SUDARSHAN RANGAPPA

www.linkedin.com/in/sudarshan-rangappa | P: +91 8302720020 | Sudarshan_rangappa@proton.me |
https://sudarshanrangappa.github.io/portfolio/

PROFESSIONAL SUMMARY

Aspiring Penetration Tester with hands-on experience in vulnerability assessment, exploit development, and red teaming simulations. Skilled in using industry tools such as **Burp Suite, Nmap, Metasploit, Nessus, Nuclei, OpenVAS, and SQLMap**. Proven ability to simulate real-world attacks, identify security gaps, and provide mitigation strategies. Strong knowledge of OWASP Top 10, web application testing, network enumeration, and post-exploitation tactics. Committed to offensive security and eager to contribute to security consulting or red team engagements.

EDUCATION

National Forensic Sciences University — Gandhinagar, Gujarat

Master of Science, Cybersecurity — Aug 2023- May 2025
Cumulative GPA: 8.24
Relevant Coursework: Threat Detection, VAPT, SIEM Operations, Network Security, Incident Response

Bengaluru City University — Bengaluru, Karnataka

Bachelors of Computer Applications — Jul 2020 - Jul 2023
Cumulative GPA: 8.16

UNIVERSITY PROJECTS

INTEGRATED CYBER DEFENCE SYSTEM [ICDE] — May 2025

Designed and deployed a scalable cybersecurity operations lab simulating enterprise-grade blue team workflows using real-world security tools and attack scenarios.

- Built a virtual SOC environment integrating industry tools: Splunk, Wazuh, Suricata, Zeek, Cowrie, OpenVAS, Shuffle
- Monitored logs from 3 endpoints (Windows Server 2025 AD, Windows 11, Ubuntu) using Wazuh and Splunk
- Created 3+ SOAR playbooks in Shuffle to automate IP blocking, alert forwarding, and GeoIP enrichment
- Simulated 10+ attack scenarios including brute-force, privilege escalation, and SSH honeypot interaction, achieving 100% detection in Splunk and Wazuh
- Achieved real-time alert correlation and incident response workflow across all components

LOCATION-BASED IOT SECURITY KEY — November 2024

Developed a location-aware authentication mechanism for IoT devices using ESP8266 (NodeMCU) and GPS module for physical-layer access control.

- Implemented geofencing logic with ±5m accuracy to dynamically permit or deny access based on GPS coordinates
- Achieved 90%+ accuracy in unauthorized access prevention in field tests
- Reduced false access triggers by tuning GPS sampling frequency and incorporating time-based validation

Skills & Certifications

Technical Skills: Vulnerability assessment, Penetration testing, Exploitation techniques, Web application security (OWASP Top 10), Reconnaissance and OSINT, Scripting (Bash, PowerShell basic), Network security, Email Security, risk-based reporting, Linux/Windows administration, MITRE ATT&CK.

Tools: Nmap, Burp Suite, SQLMap, Metasploit, Nessus, OpenVAS, Nikto, Nuclei, Dirbuster, theHarvester, Maltego, Recon-ng, Shodan, Netcat, Aircrack-ng, Searchsploit, ExploitDB.

Certifications & Training: Certified Ethical Hacker [CEHv11], Fundamentals of Deep Learning [Nvdia], Basel's Open Source Intelligence [OSINT], Cyber Threat Intelligence 101 [ArcX]