Reflective Essay

Diane Gilzow

Old Dominion University

IDS 493 - Electronic Portfolio Project

Dr. Gordon-Phan

May 5, 2026

Abstract

This reflection essay examines the development of three cybersecurity skills I've developed in my academic career: Linux system administration and security, risk assessment analysis, and ethical hacking. Through coursework, lab assignments, and internships, I analyze how these skills were developed and applied in both academic and real-world settings. Each artifact demonstrates a different aspect of cybersecurity and how I've applied them.

Introduction

Throughout my journey in my cybersecurity program, I've learned that cybersecurity isn't just about technical skills, it's about connecting different types of knowledge and applying them in real situations. Instead of learning things in isolation, I had to combine ideas from cybersecurity, IT, interdisciplinary studies, ethics, and communication to solve problems.

The three main skills I developed are Linux system administration and security, risk assessment analysis, and ethical hacking. These skills all connect to different parts of cybersecurity work. Linux helped me understand how systems actually run and how to secure them, risk assessment taught me how to evaluate and prioritize threats, and ethical hacking helped me understand how attackers think and secure systems through their techniques. Each of these skills came from different assignments and experiences that helped me grow both technically and professionally.

Linux System Administration and Security

One of the first major skills I developed was Linux system administration and security. When I first started taking classes at ODU, one of the first courses I took was an introductory Linux class that covered the basics of the operating system and how to use the terminal to execute commands. Initially, I was unfamiliar with Linux and wasn't sure what to expect, but I was excited to learn something new that was directly relevant to cybersecurity. Little did I know that Linux would become one of the foundational skills I would continue building throughout my studies.

One of the first assignments that I did that helped me be more proficient with Linux was a file permissions lab assignment. In this assignment, I worked with user accounts, groups, and directory permissions to control access within a Linux environment. I created multiple users and

groups, assigned primary and secondary group memberships, and configured shared directories with specific permission levels. One of the most important parts of this lab was using octal permissions and the umask command to control default file permissions. I also tested how different permission settings affected access by switching between user accounts and attempting to access shared files. This helped me clearly understand how Linux enforces security through access control and how small configuration changes can have a big impact on system security.

Another artifact that strengthened my understanding of Linux security was a steganography lab using the steghide tool. In this assignment, I learned how information can be hidden inside image files, which introduced me to the concept of steganography and how it differs from cryptography. I used steghide to embed a text file into an image, set a password for protection, and then extracted the hidden message to verify the process. This exercise helped me understand that security is not only about restricting access but also about concealing information in ways that make it less detectable. It also expanded my perspective on how data can be protected and manipulated within systems.

The third artifact that contributed to this skill was a task automation lab assignment using Bash shell scripting and crontab scheduling. In this assignment, I wrote a shell script to automate system backups for a user's home directory. The script created a tar archive, applied compression, and moved the backup to a designated directory. I also used crontab to schedule the script to run automatically for a set period of time before cancelling the job. This assignment helped me understand how automation can improve system efficiency and reliability, especially in system administration tasks where repetitive processes are common.

Through these artifacts, I developed a much deeper understanding of Linux system administration and security. This skill is especially important for my cybersecurity career goals

because many systems, servers, and security tools operate in Linux environments. Understanding how to configure and secure these systems gives me a strong technical foundation that I can build on in professional roles.

Risk Assessment Analysis

Another major skill I developed throughout my program is risk assessment analysis. This involves identifying security risks, evaluating how serious they are, and deciding what should be prioritized based on potential impact. At first, I thought this skill would just be about finding vulnerabilities, but I quickly learned that it also requires communication, structured thinking, and understanding how organizations actually operate.

One of the most important experiences I had with this skill was during my ODU Cybersecurity Clinic internship, where I worked within a team with local businesses that needed cybersecurity support, and the organization that I worked with was the Norfolk Botanical Garden. During the internship, my team and I visited the office of one of their IT workers and received a tour of their environment. Additionally, we asked questions about their security posture and concerns. This helped me understand how cybersecurity looks in a real organizational setting, not just in a lab. Based on this visit, my team and I created a report and presentation that outlined their potential risks and provided recommendations for improvement. This experience taught me how important it is to gather information directly from stakeholders and translate technical findings into practical advice that an organization can actually use.

Another artifact I want to showcase was a project from my Information Assurance class, where I took on the role of an incoming Chief Information Assurance Officer (CIAO) for a fictional company, ABC Inc., after they experienced a ransomware attack. In this scenario, I conducted a full vulnerability assessment, created a threat matrix, and developed a strategic

response and recovery plan, which included a communication plan. What made this assignment challenging was that I had to think at a leadership level rather than just a technical one. I wasn't just identifying issues, I also had to prioritize them and recommend long-term improvements for the organization. This helped me understand how cybersecurity professionals need to balance technical analysis with business impact.

