

# ZaydKirk

## Penetration Testing Architect

☎ (303) 555-0184 ✉ zayd.kirk@protonmail.com 🔗 linkedin.com/example/zaydkirk 📍 Aurora, CO 80012

### SUMMARY

Penetration Testing Architect with 15+ years guiding **offensive security** across applications, APIs, networks, **cloud environments**, **identity platforms**, and enterprise infrastructure. Hands-on work covers reconnaissance, enumeration, vulnerability analysis, controlled exploitation, post-exploitation, attack-path chaining, **source-code-assisted testing**, and security architecture review. Built repeatable methodologies, custom tooling, evidence standards, severity criteria, reporting practices, and remediation verification for AWS, Azure, Kubernetes, Active Directory, CI/CD pipelines, and distributed systems. Partnered with architects, developers, cloud engineers, and infrastructure teams to prevent vulnerability classes before production. Mentored penetration testers, reviewed high-risk reports, researched emerging vulnerabilities, and explained technical risk to varied stakeholders. Ready to help Northstar Offensive Security Group advance scalable testing, continuous validation, and practical architectural risk reduction.

### EXPERIENCE

#### Penetration Testing Architect

Cinder Peak Security 📅 March 2023 - Present 📍 Boulder, CO

Set technical direction for offensive security across SaaS applications, APIs, AWS, Kubernetes, corporate identity, and internal infrastructure. Led high-risk assessments, established organization-wide standards, reviewed designs, built automation, and mentored eight testers without direct management authority.

- Set testing direction across SaaS, APIs, AWS, Kubernetes, identity, and internal **infrastructure** engagements.
- Created rules, evidence, severity, reporting, and retest **standards** for high-risk offensive security assessments.
- Chained IAM weaknesses, exposed secrets, and routing errors across AWS accounts to demonstrate administrative **attack paths**.
- Built Python and Go automation around Nmap, **Burp Suite**, cloud APIs, BloodHound, and custom payloads.
- Reviewed designs before release, strengthening authorization, secrets, segmentation, admission controls, and **CI/CD** supply chains.
- Mentored eight testers through **exploitation** challenges, report reviews, and unusual cloud identity findings.

#### Principal Offensive Security Engineer

Blue Meridian Technologies 📅 January 2020 - February 2023 📍 Austin, TX

Directed complex web, API, network, and cloud assessments for distributed financial-services platforms across Azure and on-premises environments. Combined source-code review, manual testing, identity analysis, CI/CD validation, report governance, and executive risk communication.

- Directed web, API, network, and cloud assessments across **Azure** and on-premises financial platforms.
- Combined source review, Burp Suite, ffuf, **sqlmap**, debugging tools, and scripts to expose logic defects.
- Modeled **Active Directory** paths with BloodHound and **PowerShell**, validating delegation weaknesses through controlled exploitation.
- Designed pull-request checks and authenticated API harnesses for **continuous security validation** within CI/CD workflows.
- Presented attack narratives to **architecture** councils, linking technical evidence with customer exposure and release risk.
- Established peer reviews for severity consistency and remediation evidence across security engagements.

#### Senior Penetration Tester

Ironwood Digital Defense 📅 June 2017 - December 2019 📍 Raleigh, NC

Executed production-scale assessments across customer-facing applications, REST APIs, Windows and Linux systems, cloud permissions, and hybrid identity environments. Combined manual analysis, safe exploit validation, **vulnerability research**, reporting, coaching, and remediation verification.

- Executed web, API, Windows, Linux, and hybrid identity tests under approved rules of engagement.
- Combined Nmap, Wireshark, Burp Suite, Metasploit, Nessus, ffuf, **Bash**, and **Python** for validation.
- Chained object references, session flaws, exposed interfaces, and cloud permissions across critical systems.
- Tested authentication, authorization, **access control**, **business logic**, TLS, and trust boundaries with reproducible evidence.
- Adapted emerging CVE proof-of-concept code for safe validation without disrupting production stability.
- Coached associate testers on **threat modeling**, attack paths, technical writing, and remediation verification.

#### Penetration Tester

Redwood Signal Labs 📅 August 2014 - May 2017 📍 Columbus, OH

Performed network, web, API, and infrastructure assessments for healthcare, retail, and manufacturing clients. Built reusable scripts, mapped identity relationships, validated findings, and translated **technical risk** into practical **remediation guidance**.

- Performed network, web, API, and infrastructure assessments across regulated client environments.
- Built Python and PowerShell scripts for **reconnaissance** across segmented **networks**, Windows domains, and Linux systems.

