Nicholas Alexander

Associate Penetration Tester

(303) 555-0148 nicholas.alexander@protonmail.com
linkedin.com/example/nicholasalexander Aurora, CO 80012

SUMMARY

Associate Penetration Tester with three years of hands-on work across authorized network, web application, and API security assessments in production-like environments. Conducts reconnaissance, enumeration, **vulnerability discovery**, manual validation, **controlled exploitation**, evidence collection, reporting, and remediation retesting with sound judgment. Applies TCP/IP, DNS, HTTP/HTTPS, Linux, Windows, Active Directory, **OWASP Top 10**, CVE, CVSS, and **rules of engagement** during practical testing. Uses Nmap, Burp Suite, Nessus, OpenVAS, Wireshark, Metasploit, ffuf, Gobuster, sqlmap, Python, Bash, and PowerShell to support repeatable assessments. Clear reports help developers, administrators, and security teams act quickly. Collaborative work with senior testers supports safe handling of complex attack paths and higher-risk findings. Ready to help Redwood Sentinel Security deliver credible assessments and practical remediation guidance.

STRENGTHS

Manual Validation
Scanner output started the work. Manual testing confirmed exploitability, removed false positives, and gave reviewers findings they could trust.

Clear Reporting
Each report connected evidence, reproduction steps, severity, impact, and remediation, helping technical teams act without guesswork.

Safe Exploitation
Approved boundaries guided every validation effort. Controlled Metasploit and sqlmap testing produced evidence without crossing engagement limits.

Attack-Path Thinking
Separate weaknesses sometimes formed one meaningful path. Linking them gave senior testers a clearer view of business risk.

Collaborative Retesting
Remediation conversations became working sessions. Follow-up tests confirmed fixes and kept unresolved high-risk issues visible.

SKILLS

Penetration Testing

Vulnerability Assessment

API Security Testing

Reconnaissance Enumeration

Vulnerability Validation

OWASP Top 10

EXPERIENCE

Associate Penetration Tester

Blue Mesa Cyber Defense January 2025 - Present Denver, CO

Leads authorized network, web application, and API assessments for production-like client environments. Converts rules of engagement into test plans, evidence standards, escalation thresholds, and client-ready reporting while coordinating with senior testers, developers, administrators, and security teams.

- Mapped **exposed services** with Nmap and Nessus across Linux and Windows targets, revealing overlooked attack surfaces.
- Validated web weaknesses through **Burp Suite**, ffuf, Gobuster, and manual testing, separating confirmed findings from **false positives**.
- Tested authentication, authorization, sessions, **access controls**, **input validation**, and business logic against OWASP-aligned criteria.
- Used Metasploit, sqlmap, Python, Bash, and **PowerShell** for controlled validation, preserving approved testing boundaries.
- Produced findings with evidence, reproduction steps, CVSS-informed severity, business impact, and practical remediation guidance.
- Retested fixes with developers and administrators, documenting verification results and escalating unresolved high-risk issues to senior testers.

Cybersecurity Analyst

Northstar Security Operations September 2023 - December 2024 Colorado Springs, CO

Supported vulnerability assessments and focused penetration tests across internal networks, web applications, APIs, and Windows services. Built repeatable reconnaissance workflows, validated scanner output, prepared technical reports, and supported remediation discussions involving Active Directory, cloud environments, and multi-stage attack scenarios.

- Built Nmap, OpenVAS, Wireshark, and Python workflows that exposed ports, versions, interfaces, and attack surfaces.
- Validated scanner results through Burp Suite requests, HTTP analysis, configuration review, and repeatable test cases.
- Investigated **OWASP Top 10** issues, **insecure configurations**, access-control gaps, and authentication weaknesses for client review.
- Connected related weaknesses into attack-path narratives, clarifying exploitability, **technical impact**, and **business risk**.
- Prepared evidence packages and reports covering affected assets, severity, reproduction steps, impact, and **remediation recommendations**.
- Presented findings during remediation discussions and retested patched systems, escalating complex **Active Directory** and cloud scenarios.

Controlled Exploitation

Attack-Path Analysis

Authentication Testing

Access Controls

Session Management

Linux Security | Windows Security

Remediation Retesting

LANGUAGES

English — Native

Spanish — Intermediate

MY CAREER

- Associate Penetration Tester at Blue Mesa Cyber Defense (1.7 Years)
- Cybersecurity Analyst at Northstar Security Operations (1.2 Years)

PROJECTS

API Authorization Test Lab 2024

A small test environment became a useful proving ground for broken access controls. Built API scenarios covering authentication, authorization, sessions, input validation, and business logic, then documented reproducible findings with remediation guidance.

Active Directory Attack Path Study 2023

One overlooked permission can reshape an assessment. Studied Active Directory attack paths in a controlled lab, combining enumeration, credential analysis, validation, and reporting to explain risk without exceeding approved testing boundaries.

LEADERSHIP & AWARDS

- Capture the Flag Mentor, Colorado Springs Cyber Defense Club, 2024 - 2025
- Vulnerability Research Workshop Lead, University Cybersecurity Society, 2022 - 2023
- CompTIA Security+ Achievement, 2023

EDUCATION

Bachelor's Degree in Cybersecurity

University of Colorado Colorado Springs GPA: 3.8 2023 Colorado Springs, CO

Coursework: *Network Security, Ethical Hacking, Digital Forensics, Secure Software Development*

CERTIFICATIONS

- CompTIA Security+ 2023
- eLearnSecurity Junior Penetration Tester (eJPT) 2024

TECHNICAL SKILLS

- **Network Assessment Tools:** Nmap, Wireshark, Nessus
- **Web Testing Tools:** Burp Suite, ffuf, Gobuster
- **Exploitation Tools:** Metasploit, sqlmap, exploit validation
- **Vulnerability Scanning:** OpenVAS, Nessus, manual validation
- **Scripting Languages:** Python, Bash, PowerShell
- **Network Protocols:** TCP/IP, DNS, HTTP/HTTPS
- **Application Security:** OWASP Top 10, input validation, business logic
- **Identity Testing:** Authentication, authorization, Active Directory
- **Risk Assessment:** CVE, CVSS, exploitability analysis
- **Security Documentation:** Penetration reports, evidence collection, remediation guidance
- **Operating Systems:** Linux, Windows, Windows services
- **Testing Methodologies:** Rules of engagement, reconnaissance, enumeration

PROFESSIONAL AFFILIATIONS

- Colorado Springs Cyber Defense Club, Capture the Flag Mentor
- University Cybersecurity Society, Vulnerability Research Workshop Lead
- OWASP Community Participant, Application Security Learning

ADDITIONAL INFORMATION

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

REFERENCES

AVAILABLE ON REQUEST