I needed to know what my organization appreciated, to what extent it could take risks and how swift a response was achievable.

In my class exercise, I committed an error. I had an excessive number of detection rules. Thousands of false alerts were generated by the system. The lesson of that failure was that security operations are about balance, which is not taught in textbooks. An ideal detection brings about alert fatigue. There is alert fatigue, which leads to operators missing actual attacks. This applied learning altered my approach to designing security systems.

According to Jacob et al. (2020), a cybersecurity professional must be aware of the human actors and their decision-making process. I continued to recall the phrase following my tabletop exercise. Organizations are not shielded by technical procedures. Individuals who adhere to process safeguard companies. Unless people know their role or are even sure about the process, the processes fail. This changed my professional philosophy, and I am no longer focused

exclusively on technical solutions. Now I ask: How will people actually execute this plan? What do they need from me in terms of support? How do I convey the message clearly under pressure? Abrahams et al. (2024) identify "leadership endorsement sets the tone for cybersecurity culture." After CS 425, I understand this deeply. Technical controls matter, but leadership and communication matter more.

Cloud Security, Encryption, and Security Policy: Integrating Knowledge

My CS 270 (Linux System), CS 301(Techniques and Operations), and CS 425 (Security Policy) projects showed cross-domain integration. CS 270 implemented basic security concepts on AWS. CS 115 made me study Python and practice cryptographic functions- my long-overlooked programming gap is now filled. CS 425 entailed the development of policies in accordance with NIST 800-53 and ISO 27001.

The initial experience of these projects was disconnected. However, it is IDS 300W that taught me to view portfolio narrative. Every project is based on prior knowledge. IT 315 gave network basics. CS 301 presented new technical challenges. CS 300 has made me understand the role of technical work in sustaining organizational operations. CS 201S has taught me that people are important. Then CS 430 trained my programming skills (a weakness I detected in CS 450). CS 425 demonstrated the way in which policy frameworks inform all technical decisions. CS 270 showed how these integrated skills could be applied to modern infrastructure. This is narrative identity: the narrative that my portfolio gives is not a set of accidental projects but a deliberate cultivation of skills.

Malware Analysis: Continuous Learning

The most challenging project was my Malware Analysis. I needed to study assembly language, reverse engineer ransomware with IDA Pro, and deassemble code. For three days, I

was completely lost. Assembly code looked like nonsense. But I kept working. I watched tutorials. I asked my classmates questions. Something finally clicked. I got the malware behavior.

The best lesson I learned in my entire degree is that cybersecurity professionals are lifelong learners. The discipline is dynamic. The tools change. The attack methods evolve. The threat landscapes change. You cannot graduate and stop learning. You have to be okay with being uncomfortable. You need to learn about new technologies quickly. You need to be okay with not knowing. Ramezan (2023) shows threat intelligence roles require programming skills and technical experience, specializing in a task, comprising 4.2% of cybersecurity jobs. This project put me into such a specialization.

How My Thinking Changed

Prior: Cybersecurity is technical. Find vulnerabilities. Implement fixes.

After: Cybersecurity is a people business. Without organizational commitment, clear communication, and leadership, technical controls fail. Cybersecurity staff need to traverse both technical and non-technical spaces.

Before: I must be informed about all about cybersecurity.

After: I ought to know how to learn anything about cybersecurity. It is a strength, not a weakness, to admit knowledge gaps and to work on them.

Interdisciplinary Integration: Why This Matters

My portfolio demonstrates something Ho et al. (2023) emphasize: "bridging technical and policy approaches" is essential.

- Technical skills (Nmap, Nessus, Metasploit, Burp Suite, Splunk, AWS, Python, IDA Pro)
- Policy understanding (NIST 800-53, ISO 27001, legal frameworks)

- Organizational knowledge (incident response, leadership, communication, risk management)

According to Yusuf (2024), "cybersecurity professionals must work in teams and communicate effectively with stakeholders." Each of the artifacts in my portfolio reflected this. The Network Security required the communication of findings to management with limited technical knowledge. The Incident Response Plan needed leading teams. The Security Policy Framework had to explain technical concepts in accessible ways. Jacob et al. (2020) explain that traditional cybersecurity education has focused on technical knowledge, which has neglected "the human actors and their decision-making process." My portfolio shows that human factors are not something apart from technical work but are integrated into it.

Conclusion

My artifacts reflect extensive knowledge of cybersecurity. However, more to the point, they are a learning process. I switched my mindset from thinking that cybersecurity is a technical thing to the fact that it is an interdisciplinary one. I shifted towards not taking hard challenges as learning opportunities. I shifted the emphasis of my attention towards people. IDS 300W helped me realize this path along portfolio narrative and narrative identity.

Ramezan (2023) confirms that the employment market needs such an integration: 84 percent of the opportunities demand professional experience, 71 percent demand certifications, and employers are looking to hire professionals who are not only knowledgeable in the technical field but also in the organizational one. My portfolio addresses this.

This reflection is the foundation of my immediate priorities: completing the certification to become a Security+ user, developing a portfolio on GitHub, and adding to my LinkedIn

profile. I do know that employers require demonstrations of lifelong learning, technical skill, and professional involvement.

My road map is simple: I am going to work as a security analyst where my skills in SIEM and incident response can be used, and then I will develop skills in pentesting (CEH) and cloud security (AWS). Then I will build upon this foundation based on the requirements of the market and my growing interests. In doing so, I will focus on both purely technical competencies and general professional ones such as policy awareness, communication, leadership, and life-long learning. Thus, under this preparation, my portfolio is to become the starting point for a career dedicated to solving real security problems of organizations.

References

Abrahams, T. O., Farayola, O. A., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Cybersecurity awareness and education programs: A review of employee engagement and accountability. *Computer Science & IT Research Journal, 5*(1), 100–119.

Ho, L., Rabiei, S. & White, D. (2023). *A comparative study of interdisciplinary cybersecurity education*. UC Berkeley School of Information. https://cltc.berkeley.edu/publication/interdisciplinary-cybersecurity-education/

Jacob, J., Peters, M., & Yang, T. A. (2020). Interdisciplinary cybersecurity: Rethinking the approach and the process. In K.-K. R. Choo, A. Dehghantanha, & R. F. Parizi (Eds.), *Advances in intelligent systems and computing* (Vol. 1055, pp. 61–74). Springer Nature Switzerland. https://doi.org/10.1007/978-3-030-31239-8_6

Ramezan, C. A. (2023). Examining the cyber skills gap: An analysis of cybersecurity positions by sub-field. *Journal of Information Systems Education, 34*(1), 94–105.

Yusuf, O. I. (2024). Bridging the gap: Aligning cybersecurity education with industry needs. *International Journal of Information Technology and Computer Engineering, 43*(1), 1–8.