Aaron Barkley

Cybersecurity Consultant | US Army Veteran | Risk & Threat Specialist
aaronjamesbarkley@gmail.com | (503) 502-9017 | www.linkedin.com/in/aaron-j-barkley | www.github.com/lumberjack3E

Summary

Cybersecurity consultant and U.S. Army veteran with hands-on experience in penetration testing, incident response, vulnerability management, and system hardening. Adept at identifying and mitigating risks across cloud and on-prem environments. Proven ability to translate complex technical findings into actionable, risk-based solutions that reduce exposure and improve overall security posture. Passionate about protecting critical systems, mentoring teams, and continuously advancing cybersecurity maturity in both private and public sectors.

Education, Certifications & Clearances

Oregon Institute of Technology, Bachelor of Science: Cyber Security
Red Hat Certified System Administrator (RHCSA) | CompTIA Security+, CySA+, & CISSP (Pending)
Security Clearance Status: Previously held Secret, TS, and TS/SCI (will require re-investigation)

Skills

Security Expertise: Incident Response, Digital Forensics, Risk Assessment, Penetration Testing, Network Defense, Security Architecture
Tools & Technologies: Metasploit, Burp Suite, Nessus, Wireshark, Nmap, Splunk, CrowdStrike, Cisco, Azure, AWS Security, Kali Linux
Programming & Scripting: Python, Bash, PowerShell, C++, SQL, HTML5, CSS, JavaScript
Security Frameworks & Compliance: NIST 800-53, MITRE ATT&CK, CIS Benchmarks, ISO 27001, FedRAMP, HIPAA, PCI DSS
Soft Skills: Leadership, Adaptability, Technical Documentation, Cross-Functional Collaboration, Client Engagement, Conflict Resolution, Report Writing

Projects and Research

Resume Compatibility Tool (In Development)
Description: Designed and developed a web-based resume analysis tool to help veterans tailor their resumes for specific roles.
Frontend: Created an intuitive UI using HTML, CSS, and JavaScript with a drag-and-drop resume upload, job description generation, and keyword alignment analysis
Backend: Built a FastAPI server to process resume and job description text, perform keyword extraction, compute match scores, and return actionable feedback.
Tech Stack: FastAPI, JavaScript, Python, HTML/CSS, Mammoth.js, PDF.js, RESTful API, JSON
Features: Real-time score calculation, missing keyword suggestions, and a dynamic job title-to-job description template generator. Integrated branding and responsive design to match NWVIT visual identity.
Future: Currently planning Phase 2 enhancements including NLP models and job board integration.

Enterprise Wi-Fi Security Overhaul
Description: Designed and implemented a secure wireless network for Molalla River Brewing Company, covering 3 buildings and 1.5 acres of outdoor event space.
Design: Installed TP-Link Omada hardware including indoor and outdoor WAPs, and a 3-in-1 Gigabit VPN Router/Switch/Controller to support business, vendor, and guest traffic.
Security: Segmented the network using VLANs to isolate IoT devices, POS systems, staff operations, and guest access. Configured firewall rules and VPNs for secure remote access and inter-network isolation.
Deployment: Coordinated physical placement of access points to optimize coverage across indoor and outdoor areas, including food truck vendor zones and event spaces.
Tech Stack: TP-Link Omada WAPs (EAP610), Omada ER7212PC router/switch, CAT6 cabling, WAP2 Enterprise, cloud-managed Omada application.
Testing: Performed pre/post-deployment Wi-Fi heat mapping, signal strength tests, and penetration testing to validate segmentation and identify residual attack paths.
Future: Delivered training material to stakeholders for ongoing network maintenance. Scalability planned to support additional food carts and outdoor venue growth.

Incident Response and Threat Hunting Lab
Description: Built a hands-on home lab to simulate attacks and practice threat detection, incident response, and adversary emulation.
Environment: Deployed and integrated Splunk, Zeek, and Elastic Stack to ingest logs and monitor traffic in a multi-segmented test network.
Threat Simulation: Executed red team tools and CTF scenarios to analyze attacker behavior and generate realistic log data.

Investigation: Documented malware behavior, phishing campaigns, and lateral movement techniques for internal reference and training.
Automation: Wrote Python and Bash scripts to parse logs, extract IOCs, and reduce manual workload in threat detection workflows.
Physical Security: Practiced physical penetration techniques including **lockpicking** and bypassing mechanical access controls to understand full-spectrum risk.
Future: Expanding lab to include cloud-based telemetry sources and EDR platforms for endpoint correlation.

