CHANDRAPRAKASH C

Aspiring Cybersecurity Intern | SOC Analyst Enthusiast

📍 Dindigul, Tamil Nadu | 📞 +91 9786475035 | 📧 cyberchandru87@gmail.com
Portfolio: https://chandruthehacker.github.io
LinkedIn: https://linkedin.com/in/chandraprakash87
GitHub: https://github.com/chandruthehacker

SUMMARY

Cybersecurity-focused Computer Science undergraduate with hands-on experience in offensive security, threat detection, and log analysis. Skilled in Python, Bash, and tools like Burp Suite and Wireshark. Built real-world projects including phishing detectors, honeypots, and log parsers. Eager to contribute to red/blue team operations and grow in a security-focused environment.

TECHNICAL SKILLS

- **Security Tools:** Burp Suite, Wireshark, Nmap, Wazuh SIEM, Metasploit
- **Programming:** Python, Bash, Flask, Regex
- **Security Areas:** Log Analysis, Threat Detection, Vulnerability Scanning
- **Networking:** TCP/IP, DNS, Firewall Rules
- **Documentation:** Security Reports, Incident Logs, Markdown Notes

EDUCATION

B.Sc. Computer Science
GTN Arts College, Tamil Nadu | 2023 – 2026

CERTIFICATIONS

- Google Cybersecurity Certificate – Coursera | April 2025
- Ethical Hacking Training – Internshala | November 2024

EXPERIENCE

Cybersecurity Project Developer – Freelance
Jan 2024 – Present

- Refined Wazuh detection rules to reduce false positives by 20%.
- Performed log analysis and drafted incident reports.
- Automated alerting with custom Python/Bash scripts.

PROJECTS 🔗 View My Projects

AI-Powered Phishing Email Detector | GitHub

- AI-based tool that classifies phishing emails using Google Gemini and regex, achieving 85% accuracy.

Admin Login Honeypot Trap | GitHub

- Deceptive login interface that captures attacker IPs and logs unauthorized credential attempts.

Log Parser Tool | GitHub

- Automated log parser for Apache/Syslog/authlog/nginx to detect brute-force patterns and generate quick insights.

AVAILABILITY

Immediate | Open to Remote, Hybrid, or On-site Roles