

# SAI PRANEETH

praneeth2006.dev@gmail.com | Vellore, India | [ping-praneeth.vercel.app](https://ping-praneeth.vercel.app) | [github.com/praneeth132006](https://github.com/praneeth132006) | [linkedin.com/in/praneeth132006](https://linkedin.com/in/praneeth132006) | [tryhackme.com/p/cyberbee132006](https://tryhackme.com/p/cyberbee132006)

## SUMMARY

Cybersecurity-focused B.Tech CSE (Cyber Security) student at VIT Vellore and open-source maintainer of RedBlueSkills, a 128-skill agent-native security library spanning 7 application surfaces, with 64 offensive techniques each paired one-to-one with a detection counterpart and 70 MITRE ATT&CK techniques mapped under CI-enforced quality gates. Also builds ForkLeaf, a local-first Markdown workspace, plus standalone security tooling: an eBPF-based Linux threat detector and an AI/LLM security gateway. Ranked top 5% on TryHackMe (Level 9, 108 rooms, 184-day streak). Seeking a security internship in SOC operations, VAPT, or detection engineering.

## EDUCATION

### B.Tech, Computer Science & Engineering — Cyber Security

Vellore, India

Vellore Institute of Technology (VIT Vellore), 2024 – 2028

CGPA: 8.48 (as of 4th semester)

Relevant coursework: Python, Object-Oriented Programming, Data Structures & Algorithms, Computer Networks, Network Security

## FLAGSHIP OPEN-SOURCE PROJECTS

### [RedBlueSkills — Creator & Maintainer](#)

Open-source agent-native security skill library, Apache-2.0 license

- Built and shipped 128 executable security skill packages (SKILL.md format) across 7 application surfaces (web app, API, mobile, network, cloud-native, CI/CD, LLM/AI), loadable by AI agents (Claude Code) or human operators for recon, exploitation, detection engineering, hardening, and incident response.
- Engineered a paired red-blue architecture covering 64 offensive techniques matched one-to-one with 64 detection and hardening counterparts, mapped to 70 MITRE ATT&CK techniques, with CI enforcing bidirectional pairing on every pull request.
- Automated quality gates in GitHub Actions (schema validation, a catalog generator, CodeQL static analysis) so every contribution is verified before merge; published counts are generated from catalog.json so CI fails if they drift, and skills are auto-flagged stale after 6 months of no revalidation.
- Validated every skill against a real lab or CTF target, stamping each with a named validator and date to keep claims provenance-backed rather than theoretical.

Stack: Python, GitHub Actions, CodeQL, MITRE ATT&CK, Claude Agent Skills, Apache-2.0

### [ForkLeaf — Local-First Markdown Workspace](#)

Open-source note-taking workspace, Apache-2.0 license

- Built a local-first Markdown workspace that stores notes as plain .md files in a GitHub repository the user already owns — wikilinks, backlinks, full-text search, a visual Mermaid diagram studio, and six export formats, all running client-side with no proprietary database to be locked into.

Stack: TypeScript, React, Turborepo, IndexedDB, GitHub API, Mermaid, Vitest, Apache-2.0

## SECURITY PROJECTS

### [KrnlSentry — eBPF Threat Detection for Linux](#)

- Built real-time Linux syscall monitoring with eBPF programs on syscall tracepoints, streaming events to user-space rules that flag privilege escalation, credential theft, process injection, and reverse shells (each alert tagged with its MITRE ATT&CK technique); ships as a single static binary via libbpf + CO-RE with nothing pre-installed on the target host.

Stack: Go, eBPF, libbpf+CO-RE, cilium/ebpf, MITRE ATT&CK, Linux internals

### [VectorShield — AI Security Gateway](#)

- Built a gateway that sits between an application and its LLM, screening every prompt and response against the OWASP LLM Top 10 (prompt injection, model denial-of-service, outbound PII/secret leakage), with a multi-tenant policy engine and a hashed-by-default audit log for compliance-safe logging.

Stack: Python, FastAPI, OWASP LLM Top 10, OpenAI/Ollama, SQLite/PostgreSQL

### [Network Traffic Analysis — Wireshark to Google Maps](#)

- Built a Python pipeline that parses raw Wireshark packet captures (.pcap) with dpkt and geolocates every source IP against the GeoLiteCity database, delivering a KML layer for Google My Maps and an interactive HTML triage dashboard.

Stack: Python 3, Wireshark, dpkt, pygeoip, simplekml

## OTHER PROJECTS

APPSC, a live exam-prep platform for APPSC aspirants (Next.js, UI/UX).

## TECHNICAL SKILLS

Offensive Security: Nmap, Burp Suite, Metasploit, Impacket, NetExec/CrackMapExec, Hydra, Gobuster, privilege escalation

OSINT & Reconnaissance: Google dorking, breach-data/username OSINT, WHOIS/DNS/subdomain recon, Maltego, theHarvester, Shodan

Defensive Security: Detection engineering, eBPF syscall monitoring, log analysis, ATT&CK mapping, incident response, system hardening, threat hunting

Network & Traffic Analysis: Wireshark, tcpdump, dpkt, pygeoip, TCP/IP, DNS, packet forensics

AI & LLM Security: OWASP LLM Top 10, prompt injection & jailbreaks, canary tokens, PII/secret egress scanning, model DoS/rate limiting

Security Engineering: GitHub Actions, CodeQL, schema validation, CI/CD, build provenance/SLSA, Apache-2.0 licensing, Git

Programming & Frameworks: Python, Go, JavaScript, TypeScript, React, Next.js, Node.js, C/C++ | Platform & Cloud: Linux, Kali Linux, AWS, Docker, Firebase, Vercel, Bash

## CERTIFICATIONS

- Open-Source Intelligence (OSINT) Fundamentals — TCM Security, August 2026; CompTIA Security+ (SY0-701) — Udemy, June 2025
- CompTIA Network+ (N10-009) — 30-hr exam-prep track, Udemy, May 2025
- Introduction to Cybersecurity — Cisco Networking Academy, July 2025; Deloitte Australia Cyber Job Simulation (Forage), June 2025
- AWS Cloud Practitioner & AWS Academy Graduate (Generative AI Foundations) — AWS Skill Builder, August 2026
- TryHackMe — Certificate of Completion, Level 9 (MAGE), 184-day streak, top 5% global rank