Introduction

My bachelor's degree in cybersecurity at Old Dominion University has been a journey of growth, challenge, and skill building. The program's interdisciplinary nature exposed me to a wide range of perspectives and technical disciplines, allowing me to approach problems with both analytical and creative thinking. Through coursework, labs, and writing-intensive assignments, I have developed a variety of professional skills that are directly relevant to my career goals in cybersecurity.

Three skills stand out as defining strengths from my academic journey: ethical hacking, programming in Python, and writing. Each of these skills was developed through different courses and experiences, yet they complement each other in ways that make me a stronger, more versatile professional. In my e-portfolio, each skill is represented by an artifact that demonstrates my ability to apply academic knowledge to practical, real-world challenges.

Skill 1: Ethical Hacking

Artifact: Penetration Testing and Vulnerability Assessment Lab Report

My Ethical Hacking and Penetration Testing course was one of the most challenging and rewarding parts of my degree. The lab assignments required me to simulate real-world hacking scenarios, using tools such as Nmap for reconnaissance, Hydra for brute force attacks, and Metasploit for exploitation. The artifact I selected for this skill is a detailed lab report documenting a full penetration testing process from reconnaissance to exploitation to post-engagement cleanup.

One of the most valuable lessons from this project was understanding the attack lifecycle. I learned how attackers gather intelligence, identify vulnerabilities, exploit weaknesses, and

maintain access. More importantly, I learned how to think defensively, predicting potential exploits and developing recommendations to close those gaps. This project taught me to follow structured methodologies like the Penetration Testing Execution Standard (PTES) and to adhere to ethical and legal guidelines.

This skill required both technical problem-solving and adaptability. For example, when a scanning tool failed due to a configuration issue, I researched and tested alternative methods rather than abandoning the task. I also had to interpret raw scan results and translate them into actionable recommendations. In professional roles such as penetration tester or product security analyst, these same skills are essential for identifying and mitigating risks before they can be exploited in the real world.

Skill 2: Programming – Python

Artifact: Python Network Security Scripts

Programming in Python has been a cornerstone of my technical development. Python's flexibility and readability make it a powerful tool for cybersecurity professionals, especially when creating automation scripts, security tools, or data analysis programs.

The artifact for this skill is a Python program I created to encrypt and securely transfer files. This project required me to work with Python's cryptography library, handle user input validation, and implement file I/O operations securely. I also learned how to structure the code into reusable functions and add meaningful comments so that others could understand and maintain my work.

Python became more than just a programming language for me; it became a problem-solving tool. For example, in one assignment, I developed a socket-based communication program that

allowed two systems to exchange encrypted messages. In another, I automated repetitive security tasks such as parsing log files for suspicious activity.

In a cybersecurity career, the ability to code is a competitive advantage. Automating many security tasks can save time, reduce errors, and increase efficiency. For instance, writing a script to scan multiple systems for vulnerabilities can replace hours of manual work. Additionally, understanding programming allows me deeper insight into how malware is written and how to defend against it.

Skill 3: Writing

Artifact: National Cybersecurity Strategy Analysis Paper

While technical skills are essential in cybersecurity, the ability to communicate clearly is equally important. My writing skills were sharpened through writing-intensive courses like IDS 300W and Cybersecurity Strategy and Policy. These classes emphasized research, organization, and the ability to explain technical concepts to nontechnical audiences.

The artifact I selected is an analysis of the 2023 U.S. National Cybersecurity Strategy. This assignment required synthesizing information from multiple scholarly sources, identifying key policy implications, and explaining them in an accessible way. I applied APA formatting, structured my arguments logically, and used evidence to support my claims.

Writing is an often-overlooked skill in technical fields, yet it is critical for creating incident reports, compliance documentation, risk assessments, and policy briefs. A penetration test, for example, is only valuable if the report clearly communicates the findings and recommendations to stakeholders. My ability to write concisely and clearly ensures that decision-makers can act on my work without confusion or misinterpretation.

Interdisciplinary Learning and Problem Solving

One of the strengths of my program was the integration of different disciplines in my learning. Ethical hacking gave me the technical expertise to find vulnerabilities. Python programming gave me the tools to automate security processes and test scenarios efficiently. Writing allowed me to communicate my results in a professional, accessible manner.

These skills often worked together in my coursework. For example, in a lab-based ethical hacking assignment, I used Python to create a script that automated part of the reconnaissance phase, then documented the entire process in a professional-style report. This combination of skills mirrors real-world cybersecurity work, where professionals must move seamlessly between technical tasks and communication with clients or stakeholders.

I also learned the importance of adaptability. In one assignment, an exploit I planned to use was patched before I could test it. Instead of abandoning the project, I researched alternative vulnerabilities, adjusted my approach, and still completed the assessment on time. This adaptability is critical in a field where technology and threats evolve rapidly.

Career Readiness

The combination of ethical hacking, Python programming, and writing has prepared me for multiple career paths, including penetration testing, product security, and threat analysis.

Ethical hacking has taught me to think like an attacker while acting as a defender, a mindset that is invaluable in threat modeling and vulnerability management.

Python programming has given me the ability to build tools, automate workflows, and adapt to emerging security challenges.

Writing ensures that my technical findings can be effectively communicated to technical and non-technical audiences alike.

These skills also align directly with the expectations in cybersecurity job postings, which often list penetration testing experience, scripting or automation capabilities, and strong communication skills as core requirements.

Conclusion

The interdisciplinary nature of my degree has been crucial to my development as a cybersecurity professional. Courses like IDS 300W prepared me to research and communicate effectively, while technical labs built my ability to perform complex security tasks.

In cybersecurity, it is not enough to find vulnerabilities; you must also have the technical skills to test them, the programming skills to build tools when needed, and the writing skills to communicate findings clearly. Ethical hacking, Python programming, and writing are more than just academic achievements; they are practical, career-ready skills that will allow me to adapt and thrive in the evolving cybersecurity landscape.

As I move forward in my career, I will continue to refine these abilities and apply them to protect systems, data, and people from emerging threats. The interdisciplinary foundation I gained at Old Dominion University ensures that I can approach problems holistically, adapt to new challenges, and communicate effectively qualities that are essential for success in any cybersecurity role.