Versailles, FR
Gainsec.com
poste@gainsecmail.com

JONATHAN “GAINSEC” GAINES

PROFILE

Offensive security researcher with 10+ years of experience in vulnerability discovery, exploit development, and reverse engineering. Author of 42 CVEs (40 independently discovered), Published in Phrack and Unredacted, and frequent speaker at industry events. Skilled across web, mobile, thick client/software, ICS/OT, IoT/embedded, external network, AI integrated, and cloud-integrated systems. Active maintainer of open-source tools and contributor to industry standard projects.

Condensed CV. Full CV, CVE list, and publications: [https:// gainsec.com/mentions-quotes] | [https://gainsec.com/wp-content/uploads/2025/09/GainesJon-CV.pdf]

SKILLS

- **Vulnerability Research** (CVE discovery, exploit development)
- **Reverse Engineering** (firmware, binaries, embedded)
- **Offensive Security** (Penetration testing, red teaming, social engineering)
- **Tooling & Automation** (Burp Suite plugins, wordlist frameworks, custom firmware)
- **Publications & Knowledge Sharing** (Phrack, open-source contributions, multitude of self-published technical articles)

CVE PORTFOLIO

- **42 total CVEs, 40 independently discovered** (2017-2025)
- *Selected Highlights:*
- Tridium Niagara AX/4 (ICS/OT) – Path Traversal, Improper Authentication (2017)
- Mealie (Web App) – RCE, SQLi, XSS (2022)
- Flock Safety Multiple Devices (IoT/Embedded) – multiple firmware & physical security flaws, Wireless RCE (2025)
- Kapsch TrafficCom AG RSUs (IoT/Embedded) – multiple critical access control bypasses (2025)
- *Full detailed list available in appendix A in full CV - [https://gainsec.com/wp-content/uploads/2025/09/GainesJon-CV.pdf*

EXPERIENCE

MANAGING SECURITY CONSULTANT, NETSPI, 3 YEARS

- Led and mentored consultants while conducting assessments across various service lines.
- Authored methodologies for advanced testing, including reverse engineering and bespoke assessments.
- Maintained hands-on technical role while supporting research initiatives.

SENIOR SECURITY CONSULTANT, NVISIUM, 1 YEAR

- Created methodologies and tooling for Red Team, phishing, and external PT services.
- Discovered vulnerabilities and developed PoCs for client and independent research.
- Delivered offensive security engagements across various service lines
- Expansions contributed to acquisition by NetSPI

SECURITY CONSULTANT - SENIOR SECURITY CONSULTANT, STRATUM SECURITY, 3 YEARS

- Delivered offensive engagements across nearly all service lines with a core focus on web app, mobile and thick clients.
- Co-spearheaded multiple service line expansion.
- Grew existing client partnerships >10%

SECURITY CONSULTANT, LEET CYBER SECURITY, 2 YEARS

- 3rd Employee
- Delivered engagements across nearly every offensive service line
- 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

INDEPENDENT CONSULTANT, HERKIMER COLLEGE, 1 YEAR

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

EDUCATION

CHAMPLAIN COLLEGE – BACHELOR OF SCIENCE – NETWORKING & CYBERSECURITY

HERKIMER COLLEGE – ASSOCIATE OF SCIENCE – CRIMINAL JUSTICE: CYBERSECURITY

PUBLICATIONS

- Phrack – *Roadside to Everyone*, Issue #72, 2025. [https://phrack.org/issues/72/16_md]
- Unredacted Magazine – *10 Minutes of Google Dorking for COVID Documents*, Issue #5, 2023. [https://inteltechniques.com/issues/005.pdf]

Full publication, talk history, and media engaement available at [https://gainsec.com/mentions-quotes/

