Benjamin Taylor

☎ 828-639-5792 | ✉ btayl106@charlotte.edu | linkedin.com/in/btayl106 | github.com/benjqminn

Education

University of North Carolina at Charlotte Charlotte, NC
M.S. Cybersecurity, Early Entry *Aug. 2025 – May 2027*

- GPA: 4.0 / 4.0

University of North Carolina at Charlotte Charlotte, NC
B.S. Computer Science, Cybersecurity Concentration *Aug. 2023 – May 2026*

- GPA: 3.84 / 4.0 | Chancellor's List

Projects

Betta Phish: Hooked? (CCI Startup Hackathon 2025, Most Creative Award)

- Led a 4-member team at UNC Charlotte's CCI Startup Hackathon to design Hooked?, a gamified phishing-awareness and financial-literacy platform, winning the "Most Creative" award out of 40+ teams.
- Developed a full-stack prototype in under 48 hours using Flask, HTMX, and React, featuring real-time scoring, XP/badge progression, and interactive phishing inbox missions.
- Built a scalable back-end for modular lesson paths and user tracking, integrating dual learning paths for cybersecurity and financial literacy.

HackTheBox Capture the Flags: National Guard, Holmes CTF & HackTheBoo 2025

- Represented UNC Charlotte's 49th Security Division in a Hack The Box CTF hosted by the North Carolina National Guard, placing 2nd out of 23 teams and capturing 40/46 flags across AI exploitation, reverse engineering, and web challenges.
- Individually competed in HackTheBoo 2025, solving 19/23 challenges and ranking Top 4% globally (120/2,893) across forensics, web, OSINT, crypto, and reverse engineering categories.
- Led UNC Charlotte's 49th Security Division team "Sherlock's Homies" in HackTheBox's first Blue CTF, placing Top 8% globally (634/7,085) through forensic flag analysis, Registry artifact parsing, and MITRE ATT&CK mapping.

Obscura: Real-Time Threat Detection Platform

- Engineered a full-stack SOC simulation platform analyzing 10K+ packets per session, with real-time detection of SYN scans, brute-force attempts, and YARA rule matches.
- Integrated Python (Flask, PyShark, YARA) backend with a React/Tailwind dashboard, enabling analysts to triage alerts 40% faster through live visualization and log interaction.
- Designed correlation pipelines that emulate enterprise SOC workflows, providing end-to-end visibility into attack chains using custom PCAP datasets.

Securing the Unseen: Hardening Cybersecurity in IoT Devices

- Authored a Medium article highlighting IoT insecurity as a public safety issue, referencing Mirai, WannaCry, and medical device vulnerabilities.
- Analyzed EternalBlue-based ransomware propagation and mapped attack chains to MITRE ATT&CK, recommending Zero Trust and segmentation defenses.
- Presented findings to 50+ students and faculty, translating complex exploits into practical security strategies.

Technical Skills

Languages: Python, C++, C, Java, JavaScript, SQL, Bash, C#, HTML, CSS

Cybersecurity & Networking: Threat Detection & IR, SIEM (Splunk, Sentinel, ELK), Packet Analysis (Wireshark, Zeek), Recon (Nmap), IDS/IPS (Snort, Suricata), Vulnerability & Risk Assessment, YARA Rules, MITRE ATT&CK

Tools & Platforms: Security Onion, Microsoft Defender, Burp Suite, Splunk, PyShark, GitHub, VS Code, VMware, VirtualBox, MongoDB, Node.js

Operating Systems: Windows 10/11, Kali Linux, Parrot OS, Ubuntu, Red Hat

Certifications

CompTIA Security+ *Dec. 2025*
AWS Certified Cloud Practitioner *Dec. 2025*
Google Cybersecurity Certificate (Coursera) *Mar. 2025*
SOC Level 1 Certificate (TryHackMe) *May 2025*
Google Business Intelligence (Coursera) *Apr. 2025*
Microsoft Office Specialist: Expert (Office 2019) *May 2023*

Campus Involvement

49th Security Division Club — *Officer* *Dec. 2024 – Present*
Organized and participated in weekly cybersecurity talks and workshops for 50+ students.

Charlotte AI Research — *Member* *Aug. 2025 – Present*
Discussed AI/ML applications for cybersecurity and threat detection.

CLT Lifters Club — *Member* *Sept. 2024 – Present*