Shubham Sharma

+91-7891464270 | shubham2chaipa1102@gmail.com | LinkedIn | GitHub

Summary

Second-year Computer Science Engineering student specializing in Cybersecurity and Digital Forensics at VIT Bhopal. Strong foundation in network security, programming, ethical hacking, and vulnerability assessment. Seeking internship or entry-level opportunities in cybersecurity, network forensics, or security operations.

Education

Vellore Institute of Technology — Bhopal, MP
B.Tech in Computer Science Engineering – Cybersecurity and Digital Forensics — *Sep 2024 – Sep 2028*

Technical Skills

Cybersecurity: Ethical Hacking, Network Forensics, Vulnerability Assessment, Digital Forensics, Security Monitoring
Network Tools: Wireshark, Nmap, Tcpdump, TShark, Aircrack-ng, Burp Suite
Penetration Testing: Kali Linux, Metasploitable 2, Hydra, Snort, Suricata
Programming Languages: Python, C++
Databases: MySQL, MongoDB
Networking Concepts: TCP/IP, DNS, HTTP/HTTPS, ARP, DHCP, OSI Model
Version Control: Git, GitHub

Projects

BruteForceLab | *Python, Tkinter, hashlib, bcrypt, itertools* | GitHub — Sep 2025

- Built GUI module and system integration for an educational brute force simulation framework supporting exhaustive, dictionary, and hybrid attack modes with real-time progress visualization using Tkinter.
- Implemented support for MD5, SHA-256, and bcrypt hashing with salting demonstration — showing bcrypt reduces attacker speed from 10^9 to $\sim 10^3$ guesses/second on identical passwords.
- Framework achieved 100% crack accuracy within configured search space; integrated entropy calculator and security recommendations to provide actionable defensive insights.

IoT Security Monitoring System (VITGuard) | *Python, MQTT, Flask, Linux auditd* | GitHub — Jan 2026

- Developed the Victim App simulation module and Security Engine for a 6-layer IoT intrusion detection system achieving sub-50ms end-to-end alert latency using Linux audit logging and Eclipse Mosquitto MQTT.
- Implemented keyword-based syscall detection with 97% accuracy and 3.2% false-positive rate, broadcasting real-time alerts over MQTT QoS=1 to a live Flask-based SOC dashboard.
- System monitors `/etc/passwd` and `/etc/shadow` access attempts, generates CRITICAL alerts within 50ms, and triggers OFFLINE status within 40 seconds of agent failure via heartbeat mechanism.

Certifications & Achievements

- **Bits and Bytes of Computer Networking** – Coursera | coursera.org/verify/7M1WXX3JI7RO
- **Kali Linux and Security Tools Practice** – Wireshark, Nmap, Burp Suite, Metasploitable 2, Hydra, and related cybersecurity tools
- **MySQL** – Completed coursework | **MongoDB** – Certification in progress

Cybersecurity Knowledge

- Understanding of ethical hacking methodology including reconnaissance, scanning, enumeration, exploitation, and reporting.
- Familiar with log analysis, IOC identification, network reconnaissance, attack surface analysis, and web application security testing.
- Knowledge of phishing, brute-force attacks, SQL injection, XSS, man-in-the-middle attacks, and defensive security practices.