Behnjamin Barlow

behnjaminhector04@gmail.com
nightwalker.cv
(931)-472-9818
Cookeville, TN

OBJECTIVE

In a Scholarship For Service (SFS) degree path designated for Cyber Defense Education by the National Centers of Academic Excellence in cybersecurity. I have a deep interest in my cyber competitions like CCDC and CPTC and hope to get a career in a cyber crime related field

EDUCATION

Tennessee Technological University (NCAE) Cookeville, TN (08/22-Present)

- Computer Science Bachelor of Engineering|Cybersecurity
- Computer Science Masters of Engineering|Cybersecurity (Exp. Fall 2027)

EXPERIENCE

Cyber Range Application Developer(05/25 - 08/25):

- Contributed to the development of Infrastructure as Code (IaC) solutions using Python, OpenTofu, and HashiCorp CDK
- Helped to automate the deployment and management of the CEROC Cyber Range on the Canonical MicroCloud hypervisor
- Worked closely with the Cyber Range Engineer to troubleshoot infrastructure problems and enhance overall system functionality

Research: Satellite Security(12/24 - Present):

- Developing encrypted verification methods to ensure trusted communication built off the block chain model
- Designing and building a physical testbed simulating a satellite constellation using Jetson Orin devices as satellites and Raspberry Pis as ground stations to model communication and network interactions

Penetration Tester - ZOE International (August 2025 - January 2026)

- Conducted comprehensive assessment, documenting numerous findings.
- Performed source code analysis to help remediate vulnerabilities.
- Utilized engagement frameworks such as Burp Suite, Metasploit, and more widely used industry tools.

COMPETITION EXPERIENCE

Application Security Lead | Tennessee Tech CCDC Nationals Team(2024-2025):

- Secured web applications and databases by hardening configurations, managing access controls, and implementing network security policies
- Hunted, detected, and neutralized real-time Red Team attacks by analyzing network traffic, investigating logs, and mitigating active threats
- Administered Linux systems and pfSense firewalls, performing OS hardening, system auditing, and automating security tasks with Bash scripts
- Architected and deployed a 16+ machine training environment, simulating attack scenarios with vulnerable services (web, mail, domain)
- Executed offensive Red Team operations within the mock environment using SliverC2 and Realm to test persistence methods and improve defensive playbooks

Web Application Penetration Tester | Tennessee Tech CPTC Team(2025–2026)

- Conducted comprehensive web application penetration tests on multi-tiered live environments, aligning findings with the OWASP Top 10 to identify and exploit critical flaws (e.g., SQL Injection, XSS, and authentication bypass)
- Developed a holistic attack narrative by collaborating with team members to correlate web application vulnerabilities with network-level findings, demonstrating full chain compromises from Layer 7 to Layer 3
- Authored professional-grade penetration test reports using Ghostwriter, detailing findings, analyzing business impact, and providing actionable, prioritized remediation strategies for development teams

Linux Subject Matter Expert | Tennessee Tech CCDC Nationals Team(2025-2026):

- Designed and deployed custom automation scripts in go and bash to rapidly enforce security policy, audit user accounts, and implement kernel-level hardening across multiple Linux machines.
- Established proactive threat hunting and forensic capabilities to detect advanced Red Team persistence, focusing on tracking covert beacons, kernel hooks, and user-space rootkits.
- Engineered dynamic, isolated testing environments featuring Red Team tactics and compromised machines to validate hardening scripts and incident response procedures in a live-fire competition scenario.
- Secured critical Linux services by implementing secure configurations, strong host-based firewall policies, and advanced file integrity monitoring.

SKILLS

- Soft Skills: Written Communication, Problem Solving, Time Management, Teamwork, Critical Thinking, Mentorship, Public Speaking.
- Offensive Cyber Tools: Mythic C2, SliverC2, Kali Linux, Burp Suite, Hashcat, Ninja Binary, Ghidra, Nmap, Persistence Techniques, Metasploit.
- Defensive & Forensics Tools: WireShark, Autopsy, FTK Imager, Iptables, PfSense, SIEM, Advanced File Integrity Monitoring, Kernel Hooks, User-Space Rootkits.
- Programming Languages: Python, Bash, C++, HTML, CSS, JavaScript, GoLang, PowerShell.
- Databases: MySQL, MongoDB. Sqlite3, PostgreSQL.
- Virtualization & Cloud: Proxmox VE, VMware, ESXi, Google Cloud Platform, Amazon Web Services, Canonical MicroCloud, OpenTofu, HashiCorp CDK.
- Infrastructure & Automation: Ansible, Salt Stack, Configuration Management, Git, GitHub, GitLab, GitKraken, TailScale, Zero Trust Architecture.
- Operating Systems: Linux (Hardening/Administration), Windows.
- Advanced Networking: Virtual Networking, DNS, VPN, Network Troubleshooting, CAN Bus/Internal Protocols.
- Specialized Concepts: Data Forensics, Computer Forensics, Data Recovery, NTA (Network Traffic Analysis), Web Security.

