ADAM RAAYMAKERS

OSCP+ Penetration Tester | DoD TS/SCI

I break into web, network, and embedded/OT systems so you can fix them before someone else does.

(520) 442-4107 | adam.raaymakers@pm.me | linkedin.com/in/adamraaymakers | adamraaymakers.com

PROFESSIONAL SUMMARY

Offensive security engineer with 10+ years in IT and 6+ in penetration testing, specializing in web application, network, and embedded/OT assessments for DoD and Fortune 100 clients. OSCP+ certified. Led red/purple team engagements simulating APT TTPs against classified developmental weapon systems, cut system vulnerabilities by 19% on a $40M risk-reduction program, and identified 150+ vulnerabilities across FedRAMP and Fortune 100 web app tests.

CERTIFICATIONS

Offensive Security Certified Professional (OSCP/OSCP+)

TCM Security Practical Junior Penetration Tester (PJPT)

Certified Legacy Off-Road Recovery Specialist (ORRS) — personal interest

CompTIA A+ | CompTIA Net+ | **CompTIA Sec+** | CompTIA Linux+ | CompTIA Pentest+ | **CompTIA SecurityX (CASP+)**

TECHNICAL SKILLS

Offensive Security & Pentesting: Penetration testing (web, network, API), red/purple teaming, APT simulation, vulnerability assessment & exploitation, threat modeling, OWASP Top 10, continuous security testing

Frameworks & Standards: MITRE ATT&CK, MITRE Caldera, NIST SP 800-53, DISA STIGs, ISO 27001, FedRAMP

Tools & Platforms: Burp Suite, Metasploit, Nmap, Cobalt Strike, Wazuh, Splunk, ELK, GOAD, Proxmox

Cloud & Infrastructure: AWS, multi-cloud, Active Directory, Linux, DevSecOps

PROFESSIONAL EXPERIENCE

Accenture Federal Services | Remote, USA | July 2025 - Present
Senior Security Consultant

- Lead penetration tests across client web applications, networks, and systems using manual exploitation and automated tooling, identifying exploitable risk and prioritizing findings by business impact
- Drive purple team exercises with Cybersecurity and Engineering teams that close the loop between findings and Incident Response, strengthening detection and remediation of active threats
- Architecting a continuous security testing platform that extends client coverage beyond point-in-time vulnerability scans

Northrop Grumman | Roy, Utah, USA | Sept 2024 – June 2025
Senior Principal Cyber Systems Engineer

- Led APT-level penetration tests against classified developmental weapon systems, identifying critical vulnerabilities before they reached operational deployment
- Led a 7-member cross-functional team on a $40M cybersecurity risk-reduction initiative, achieving a 19% decrease in weapon system vulnerabilities
- Co-authored system-level cyber test procedures that became the weapon system-wide standard for cyber testing guidance
- Built and taught a hands-on “Pentesting Foundations” boot camp (threat modeling, OWASP Top 10, reconnaissance, exploitation, reporting) and mentored 8 junior analysts into independent testers

Booz Allen Hamilton (End of Contract) | Remote, USA | Aug 2023 - Sept 2024
Information System Security Engineer

- Led IT modernization migrating legacy systems to secure cloud environments while maintaining compliance and improving security posture
- Embedded DevSecOps practices across the development lifecycle, reducing production vulnerabilities by 16%

Vaultes | Remote, USA | Nov 2022 - May 2023
Senior Security Consultant

- Supported a major federal client through a full legacy system upgrade, achieving 100% successful compliance assessments during transition
- Delivered FedRAMP penetration tests for small businesses, identifying 150+ vulnerabilities and providing remediation roadmaps that accelerated compliance

NetSPI | Remote, USA | June 2022 - Sept 2022
Web Application Penetration Tester

- Led 25+ web application penetration tests for Fortune 100 clients, identifying critical OWASP Top 10 flaws
- Translated technical findings into business-risk recommendations in reports that drove prioritized remediation

Dark Wolf Solutions | Hill AFB, UT, USA | May 2021 - May 2022
Cyber Security Engineer

- Developed attack path vectors with MITRE Caldera and mapped threat scenarios to MITRE ATT&CK for red/purple team exercises
- Partnered with cloud architects to integrate multi-cloud environments into a centralized SIEM, improving threat detection coverage

KBR Aero (End of Contract) | Hill AFB, UT, USA | Oct 2020 - April 2021
Cybersecurity Engineer

- Assessed aircraft weapon systems and developed testing protocols that identified 11+ critical vulnerabilities
- Revamped the Authority to Operate package with advanced threat modeling, and established cybersecurity baseline standards for embedded aviation systems across multiple platforms

Leidos | Hill AFB, UT, USA | May 2020 - Sept 2020
Cyber Security Analyst (SOC)

- Correlated security events across 500+ systems using Splunk and ELK, identifying and mitigating incidents and mapping them to MITRE ATT&CK
- Produced security trend analysis for senior management that informed strategic security investment decisions

ManTech (End of Contract) | Hill AFB, UT, USA | Dec 2019 - April 2020
Information Assurance Specialist II

- Maintained information assurance sustainment (change management, account lifecycle) in compliance with NIST SP 800-53, DISA STIGs, and ISO 27001.

BAE | Eglin AFB, FL, USA | Dec 2017 - Nov 2019
F-35 Field Service Engineer

- Administered Active Directory, DNS, DHCP, and domain controllers for F-35 training systems across CONUS/OCONUS and implemented NIST 800-53 and STIG controls for classified training environments.

United States Air Force (RET) | Everywhere, USA | Mar 2002 - Dec 2022
Aircraft Mechanic

- Led aircraft launch/recovery operations and maintenance supporting 8,000+ annual flying hours at 82% mission-ready
- Provided system administration for aircraft technical order systems, ensuring secure access and data integrity in a high-availability environment

EDUCATION

Western Governors University | January 2026
Master of Business Administration (MBA), Information Technology Management

University of Maryland | June 2021
Bachelor's, Computer Networks & Cyber Security

PROFESSIONAL TRAINING & INDEPENDENT PROJECTS

- White Knight Labs: AI-Powered Red Teaming & C2 Operator Creation (In-Work)
- Independent project — Advanced Home Laboratory: Build and maintain a Proxmox-based penetration testing lab (GOAD, Wazuh) plus a local LLM inference environment (llama.cpp) wired into offensive tooling for red teaming and recent-CVE exploitation.