Braeden Allen

braeden.allen.applications@gmail.com || *860.597.9231* || *www.linkedin.com/in/braeden-allen*

----------Professional Statement----------

Cybersecurity and Computer Science undergraduate with a concentration in NSA-accredited Cyber Operations and a strong foundation in both offensive and defensive security. Ranked in the global top 900 on Hack The Box, with hands-on experience in penetration testing, vulnerability assessment, threat detection, and log analysis. Proficient in Python, C++, and Linux environments, with practical skills using tools like Wireshark, Metasploit, and Splunk. Proven collaborator and fast learner, eager to contribute to red and blue team operations in a cybersecurity analyst role.

----------Skills----------

Cybersecurity Tools & Frameworks: Kali Linux, Metasploit, Wireshark, Volatility, Autopsy, Nmap, John the Ripper, Burp Suite, Splunk, CVE/CVSS, ATT&CK, OWASP, NIST
Scripting & Programming Languages: Python, C, C++, SQL, Bash, Java
Operating Systems: Linux (Kali, Ubuntu, Arch), Windows, MacOS, Unix
Networking & Protocols: TCP/IP, UDP, IPv4/IPv6, Subnetting, Routing (RIP), SSH, Ethernet, Cisco IOS, Network Administration
Red Team Skills: Vulnerability scanning, exploitation, OSINT, password cracking, reverse engineering
Blue Team Skills: Log analysis, network traffic analysis, intrusion detection, incident response
Soft Skills: Critical Thinking, Communication, Mentoring, Time Management, Adaptability

----------Education----------

University of New Haven, West Haven, Connecticut
Bachelor of Science, Computer Science
Concentration in Cybersecurity (NSA Cyber Operations)
GPA: 3.97/4.0
Anticipated Graduation Date: Spring 2026

----------Relative Experience----------

MITRE eCTF team

- Designed and implemented a secure boot and attestation protocol for an embedded medical device using RNG, AES-128, SHA-256, and public key cryptography
- Enabled trusted communication between the processor and components via secure token exchange
- Gained hands-on experience with UART and I2C while working with the MAX78000FTHR development board
- Ranked 31st out of 121 teams in MITRE's Embedded CTF competition

Cybersecurity Club (Cyber@CIT)

- Participated in weekly meetings focused on global cyber news, red team skills, and CTF competitions
- Placed 2nd in a semester-wide CTF, competing in categories like forensics, OSINT, and reverse
- Co-developed and hosted a CTF event with challenges in digital forensics, enumeration, and crypto
- Built hands-on experience in Kali Linux using tools such as Nmap, FeroxBuster, JohnTheRipper and Wirehsark

Peer Tutor in Computer Science and Cybersecurity

- Tutored students in CS and cybersecurity topics, including algorithms, system security, and programming
- Assisted peers with academic tools and coursework in the Center for Learning Resources
- Led workshops to improve student success and technical confidence in core CS courses

----------Certifications and Honors----------

Awards: Dean's List (Fall 2023, Spring 2024, Fall 2024, Spring 2025), Tau Sigma Transfer Honors Society, Upsilon Pi Epsilon, Computer Science Undergraduate of the Year (2024-2025)
Certifications: Introduction to Cisco Packet Tracer, CRLA Level I/II (Tutor Certification), Red Hat Enterprise System Administration

----------Projects----------

Penetration Test – Kumquat Global (Cybersecurity Project)

- Simulated full penetration test of a fictional enterprise environment
- Conducted OSINT, enumeration, exploitation, and post-exploitation using tools like Nmap, Gobuster, Hydra, and Metasploit
- Delivered a professional-style report with risk analysis and mitigation strategies

Software Projects (Python & C++)

- Developed *Ocean Defender*, a 2D Python game using Pygame with collision detection, scoring, and dynamic difficulty
- Built *Can't Stop* in C++ using OOP principles, STL containers, and unique_ptr for safe memory management

Virtual Network Simulation (Cisco Packet Tracer)

- Designed and configured a scaled-down CAN using virtual routers and switches
- Set up static routing, RIP, VLAN segmentation, and basic ACLs to simulate enterprise-grade networking

Hack The Box (Red & Blue Team Platform – Global Top 900)

- Ranked in the top 900 globally on Hack the Box, demonstrating proficiency in offensive cybersecurity
- Solved multiple Sherlocks (forensics challenges) to build blue team capabilities including log analysis, memory forensics, and incident reconstruction
- Completed a wide range of Machines to develop skills in privilege escalation, web exploitation, reverse engineering, and lateral movement