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 — *Aug. 2025 – May 2027*
- GPA: 4.0 / 4.0

University of North Carolina at Charlotte — Charlotte, NC
B.S. Computer Science, Cybersecurity Concentration; Minor in Mathematics — *Aug. 2023 – Dec. 2026*
- GPA: 3.85 / 4.0 | Chancellor's List

Projects

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.

HackTheBox Holmes CTF: Incident Response Investigation
- Served as Team Captain of "Sherlock's Homies," representing UNC Charlotte's 49th Security Division and leading 5 members to a Top 8% global finish (634/7,085 teams).
- Captured 25+ forensic flags through Windows endpoint analysis, Registry artifact parsing, and attacker TTP correlation, driving comprehensive incident reconstruction under competitive time constraints.
- Delivered actionable findings on persistence, lateral movement (`wmiexec.py`), and credential abuse by leveraging Volatility3 memory forensics and Ubuntu log analysis, mapped to MITRE ATT&CK.

Securing the Unseen: Hardening Cybersecurity in IoT Devices
- Published a Medium research article framing IoT device insecurity as a public safety issue, citing Mirai, WannaCry, and St. Jude vulnerabilities.
- Analyzed EternalBlue exploitation and ransomware propagation; mapped attack chains to MITRE ATT&CK and proposed Zero Trust, segmentation, and endpoint hardening strategies.
- Delivered a technical presentation of findings to 50+ students and faculty, translating complex cyber threats into actionable defense strategies.

Python Recon Tools Suite
- Built a modular CLI toolkit (port scanner, banner grabber, Nmap wrapper) to automate service discovery and footprinting.
- Implemented resilient networking (threading/async, rate-limit handling) and robust parsing to produce structured JSON outputs for downstream analysis.
- Implemented modular architecture to support extended parsing and live logging for tool chaining.

Technical Skills

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

Cybersecurity & Networking: Threat Detection & IR, SIEM (Splunk, Sentinel, ELK), Packet Analysis (Wireshark, Zeek), Recon (Nmap, Banner Grabbing), IDS/IPS (Snort, Suricata), Detection Engineering, 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

Certified in Cybersecurity (CC) ($(ISC)^2$) — *Apr. 2025*
Google Cybersecurity Certificate (Coursera) — *Mar. 2025*
SOC Level 1 Certificate (TryHackMe) — *May 2025*
Google Business Intelligence (Coursera) — *April 2025*
Scientific Computing with Python (freeCodeCamp) — *April 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*