Final Reflective Essay

Reema Chakma

Old Dominion University

IDS 493: Electronic Portfolio Project

Dr. Sherron Gordon-Phan

May 05, 2026

Abstract

This reflection highlights my development of technical, analytical, and interpersonal skills through academic coursework, lab activities, internship experience, and professional development opportunities. Each skill area is supported by three artifacts that demonstrate my learning and practical application of cybersecurity concepts. As a cybersecurity student preparing for a career as a security analyst or system administrator, I have engaged in hands-on technical experiences such as Linux administration, shell scripting, SQL injection testing, and user access management, which strengthened my technical foundation. I have also developed strong analytical skills through case studies on data ethics, professional ethics, and a machine learning-based intrusion detection system using Gradient Boosting. In addition, my interpersonal skills have been enhanced through teamwork in class projects, internship collaboration with the City of Suffolk IT team, and communication-focused workshops. Together, these experiences demonstrate my ability to approach cybersecurity as an interdisciplinary field that integrates technology, ethics, and human interaction.

Introduction

The field of cybersecurity is constantly evolving as organizations continue to face cyber attacks such as, data breaches and ransomware attacks. In this rapidly changing environment, cybersecurity professionals must develop not only strong technical expertise, but also analytical thinking and interpersonal skills such as teamwork, communication, adaptability, and research.

As a cybersecurity student preparing for a future role as a security analyst or system administrator, I have built a combination of technical, analytical, and interpersonal skills through my coursework, job experiences, and internship opportunities. These experiences have helped me understand cybersecurity as an interdisciplinary field that must be examined from multiple perspectives, including law and ethics, social sciences, and technology.

Throughout my academic journey, I have engaged in projects, assignments, and labs that have strengthened both my technical and analytical skills. In addition, my job experiences and internship opportunities have exposed me to real-world challenges, further enhancing my interpersonal skills such as communication, teamwork, and problem-solving. The artifacts included in my portfolio demonstrate how I applied my technical skills, problem-solving skills, research, and teamwork skills.

Technical Skills

One of the most important skills I developed throughout my academic experiences is technical proficiency. Technical skills are essential in this field because cybersecurity professionals are responsible for protecting systems, networks, and sensitive information from cyber threats and vulnerabilities. Through courseworks, labs, and projects, I learned foundational

cybersecurity concepts such as network security, firewalls, encryption, system hardening, access control, threat detection, and risk management. Additionally, I have applied my technical skills through hands-on experience with Linux fundamentals and Python programming. These skills are highly valuable in cybersecurity because Linux is widely used in servers, security tools, and enterprise environments, while Python enables cybersecurity professionals to automate tasks, analyze data, and develop scripts for system monitoring, vulnerability assessment, and incident response. Developing proficiency in these areas has strengthened my ability to solve technical problems efficiently and adapt to real-world cybersecurity challenges.

The three artifacts I have included to demonstrate my technical skills are a shell scripting lab, an SQL injection lab, and a Linux-based lab assignment focused on user groups and permission management. These artifacts highlight my ability to work with operating systems, understand cybersecurity vulnerabilities, and apply technical knowledge in practical, hands-on environments.

Artifact 1: In this lab, I created shell scripts using the Nano editor and applied various Linux commands to navigate and manage files within the Linux environment. I used commands such as chmod to assign executable permissions to script files and implemented conditional statements to control program flow and automate specific tasks. This lab strengthened my understanding of Linux fundamentals, scripting, and automation, which are essential technical skills in cybersecurity.

Artifact 2: In this lab, I performed SQL injection attacks within a controlled virtual environment using Damn Vulnerable Web Application hosted on a virtual machine alongside Metasploitable2. The objective of the lab was to understand how attackers exploit insecure database queries to

gain unauthorized access to sensitive information. Through this exercise, I learned how SQL injection vulnerabilities occur, how malicious queries can manipulate databases, and why secure coding practices and input validation are critical in cybersecurity. This hands-on experience strengthened my understanding of web application security, ethical hacking concepts, and vulnerability assessment techniques.

Artifact 3: In this lab, I created multiple user groups in Linux, including employee, payroll, and admin groups, and assigned file and directory permissions based on their specific job roles and responsibilities. Using Linux user and group management commands, I configured access controls to ensure that each group could only access the resources necessary for their tasks. For example, the payroll group was granted access to sensitive payroll files, while administrative privileges were limited to the admin group. This activity helped me understand the principle of least privilege and the importance of role-based access control in cybersecurity. Through this hands-on experience, I strengthened my knowledge of Linux administration, system security, and access management practices commonly used in real-world organizational environments.

Analytical Skills

Now, I will discuss my analytical skills through three different artifacts that demonstrate my ability to evaluate problems, interpret information, and make informed decisions from multiple perspectives.