- Validated injection, **authentication**, configuration, and privilege findings with Burp Suite, Nmap, and **Metasploit**.
- Mapped Active Directory trust relationships and permissions into remediation-focused attack-path diagrams.
- Wrote executive and technical reports with severity rationale, fixes, verification steps, and compensating controls.
- Supported senior consultants during complex engagements and client readouts on systemic weaknesses.

## Associate Security Consultant

Harbor Ridge Security Consulting 📅 September 2011 - July 2014 📍 Richmond, VA

Conducted supervised vulnerability assessments and penetration tests for web **applications**, enterprise networks, Linux servers, and Windows environments. Applied core network security concepts, validated exploitable findings, maintained evidence, and developed clear client communication skills.

- Conducted supervised web, network, Linux, and Windows assessments within approved consulting scopes.
- Applied **TCP/IP**, DNS, **HTTP/HTTPS**, TLS, routing, segmentation, and service knowledge to plan testing.
- Validated findings with Nmap, Nessus, Burp Suite, **Wireshark**, Metasploit, and Bash scripts.
- Documented authentication, **authorization**, injection, configuration, and privilege-escalation issues with reproducible evidence.
- Maintained engagement notes, evidence repositories, remediation trackers, and retest results for quality reviews.
- Presented selected findings to administrators and **developers**, supporting collaborative remediation planning.

## PROJECTS

### Continuous Cloud Security Validation Framework 📅 2024

Created reusable assessment workflows for AWS and Kubernetes trust boundaries, combining cloud APIs, identity analysis, evidence capture, and remediation verification for recurring validation.

### Source-Assisted API Attack Path Methodology 📅 2022

Built a manual API testing approach joining source review, authorization analysis, business logic testing, and controlled exploit validation for distributed services.

### Active Directory Identity Exposure Research 📅 2018

Mapped identity relationships with BloodHound and PowerShell, producing controlled attack scenarios that clarified privilege escalation risk and practical defensive priorities.

## LEADERSHIP & AWARDS

- SANS NetWars Advanced Cyber Defense finalist, 2021
- Client Impact Award, Blue Meridian Technologies, 2022
- Security Research Recognition, Redwood Signal Labs, 2016

## EDUCATION

### Bachelor's Degree in Cybersecurity

Virginia Commonwealth University 🎓 GPA: 3.7 📅 2011 📍 Richmond, VA

***Coursework:** Network security, secure software development, digital forensics, risk analysis*

## CERTIFICATIONS

- Offensive Security Certified Expert (OSEP) 📅 2024
- GIAC Cloud Penetration Tester (GCPN) 📅 2025
- Offensive Security Web Expert (OSWE) 📅 2022
- Offensive Security Certified Professional (OSCP) 📅 2016
- GIAC Web Application Penetration Tester (GWAPT) 📅 2018

## TECHNICAL SKILLS

- **Offensive Security Tools:** Burp Suite, Metasploit, Nessus
- **Network Assessment:** Nmap, Wireshark, TCP/IP
- **Web Testing:** OWASP, HTTP/HTTPS, TLS
- **Cloud Platforms:** AWS, Azure, Google Cloud
- **Identity Platforms:** Active Directory, IAM, BloodHound
- **Scripting Languages:** Python, Go, PowerShell
- **Shell Environments:** Bash, Linux, Windows
- **API Testing:** REST, authentication, authorization

- **Application Testing:** ffuf, sqlmap, source-code review
- **Container Security:** Kubernetes, admission controls, container security
- **CI/CD Security:** GitHub Actions, pull-request checks, supply-chain security
- **Reverse Engineering:** debugging tools, reverse-engineering tools, exploit development

**SKILLS**

---

- |                                   |                          |                         |                            |
|-----------------------------------|--------------------------|-------------------------|----------------------------|
| • Penetration Testing             | • Attack-Path Analysis   | • Active Directory      | • Technical Reporting      |
| • Offensive Security Architecture | • Vulnerability Research | • CI/CD Security        | • Remediation Verification |
| • Web and API Security            | • Exploit Validation     | • Supply-Chain Security | • Security Architecture    |
| • Cloud Security                  | • Threat Modeling        | • Reverse Engineering   |                            |

**PROFESSIONAL AFFILIATIONS**

---

- OWASP Colorado Chapter volunteer speaker, 2023 - Present
- Mentor, University of Colorado Cybersecurity Clinic, 2021 - Present
- Contributor, Open Source Security Testing Community, 2018 - Present

**LANGUAGES**

---

- English (Native)
- Spanish (Intermediate)

**ADDITIONAL INFORMATION**

---

**Work Status** : Authorized to work in United States. No sponsorship required.

**REFERENCES**

---

AVAILABLE ON REQUEST