PRATEEK PUROHIT

+91-8280938043 prateekpurohit171@gmail.com linkedin github leetcode

SUMMARY

Cybersecurity-focused developer experienced in **network threat detection**, **API security**, and **post-quantum cryptography**. Built systems spanning **traffic fingerprinting**, and **kernel-level (eBPF) observability**, mapped to **OWASP** and **MITRE** frameworks for real-world adversary defense.

EDUCATION

Vellore Institute of Technology, Vellore **August 2023 – June 2027**
B.Tech in Computer Science and Engineering (Specialization in Information Security) *CGPA 9.03*

SKILLS

Programming Languages: Golang, Python, Java, C, C++
Frameworks & Libraries: Gin, FastAPI, Libsodium, OpenSSL, eBPF (BCC)
Tools & Technologies: Git, Linux, SQL, Docker, Podman, AWS, Burp, PentAgi, NGINX, Nuclei, Kafka, Kubernetes, PostgreSQL, MongoDB, Redis

EXPERIENCE

QNu Labs **March 2026 – Present**
Backend Developer Intern *Remote*

- Devised and secured high-performance **APIs** using **gRPC** and **Post-Quantum Cryptography (PQC)** primitives such as **ML-KEM** and **ML-DSA**, improving communication security against quantum threats by 95%.
- Fortified **transport layer security** by integrating hybrid key exchange (**X25519 + PQC**) and implementing **pcap-based telemetry** for real-time traffic visibility, reducing latency by **30%** while enhancing **observability** and **threat detection**.

PROJECTS

Karaxys | *Real-time API Security Platform & Agentic Security (Vanguard)* | ***Karaxys Website***

- Architected the **API Security** system using **eBPF** kernel probes for full-visibility traffic capture, feeding a Redpanda-based streaming pipeline that auto-discovers endpoints, classifies **PII**, flags shadow APIs, and redacts sensitive data before storage, backed by a Nuclei based scanner for **vulnerability assessment**.
- Developed **Vanguard**, an agentic-security layer that hooks into Claude Code, Cursor, and Gemini CLI to block destructive agent actions instantly, verifies agent behavior against kernel-level ground truth to catch **jailbreaks**, and red-teams MCP servers for **prompt injection risks**.
- Underneath, the tool leverages **per-CPU sharded ring buffers** for lock-free event capture, a **stateless scanner-worker pool** with concurrency caps and rate limiting for controlled horizontal scaling, and **dead-letter recovery** for safe retries, together enabling high-throughput, fault-tolerant scanning.
- Combined passive discovery, active testing, and agent defense into one kernel-verified platform, mapped to **OWASP API Top 10**, **OWASP Agentic Top 10**, and **MITRE ATLAS**, with a **Next.js** dashboard for scans, findings, and policy management.
- **Tech Stack:** Next.js, Tailwind, Go, MongoDB, Redpanda, Valkey, MinIO, Docker, eBPF, Nuclei

Sybil | *Real-Time Network Threat Detection & JA4 Fingerprinting Engine* | ***Github***

- Built a **network traffic analysis** tool in **Go** using dual **pcap/eBPF** capture backends to passively fingerprint TLS ClientHellos via **JA4**, classifying traffic into behavioral categories for real-time threat triage.
- Designed a weighted **anomaly-scoring model** combining resource-diversity, request velocity, and burstiness signals with **Redis**-backed rolling state, triggering progressive mitigation actions (delay, rate-limit, challenge, block) at defined risk thresholds.
- Integrated **JA4 fingerprint enrichment** via a queryable libSQL/Turso database to correlate live traffic against known client reputations, improving detection accuracy beyond raw endpoint-diversity heuristics.
- Instrumented full **observability** with **Prometheus** metrics and **Grafana** dashboards, exposing endpoints for monitoring of the detection pipeline.
- **Tech Stack:** Go, eBPF, libpcap, Redis, Prometheus, Grafana, Docker, JA4/JA4+, libSQL

Sagiri | *SSH Honeypot & Attacker Behavior Emulation Framework* | ***Github***

- Developed a **deception-based SSH honeypot** in **Go** that emulates a vulnerable Fedora Linux shell to capture and analyze unauthorized access attempts and adversary tactics in a controlled, isolated environment.
- Implemented a fake in-memory filesystem seeded with decoy credentials, SSH keys, and backups to bait and profile attacker exfiltration behavior.
- Engineered a **tarpit mode** to degrade automated brute-force tooling via deliberate byte-level response delays, increasing attacker dwell time for extended observation.
- Formulated structured, rotation-safe **audit logging** to separately capture credential-harvesting attempts and full command payloads, enabling post-incident forensic review.
- **Tech Stack:** Go, SSH (golang.org/x/crypto/ssh)

ACHIEVEMENTS

Published Patent — A System for Privacy-Preserving Collaborative Machine Learning and Method of Operation in Cloud Computing. **March 2026**
Yantra Central Hack | ***Github*** — Recognized as a Top 12 Finalist for developing an **Ethereum-based** decentralized identity system using **smart contract wallets** and **ZK-SNARKs** for gas-optimized credential verification. **February 2026**
Certifications: Cyber Security Analyst 2025 (IBM), Network Security 2024 (Google), Penetration Testing (MOOC)