# CHIRAG R SHETTY

+91-xxxxxxxxxx | chiragrshetty12@gmail.com | Bengaluru
LinkedIn | GitHub | Cybersecurity E-Portfolio | TryHackMe

## SUMMARY

Detail-oriented cybersecurity graduate with hands-on experience in SOC analysis, vulnerability assessment, penetration testing, and AI-driven security practices. Proficient in industry-standard tools including Burp Suite, Nmap, Metasploit, and Splunk, with strong practical knowledge of MITRE ATT&CK framework and OWASP Top 10 standards. Demonstrated ability to identify, exploit, and document security vulnerabilities across network and web application environments. Ranked in the top 7% globally on TryHackMe with 5200+ points across 60+ hands-on labs covering SOC operations, VAPT, and AI security. Backed by multiple industry certifications including Google Cybersecurity and IBM Ethical Hacking, with a growing project portfolio demonstrating real-world security operations expertise.

## EDUCATIONAL QUALIFICATIONS

❖ **Bachelor of Computer Applications(BCA) - Jain University** **Jul 2023 – May 2026**
- **CGPA** :- 8.00
- **Course Framework** : Computer Networks ,Operating Systems ,C ,Java ,Python

❖ **Pre-University – St Joseph's pre-university college** **Jun 2021 - May 2023**
- **Aggregate :-** 78%

❖ **10th- Sri Devaraj Urs International Residential School** **Jun 2020 – Mar 2021**
- **Aggregate :-** 76%

## PROJECTS

❖ **AI-Powered Log Analysis using Splunk**
- Developed an **AI-Powered SOC Security Analytics Dashboard** using Splunk, Python, Streamlit, and Gemini AI to analyze and investigate security events.
- Implemented **threat detection, risk scoring, severity classification,** and **MITRE ATT&CK mapping** for SSH brute-force attacks, root account attacks, and account compromise scenarios.
- Integrated **Splunk SDK and custom SPL queries** to process 1,000+ security events and generate interactive dashboards, AI-assisted incident analysis, and CSV-based downloadable security reports.

❖ **End-to-End VAPT and Exploitation using Nmap, Nessus, and Metasploit**
- Performed Vulnerability Assessment and Penetration Testing (VAPT) across network infrastructure, using **Nmap** for reconnaissance, host discovery, and port scanning. Performed vulnerability assessment using **Nessus** and prioritized risks based on severity based on CVSS.
- Exploited identified vulnerabilities using **Metasploit** Framework to gain system access in a controlled lab environment, validating real-world attack vectors.
- Executed post-exploitation activities including privilege escalation, system enumeration, and session management. Documented findings and remediation strategies in technical reports.

❖ **Web Application Security Testing using DVWA and Burp Suite**
- Conducted web application penetration testing on DVWA using **Burp Suite**, identifying 4+ critical vulnerabilities including SQL Injection and Cross-Site Scripting (XSS).
- Exploited multiple web vulnerabilities in a controlled lab environment, demonstrating real-world attack scenarios and business impact and Mapped and documented according to OWASP TOP10.

## SECURITY TOOLS

- **SIEM & Log Analysis:** Splunk
- **Vulnerability Assessment & Penetration Testing (VAPT):** Nmap, Metasploit, Burp Suite
- **Network Security Monitoring:** Wireshark, Snort, Suricata
- **Threat Intelligence & OSINT:** Maltego, VirusTotal, Shodan
- **Operating Systems:** Kali Linux
- **Scripting & Automation:** Bash Scripting, Python
- **Firewall Technologies:** Palo Alto Networks (Foundational)

## TECHNICAL SKILLS

- Log Analysis
- Generative AI
- Computer Networks
- Vulnerability Management
- Incident Response
- Firewall Configuration
- Penetration Testing
- Operating Systems
- Threat Detection

## CERTIFICATIONS

- **Google Cybersecurity Professional Certificate** - Coursera
- **IBM Ethical Hacking with Open Source Tools Professional Certificate** – Coursera
- **IBM Generative AI for Cybersecurity Professional Certificate –** Coursera
- **CompTIA Security+ (SY0-701)** — In Progress (Expected By Sep 2026)

## VIRTUAL EXPERIENCE

❖ **Tata Cybersecurity Analyst Virtual Experience** — Forage **JUN 2026**

- Analyzed simulated security incidents to identify attack vectors & recommend mitigation strategies.
- Assessed network architecture and proposed improvements to strengthen organizational defenses.
- Developed incident response documentation aligned with industry frameworks.

## ACHEIVEMENTS

- Achieved a **Top 7%** global rank on TryHackMe by completing **60+** hands-on labs, earning **5200+** points,practical experience in VAPT, SOC Labs and AI Security.

## WORKSHOPS,TRAINING

- Participated in a **Cybersecurity Conference** covering foundational concepts of ethical hacking, security principles, and hacking techniques.
- Completed **CompTIA Server+** training with hands-on exposure to server administration, infrastructure fundamentals and tools like Cisco Packet Tracer.

## ADDITIONAL INFORMATIONSS

- **LANGUAGES:** English, Kannada, Telugu, Hindi
- **HOBBIES:** Traveling, Badminton, Cricket, Cooking

## DECLARATION

I hereby declare that the information furnished above is true to the best of my knowledge.

**Place** : Bengaluru CHIRAG R SHETTY