LEADERSHIP EXPERIENCE

Agile Scrum Master for the Tennessee Tech School of Music Adjudication System (04/25 - 12/25):

- Served as Scrum Master for a 6-person team , coordinating all sprints, managing the product backlog, and ensuring the timely delivery of a fully digital music jury scheduling and evaluation platform
- Oversaw the design and implementation of security features, including Azure Active Directory (Azure AD) authentication for faculty , Role-Based Access Control (RBAC) via SharePoint Groups, and strict Least-Privilege Enforcement , ensuring compliance with institutional data management standards.
- Successfully developed the platform entirely within the university's existing Microsoft 365 licensing (SharePoint Online, Power Automate, Forms, Bookings, Teams) , delivering a fully digital, integrated, and sustainable solution that eliminated the need for expensive third-party platforms and reduced administrative workload.
- Directed the design of a NoSQL/List-based data model and managed the core Power Automate workflows and Excel Office Scripts responsible for automated data routing and feedback generation

Tennessee Tech Cyber Eagles Volunteer | President (05/25 - Present):

- Engineered and Deployed the Official Club Website (cybereagles.org), establishing a permanent static site using free hosting to ensure technical longevity and resource efficiency.
- Coordinated and Hosted regular club meetings, securing engagement from guest speakers from leading technology companies and government agencies.
- Developed and executed outreach initiatives with related academic departments and student groups, successfully increasing club visibility and membership.
- Managed administrative operations, partnering with university administration and student organizations to manage budgets, secure necessary funding, and ensure smooth club operations.

ON CAMPUS EXPEREINCE

Tennessee Tech Cyber Interest Group Mentor (09/24 -Present):

- Developed and Led Technical Training Sessions on complex cybersecurity topics, including digital forensics, privilege escalation, and rootkits, preparing students for real-world offensive and defensive security challenges
- Designed and Delivered Educational Content, including detailed meeting agendas, presentations (slides), and practical labs to clarify concepts for a diverse audience
- Cultivated a Dynamic, Collaborative Learning Environment for students across all skill levels, significantly improving group knowledge and practical application skills in areas like network defense and ethical hacking
- Utilized LXD cyber range with SaltStack to create secure, repeatable, and realistic training environments for hands-on practice, mirroring professional cybersecurity lab setups
- Collaborated with fellow mentors and group leads to strategize meeting schedules and content flow, ensuring timely and smooth execution of all training sessions

---

OTHER EXPERIENCE

Personal Website:

- Established and Maintained a permanent static website, nightwalker.cv, utilizing free software hosting solutions to ensure optimal resource efficiency.
- Configured a custom domain (nightwalker.cv) to serve the site, centralizing professional content, public code repositories (GitHub), and academic projects.
- The site serves as a technical portfolio Including detailed insights into cybersecurity work, showcasing technical proficiency and professional contribution

Cyber Truck Challenge 2025:

- Performed specialized security assessments targeting vehicle communication systems and embedded hardware, including analysis of CAN Bus and internal protocols.
- Utilized deep analysis techniques to exploit security vulnerabilities in the simulated automotive environment.

Home Lab:

- Managing a high-performance virtualization cluster using dual Proxmox hypervisors, providing 50 CPU cores and 200 GB of RAM to support complex, resource-intensive cybersecurity operations.
- Established secure, isolated virtual ranges dedicated to specialized training and testing, including local malware analysis, Command and Control (C2) testing, and execution of complex Linux scripting tasks
- Supported competitive cybersecurity training (CCDC) by designing and deploying complex server infrastructure and mock competition environments for team exercises
- Configured and utilized an Ubiquiti managed switch to implement robust network segmentation, traffic control, and efficient management across all lab resources
- Designed and deployed a dedicated Raspberry Pi appliance to function as a Tailscale router and VPN endpoint, enabling secure, encrypted remote access to the entire lab network
- Automated lab functionality by implementing Wake-on-LAN (WoL) via the Raspberry Pi, allowing remote power cycling of the Proxmox servers to optimize energy consumption and accessibility
- Developed a plan for advanced digital forensics capabilities, designating existing hardware and leveraging specialized tools (e.g., drive duplicators, write blocker equipment, forensic bridges) to build a dedicated acquisition and analysis station