TALKS

- *Hold my Redbull; Undergraduate Red Teaming* ANYCON, 2017. [https://www.youtube.com/watch?v=9vgpqRzuvLk]
- *TL;DR The Silk Road & Ulbricht vs. U.S. CyBeer*, 2018. [https://www.youtube.com/watch?v=0C0kZC25XaY]
- *OSINT Escapades,* Private Organization Event, 2021.
- *Cheap 'n' Easy Phishing That Actually work; How I compromised a trillion-dollar organization for under $150*, DefCon Paris, 2023. [https://www.youtube.com/watch?v=Ed10qIBFYnE]
- *Academic Degrees vs Certifications vs CVEs vs Experience*, DefCon Paris 2023. [https://defconparis.org/index.php/2023/03/26/2023-apr-24/

MEDIA ENGAGEMENT

- Quoted and cited as a subject-matter expert in international outlets including: The Register, Bleeping Computer, Security Week, The Mirror, TechTarget, Info Security Magazine, Security Boulevard, and others.

- Referenced in vendor advisories and press releases (e.g. Kapsch TrafficCom AG, Flock Safety, Tridium Niagara)
- Incorporated into official databases and advisories (NVD, CISA ICS, GitHub advisories).

PODCAST APPEARANCES

- Guest on Security Weekly – Interview Episode, 2017.
- InfoSec Chat with InfoSec Pat (Recurring Guest), 2020 – 2025.
- Guest on Swiping Sunday, 2020.

SAMPLE EMPLOYER PUBLISHED

- Stratum Security – PoC for CVE-2017-16744 and CVE-2017-16748, 2018. [https://blog.stratumsecurity.com/2018/09/06/cve-2017-16744-and-cve-2017-16748/]
- nVisium – A Step-By-Step Guide to Uncovering Data Leaks, 2022 [https://web.archive.org/web/20220807212720/https://blog.nvisium.com/how-to-find-a-data-leak-in-50-easy-steps]

SAMPLE SELF-PUBLISHED

- M5NanoC6 Zigbee Sniffer — Authored novel technical instructions and custom firmware to capture Zigbee traffic using the M5NanoC6 platform, 2024. [https://gainsec.com/2024/08/13/m5nanoc6-zigbee-sniffer/]
- Reverse Engineering the MISIRUN Instant Print Camera, 2025 – Technical walkthrough of how I reverse engineering a camera and modified the boot image. [https://gainsec.com/2025/04/01/reverse-engineering-kids-instaprint-camera/]
- Sniffing V2X/DSRC with a LibreSDR B210/B220 AD9361 on Linux – In-depth guide to configuration a LibreSDR with GNURadio on Linux for sniffing V2X or DSRC traffic. Includes step-by-step installation, Wireshark integration and pcap validation, 2025. [https://gainsec.com/2025/01/25/sniffing-v2x-dsrc-with-libresdr-b210-b220-ad9361-on-linux/]
- Using Nexus 6P and QCSuper to Sniff LTE, 2025. Technical guidance on setting up and using QCSuper to sniff LTE traffic. [https://gainsec.com/2025/05/28/using-a-nexus-6p-and-qcsuper-to-sniff-lte/]
- Quick & Simple Guide to a Local AI Stack - Multipart series covering how to set up and run a powerful local AI stack, 2025. [https://gainsec.com/2025/06/01/the-quickest-and-simplest-guide-to-spinning-up-a-powerful-local-ai-stack-part-1/]

SELECTED OPEN-SOURCE PROJECTS

- Creator, GoldenNuggets - (Burp Suite extension – 211 stars) [https://github.com/GainSec/GoldenNuggets-1]
- Creator, TreeHouse Wordlists - (custom wordlists for pen testing) [https://github.com/GainSec/TreeHouse-Wordlists]
- Creator, GainSec in the Middle - (custom MITM router/AP setup for IoT/embedded testing) [https://github.com/GainSec/gainsec-in-the-middle]
- Creator, RTLOify – (Script to create strings, change filenames or entire directories containing RTLO override bypasses and fuzzing) – [https://github.com/GainSec/RTLOify]
- Creator, Mac OSX Application Fingerprint and Security Tool – (Script to automate some checks performed during MacOS app or iOS mobile pen tests.) [https://github.com/GainSec/Mac-OSX-Application-Fingerprint-And-Security-Tool]
- Contributor: SecLists, Evil M5Stack