Artifact 1: One artifact that demonstrates my analytical skills is a case analysis focused on user data privacy and organizational data practices. In this assignment, I analyzed how organizations collect, process, store, and use user data while evaluating the ethical concerns associated with these practices. I examined issues such as user consent, data privacy, transparency, and the

responsibilities of organizations in protecting sensitive information. This analysis required me to think critically about the balance between business operations and ethical decision-making, while also considering the legal and social implications of data misuse. Through this assignment, I strengthened my ability to assess cybersecurity and privacy issues from both technical and ethical perspectives.

Artifact 2: Another artifact that highlights my analytical skills is a case analysis on professional ethics in cybersecurity and information technology. In this assignment, I analyzed the case of a software engineer who knowingly developed code for a pharmaceutical quiz application that consistently recommended the same drug regardless of the user's actual responses. I evaluated the ethical issues involved in the case, including professional responsibility, honesty, consumer safety, and the potential consequences of biased or misleading software systems. Using ethical frameworks and professional standards, I examined how the engineer's actions could negatively impact public trust, healthcare decisions, and organizational integrity. This assignment strengthened my ability to critically analyze ethical dilemmas, assess the broader social impact of technology, and understand the importance of ethical decision-making in cybersecurity and IT field in general.

Artifact 3: Another artifact that demonstrates my analytical skills is a machine learning project focused on developing an Intrusion Detection System (IDS) using advanced boosting techniques such as Gradient Boosting. In this project, using a sample dataset, I trained the model to classify network traffic data as either normal or abnormal in order to detect potential cyber threats and malicious activity. After training the model, I evaluated its performance using several metrics, including the confusion matrix, accuracy score, precision, recall, F1-score, and ROC-AUC score. I then analyzed the results to identify the model's strengths, limitations, and overall effectiveness

in detecting intrusions. Finally, I prepared a detailed analysis report summarizing the findings and model performance. This project strengthened my analytical thinking, data interpretation, and problem-solving skills while also expanding my understanding of machine learning applications in cybersecurity.

Interpersonal Skills: Team Work/Communication/Collaboration

Now, I will discuss my interpersonal skills, which include teamwork, collaboration, and communication. These skills are essential in cybersecurity because professionals often work in team-based environments where clear communication and coordination are critical for identifying, responding to, and mitigating security threats effectively.

Artifact 1: To demonstrate my teamwork skills, I have included my final executive team reflection slides from my internship experience with the City of Suffolk. During this internship, I collaborated closely with both my team members and the City of Suffolk IT department to identify and assess potential cybersecurity vulnerabilities within their systems. Throughout the process, I also practiced professionalism, empathy, time management, and strong work ethics while working with individuals from diverse backgrounds. This experience strengthened my ability to function effectively in a team-oriented environment and reinforced the importance of collaboration in addressing real-world cybersecurity challenges.

Artifact 2: Another artifact that demonstrates my teamwork skills is an image from a practice session in my CYSE 368 internship course. In this session, I was randomly assigned to a team and given a real-world cyberattack scenario to analyze. Our team collaborated to identify the issue, discuss potential threats, and develop effective mitigation strategies. We worked together by sharing ideas, and combining our individual perspectives to arrive at different solutions. In

addition, we presented our findings to the entire class, which helped strengthen our communication skills and ability to explain technical concepts clearly to an audience. This experience highlighted the importance of collaboration, and effective communication in solving cybersecurity challenges.

Artifact 3: Another artifact that demonstrates my teamwork and communication skills is an image from a professional career development workshop on oral history. In this workshop, I partnered with another student to practice structured interview techniques, where we took turns acting as both the interviewer and the interviewee. This activity required active listening, clear communication, and the ability to ask thoughtful, open-ended questions while maintaining a professional and respectful dialogue. Working closely with a partner helped me strengthen my ability to collaborate effectively in a one-on-one setting. This experience also enhanced my communication skills, which are essential in cybersecurity roles that involve gathering information, conducting assessments, and engaging with stakeholders.

Last Remarks

Cybersecurity is vast, and it is continuing to grow as technological advancements keep growing. As technology grows, cyber attackers are also becoming increasingly sophisticated in their methods and tactics. . In order to better protect our systems, cybersecurity professionals must stay ahead of attackers, and that requires both technical and interpersonal skills such as communication and teamwork. A single individual or entity cannot effectively address these complex issues alone; therefore, teamwork is very important to effectively address any security problem.

In addition, cybersecurity is an interdisciplinary field that connects multiple domains such as technology, law, ethics, psychology, and social sciences. Understanding how users behave, how organizations handle data, and how laws regulate information security all contribute to building stronger and more secure systems. By integrating these interdisciplinary concepts with technical expertise and collaboration, cybersecurity professionals can develop more effective solutions to emerging threats.

Conclusion

In conclusion, my academic and professional experiences have played a significant role in preparing me for a career in cybersecurity. The combination of technical labs, analytical case studies, and collaborative team-based activities has helped me build a strong skill set that aligns with my career goals and industry expectations. These experiences have not only strengthened my understanding of cybersecurity concepts but have also improved my ability to apply them in real-world situations. Going forward, I plan to further strengthen these skills so I can grow into a more effective, ethical, and adaptable cybersecurity professional who is well-prepared to tackle and respond to any cybersecurity challenges.