Benjamin Taylor

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

Education

University of North Carolina at Charlotte Charlotte, NC

B.S. Computer Science, Cybersecurity Concentration; Minor in Mathematics *Aug. 2023 – May 2026*

- GPA: 3.88 / 4.0 | Chancellor's List

Projects

Obscura: Real-Time Threat Detection Platform

- Developed a full-stack SOC simulation tool to analyze .pcap logs, detect SYN scans, brute-force attempts, and YARA rule matches.
- Integrated a Python (Flask, PyShark, YARA) backend with a React/Tailwind dashboard to visualize alert feeds and perform live log triage.
- Built detection pipelines and correlation logic to simulate real-world SOC workflows using custom PCAPs.

Python Recon Tools Suite

- Built a suite of CLI-based network reconnaissance tools including a threaded port scanner, banner grabber, and automated Nmap wrapper.
- Used Python sockets and subprocess modules to streamline enumeration tasks in offensive security labs and project environments.
- Implemented modular architecture to support extended parsing and live logging for tool chaining.

WannaCry Research & Ransomware Response Strategy

- Delivered technical presentation analyzing the EternalBlue exploit and ransomware propagation through SMB vulnerabilities.
- Mapped the WannaCry attack chain to MITRE ATT&CK and proposed segmentation and endpoint hardening strategies.
- Demonstrated how patch lag, unmonitored ports, and legacy systems expose networks to ransomware outbreaks.

Securing the Unseen: Hardening Cybersecurity in IoT Devices

- Published a research article on Medium examining IoT vulnerabilities and the ethical responsibility of securing smart devices.
- Analyzed real-world cases like Mirai, WannaCry, and St. Jude to propose defense strategies including Zero Trust and stronger regulation.
- Framed cybersecurity as a public safety issue, supported by historical context and the ACM Code of Ethics.

Technical Skills

Languages

- Python, JavaScript, C, C#, Java, SQL, HTML/CSS, Bash

Cybersecurity & Networking

- SIEM Analysis (Microsoft Sentinel, Splunk, ELK Stack), Packet Analysis (Wireshark, Zeek), Threat Detection, Incident Response, Detection Engineering, Risk Assessment, Reconnaissance (Nmap, Banner Grabbing), MITRE ATT&CK Mapping, YARA Rules

Tools & Platforms

- Wireshark, Zeek, Security Onion, Microsoft Defender, MongoDB, Node.js, GitHub, Burp Suite, Brim, Suricata, PyShark, VS Code

Operating Systems

- Windows 10/11, Kali Linux, Virtual Machines (VirtualBox, VMware)

Certifications

CompTIA Security+	*Expected May 2025*
Certified in Cybersecurity (CC) ((ISC)^2)	*Apr. 2025*
AWS Certified Cloud Practitioner	*Expected 2025*
Microsoft Certified: Azure Fundamentals	*Expected 2025*
Google Cybersecurity Certificate (Coursera)	*Mar. 2025*
SOC Level 1 Certificate (TryHackMe)	*May 2025*
Microsoft Office Specialist: Expert (Office 2019)	*May 2023*

Campus Involvement

49th Security Division Club, *Officer*	*Dec. 2024 – Present*
CLT Lifters Club, *Member*	*Sept. 2024 – Present*