DHRUV CHOPRA

+91 8052170430 | thisisdhruvchopra@gmail.com | dhruvchopra.info | LinkedIn | GitHub

EDUCATION

Dr. A. P. J. Abdul Kalam Technical University, Lucknow *Jun 2025*
B.Tech | Computer Science & Engineering

CERTIFICATIONS

- Executive PG Certification in Cloud Computing & DevOps | iHUB DivyaSampark @ IIT Roorkee

WORK EXPERIENCE

Associate – Deception Technology | C3iHub, IIT Kanpur *Jul 2025 – Present*

- Built a high-fidelity **HTTP honeypot** mirroring SAIL BSP's production web surface with induced CVEs and custom vulnerability layering, attracting real-world **botnet and APT-class traffic** and increasing attacker dwell time by ~3x over standard low-interaction deployments.
- Deployed **Cowrie and Dionaea** across SSH, FTP, and ICS endpoints; orchestrated the full **IT/OT honeypot stack on Kubernetes** managing multi-node clusters, pod scheduling, namespaces, and HPA, maintaining **99.9% sensor uptime** across 6 concurrent deception endpoints.
- Analyzed attacker **TTPs** through **payload inspection, HTTP fingerprinting,** and credential capture; produced weekly **threat intelligence reports** that tracked 3+ active botnet campaigns targeting critical **industrial infrastructure**.

Research Intern – Deception Technology | C3iHub, IIT Kanpur *May – Jul 2025 | 2 months*

- Shifted from DevOps into **DevSecOps** by auditing **CI/CD pipelines** and container configs for security misconfigurations using **OWASP Top 10** and **CIS benchmarks** on live client infrastructure, cutting identified attack surface by ~30%.
- Studied **MITRE ATT&CK** for TTP-based attacker behaviour mapping and built network security foundations in **CIDR, subnetting, VPC design,** and routing, directly applied to honeypot sensor placement and network segmentation decisions.

DevOps Intern | C3iHub, IIT Kanpur *Feb – Jun 2024 | 5 months*

- Containerised and deployed microservices using **Docker and Kubernetes** with 99.8% uptime; provisioned **AWS infrastructure** (EC2, VPC, S3, Lambda) with **Terraform and Jenkins**, cutting deployment time by 40% and manual effort by 60%.
- Set up **continuous monitoring and alerting** using the **ELK Stack** across Kubernetes clusters, improving incident detection time by 35% and cluster performance by 15%.

PROJECTS

ADAPT Framework Replication — Adaptive Camouflage-based Deception Orchestration | 2026 | Reference link

- Replicated the full **ADAPT honeynet** on physical hardware — 6-VM network across two privilege tiers (researcher and professor machines), HTTP/FTP servers, and OpenVPN backbone; deployed all three **APT attack paths (APT-40, APT-28, Lazarus/APT-38)** with **MITRE TTP-aligned** honey credentials and strategically induced vulnerabilities.
- Built and deployed **Chatterbox**, a covert log-exfiltration app that transmitted system logs from all 6 VMs to a **Kafka broker** over an encrypted channel; wired the full **threat intelligence pipeline** (Kafka to Elasticsearch to dashboard) for near real-time **attack path correlation** and MITRE TTP mapping.
- Did a post-replication critical evaluation of the framework — found that **CVE-2021-41773** and **CVE-2022-0847** are fully patched and no longer representative of real **APT tradecraft**; documented findings in an independent technical review submitted for publication.

Honeypot Log Analyser | 2025 | GitHub link

- Built a **Python toolkit** for HTTP honeypot log analysis using a priority-ordered **regex classification engine** to sort attack events (**command injection, path traversal, CMS scanning**) into High/Medium/Low severity tiers, handling 10,000+ log entries per weekly cycle.
- Added **MaxMind GeoLite2** for attacker IP geolocation and origin profiling, and built **credential extraction modules** to pull username/password attempts from HTTP POST payloads, cutting manual threat analysis time by ~50%.

SKILLS

Security: Honeypot Design & Deployment, Deception Technology, Threat Intelligence, TTP Analysis, Payload Inspection, Log Analysis, Credential Forensics, Cowrie, Dionaea, OWASP Top 10, MITRE ATT&CK, CVE Analysis, Network Segmentation
Cloud & DevSecOps: AWS (EC2, Lambda, VPC, S3, Autoscaling), Azure, Docker, Kubernetes (HPA, Ingress, Namespaces), Terraform, Jenkins, Ansible, CI/CD, ELK Stack, Kafka, Elasticsearch, OpenVPN
Network & Recon: Wireshark, Nmap, Netcat, tcpdump, CIDR & Subnetting, VPC Design, Network Segmentation
Security Tools: Burp Suite, T-Pot, Honeyd, Shodan, AbuseIPDB, VirusTotal, Kali Linux, Ubuntu
Languages: Java (since 2016), Python, YAML
Other: DSA & Algorithms, Git, Open-Source Contributor

ACTIVITIES & ACHIEVEMENTS

TCS Code Vita S11 (2023) — Ranked 1788 globally in Round 2 out of 200,000+ participants. **LeetCode** — 700+ problems. Handle: thisisdhruvchopra | **HackerRank** — 4★ Java | 5★ Problem Solving. Handle: dchopra92
Leadership — School Captain and CS Club President; ran a statewide techno-cultural event with 300+ participants from 15+ schools. **Debating** — National-level MUN debater, 10+ events, won a few.
Subjects of Interest: Design & Analysis of Algorithms | Data Structures | Theory of Automata & Formal Languages | Computer Networking | Network Security | Cloud Security