Relevant Work Experience

Strateg-ize | **Technology & Cybersecurity Consultant** *March 2024 to Current*
Advised businesses on technology solutions and cybersecurity best practices, ensuring alignment with industry regulations and risk management frameworks.
Guided clients in selecting and deploying secure IT infrastructure — including cloud platforms, firewall configurations, and endpoint protection — aligned with compliance and business requirements.
Delivered strategic cybersecurity guidance that helped clients reduce exposure by identifying critical vulnerabilities and prioritizing investments based on risk impact and compliance needs.
Executed penetration tests and vulnerability assessments across AWS and on-premise environments, identifying misconfigurations, privilege escalation paths, and insecure interfaces.

Northwest Veterans in Technology (NWVIT) | **Vice President** *January 2025 to Current*
Lead NWVIT, a professional development nonprofit for veterans in tech, providing strategic direction, event planning, and advocacy.
Organize networking events, mentorship programs, and job fairs that result in direct hiring opportunities.
Build partnerships with employers and sponsors to create career pipelines and promote veteran inclusion in cybersecurity.

Additional Work Experience

Oregon Institute of Technology | **Veteran Resource Officer** April 2023 – June 2024
Supported student veterans with education, career resources, and VA benefits, ensuring successful transitions to higher education.
Represented OIT at congressional and Senate meetings, advocating for federal and state policy changes that improved education and transition support for student veterans.
Built partnerships with veteran organizations to expand student support services.

Clackamas County | **Building Maintenance Specialist** December 2016 – May 2021
Performed preventive maintenance and repairs on county facilities, including HVAC, plumbing, and electrical systems, ensuring compliance with safety standards.
Managed vendor coordination and emergency response operations, reducing downtime during critical failures.
Led OSHA and ADA compliance inspections across multiple government facilities, implementing corrective actions that reduced violation risk and improved safety audit scores.
Contributed to disaster recovery planning and infrastructure resilience protocols.

Leatherman Tool Group | **CNC Production Machine Operator III** August 2012 – November 2016
Operated and programmed CNC machines for precision manufacturing of multi-tools, maintaining strict quality and efficiency standards.
Assisted in troubleshooting machining issues and optimizing production processes, reducing downtime and improving throughput.
Conducted quality control inspections, ensuring compliance with manufacturing specifications and industry standards.
Partnered with R&D to prototype and optimize CNC machining processes for new product lines, reducing setup time and tooling costs by 20%.
Authored technical documentation to track machining efficiency and quality trends, helping leadership improve production planning and reduce downtime.
Trained and mentored junior operators on machine setup, troubleshooting, and quality control, improving overall team proficiency.

Washington Army National Guard | **Administrative Specialist (71L) / Human Resources Specialist (42A)** June 2004 – July 2009
Managed personnel records, processing promotions, transfers, and separations.
Maintained accurate payroll and personnel records, improving administrative efficiency and supporting unit readiness.
Provided administrative support for unit operations and ensured compliance with military regulations.
Processed security clearance documentation and personnel evaluations, maintaining strict confidentiality and regulatory adherence.

U.S. Army - Operation Iraqi Freedom | **Internment/Resettlement Specialist (31E)** June 2006 – November 2007
Supervised and secured high value detainees and POWs in a military internment facility.
Conducted security screenings and maintained detainee records.
Assisted in the transport and movement of detainees between facilities.

Provided intelligence support through detainee interviews and assessments, contributing to mission planning and security operations.

Technical Proficiencies

Python | C++ | PowerShell | Bash | SQL | YAML | JSON | Linux | Windows Server | MacOS | AWS | Azure | Cloud Security | IAM | Zero Trust Architecture | Penetration Testing | Incident Response | Forensics (Autopsy, Volatility, FTK) | Kubernetes | Docker | Terraform | Splunk | Nmap | Wireshark | Metasploit | Nessus | Burp Suite | Snort | Suricata | OSSEC | CrowdStrike | Cisco Firepower | ELK Stack | Graylog | MITRE ATT&CK | Active Directory Security | Windows Defender ATP | Okta | NIST CSF | SOC 2 | ISO 27001 | HIPAA Compliance