Cameron Jones

crayjones2007@gmail.com
linkedin.com/in/cameron-ray-jones/
github.com/Crayjones
931-510-3441
Cookeville, TN

EDUCATION

Tennessee Technological University (Expected Graduation: May 2028)

Bachelor's of Science in Computer Science

- **GPA: 3.91**

CERTIFICATIONS

Zero-Point Security Ltd - Red Team Operator (Jan 2026)
GIAC Foundational Cybersecurity Technologies (Sept 2023)

PROJECTS

Tomoe – Cross-Platform Windows Administration Tool

- Developed a Python utility for remote Windows administration supporting WinRM and SMB protocols
- Implemented multi-threaded credential testing and command execution across multiple hosts simultaneously
- Created recursive file transfer functionality supporting individual files and directory structures across both protocols

Cybersecurity Homelab

- Deployed a segmented network using OPNsense across three interfaces (WAN, LAN, OPT1), restricting WAN access exclusively to the Proxmox management interface and isolating lab environments in OPT1 from core infrastructure.
- Implemented Zero Trust security model using Keycloak SSO and Cloudflare Zero Trust application policies to protect Proxmox web interface and Apache Guacamole, accessible only to authenticated users via secure cloudflare tunnels.
- Developed Infrastructure as Code solution using Terraform to automate deployment of Ubuntu and Kali jumpbox templates, automatically provisioning Keycloak user accounts and Guacamole connection profiles for seamless user access.
- Designed scalable lab environment with future plans to automate VLAN provisioning through Terraform and develop bash-based management scripts for streamlined infrastructure administration.

COMPETITION EXPERIENCE

Collegiate Cyber Defense Competition – Competitor (Feb 2026 - Apr 2026)

- Placed 1st overall in SECCDC Qualifiers, advancing to the regional competition.
- Secured and maintained Windows Server infrastructure while defending against an active red team.
- Developing scripts to automate hardening, firewall configuration, and management of Windows systems.

Collegiate Penetration Testing Competition – Alternate (Oct 2025 - Jan 2026)

- Performed active reconnaissance on Windows systems.
- Helped with team training by organizing meetings and setting up exercises.
- Constantly prepared to substitute in by actively completing Hack The Box challenges (system penetration testing challenges), updating my checklist, and working with competitors to stay engaged with what they work on and learn at practices.

Department of Energy CyberForce Competition – Competitor (Nov 2025)

- Placed 3rd nationally out of 96 teams in an 8 hour Defensive and Capture the Flag Challenge.
- Worked within a team to defend a network of 6 Windows and Linux Virtual Machines simulating a oil rig, placing 1st in defense
- Solved Anomalies (CTF challenges) relating to malware analysis, forensics, energy, log analysis, cryptography, and stenography.

CyberPatriot – Competitor (Apr 2024 - Mar 2025)

- Achieved 1st Place in Tennessee by successfully defending multiple systems against known vulnerabilities.
- Hardened Windows 10/11 Pro and Windows Server 2019/2022 environments by configuring security policies, managing user permissions, and removing malware under time-sensitive conditions.
- Engineered a PowerShell script to automate the auditing of local and Active Directory user accounts, significantly reducing the time to identify and flag unauthorized credentials

ON CAMPUS INVOLVEMENT

CyberEagles Club – Club Mentor (Sept 2025 - Present)

- Developing labs that give students an interactive, asynchronous, and synchronous experience to reinforce what was learned from the presentation.

SKILLS

- Offensive Cyber Tools: Mythic C2, Cobalt Strike, Wireshark, Hashcat, Nmap.
- Defensive Cyber Tools: Wireshark, Autopsy, SysInternals Suite, Ghidra.
- Programming Languages: Python, PowerShell, HTML, JavaScript.
- Operating Systems: Windows (10, 11), Windows Server (2019, 2022), Linux (Kali, Ubuntu).
- Virtualization & Infrastructure: VMware ESXI, Proxmox, pfSense, Terraform.
- Source Control: Git, GitHub.