David Johnston

Penetration Tester Intern

(253) 555-0148 david.johnston@example.com
linkedin.com/example/davidjohnston Tacoma, WA 98402

STRENGTHS

Evidence discipline
Kept commands, screenshots, scope notes, and cleanup records together; reviewers could follow each finding without guesswork.

Quiet analysis
Compared scanner output with manual testing before speaking up, helping teams focus on findings that held up.

Clear reporting
Turned technical observations into concise risk, reproduction, and remediation notes that faculty reviewers could act on.

Ethical judgment
Stopped at authorized boundaries during lab work; that restraint protected training data and earned peer confidence.

Peer collaboration
Shared safe testing methods during club workshops, giving classmates room to ask questions and practice responsibly.

SKILLS

Penetration Testing
Vulnerability Assessment
Reconnaissance Enumeration
Web Application Security
OWASP Testing Concepts
Kali Linux Nmap Burp Suite
Metasploit Wireshark Linux
Windows Technical Reporting
Remediation Retesting

SUMMARY

Cybersecurity student pursuing **penetration testing** work with hands-on academic practice across **web applications**, networks, Linux, and Windows environments. Authorized lab assessments have included reconnaissance, scanning, enumeration, **controlled exploitation**, vulnerability validation, evidence collection, and remediation retesting. Work with Nmap, Burp Suite, Metasploit, Wireshark, Kali Linux, and OWASP guidance has built a careful approach to distinguishing confirmed findings from false positives. Technical reports document risk, reproduction steps, screenshots, scope, and practical remediation guidance. Faculty reviewers and student teams have received concise briefings that connect security observations with clear next actions. Current studies in network defense, secure coding, operating systems, and digital forensics support continued growth in **security assessment** methodology. Ready to contribute disciplined testing, clear communication, ethical judgment, and steady curiosity to Cascade Secure Systems.

EDUCATION

Bachelor's Degree in Cybersecurity

University of Washington Tacoma GPA: 0 2027 Tacoma, WA

Coursework: *Network defense, secure coding, operating systems, digital forensics*

TECHNICAL SKILLS

- **Security Testing:** Penetration testing, vulnerability assessment, ethical hacking
- **Reconnaissance Tools:** Nmap, Wireshark, service enumeration
- **Web Testing:** Burp Suite, OWASP guidance, browser inspection
- **Exploitation Tools:** Metasploit, controlled exploitation, proof-of-concept requests
- **Operating Systems:** Kali Linux, Linux, Windows
- **Networking:** TCP/IP, DNS, HTTP
- **Assessment Methods:** Black-box testing, scanning, enumeration
- **Finding Validation:** False-positive analysis, reproduction, evidence collection
- **Reporting:** Technical reports, risk analysis, remediation recommendations
- **Remediation Testing:** Retesting, verification appendices, closure records
- **Security Documentation:** Scope records, timestamps, screenshots
- **Application Security:** Authentication, session management, access control

EXPERIENCE

Penetration Tester Student Researcher

University Cybersecurity Lab September 2025 - Present Tacoma, WA

Supports authorized security assessments across isolated Linux and Windows lab **networks**, guiding scope definition, evidence quality, reporting, remediation verification, and peer review.

- Defined assessment scope before lab exercises, protecting test boundaries and confidential training data.
- Mapped isolated hosts with Nmap and Wireshark, connecting exposed services with plausible attack paths.
- Validated **Burp Suite** findings against OWASP guidance, removing scanner observations lacking reproducible evidence.
- Built controlled **Metasploit** demonstrations for vulnerable systems, recording commands, evidence, and cleanup steps.
- Prepared concise reports with **risk** context, **reproduction steps**, screenshots, and remediation recommendations.
- Retested patched **systems** and updated records, confirming fixes without expanding authorized testing scope.

LANGUAGES

English — Native

Spanish — Beginner

MY CAREER

- Penetration Tester Student Researcher at University Cybersecurity Lab (1 Years)
- Penetration Tester, Academic Project at Secure Web Application Capstone Project (4 Months)
- Junior Penetration Testing Analyst at Cyber Defense Club Lab Practicum (1.2 Years)

Penetration Tester, Academic Project

Secure Web Application Capstone Project | January 2026 - May 2026 | Tacoma, WA

Completed a supervised black-box assessment of a faculty-provided inventory application, producing reproducible findings, sanitized evidence, remediation priorities, and verification records.

- Defined a black-box plan covering authentication, sessions, input validation, and access control.
- Used **Burp Suite** and manual requests to reproduce three OWASP-aligned weaknesses safely.
- Created sanitized proof-of-concept requests, allowing classmates to reproduce findings without exposing credentials.
- Compared automated scan output with manual validation, removing non-reproducible observations from final reporting.
- Presented remediation priorities, linking server-side authorization and input handling with reduced exposure.
- Repeated assessment after code changes and recorded closure evidence in a verification appendix.

Junior Penetration Testing Analyst

Cyber Defense Club Lab Practicum | September 2024 - December 2025 | Tacoma, WA

Completed supervised network and web security exercises in segmented student labs, applying foundational protocols, operating system knowledge, ethical testing practices, and clear technical communication.

- Completed supervised exercises with **Kali Linux**, **Nmap**, Burp Suite, and Metasploit modules.
- Practiced **reconnaissance**, **enumeration**, password-hash analysis, and vulnerability verification against intentionally vulnerable machines.
- Applied **TCP/IP**, DNS, HTTP, Linux permissions, and **Windows** service concepts during analysis.
- Maintained notes with timestamps, commands, screenshots, impact observations, and cleanup confirmation.
- Traced tabletop findings to affected assets, then proposed containment or hardening steps.
- Delivered a web testing demonstration emphasizing authorization, scope discipline, and responsible disclosure.

PROJECTS

Secure Web Application Assessment | 2026

Built a supervised black-box assessment for a local inventory application. Reproduced OWASP-aligned weaknesses, prepared sanitized evidence, presented remediation priorities, and verified fixes after code changes.

Segmented Network Security Lab | 2025

Assessed intentionally vulnerable Linux and Windows systems within an authorized student environment. Mapped services, validated attack paths, recorded evidence, and practiced cleanup after controlled demonstrations.

LEADERSHIP & AWARDS

- Dean's List, University of Washington Tacoma, Fall 2025
- Second Place, Cyber Defense Club Vulnerability Analysis Challenge, 2025
- Undergraduate Research Poster Recognition, University Cybersecurity Lab, 2026

CERTIFICATIONS

- Google Cybersecurity Professional Certificate | 2025
- PortSwigger Web Security Academy: Web Application Security Fundamentals | 2026

PROFESSIONAL AFFILIATIONS

- Workshop Coordinator, Cyber Defense Club, 2025 - 2026
- Peer Lab Mentor, University Cybersecurity Lab, 2026
- Participant, Pacific Northwest Collegiate Capture-the-Flag Competition, 2025

ADDITIONAL INFORMATION

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

REFERENCES

AVAILABLE ON REQUEST