Liam Wells

(512) 555-0148 liam.wells@protonmail.com linkedin.com/example/liamwells Austin, TX 78701

SUMMARY

Senior IT **Penetration Tester** with more than five years delivering network, web, API, **Active Directory**, cloud, wireless, and **Microsoft 365** assessments for consulting clients. Leads scope definition, rules of engagement, reconnaissance, exploit validation, evidence handling, reporting, retesting, and executive readouts across concurrent engagements. Hands-on work includes Kali Linux, Burp Suite, Metasploit, Nmap, Nessus/Tenable, BloodHound, Python, PowerShell, Bash, GitHub, Splunk, Microsoft Sentinel, Azure, and Microsoft 365. OSCP-certified practitioner with strong Windows, Linux, TCP/IP, DNS, identity, authentication, and cloud security knowledge. Collaborates with SOC teams during red team and **purple team** exercises, tests AI-enabled applications against LLM risks, and turns technical findings into prioritized remediation. Ready to help Northstar Cyber Advisory deliver clear, defensible security guidance that clients can act on.

EXPERIENCE

Senior Penetration Tester

January 2024 - Present

Ironclad Security Partners

Austin, TX

Leads concurrent external, internal, web, API, Active Directory, Azure, and Microsoft 365 assessments. Owns engagement scope, testing strategy, exploit validation, evidence quality, client reporting, remediation workshops, and executive communication. Guides peer review and reusable tooling contributions across consulting engagements.

- Led concurrent network, web, API, Azure, and Microsoft 365 assessments through executive readouts.
- Validated High and Critical findings with **Kali Linux**, Nmap, Nessus, **Burp Suite**, and Metasploit.
- Mapped Active Directory attack paths, exposing **privilege escalation** and **lateral movement** risks for infrastructure owners.
- Tested AI applications for prompt injection, data exposure, insecure output, and tool-calling abuse.
- Connected Splunk and Sentinel telemetry with purple team findings, improving SOC detection discussions.
- Produced test plans, reports, **risk ratings**, exploit artifacts, and prioritized remediation guidance for clients.
- Reviewed Python, **PowerShell**, and Bash utilities through GitHub pull requests, improving testing repeatability.

Penetration Tester

January 2022 - December 2023

Red Mesa Cyber Consulting

Denver, CO

Executed network, wireless, web, API, cloud, and Microsoft 365 assessments for mid-market and enterprise clients. Managed reconnaissance, scan tuning, authenticated access, Active Directory analysis, reporting, remediation workshops, and retesting while translating technical vulnerabilities into clear business risk.

- Executed network, **wireless**, web, API, cloud, and **Microsoft 365** testing for consulting clients.
- Tuned **Nmap** and **Nessus** scans before manual verification, reducing unsupported findings in reports.
- Coordinated least-privilege access, protected secrets, and confirmed credential rotation during engagement closeout.
- Investigated **Active Directory** permissions, DNS integration, users, groups, and policies with **BloodHound** analysis.
- Prepared Word and PowerPoint reports that converted vulnerabilities into prioritized corrective actions.
- Reproduced original conditions during retesting, confirming fixes addressed root causes for stakeholders.

Security Assessment Analyst

June 2021 - December 2021

BluePeak Managed Security

Phoenix, AZ

Supported senior testers during scoped internal network and web assessments. Prepared target inventories, evidence folders, engagement notes, scripts, quality checks, and supervised client explanations while building practical capability across Windows, Linux, Active Directory, GitHub, and **security** assessment workflows.

- Prepared target inventories and evidence folders for scoped internal network and web assessments.
- Used Nmap, Nessus, **Burp Suite**, Windows, and Linux skills to identify exposed services.
- Built **Python** and PowerShell scripts for repeatable host checks and report preparation.
- Reviewed **Active Directory** users, groups, **DNS** records, and policies in approved environments.
- Checked reproduction steps, screenshots, severity rationale, and **remediation** language during report quality assurance.
- Presented retest observations in supervised meetings, clarifying technical issues for infrastructure stakeholders.

PROJECTS

LLM Application Abuse-Case Harness 2025

Most AI security failures begin with an overlooked assumption. Built a structured prompt-testing concept for LLM integrations, covering prompt injection, sensitive data exposure, insecure output handling, and tool-calling abuse. Mapped cases against OWASP Top 10 for LLM Applications and documented API-driven validation paths for repeatable client assessments.

Active Directory Attack Path Atlas 2024

A permission that looks harmless can open a route across an enterprise. Created a lab-based attack-path reference covering BloodHound analysis, Kerberos, NTLM, group policy, privilege escalation, lateral movement, root-cause review, and prioritized remediation guidance for infrastructure teams.

LEADERSHIP & AWARDS

- Dean's List, Arizona State University, 2020 and 2021
- Cyber Defense Scholarship, Arizona State University, 2021
- Top-10 Finalist, Southwest Collegiate Capture the Flag, 2020

EDUCATION

Bachelor of Science in Cybersecurity 2021

Arizona State University GPA: 3.8 *Tempe, AZ*

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

CERTIFICATIONS

- Offensive Security Certified Professional (OSCP) 2023
- Microsoft Certified: Security Operations Analyst Associate 2024
- AWS Certified Cloud Practitioner 2022

TECHNICAL SKILLS

- **Offensive Security Tools:** Kali Linux, Burp Suite, Metasploit, Nmap
- **Vulnerability Assessment:** Nessus, Tenable, Scan Tuning, Manual Verification
- **Active Directory:** BloodHound, Kerberos, NTLM, Group Policy
- **Identity Protocols:** DNS, SAML, OAuth 2.0, OpenID Connect
- **Operating Systems:** Windows, Linux, Microsoft 365, Microsoft Office
- **Cloud Platforms:** Microsoft Azure, AWS Cloud, Cloud Identity Services
- **Security Operations:** Splunk, Microsoft Sentinel, SIEM, SOC Workflows
- **Scripting Languages:** Python, PowerShell, Bash, API Test Harnesses
- **Development Collaboration:** Git, GitHub, Pull Requests, Peer Review
- **Delivery Automation:** GitHub Actions, Azure DevOps Pipelines, Docker, CI/CD
- **Security Frameworks:** PTES, OWASP, OWASP Top 10 for LLM Applications, SANS
- **Application Security:** Authentication, Session Management, Access Control, Injection
- **Testing Engagements:** Network Testing, Web Testing, API Testing, Wireless Testing
- **Reporting Applications:** Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Executive Reports
- **AI Security Testing:** Prompt Injection, Sensitive Data Exposure, Insecure Output Handling, Function Calling Abuse

SKILLS

- Penetration Testing
- Black Box Testing
- Active Directory
- Web Application Testing
- API Security Testing
- Cloud Security
- Microsoft 365
- Wireless Assessments
- Red Team Exercises
- AI/LLM Security
- Remediation Validation
- Technical Reporting
- Executive Presentations
- Threat Hunting
- Social Engineering

PROFESSIONAL AFFILIATIONS

- Cybersecurity Club Technical Workshop Lead, Arizona State University, 2020 - 2021
- Collegiate Cyber Defense Competition Team, Arizona State University, 2019 - 2021
- Peer Mentor, Information Assurance Student Lab, 2021

LANGUAGES

- English (Native)
- Spanish (Intermediate)

ADDITIONAL INFORMATION

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

REFERENCES

AVAILABLE ON REQUEST