Finally, the last artifact I want to highlight for this skill was a threat modeling lab assignment from my ethical hacking course. In this assignment, I identified critical assets within a system, such as ID card data, cloud databases, access control servers, mobile applications, IoT door controllers, and access logs. For each asset, I analyzed why it was important and how it could be targeted. I then created a STRIDE threat model to identify potential threats across system components, such as spoofing, information disclosure, denial of service, and tampering. After that, I used a DREAD-based scoring system to evaluate and rank the risks based on factors like damage, exploitability, and affected users. Finally, I mapped each threat to mitigation strategies using the MITRE ATT&CK framework. This assignment helped me connect technical system design with structured risk analysis. Instead of just thinking about what could go wrong, I had to evaluate how likely each threat was and what defenses would actually reduce risk.

These three artifacts helped me understand that risk assessment is not a one-time task, but a continuous process that combines technical analysis, communication, and decision-making. I learned how to analyze systems from multiple perspectives and prioritize what matters most. This skill is especially important in cybersecurity careers, where professionals are expected to assess risk quickly, explain it clearly, and recommend practical solutions.

Ethical Hacking

The third major skill I developed throughout my cybersecurity program is ethical hacking, which focuses on identifying vulnerabilities by thinking from an attacker's perspective. Before taking this course, I mainly saw cybersecurity as defensive, but ethical hacking helped me understand that in order to protect systems, you also need to understand how they can be attacked. This skill required both technical knowledge and a different way of thinking, where I had to approach systems with curiosity and persistence.

The first artifact that helped me develop this skill was a passive reconnaissance lab. In this assignment, I used tools like Shodan, WHOIS, and Netcraft to gather information about systems without directly interacting with them. I searched for publicly accessible devices, such as web cameras and servers, and analyzed details like open ports, domain names, and known vulnerabilities. I also research CVEs associated with these systems and connected them to techniques in the MITRE ATT&CK framework. This lab showed me how much information is publicly available and how attackers can use that information to identify potential targets. It also helped me understand that security starts with minimizing exposure, since even small details can be used against a system.

The next artifact was an active reconnaissance and vulnerability scanning lab. In this assignment, I moved from passive observation to directly interacting with a target system. I used tools like dig and host to check if a domain was live, performed DNS enumeration using dnsenum, and used Nmap to conduct ICMP and TCP sweeps as well as port scanning. I also used NSE scripts to identify known vulnerabilities and attempted brute-force attacks using different protocols. This lab helped me understand how attackers actively probe systems to gather deeper information and identify entry points. It also showed me how different tools can be combined to build a more complete picture of a target's security posture.

The final artifact was a web application security lab using DVWA and Mutillidae, where I practiced exploiting vulnerabilities in a controlled environment. In this assignment, I performed an SQL injection attack by inputting a statement that always evaluates to true, which allowed me to retrieve all user records from the database. I also used tools like sqlmap to automate the discovery of injection points and payloads. Additionally, I explored how different security levels and features in DVWA and Mutillidae affect vulnerability exposure. This lab helped me understand how common web vulnerabilities work in practice and how easily they can be exploited if proper security controls are not in place.

Overall, this skill changed the way I think about cybersecurity. Instead of only focusing on defense, I now consider how systems can be attacked and where they might be vulnerable. Ethical hacking requires creativity, attention to detail, and persistence, especially when things don't work on the first try. These are all skills that are important in cybersecurity careers, where professionals are expected to identify and fix vulnerabilities before they can be exploited by real attackers.

Conclusion

Looking back on my experience in my cybersecurity journey, I can clearly see how much I've developed both technically and professionally. The three main skills I built are in Linux system administration and security, risk assessment, and ethical hacking. Each represents a different part of cybersecurity, but together they form a complete skill set. Linux gave me the foundation to understand and manage systems, risk assessment taught me how to evaluate and prioritize threats, and ethical hacking helped me think from an attacker's perspective to identify vulnerabilities.

One of the biggest takeaways from this program is how important interdisciplinary thinking is in cybersecurity. None of these skills exist on their own. For example, ethical hacking connects directly to risk assessment because identifying vulnerabilities is only useful if you can evaluate their impact. Similarly, Linux system administration supports both areas because understanding how systems are built and configured is necessary to both defend and test them.

Overall, my journey at ODU has helped prepare me for a career in cybersecurity by giving me both the technical foundation and the mindset needed to succeed. I now feel more confident in my ability to analyze systems, assess risks, and identify vulnerabilities in a structured and meaningful way. Moving forward, I plan to continue building on these skills and applying them in real-world environments. This reflection has helped me see how far I've come and how these experiences have shaped my readiness for the cybersecurity field.