Sri Bharath

bharathsri05@gmail.com — +91 9361251549 — linkedin.com/in/sribharath-

Summary

Dedicated and detail-oriented cybersecurity enthusiast with hands-on experience in defensive security, red teaming, and log monitoring. Strong knowledge of SIEM tools, Linux environments, and Windows AD infrastructure. Skilled in detecting, analyzing, and responding to cyber threats using industry-standard tools and frameworks. Demonstrated ability to work in team-based environments with a proactive learning mindset. Actively building labs, exploring attack vectors, and staying updated on emerging threats to deliver real-world security solutions.

Skills

Programming: Python
Security Ops: SIEM (Splunk, Wazuh), Threat Detection, Incident Response
Offensive Security: Red Teaming, Vulnerability Analysis, C2 Frameworks
Network/System Security: Privilege Escalation, Web Security, Active Directory
Frameworks: MITRE ATT&CK, OWASP, ISO 27001, HIPAA
Platforms: Linux, Windows
Tools: Burp Suite, Nessus, Wireshark, OpenVAS, PowerShell
Soft Skills: Communication, Critical Thinking, Teamwork

Education

Red Team Hacker Academy, Chennai
Advanced Diploma in Cyber Defense (ADCD) — Sep 2024 – Present

Sri Manakula Vinayagar Engineering College
B.Sc. in Computer Science – CGPA: 7.8 — Nov 2021 – Jul 2024

Krishnasamy Hr. Sec. School
Higher Secondary – 62.3% — 2021

Projects

Active Directory Lab Setup
Designed a virtualized Windows Server AD lab using VirtualBox. Configured Domain Controller, DNS, DHCP, and Group Policy Objects (GPO). Created multiple user accounts with permissions. Simulated brute-force and lateral movement attacks for detection and hardening.

Wazuh SIEM Threat Monitoring (Multi-OS)
Deployed a centralized Wazuh SIEM stack on Ubuntu with Filebeat and ELK integration. Configured agents across Windows, Fedora, and Kali Linux. Created rules to detect user login anomalies, registry changes, and file integrity issues. Built custom dashboards for real-time analysis.

Certifications

- Certified Ethical Hacker (CEH Master) – In Progress
- Cyber Threat Management – Cisco Networking Academy
- Phishing Email Analysis – LetsDefend
- Email Header Analysis – LetsDefend
- Advanced Diploma in Cyber Defense (ADCD)

Hands-on Practice

- Regularly perform SOC and Blue Team labs on LetsDefend and TryHackMe (over 100+ tasks completed).
- Built detection use-cases using Wazuh and ELK stack for login anomalies, port scans, and file modifications.
- Practiced offensive techniques like XSS, SQLi, and Privilege Escalation in HackTheBox and TryHackMe.
- Set up Suricata and Zeek sensors for packet inspection and log enrichment in lab environments.
- Monitor real-time alerts, analyze PCAPs, correlate incidents with MITRE ATT&CK tactics, and create incident reports.