

# UDIT CHHIPA

Security Engineer | Computer Science Engineer

Jaipur, India

+91 78520-91947 | [udit7852@gmail.com](mailto:udit7852@gmail.com)

[LinkedIn](#) | [GitHub](#)

## EDUCATION

### Jaipur National University

B.Tech in Computer Science (Specialization in Cybersecurity)

Jaipur, Rajasthan

Sep. 2023 – June 2027

- Relevant Coursework: Data Structures & Algorithms (DSA), Operating Systems, Computer Networks, Database Management Systems (DBMS), Cloud Security.

## TECHNICAL SKILLS

**Languages:** Python (Advanced), Java (DSA), Go (Golang), HTML, CSS, JavaScript, SQL, JavaScript, Bash

**Security Tools:** Burp Suite, Metasploit, Wireshark, Nmap, OWASP ZAP, Docker, Kubernetes

**Core Concepts:** Network Security, Threat Modeling (STRIDE), Zero Trust, Digital Forensics, CI/CD Security

**Data & AI:** Pandas, NumPy, OpenAI API Integration, Log Analysis, Selenium

## PROJECTS

### AutoRed: AI-Powered Vulnerability Scanner | Python, OpenAI API, Selenium

- Architected an automated vulnerability assessment tool that crawls web applications to detect OWASP Top 10 vulnerabilities (XSS, SQLi), increasing scan coverage by **40%**.
- Integrated **LLMs (OpenAI API)** to analyze scan logs and auto-generate professional penetration testing reports, reducing manual documentation time by **90%**.
- Implemented Natural Language Processing (NLP) to classify false positives, ensuring high-accuracy results.

### Smart Network Observability Dashboard | Python, Flask, Ngrok

- Constructed a lightweight network monitoring platform using **Flask** to visualize system performance and packet traffic, improving real-time visibility by **3x**.
- Deployed **Ngrok** tunneling to establish secure, encrypted remote access to the dashboard from external networks for authorized testing.
- Formulated a real-time alerting system that identifies suspicious spikes or unauthorized connections, cutting incident response time by **50%**.

### High-Performance Honeypot (Deception Tech) | Go (Golang), Concurrency

- Built a low-interaction honeypot in **Go (Golang)** that simulates vulnerable service ports to deceive attackers and capture threat intelligence.
- Refactored core networking modules to use Go routines, handling **10x more simultaneous connections** than the initial Python prototype.
- Designed a logging pipeline to capture attacker payloads and IP metadata for forensic analysis.

### Forensic Data Analysis Pipeline (IPDR/CDR) | Python, Pandas, SQL

- Spearheaded a data processing tool to normalize and analyze over **100,000+** raw log entries (Call Detail Records) for forensic investigations.
- Programmed algorithmic filters to detect suspicious communication patterns and anomalies, successfully simulating fraud detection systems.
- Automated the generation of visual reports using Matplotlib, reducing manual analysis time by **40%**.

## EXPERIENCE

### Security Engineering Intern

ShadowFox

July 2025 – Present

Remote / Hybrid

- Executed Dynamic Application Security Testing (DAST) on web infrastructure, identifying **15+ critical vulnerabilities** and collaborating with developers on remediation.
- Engineered custom Python automation scripts to streamline reconnaissance and vulnerability scanning, reducing manual testing overhead by **20%**.
- Orchestrated network traffic analysis and packet inspection using Wireshark to identify and patch insecure transmission protocols.

## ACHIEVEMENTS

---

**TryHackMe:** Ranked in the Top **10%** globally; completed advanced paths in Web Fundamentals.

**Hack The Box:** Active participant in solving "Hard" tier machines and Pro Labs scenarios.

**Coding:** Solved 200+ DSA problems on LeetCode/Hackerrank (Java/Python).