Aaron Anderson google sites Cyber Portfolio
Colorado Springs, CO | aaron.anderson5459@gmail.com | 253-970-3789 | / www.linkedin.com/in/aaron-anderson-cybersecurity

CERTIFICATIONS & SKILLS PROFILE

Certifications: CompTIA Security+, Scrum Fundamentals Certified, Google Project Management, Microsoft Innovative Educator, Edge Coach Training, Culturally Responsive Teaching & The Brain, AWS Cloud (Expected October 2025)
Operating Systems: Windows OS, macOS, Linux
Networking: Basic Networking Protocols, Firewalls and Security Configuration, VPN, LAN/WAN Configuration, Wi-Fi Security, Networking Monitoring Tools, Network Addressing
Programming Languages: Python, Bash/Shell Scripting, SQL, HTML/CSS, JavaScript
Tools: LabShock, Amass, theHarvester, Maltego, Shodan/Censys, Metasploit, SearchSploit, Hydra, John the Ripper, CeWL, Wireshark, Nmap, Metasploit, Kali Linux, Burp Suite, Splunk, Nessus, OpenVAS, OWASP ZAP, Aircrack-ng, ophcrack, GitHub

EDUCATION

University of Colorado - Boulder Boulder, CO
Cybersecurity Certificate 09/2024 – 07/2025
Courses: Network and Application Security, Incident Handling, Cyber Forensics, Malware Analysis, Ethical Hacking

Central Washington University Ellensburg, WA
Bachelor of the Arts – Elementary Education
Middle Level Mathematics/Middle Level Science – Dual Minors

PROFESSIONAL PROJECTS

Cybersecurity Labs & Projects | HSOC Cyber 02/2025-Present

LabShock | ICS/OT Security & Modbus MITM Attack
- Configured Kali Linux with IP forwarding, ARP spoofing, and Scapy/NetfilterQueue to intercept and manipulate Modbus traffic between HMI and PLC.
- Analyzed packet structures and successfully altered register values in real-time to simulate industrial sabotage.
- Demonstrated the importance of monitoring industrial protocols in OT networks and reinforced the need for layered ICS defense strategies.

SIEM Deployment & Monitoring | Wazuh & Splunk Enterprise
- Deployed **Wazuh** and **Splunk Enterprise** within a VirtualBox lab environment to build a functional SIEM.
- Collected, parsed, and analyzed logs from endpoints and network traffic to detect suspicious behavior.
- Created custom dashboards and alerts, demonstrating detection of brute force, privilege escalation, and abnormal logins.

Boss of the SOC (BOTS) | Splunk Blue Team Challenge
- Investigated a **website defacement attack scenario** using Splunk queries and dashboards.
- Correlated attacker IPs, suspicious web requests, and compromised user accounts to determine root cause and attack vector.
- Produced a case study report with detailed evidence, highlighting Splunk's role in modern SOC operations.

Home Network Hardening Project | HSOC Fellowship Deliverable
- Conducted a full audit of personal home network, documenting connected devices, router firmware, and open ports.
- Implemented segmentation, WPA3 encryption, firmware updates, and firewall rule hardening to mitigate attack surface.
- Delivered a comprehensive security report mapping vulnerabilities and countermeasures, aligned with **Security+** best practices.

Digital Forensics & Incident Response | CU Boulder Fellowship Badge
- Utilized **Autopsy** and **Volatility** for forensic analysis of compromised system images.
- Extracted, correlated, and analyzed artifacts to reconstruct timeline of attacker activity.
- Developed step-by-step IR documentation for evidence preservation, chain of custody, and forensic readiness.

Security+ Escape Room | Gamified Cybersecurity Training
- Designed an **interactive, Twine-based Security+ escape room** covering core exam topics (threats, controls, response).
- Implemented branching storylines, scoring, and hints to simulate real-world decision-making under pressure.
- Showcased ability to translate technical knowledge into **engaging cybersecurity education tools**.

Packet Capture & Analysis | TCPdump & Wireshark
- Captured live traffic using **tcpdump**, filtering for suspicious processes (e.g., MsMpEng.exe and PowerShell).
- Imported into **Wireshark** for deep inspection of anomalies and decoded HTTP/S traffic.
- Highlighted the role of packet analysis in detecting persistence, exfiltration, and adversary tactics.

Offensive Security Tools | Password Cracking & Enumeration

- Used **Hydra**, **John the Ripper**, and **Hashcat** to conduct online/offline password cracking labs.
- Leveraged **CeWL** and **Patator** to generate custom wordlists and brute-force credentials.
- Documented success/failure cases, demonstrating both **attack execution** and **defensive mitigations**.

Open-Source Intelligence (OSINT) | NCL Gymnasium Challenge

- Conducted intelligence gathering using **theHarvester, Maltego, and Shodan**.
- Identified subdomains, email addresses, and exposed assets for a simulated target organization.
- Reinforced the role of OSINT in penetration testing, red team ops, and incident reconnaissance.

