KARAN DESAI

(+91) 7284910849 | desaikaran.me@gmail.com | LinkedIn | GitHub | Portfolio

PROFESSIONAL SUMMARY

Security-focused software engineer with hands-on experience in penetration testing, embedded systems security, and application security assessments. Active contributor to Metasploit Framework with production-grade security tool development in Go, Python, and Ruby. Experienced in VAPT, OWASP Top 10, network protocol analysis, SIEM/log correlation, and threat intelligence — with a home lab built on enterprise-grade infrastructure (Proxmox, pfSense, Splunk). Seeking to apply offensive security and backend engineering skills to embedded product and cloud security testing at Vertiv.

TECHNICAL SKILLS

Security & Pentesting:	VAPT, OWASP Top 10, Metasploit Framework, Penetration Testing, Threat Modeling, SAST, API Security, CTFs, eJPT
Languages:	Go, Python, Ruby, C++, Bash, Node.js, JavaScript, SQL
Embedded & Low-Level:	Socket programming (SO_BINDTODEVICE, IP_BOUND_IF), binary analysis, Firejail isolation, Linux internals
Cloud & DevOps:	AWS, Azure, Docker, GitHub Actions, CI/CD Pipelines, GCP (familiar)
Networking:	VLANs, pfSense, TCP/IP, Layer 2/3, firewall rules, protocol analysis, Wireshark, network segmentation
SIEM & Monitoring:	Splunk, Kafka, Apache Flink, log analysis, anomaly detection, intrusion detection
Tools:	Wireshark, Nmap, Splunk, IDA Pro (familiar), BinWalk (familiar), MetaSploit, Git/GitHub/GitLab
Frameworks:	FastAPI, Flask, Express.js, REST APIs, JWT, RBAC, OAuth2
Databases:	PostgreSQL, MySQL, MongoDB, Redis
Certifications:	eJPT (eLearnSecurity, 2026) | Google Cybersecurity Professional Certificate (2024) | IBM Cloud Computing Fundamentals (2026) | Nutanix Hybrid Cloud Fundamentals (2026) | Cybersecurity: Risk & Compliance — Univ. of San Diego (2024)

PROFESSIONAL EXPERIENCE

Open Source Security Contributor — Rapid7 Metasploit Framework (rex-socket)

Remote | Jan 2026 – Present

- Shipped production Ruby code to Metasploit Framework (50,000+ GitHub stars) — one of the world's leading open-source penetration testing platforms.
- Engineered cross-platform interface socket binding (SO_BINDTODEVICE / IP_BOUND_IF / getifaddrs) across Linux, macOS, and Windows, unblocking broadcast-capable DHCP attack modules used in embedded network assessments.
- Hardened implementation with param.dup mutation guards, proxy-incompatibility checks, and SystemCallError rescue blocks; resolved 4 rounds of maintainer review with 0 regressions.
- Validated changes with a 178-test suite achieving 100% pass rate across all platforms; PR approved by core maintainer smcintyre-r7.

Co-Founder & Lead Security Engineer — Pitch (Social Networking Startup)

Remote | Jan 2025 – Jun 2025

- Secured a React Native + Node.js platform for 100+ users by enforcing JWT/RBAC authentication, API rate limiting, and OWASP Top 10 input validation — eliminating injection and broken-auth attack vectors.
- Slashed deployment cycle time by 40% via GitHub Actions CI/CD pipelines, ensuring repeatable, tamper-resistant releases on AWS and Azure.
- Reduced unauthorized access incidents to zero post-launch through layered access control and security hardening across all API endpoints.

ETL Developer Intern — Brown-Fox Consultancy

Ahmedabad, India | Jun 2023 – Aug 2023

• Automated Python-based ETL pipelines processing 10,000+ records/run, cutting weekly processing time by 25% (4 hrs → 3 hrs) and manual verification effort by 30%.

SECURITY PROJECTS

Maya: Autonomous Deception & Threat Intelligence Framework — Go · Distributed Systems · ML (2026)

• Architected a Go-based autonomous honeypot platform using parallel shadow infrastructure to trap and fingerprint post-compromise attackers across distributed nodes.

• Tagged 100% of attacker activity to MITRE ATT&CK; TTPs, enabling structured threat intelligence output for incident response and vulnerability management teams.

Rootless: Secure Sandboxed Pentesting Console — Electron · FastAPI · Go · Firejail (2025)

• Eliminated host-system compromise risk by sandboxing all pentest tool execution via Firejail process isolation and least-privilege filesystem restrictions.

• Achieved sub-100ms tool launch latency using a Go execution engine behind a FastAPI REST layer, handling 3-tier architecture (Electron UI → Python API → Go backend).

TraceProbe: Real-Time Log Analysis & Anomaly Detection — Apache Kafka · Apache Flink · Go (2025)

• Reduced simulated mean time to detect (MTTD) by 60% using a Kafka + Flink streaming pipeline with stateful anomaly detection and real-time alert rules.

• Processed 50,000+ log events/minute with consistent sub-second latency, surfacing suspicious patterns applicable to embedded and cloud product security monitoring.

Cybersecurity Home Lab — Proxmox · pfSense · VLANs · Splunk (2025)

• Stood up an enterprise-grade virtualized environment with 4+ isolated VLANs, pfSense firewall policies, and segmented attack/defense subnets on Proxmox — mirroring real embedded network topologies.

• Correlated Wireshark captures with Splunk SIEM across 10+ simulated intrusion scenarios, sharpening threat detection and incident response skills.

EDUCATION

B.Tech in Computer Science — Symbiosis Institute of Technology, Pune, India

Aug 2023 – Present

Diploma in AI & ML (GPA: 8.1/10) — LJ University, Ahmedabad, India

Jun 2020 – May 2023

LEADERSHIP & COMMUNITY

Cybersecurity Co-Lead — ACM SIT Pune (2024 – Present)

• Spearheaded 6+ cybersecurity workshops and CTF competitions for 150+ students, covering incident response, threat detection, and live attack/defense scenarios.

Student Ambassador — Google Gemini (2025 – Present)

• Facilitated 4+ cloud computing and AI development workshops reaching 100+ students, driving hands-on adoption of Google Cloud and Gemini APIs.