Vinayak Tyagi

Jaipur, India Email: vinayaktyagi.ed@gmail.com LinkedIn: linkedin.com/in/vinayaktyagi10 GitHub: github.com/vinayaktyagi10

Summary

CS student operating a live SSH honeypot across **35,000+** real attacker sessions and maintaining production deployment infrastructure for **2,160 students**. Focused on systems security, Go, and infrastructure engineering.

Education

Manipal University Jaipur Jaipur, India
B.Tech, Computer Science & Engineering | CGPA: 8.06 *2024 – 2028*

Experience

DevOps Intern Aug 2025 – Present
Software Development Centre, MUJ *Jaipur, India*

- Identified and patched **CVE-2025-55182** (CVSS 10.0, critical — unauthenticated RCE in React Server Components) across **8 production services** within **24 hours** of disclosure; hardened all Docker images to non-root execution during the same rollout.
- Restructured Dockerfiles and authored incremental **GitHub Actions** build workflows across **45 repositories** — reduced image sizes by up to **82%** (2 GB → 358 MB) and **79%** (786 MB → 164 MB), cutting registry storage and deployment times across the CI/CD fleet.
- Deployed **Tailscale** Zero Trust mesh across Hostinger and bare-metal nodes, eliminating all public SSH exposure; enforced kernel-level resource governance via **cgroups** across the containerized production fleet to prevent resource contention across co-located services.
- Maintain deployment infrastructure for **3 production academic platforms** (NPTEL certificate verification, Elective Management System, IT ticketing) serving **2,160 CSE students** at Manipal University Jaipur across 45 repositories.
- Migrated application static data to self-hosted **MinIO** S3-compatible object storage; implemented and verified automated rsync snapshot system to bare-metal with tested **1-hour RPO** and **sub-5-minute RTO** across 7 production databases and Docker volumes.

Projects

MIRAGE | *Production SSH Honeypot & Threat Intelligence Platform* | Go • PostgreSQL • Docker • Cloudflare Live

- Deployed an internet-facing SSH honeypot capturing **35,000+ real attacker sessions**; engineered from scratch in **Go** with custom TCP listener, SSH handshake via `golang.org/x/crypto/ssh`, `PasswordCallback` credential capture, PTY handling, and a fake interactive shell with stateful directory traversal and sanitized I/O.
- Persisted sessions to **PostgreSQL** across 5 normalized tables with JSONB session documents; exposed via a secured **REST API** (Chi router, API key middleware) tunneled through **Cloudflare** with no public infrastructure exposure.
- Identified coordinated botnet behavior via **SQL CTE clustering** — 13 IPs hitting at exactly 1,522 or 761 sessions each — and Solana-validator credential targeting (`sol`, `validator`, `node`) across automated scanners; publishing findings as structured threat intelligence.
- Automated CI/CD deploy-on-push via **GitHub Actions**; daily workflow fetches live sensor stats and publishes to the project page with no API URL or key exposed client-side.
- Designed and implemented all Go infrastructure components — SSH emulator, capture pipeline, REST API, and fake shell; co-authored with one collaborator on ML classification layer (PyTorch behavioral embeddings).

GoalPost | *OKR Platform* | Next.js 14 • TypeScript • Supabase • Microsoft Entra ID *Hackathon — Solo*

- Built a full-stack OKR platform with **Microsoft Entra ID** SSO (OAuth 2.0), three-tier role-based access control (Employee / Manager / Admin), QoQ analytics dashboard, and automated email notifications via Resend — shipped solo within hackathon constraints.

Open Source

Honeynet Project | *EventHorizon* | github.com/honeynet/eventhorizon

- Added real-time attacker input capture to the **Telnet tarpit** in **C** — non-blocking `read()` after each IAC write, sanitizing non-printable bytes and emitting per-keystroke metrics via `sendMetric`.
- Extended **Go** Prometheus exporter with a `telnet_pit_input` CounterVec enabling per-session behavioral metrics; PR merged to main by Honeynet maintainers.

Technical Skills

Languages: Go, Python, Bash, TypeScript, C, Java

Frameworks & Tools: FastAPI, Next.js, Docker, Caddy, Git, GitHub Actions, Ollama, sentence-transformers

DevOps & Infrastructure: Docker Compose, Cloudflare, Tailscale, Prometheus, Grafana, MinIO, Linux

Databases: PostgreSQL, Redis, MongoDB, SQLite, Supabase