Cybersecurity Labs & Projects | University of Colorado - Boulder 09/2024 – 08/2025

How to Shop & Tamper | *Modifying URL and Parameter Tampering*

- Identified areas where inadequate validation could make applications vulnerable to attacks, specifically through URL modification and parameter tampering.
- Conducted a detailed analysis of web application inputs and manipulated URL parameters to observe how changes affected access permissions and data visibility.
- Successfully highlighted the critical need for strong input validation within web applications, reinforcing secure coding practices as a priority for development teams.

Malware Investigation | *Using VirusTotal platform to ID potentially harmful files*

- Assessed a specific file for any malicious intent or harmful indicators by analyzing it with VirusTotal's suite of antivirus engines and threat intelligence.
- Carefully reviewing each flagged result, identified indicators of malicious intent, such as specific malware signatures, associated threats, and historical records of similar files.
- Analysis successfully flagged the suspicious file as potentially malicious, reinforcing the critical role of thorough file scanning in proactive threat detection.

Analyzing with Wireshark | *Analyze .pcap file using Wireshark*

- Analyzed the .pcap file by filtering for particular types of packets, such as DNS and Ping packets, to trace interactions with a specific host and uncover details about the source IP addresses involved.
- Conducted a targeted search for packets directed to the 8.8.8.8 host, a common DNS server, to understand communication paths and potential security concerns.
- Analysis successfully identified critical IP address information of the source hosts, providing valuable insights into the network's communication behavior and potential vulnerabilities.

PROFESSIONAL EXPERIENCE

HSOC Cyber, Remote, USA 03/2025 - Present

HSOC IT Cyber Operations Lead

Participate in hands-on, performance-based cybersecurity fellowship focused on real-world readiness through offensive and defensive security training, critical thinking, and open-source tool mastery.

- Direct day-to-day cyber operations, leading a cross-functional team in threat detection, incident response, and proactive risk management across home lab, training, and enterprise-grade SOC environments.
- Design and implement scalable SOC processes, transitioning from a Home Security Operations Center (HSOC) to an Enterprise SOC (ESOC), integrating open-source and commercial tools (Splunk, Wazuh, Zeek, TheHive).
- Manage security monitoring workflows, including log ingestion, SIEM rule creation, dashboarding, and escalation procedures aligned with MITRE ATT&CK, NIST CSF, and CIS Controls.
- Oversee vulnerability management lifecycle: scanning, prioritizing, patching, and verifying remediation of risks across hybrid environments.
- Build and execute incident response playbooks covering phishing, malware, insider threats, and network intrusions; reduced mean time to detect (MTTD) and mean time to respond (MTTR).
- Mentor and train junior analysts and fellows, teaching CompTIA A+, Security+, and PenTest+ topics while reinforcing hands-on skills through custom labs and capture-the-flag (CTF) scenarios.
- Coordinate cybersecurity projects end-to-end, including requirements gathering, tool deployment, documentation, and executive reporting for stakeholders.
- Strengthen home and enterprise network defenses through hardening, segmentation, firewall/IDS tuning, and endpoint security baselines.
- Spearhead performance measurement by establishing KPIs (alert fidelity, detection coverage, SOC maturity), delivering regular status updates to leadership.
- Built and maintain a virtual cybersecurity lab using Kali Linux, Ubuntu, and Windows 11 to simulate real-world scenarios involving penetration testing, vulnerability analysis, and system hardening.

- Utilize industry-standard tools like Nmap, Wireshark, Hashcat, and John the Ripper to conduct reconnaissance, password cracking, and network traffic analysis in lab-based projects.
- Contribute to the National Cyber League (NCL) Spring 2025 games, practicing Capture the Flag (CTF) techniques and ranking in the top 10% nationally.

Kroger, Falcon, CO 01/2024 – Present

Department Head / Cheese Lead

Manage department operations while integrating project management practices to improve efficiency, employee performance, and customer satisfaction.

- Manage department operations, integrating project management practices to improve efficiency and customer satisfaction.
- Increase department efficiency by streamlining processes and implementing innovative management strategies, resulting in a 15% reduction in operational waste and shrink.
- Collaborate with district staff and vendors to create engaging and theatrical customer experiences, increasing customer satisfaction scores by 20%.

University of Washington, Seattle, WA 11/2022 – 07/2023

Project Manager

Managed large-scale, cross-functional projects aimed at improving organizational processes and systems, collaborating with multiple teams and ensuring timely delivery of project goals.

- Led cross-functional IT projects to enhance organizational processes and systems, collaborating with multiple teams to ensure timely delivery of project goals.
- Implemented process improvement initiatives, resulting in a 20% improvement in project delivery times.
- Developed risk mitigation strategies to address potential project risks and system vulnerabilities, enhancing overall project success and security.

Tacoma Public Schools, Tacoma, WA 01/2011 – 08/2022

Educator

Led educational programs, facilitated professional development, and managed virtual and in-person classrooms, applying project management and technical skills to enhance educational outcomes.

- Developed data-driven improvement strategies by analyzing student performance data, increasing student success rates by 15% through personalized learning plans and feedback mechanisms.
- Facilitated professional development sessions for up to 50 staff members, improving their proficiency with digital tools and leading to a 10% improvement in virtual instruction efficiency.
- Helped create an entirely on-line school for Tacoma Public Schools during COVID, building all lessons, structures, and processes from the ground up.