

JAY LALKIYA

Cyber Security Trainee

Ahmedabad, Gujarat, India — +91 8200411490 — jaylalkiya02@gmail.com
linkedin.com/in/jay-lalkiya — github.com/jaylalkiya — jaylalkiyaportfolio.vercel.app

SUMMARY

BCA graduate (84.09%) currently 300+ hours into an NSQF Level 4 cyber security program, looking for an entry-level SOC or security analyst role. Outside coursework I build my own security tools in Python — recon automation, a MITRE ATT&CK-mapped honeypot, an authorized load-testing console, a wireless intrusion monitor, and a steganography / steganalysis tool. Comfortable in Linux/Kali, Wireshark, Nmap and TryHackMe labs.

TECHNICAL SKILLS

Security: Network security, wireless security, threat detection, detection engineering, MITRE ATT&CK mapping, packet analysis, alert triage, incident response fundamentals, vulnerability scanning, access control, web application security, applied cryptography, VAPT (vulnerability assessment and penetration testing)

Tools: Wireshark, Nmap, Nuclei, Nikto, TryHackMe, Kali Linux, Windows netsh, WLAN API, Git, GitHub, VS Code

Programming: Python, Java, JavaScript, SQL

Networking and Systems: TCP/IP, DNS, DHCP, 802.11 beacons and BSSIDs, firewalls, Windows, Linux

PROJECTS

Recon-Raptor – Automated Recon Pipeline (Python, Bash) — github.com/jaylalkiya/Recon-Raptor

- Chained nmap, nuclei, nikto and directory brute-forcing into one run with a Tkinter GUI, rolling results into a severity-ranked HTML/JSON report.
- Built to run unattended on a Kali box — missing tools are skipped gracefully so a scan never hard-fails.

GullakTrap – Multi-Protocol Honeypot (Python, Flask) — github.com/jaylalkiya/GullakTrap

- Stood up 7 fake services (HTTP, FTP, SSH, Telnet, SMB, SMTP, SNMP) and auto-tagged every captured event with a MITRE ATT&CK technique and severity score.
- Shipped a red-team attack simulator so the full detection pipeline — honeypot to dashboard — can be proven end-to-end without waiting for a real intruder.

ScopeStorm – Authorized Load & Resilience Console (Python) — github.com/jaylalkiya/ScopeStorm

- Built scope locking, a hash-chained tamper-evident audit log and an auto-abort safety threshold so a load test can't exceed its authorized Rules of Engagement.
- Added deconfliction markers on every request so a blue team can tell the test apart from a real attack.

Wifi-Sentry – Rogue Access Point Monitor (Python) — github.com/jaylalkiya/Wifi-Sentry

- Wrote 7 detection rules — evil twins, open-network downgrades, KARMA responders, SSID bursts — and mapped each one to MITRE ATT&CK.
- Reads beacon data via Windows netsh/WLAN API with no monitor-mode adapter needed; alerts export as JSONL for SIEM ingestion, validated with 99 unit tests against saved packet captures.

Other projects: StegoVault – AES-256-GCM steganography with an RS-Analysis steganalysis detector (Python, NumPy); CodeShelf – Java/JSP/MySQL web app with role-based access control. Both on GitHub.

EXPERIENCE

Developer Intern – TechRover Solutions (Dec 2025 – Jan 2026)

- Built REST APIs for authentication, sessions and CRUD operations on a React.js/Node.js/PostgreSQL ticket-booking system.
- Designed the PostgreSQL schema and integrated the frontend and backend modules end-to-end.

TRAINING AND CERTIFICATIONS

Cyber Security Program, NSQF Level 4 – Adani Skill Development Centre, Ahmedabad (2026 – Present, 300+ hours, in progress)

Covered so far: networking and TCP/IP, Linux basics, firewalls and access control, web application security basics. Still to come: threat mitigation, audit and compliance, SOC monitoring and escalation, VAPT.

React JS / Node JS Training – TechRover Solutions (Dec 2025 – Jan 2026, 120 hours)

EDUCATION

Bachelor of Computer Applications (Honours) – Dr. V. R. Godhaniya IT College, Porbandar

Bhakta Kavi Narsinh Mehta University (2023 – 2026) — CGPA: 8.48, 84.09%

ADDITIONAL INFORMATION

Languages: English, Hindi, Gujarati — **Availability:** Immediate, open to relocation or remote