Jenn Shagrin

Independent Security Researcher

Albuquerque, NM | jennshagrin@proton.me

linkedin.com/in/jenn-shagrin | github.com/jennshaggy | **Portfolio:** jennshaggy.github.io

Focus

I work in offensive security: penetration testing, independent vulnerability research, and AI security. I test systems, follow attack paths, reverse binaries, build security tools, analyze forensic evidence, write detections, and thoroughly enjoy what I do.

Selected Research

Independent Security Researcher | 2026-Present
Independent | Authorized Coordinated Disclosure

Privileged Credential Exposure Through an Authorization Chain
Intigriti submission | 2026

- Identified an authorization-chain flaw that let a read-only administrative account export hidden privileged-account authentication material and retrieve the root-owned export over FTPS.
- Verified each stage through role comparison, Argon2id format analysis, permission review, controlled retrieval, and matching SHA-256 hashes.
- Submitted one high-severity report to the program; a second report documenting the complete chain is saved in Intigriti pending triage of the first.

Active Directory Attack-Chain Portfolio
Kerberos | AD CS | BloodHound

- Executed and documented Kerberoasting, BloodHound path analysis, targetedKerberoast.py, remote execution, and ESC1 certificate abuse across Operation Endgame and Ledger.

Cyber Apocalypse 2026 Portfolio
Web Exploitation | Reverse Engineering | AI/ML Security

- Recovered a custom four-byte VM from a stripped ARM64 binary, then wrote a Python disassembler, emulator, and inverse solver that reproduced the accepted input through forward execution.
- Chained web, service, and model flaws across Signetry, Archonyx, and Assay, including stored client-side execution, unsafe ZIP extraction, Java deserialization, race-condition abuse, model extraction, evasion, and backdoor recovery.

Hayabusa MCP and CyberStrike Harness
Python | MCP | EVTX | Fedora Linux

- Shipped a security-hardened Hayabusa MCP server and evidence-controlled agentic security harness; verified genuine MCP orchestration, passed 312 tests and Ruff checks, and completed reproducible forensic analysis with evidence provenance.

Technical Range

Offensive security: Web application and API testing, Active Directory attack paths, privilege escalation, reverse engineering, LLM red-teaming, OSINT, post-exploitation, and technical reporting

Tools and development: Python, Go, Bash, Java, Burp Suite, BloodHound, Impacket, Nessus, Ghidra, Wireshark, Hayabusa, Git, GitHub Actions, Ruff, and pytest

Detection and analysis: Sysmon, Windows EVTX, Splunk, Elastic, packet analysis, malware triage, DFIR, cloud audit logs, identity-focused investigation, and detection engineering

Platforms and frameworks: Windows, Linux, Active Directory, Proxmox, AWS, Azure, Microsoft 365, MCP, MITRE ATT&CK, MITRE ATLAS, OWASP Top 10, and OWASP LLM Top 10

Security Tooling

organAIzedcrime
Go | AI/ML Security | MITRE ATLAS

Built a Go CLI mapping adversarial AI techniques, tools, and validated payloads to MITRE ATLAS, with HTTP and Ollama execution modes plus cross-platform releases.

aismon
Python | Sysmon | Detection Engineering

- Built a Python detector for AI-related Windows Sysmon Event ID 1 activity using 35 YAML rules, secure XML parsing, API-key redaction, schema validation, false-positive coverage, and 69 passing tests.

Professional Foundation

Head of IT / System Administration | 2022-2024
Invasion Group & Righteous Babe Records

- Managed and hardened multi-site infrastructure across web platforms, endpoints, identity and access, payroll, content delivery, vendors, and user support.

Independent Technology Consulting | 2005-Present
Selected Engagements

- Supported business technology for 20+ years across devices, accounts, hosting, DNS and firewalls, backups, Google Workspace, Microsoft 365, and mixed-network troubleshooting.

Online Booking Department Developer and Administrator | Feb 2009-Jan 2011
Starving Students

- Developed and administered the company's first online chat and booking platform, then managed a five-person online leads department covering workflow standards, lead routing, and daily operations.

Community

Vice President, Cybersecurity Club | 2026-Present
California Institute of Applied Technology

- Co-founded the weekly Beginners CTF and co-led sessions with a CEH instructor, advising participants through challenges including TryHackMe's ContAInment AI-security room.

Co-Founder | 2021-Present
Crumpled Thoughts, 501(c)(3)

- Provide technology and operational oversight for literacy, technology education, cybersecurity, and digital-safety programs in New Mexico and Virginia.

Credentials

TCM Security: PNPT - In Progress
CompTIA: Security+ ce, Network+ ce, and A+ ce
Additional: ISC2 CC; AWS Academy Cloud Foundations; EC-Council ADG Verified in Defend
TryHackMe: Top 1% globally | Legend | jenn_notabot

Education

A.A.S., Computer Information Systems, Cybersecurity | Summa Cum Laude | Completed Jul 2026
California Institute of Applied Technology | GPA: 4.0

Applied Bachelor's Degree, Computer Information Systems | Expected Mar 2028
California Institute of Applied Technology | Cybersecurity Concentration | Begins Sep 2026