Bryan Emtman

+82 10 7582-6938 | bryan.a.emtman.mil@army.mil | https://github.com/bryanemtman

Summary

Cybersecurity professional with hands-on experience in network attack simulation, defensive monitoring, and security automation. Skilled in Python, Bash, and PowerShell scripting, Windows/Linux administration, and network security fundamentals, with CompTIA Security+, Network+, and A+ certifications supporting readiness for Cyber Operations roles.

Skills

Windows/Linux system administration - Experienced in configuring, troubleshooting, and maintaining operating systems, user accounts, and Active Directory environments.

Python, Bash, and PowerShell scripting - Developed automation scripts and utilities to streamline tasks, monitor systems, and support cybersecurity lab projects.

Network security/Vulnerability assessment - Skilled in using tools such as Nmap and Metasploit to identify vulnerabilities, assess risks, and support secure network operations.

Work Experience

Motor Transport Operator   Oct 2024 - Present
A CO, 602 ASB, 2 CAB, 2ID, APO, AP 96271

- Leads a section of 10 Soldiers in fuel distribution and convoy operations; conducted over 50 successful fuel missions and issued more than 120,000 gallons of JP-8 with zero safety incidents.
- Enforces safety and maintenance standards for all vehicles and equipment, maintaining 100% accountability and full mission capability across the fleet.
- Served as Company Retention NCO and Unit Deterrence Leader, achieving 100% retention rates for FY25 and FY26 and ensuring compliance with Army substance abuse prevention policies.
- Trains and mentors Soldiers on convoy procedures, trailer operations, and crew-served weapon systems, fostering discipline, readiness, and professional development within the section.

Company Communication Representative   Jan 2021 - Oct 2024
H FSC, 4-70 AR, 1 ABCT, 1 AD, FORT BLISS, TX 79918

- Served as the Company's S6 representative, maintaining and troubleshooting military communication systems and cryptographic keying material.
- Provided Tier 1 Help Desk support, diagnosing and resolving hardware, software, and network issues for 125+ end users.
- Assisted and trained Soldiers across multiple Companies and Battalions on secure communications procedures and equipment operation.
- Coordinated with Battalion and Brigade S6 personnel to ensure compliance with network security requirements and system readiness.
- Contributed to operational readiness by ensuring communications assets remain functional, secure, and fully accountable.

Heavy Vehicle Driver   May 2020 - Oct 2024
H FSC, 4-70 AR, 1 ABCT, 1 AD, FORT BLISS, TX 79918

- Operated and maintained tactical vehicles and trailers in support of over 200 ammunition and supply missions, achieving zero safety incidents or equipment losses.
- Directed and supervised the safe loading, transportation, and offloading of munitions and cargo in compliance with Army explosive safety and accountability standards.

- Managed the receipt, storage, and issue of ammunition, enforcing quality assurance procedures, and maintaining precise inventory control.
- Trained and mentored Soldiers in ammunition handling, convoy operations, and equipment readiness, enhancing platoon efficiency and technical proficiency.

Education

American Public University System, Charles Town, WV   2023 - Present
> AS in Cybersecurity (42/60 credits complete) - 3.73 GPA

Eastern Washington University, Cheney, WA   2017 - 2019
> BA in General Studies (48/120 credits complete) - 3.49 GPA

Mead Senior High School, Spokane, WA   2015 - 2019
> High School Diploma - 3.68 GPA, Honor Role

Certifications

CompTIA Security+ (SY0-701)	Certified Jan 2026
CompTIA Network+ (N10-009)	Certified Nov 2025
CompTIA A+ (220-1101/1102)	Certified Aug 2025

Projects

Network Attack Simulation & Defense Lab (Python)
- Designed and implemented a Python-based ARP spoofing and man-in-the-middle (MITM) simulation to demonstrate interception and manipulation of network traffic.
- Analyzed ARP packet structures, Ethernet frames, and TCP/IP behavior to understand exploitation techniques and associated defensive considerations.
- Implemented packet forwarding and cleanup mechanisms to safely restore network state after execution.
- Developed practical understanding of Layer 2 attacks, network trust relationships, and mitigation strategies.

Covert Channel & Detection Awareness Project (Bash & PowerShell)
- Developed ICMP-based payload scripts to demonstrate covert data exfiltration through non-traditional network channels.
- Implemented payload chunking, timing controls, and reassembly logic to simulate real-world evasion techniques.
- Analyzed IDS/IPS blind spots and network traffic patterns to better understand detection limitations.

Windows Security Monitoring & Automation (PowerShell)
- Developed PowerShell tools to parse Windows Security Event Logs and enrich failed login attempts with geolocation data.
- Built a File Integrity Monitoring (FIM) solution using cryptographic hashing to detect unauthorized file or directory changes.
- Automated alerting and reporting workflows to support incident detection and system hardening.
- Strengthened expertise in Windows internals, event logging, and defensive security practices.