Heliene Ella Lee Jimenez Macaraeg

Old Dominion Universty

IDS493 Electronic Portfolio Project

Professor Andrews

April 14, 2025

Pursuing a degree in cybersecurity through an interdisciplinary program has equipped me with a diverse skill set that blends technical expertise with human-centered problem-solving. This program drew from computer science, information systems, criminal justice, ethics, and writing-intensive coursework, all of which helped shape me into a well-rounded cybersecurity professional. As I reflect on my academic and professional journey, three key skills stand out: technical cybersecurity proficiency, collaborative leadership, and a commitment to excellence. These strengths are not abstract traits—they are grounded in artifacts I created, challenges I overcame, and theories I applied in real-world contexts. Together, they reflect how this program has prepared me to enter the cybersecurity workforce with confidence, adaptability, and purpose.

My technical proficiency in cybersecurity has grown substantially through coursework, certifications, and hands-on experience. Earning credentials like CompTIA Security+, the Google Cybersecurity Certificate, and the Certified in Cybersecurity certification from ISC2 provided me with a strong foundation in risk management, threat detection, and secure system design. These certifications were more than academic milestones—they gave me practical tools I applied during real projects. For example, during my internship at Oak Ridge National Laboratory, I developed an intrusion detection system (IDS) for vehicles using CAN bus data. I initially trained the system on standardized datasets, but soon discovered they weren't compatible with real-world data from semitrucks. This forced me to rethink my approach. I learned to identify the differences between standard and extended CAN formats and built separate autoencoder models accordingly. I also combined machine learning with rule-based logic to reduce false positives, which was key to making the IDS viable in a live environment. This hands-on experience pushed me to bridge theoretical knowledge with real-world engineering challenges. The interdisciplinary aspect was clear—I had to combine knowledge

from computer science, data analytics, and even automotive engineering. These are the kinds of problems cybersecurity professionals face on the job, and this project helped me build the mindset and adaptability needed to tackle them.

While technical skill is essential, I've also learned that cybersecurity is a team effort. One of the most formative collaborative experiences I had was during the Innovate Cyber Challenge. My team chose to address a cybersecurity education gap affecting older adults, many of whom are not tech-savvy and are often targeted by scams. We created and prototyped physical booklets tailored to their needs, using accessible language and visuals to explain basic cybersecurity practices. The interdisciplinary nature of this project—combining cybersecurity, communication, psychology, and design—taught me how important it is to consider the user, not just the technology. Our team had to balance technical accuracy with clarity and empathy. It wasn't easy; we had to make compromises, resolve disagreements, and constantly revise our approach based on feedback. But in the end, we succeeded—we won the challenge. That experience taught me how to work across disciplines and how to think about cybersecurity not just as a technical field, but as a human one. It also reinforced my interest in penetration testing, where understanding the human factor is often just as important as technical skill. Knowing how users behave, how systems are misused, and how attackers exploit everyday habits is essential to building better defenses.

My experience as a Teaching Assistant in the Cybersecurity Internship Clinic further developed my leadership and mentoring skills. One of my core responsibilities was to help students prepare for interviews with local small businesses, where they would assess cybersecurity risks and offer recommendations. I quickly realized that many students didn't

know how to ask the right questions to get meaningful answers from business owners. I started guiding them through interview prep—what to ask, how to follow up, and how to think like a security consultant. Helping them grow not only reinforced my own understanding of cybersecurity fundamentals, but also taught me how to lead without taking over. I had to give them room to think for themselves while still providing a safety net of support. This leadership role required skills from communication, pedagogy, and psychology—all of which came into play through this interdisciplinary program. It also gave me a taste of what it's like to work with clients, which is a huge part of being a penetration tester. Communicating findings clearly, building trust, and translating technical insights into business terms are just as important as technical testing skills.

My commitment to excellence is something I've carried throughout this program, and it's reflected in both my academic and professional work. I maintained a high GPA while balancing multiple internships and leadership roles. That took a lot of discipline, time management, and organization. I take pride in producing high-quality deliverables, whether it's a technical report, a team project, or a presentation. I've learned how to manage competing deadlines, juggle responsibilities, and adapt when things don't go as planned. For example, when I interned at G2 Ops, I created a dashboard that tracked software products using systems engineering principles. I had never worked with those tools before, but I was able to learn quickly, ask the right questions, and deliver something the team could use. That experience, like many others in this program, showed me that excellence isn't about never making mistakes—it's about showing up prepared, putting in the work, and being open to growth.

Looking back, I can see how the interdisciplinary nature of this program has shaped the way I think and work. Courses like IDS 300W helped me develop writing and research skills that are essential for technical communication. I learned to synthesize complex ideas from fields like ethics, law, and philosophy, and apply them to cybersecurity issues like surveillance, privacy, and data ownership. These aren't just academic exercises—they're real issues in the field. Writing about the ethics of Google Street View, for example, helped me understand how power imbalances and informational dignity shape user experiences. That perspective now informs the way I think about penetration testing—not just from a technical standpoint, but from a moral one. Being an interdisciplinary thinker means understanding the big picture: how technology affects people, how laws shape behavior, and how different fields intersect in complex systems.

Altogether, this program has prepared me to pursue a career in penetration testing with a strong foundation in both theory and practice. I'm continuing my education by pursuing a master's degree in cybersecurity, and I feel confident entering the workforce with the skills I've built. From coding intrusion detection systems to mentoring peers, from writing research essays to leading team projects, I've learned how to adapt, communicate, and contribute in a rapidly evolving field. This program didn't just teach me cybersecurity—it taught me how to think critically, act ethically, and grow continuously. And that's exactly what I plan to carry forward into my career.