

Likith Aswathanarayana

likith3@proton.me — +91 80734 37235 — linkedin.com/in/likith3 — github.com/bytesbylikith

Profile

Cybersecurity practitioner and CTF competitor with hands-on experience in offensive security, digital forensics, and reverse engineering. Built and deployed lab environments and CLI tools used in training; consistently deliver measurable results (Top 1% on CTFtime). Seeking an entry-level role to apply exploitation, analysis, and automated tooling skills in a security team.

Skills

- **Penetration Testing & Exploitation:** Metasploit; Hydra-style brute force; SQLi, XSS, IDOR, SSRF, file upload testing (10+ practice labs).
- **Network Analysis:** Wireshark — capture, protocol analysis, filtering; analyzed 1000+ captured packets.
- **Forensics & Stego:** Steghide, zsteg, stegsolve, file carving, metadata analysis; authored 5+ challenge tasks.
- **Reverse Engineering:** Ghidra, objdump, strings.
- **Scripting & Automation:** Python, Bash, basic C.
- **Platforms:** Kali Linux, VirtualBox (Metasploitable & custom VMs), HackTheBox, Try-HackMe, CTFtime.

Experience

Triada CTF Apr 2023 – Present
Team Member & CTF Player

- Achieved **Top 1% ranking on CTFtime** (34 / 6000+ Indian teams, 2025) through consistent performance in national-level competitions.
- Directed and facilitated **3 beginner-focused CTF workshops**, mentoring 50+ participants and simplifying complex security concepts.
- **Authored 10+ CTF challenges** (stego, forensics, reverse engineering) used for team practice and training.
- Built **automation scripts in Python/Bash** to streamline exploitation workflows and analysis tasks.
- Produced **writeups and walkthroughs** shared with 200+ security learners, improving community knowledge.

Technical Projects

- **SmartBruteRL:** Built a CLI brute-force tool (Hydra-inspired) enhanced with reinforcement learning; validated on SSH, FTP, Telnet, and 3 web applications in lab setups.
- **Snapper (MITM Tool):** Developed a CLI utility for ARP spoofing, packet sniffing, and traffic manipulation; demonstrated in 5+ controlled lab environments.
- **Web Pentesting Playground:** Deployed a vulnerable web application with 3 user roles and 10+ challenge modules to practice SQLi, XSS, IDOR, SSRF, and file uploads.
- **TRIADA Labs (CTF Platform):** Designed and implemented a full-featured CTF platform (React/Node.js/MySQL) hosting 50+ challenges and supporting 200+ active users.

Education

Yenepoya Deemed to be University

2023 – 2026

BCA — Cyber Security, Ethical Hacking & Digital Forensics

Certifications

- Google Cybersecurity Professional Certificate (Coursera)
- Wireshark Guided Project (Coursera)
- Metasploit Guided Project (Coursera)

Achievements

- Runners-Up — **Seaside Threat Hunting Village CTF**.
- Consistently ranked in the **Top 5% across national CTFs**, demonstrating practical exploitation and analysis skills.

Interests & Hobbies

- **Teaching & Collaboration:** Delivered 10+ security demos and labs; coordinated multi-team challenge builds.
- **Personal:** Tabla (5+ years), reverse engineering, CTF challenge design.