Yuan Gilbert

Lead Penetration Tester

(303) 555-0184 yuan.gilbert@example.com linkedin.com/example/yuangilbert Denver, CO 80206

SUMMARY

Lead penetration tester with more than four years delivering network, web, API, **Active Directory**, cloud, **Microsoft 365**, and wireless assessments for consulting clients. Defines scope, **rules of engagement**, test objectives, access controls, and evidence practices before safe execution. Validates exploitability through Kali Linux, Burp Suite, Metasploit, Nmap, Nessus, BloodHound, Python, PowerShell, and Bash. Maps identity attack paths, reviews authentication and authorization, tests LLM-enabled applications, and supports red team and purple team exercises with SIEM telemetry. Produces clear test plans, technical reports, executive readouts, **proof-of-exploit** evidence, remediation workshops, and retest memoranda. OSCP-certified with practical PTES, OWASP, SANS, Azure, Microsoft 365, Git, Splunk, Sentinel, and responsible AI-assisted development experience. Ready to help Northstar Cyber Advisory deliver safe, credible assessments that give clients clear actions and lasting risk reduction.

EXPERIENCE

Lead Penetration Tester

Redwood Security Partners September 2024 - Present Denver, CO

Leads concurrent consulting assessments across networks, applications, identity, cloud, Microsoft 365, wireless environments, and LLM features. Owns scope, technical execution, client communication, reporting, remediation validation, and shared tooling delivery.

- Aligned assessment objectives and rules of engagement with client risk before authorized testing began.
- Validated high-risk findings through Nmap, Nessus, **Burp Suite**, Metasploit, and manual exploit verification.
- Mapped Active Directory attack paths with BloodHound, linking permissions and Group Policy weaknesses to owners.
- Presented **executive readouts** with proof-of-exploit evidence, **risk ratings**, and prioritized remediation sequencing.
- Reviewed LLM features for **prompt injection**, data exposure, output handling, and tool-calling abuse.
- Validated Splunk and Microsoft Sentinel detections during red team and **purple team** exercises.
- Maintained Git repositories, **pull requests**, code reviews, GitHub Actions, and sanitized AI-assisted utilities.

Senior Security Consultant

Cobalt Ridge Consulting June 2022 - August 2024 Salt Lake City, UT

Delivered independent and team-based security assessments for enterprise and mid-market clients. Managed authenticated access, workpapers, technical findings, executive communication, remediation workshops, and retesting across application, identity, cloud, and network engagements.

- Delivered scoped network, web, API, **Microsoft 365**, and internal assessments for enterprise clients.
- Tuned Nessus and Nmap discovery, then verified findings manually through Burp Suite and **Metasploit**.
- Tested authentication, sessions, authorization, injection, deserialization, **business logic**, OAuth, SAML, and **OpenID Connect**.
- Explained BloodHound attack paths involving DNS, permissions, Kerberos, NTLM, escalation, and lateral movement.
- Coordinated least-privilege credentials, **secret handling**, **access removal**, and complete engagement workpapers.
- Produced Word, Excel, and PowerPoint reports that guided remediation workshops and retest decisions.
- Supported phishing, vishing, SIEM triage, and purple team validation using PTES, OWASP, and SANS.

Cybersecurity Assessment Intern

University Cyber Defense Lab January 2022 - May 2022 Boulder, CO

Supported supervised assessment work in isolated Windows, Linux, web, API, and Active Directory labs. Built controlled test cases, automation scripts, evidence packages, detection reviews, and concise presentations for faculty and student SOC audiences.

- Executed supervised **reconnaissance** and vulnerability assessments with **Kali Linux**, Nmap, Nessus, and Burp Suite.
- Recorded **authentication**, access-control, **injection**, and session findings through reproducible controlled workpapers.
- Visualized lab Active Directory attack paths with **BloodHound** and validated approved escalation scenarios.
- Wrote Python, PowerShell, and Bash utilities for scan preparation and **evidence** organization.
- Matched simulated attacker actions with Splunk alerts during a supervised purple team exercise.
- Presented assessment findings, business risk, remediation priorities, and retesting criteria to faculty reviewers.

PROJECTS

LLM Application Security Test Harness 2025

Built structured prompt tests and API-driven cases for prompt injection, sensitive data exposure, insecure output handling, and tool-calling abuse. Work reflects a belief that safer technology gives clients confidence to innovate responsibly.

Purple Team Detection Validation Range 2023

Created an isolated range linking attacker behaviors with Splunk telemetry, alert triage, and threat-hunting scenarios. Clear evidence helped student defenders connect security work with people who depend on reliable services.

LEADERSHIP & AWARDS

- Cyber Defense Showcase Best Assessment Report, University of Colorado Denver, 2022
- Regional Collegiate Purple Team Challenge, Second Place, 2021
- Cybersecurity Scholarship Recipient, University of Colorado Denver, 2020 - 2022
- Dean's List, University of Colorado Denver, 2021

EDUCATION

Bachelor's Degree in Cybersecurity

University of Colorado Denver GPA: 3.8 2022 Denver, CO

Coursework: *Network security, ethical hacking, digital forensics, secure software development*

CERTIFICATIONS

- OSCP 2024
- CompTIA PenTest+ 2023
- AWS Certified Cloud Practitioner 2025
- Microsoft Certified: Security, Compliance, and Identity Fundamentals 2023

TECHNICAL SKILLS

- **Offensive Security Tools:** Kali Linux, Burp Suite, Metasploit, Nmap
- **Vulnerability Assessment:** Nessus, Tenable, scan tuning, manual verification
- **Active Directory:** BloodHound, Group Policy, Kerberos, NTLM
- **Web and API Security:** Authentication, session management, injection, deserialization
- **Identity Protocols:** SAML, OAuth 2.0, OpenID Connect, DNS
- **Cloud and Microsoft:** Microsoft Azure, Microsoft 365, cloud identity, security services
- **Scripting Languages:** Python, PowerShell, Bash, automation
- **SIEM Platforms:** Splunk, Microsoft Sentinel, alert triage, log investigation
- **Source Control:** Git, GitHub, branching, pull requests
- **DevOps Tools:** GitHub Actions, Azure DevOps, Docker
- **Security Frameworks:** PTES, OWASP, SANS, OWASP Top 10 for LLM Applications
- **Office Applications:** Microsoft Word, Microsoft Excel, Microsoft PowerPoint
- **AI Security Testing:** Prompt injection, abuse-case libraries, API test harnesses
- **Social Engineering:** Phishing, vishing, baiting, tailgating
- **Professional Deliverables:** Test plans, technical reports, executive summaries, retest memoranda

SKILLS

- Penetration Testing
- Network Security
- Web Application Testing
- API Security
- Active Directory
- Cloud Security
- Microsoft 365
- Red Team Operations
- Purple Team Operations
- Vulnerability Assessment
- Risk Reporting
- Threat Hunting
- Security Testing
- Client Presentations
- Remediation Validation

PROFESSIONAL AFFILIATIONS

- Colorado Cybersecurity Student Association, Assessment Workshop Coordinator, 2021 - 2022
- University Cyber Defense Lab, Peer Mentor, 2021 - 2022
- Collegiate Cyber Defense Competition Team, Blue Team Analyst, 2020 - 2022

LANGUAGES

- English (Native)
- Spanish (Intermediate)

ADDITIONAL INFORMATION

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

REFERENCES

AVAILABLE ON REQUEST