Jon “GainSec” Gaines

E: jobs@gainsecmail.com **L:** linktr.ee/gainsec **S:** linkedin.com/in/gainsec
G: github.com/gainsec **W:** gainsec.com

Champlain College - B.S. Computer Networking & Cybersecurity

Summary

Offensive security leader, operator, and researcher with over a decade across but not limited to web, mobile, thick client, IoT/embedded, cloud-integrated, and AI-integrated applications. Discovered 50(+ >10 Pending) CVEs spanning ICS/OT, mobile, firmware, Windows, and web. Built and scaled new service lines, led teams, and delivered research, talks, and open-source tooling.

Highlights

- **50 CVEs disclosed** (48 Independently); advisories, coordinated disclosures, deep dive write-ups, formal white papers
- **Team lead** for 8+ consultants; multiple promotions driven through formal mentorship
- **Drove new service lines** at two firms contributing to revenue growth and acquisition outcomes
- **Publications** in Phrack and Unredacted; cited in technical articles; speaker (DEFCON Paris, Cybeer, ANYCON)
- **Creator/maintainer** of exploitation, automation, and assessment tools; contributor to SecLists and Evil M5Stack

Work Experience

Herkimer College – Adjunct Instructor (*Jan 2026 – Present*)

- Teach the Introduction to Information Security Mgmt class

GainSec - Founder (*Jun 2019 – Present*)

- White Label offensive security services
- A la carte offensive security services
- Independent security research (48 CVEs responsibly disclosed spanning web, mobile, IoT/embedded, and software)
- Open-source development & contributions
- Published technical research (*Phrack, Unredacted Magazine)*
- Regular self-published technical and leadership insights,
- Lecture at international industry events

Contrast Security – Principal Security Researcher (*Oct 2025 – November 2025*)

- Conduct advanced research in application security, driving innovation and improvements in runtime protection technologies.
- Design and execute both basic and applied research projects independently and collaboratively within the security research team.
- Partner with product teams and customers to identify emerging research opportunities and security challenges.
- Integrate LLM driven tools to enhance research automation, report generation, and exploit surface mapping across multiple languages and frameworks.
- Drive AI integration into application security workflows, leveraging machine learning for vulnerability detection, exploit pattern recognition, and threat intelligence correlation.
- Lead efforts in collecting and analyzing data on programming languages, libraries, licenses, and application security trends.
- Assess and validate newly disclosed vulnerabilities (CVEs) and external threat intelligence to determine product impact.
- Author and presented original security research through technical blogs, conference talks, and internal knowledge-sharing sessions.
- Deliver tier-3 incident response and deep-dive analysis for escalated security reports and vulnerabilities.
- Mentor junior researchers and engineers, providing guidance in security research methodologies and exploit development.

NetSPI - Managing Security Consultant (*Dec 2022 – Oct 2025*)

- Led 8+ consultants (Consultant 1 → Principal): operating procedures, technical cadences, 1:1s, performance reviews, utilization tracking, promotions, and continuous training
- Owned delivery for web, mobile, and thick client testing; expand coverage to IoT, cloud-integrated, AI-integrated apps, and source reviews; handle bespoke, non-standard engagements

- Authored methodology updates and drafted the career roadmap adopted org-wide for performance reviews and role definitions (final ownership with Sr. Manager, with limited additions beyond my draft); created managing-consultant training and executed it to the promotion of new MCs.
- Bridged consulting, engineering, leadership, and sales to align security strategy, unblock delivery, and support service-line and operational expansion; assist on presales and client calls

nVisium (Acquired by NetSPI) - Senior Security Consultant (*Jul 2021 – Dec 2022*)

- Launched new service lines: Red Team, External PT, Phishing; wrote methodologies, SOPs, deliverables; mentored cross-training; executed engagements end-to-end
- Supported sales in scoping and solutioning; expansion of existing accounts and net-new wins contributed to revenue growth culminating in acquisition by NetSPI
- Delivered core web/mobile/thick client testing and source code reviews

Stratum Security - Security Consultant - Senior Security Consultant (*Jun 2018 – Jul 2021*)

- Co-spearheaded new offerings: Phishing, Red Team, External/Internal PT, Thick Client, Host-based testing; defined methodology and delivered initial engagements
- Grew existing client partnerships >10% and added >5 new clients
- Executed web/mobile app testing and select red team/phishing ops; scaled methodologies for repeatable delivery

Leet Cyber Security - Security Consultant (3rd Employee) (*Jun 2016 – Jun 2018*)

- Delivered engagements across nearly every offensive service line (external/internal, web/mobile/thick client, phishing/vishing, social engineering, physical, red team, source review, cloud, architecture, more).
- Created new methodologies, onboarding program, and cross-training guidelines, enabling others to scale delivery.
- Contributions directly tied to $1M revenue growth goal attainment.
- Managed internship program and mentored consultants.

Herkimer College - Independent Consultant (*Aug 2015 – May 2016*)

- Contributed to cyber security curriculum redesign
- Created CTF driven lab
- Contributed to academic grant application