ERNEST ALLARD
Pasco, WA 99301
(207) 272-6569 | allard.ernie@gmail.com
www.linkedin.com/in/ernest-allard
https://github.com/ernestallardCySec

PROFESSIONAL SUMMARY

Veteran cybersecurity professional with over 8 years of experience across military and civilian sectors, including roles at the Pacific Northwest National Laboratory and the U.S. Navy. Entry-level Product Security Engineer leveraging hands-on cybersecurity experience, strong Linux security expertise, and a solid foundation in secure software practices to support secure product development and risk mitigation.

- Security Testing
- Linux Security
- Scripting
- Orchestration
- Cloud & DevOps
- Collaboration & Communication

EDUCATION

Bachelor of Applied (B.A.S) Science in Cybersecurity | Columbia Basin College | Mar. 2024

CERTIFICATIONS

CompTIA Security+
CompTIA Network+
Studying for CSSLP certification

TECHNICAL PROJECTS

Home IDS Automation Project
Developed a home intrusion detection system using Suricata and Home Assistant; automated alerting and visualization via Python, JSON, and custom sensors.
Real-time alerts deliver push notifications with critical metadata; the live dashboard summarizes threat activity.
Zero third-party brokers required, keeping the system lean and secure.

Ansible CIS Hardening for RHEL9
Created a Ansible playbook and role that automates CIS-style security hardening on Red Hat Enterprise Linux 9. Run the playbook to remediate any drift or schedule this playbook in CI/CD for continuous compliance.

RELEVANT SKILLS

Security Testing

- Conducted penetration testing on operational technology systems for DHS and CWMD programs, uncovering exploitable vulnerabilities using OWASP Top Ten.
- Performed analysis using Wireshark and Security Onion to validate TLS configurations and detect anomalous traffic.
- Identified misconfigured network services on government installations, enabling patching efforts that mitigated high-risk exposures.

Linux Security

- POSIX Permissions & ACL: Implemented POSIX file permissions and Access Control Lists to enforce least-privilege access and protect sensitive data.
- SELinux Policy Modules & Secure Boot: Developed custom SELinux policy modules and configured basic secure-boot mechanisms to ensure system integrity and prevent unauthorized code execution.
- VM & Hypervisor security basics: Hardened virtual machines and hypervisors through isolation best practices, patch management, and configuration of security extensions.

Scripting

- Beginner/Intermediate experience with Python (pytest, requests).
- Beginner with C++. Willing to learn Go/Bash/C
- Beginner with Ansible playbooks

Cloud & DevOps

- Built my AWS S3 website to showcase current & future personal projects.
- Beginner experience with Git/GitHub workflows.

Risk Management

- Executed security control reviews using NIST 800-53R5 for U.S. Army facility, identifying and correcting noncompliant controls.
- Enforced physical security compliance measures across nuclear security operations.

Team Leadership & Training

- Mentored 30 personnel, providing development and cybersecurity instruction in lab and field environments.
- Delivered cybersecurity awareness training to college students focused on Hydropower Critical Infrastructure.
- Led compliance during multi-unit operations, maintaining zero loss incidents and 100% equipment accountability.

System Administration

- Installed, configured, and secured network appliances for lab and operational use cases.
- Oversaw software/hardware patches and version controls, ensuring baseline compliance and minimizing vulnerabilities.
- Implemented Linux-based administration tools for server management and secure scripting operations.

Technical Writing

- Drafted operational reports, incident summaries, and technical assessments for internal and external stakeholders.
- Authored policy guidance and standard operating procedures for cyber assessments.
- Maintained detailed logs and asset tracking by NIST and DoD directives.

Stakeholder Engagement

- Coordinated directly with DHS sponsors and military liaisons to provide assessment outcomes and secure solutions.
- Provided technical assistance and mentoring to junior technicians in lab and field operations.
- Engaged with cross-functional teams to align cybersecurity priorities with mission objectives.

PROFESSIONAL EXPERIENCE

Pacific Northwest National Laboratory | Richland, WA **Jun. 2022 – Present**
Cybersecurity Research Assistant

- Conducted cybersecurity risk assessments for military and government networks, applying NIST 800-53R5 standards.
- Facilitated Red vs. Blue Team Exercises with Security Onion: Deployed and monitored Security Onion sensors during red team engagements, capturing IDS and host-based telemetry.
- Delivered training to interns and critical infrastructure partners, improving cybersecurity posture across agencies.
- Analyzed traffic using Wireshark to validate TLS compliance and detect unauthorized encryption anomalies.
- Provided testing insights for DHS/CWMD programs, influencing mitigation strategies and risk remediation.

United States Navy | **Jul. 2016 – Jan. 2021**
Security Technician / Team Leader

- Supervised 30 personnel in technical and security operations; mentored junior staff in professional development and cybersecurity principles.
- Directed the secure operation and movement of over $500K in government assets with zero loss or incident during hazardous duty assignments.
- Managed physical site security, including intrusion detection, access control systems, and surveillance, securing a nuclear facility against breaches.
- Maintained compliance with security regulations and policies, reviewed asset protection protocols, and coordinated incident response with leadership.
- Led logistics planning and communication for equipment and personnel across multiple departments, ensuring timely and secure delivery of mission-critical items.