

SIVADHARANI

Mail - sivadharani823@gmail.com | Ph - +91 7339327561

LinkedIn - [linkedin.com/in/sivadharani23/](https://www.linkedin.com/in/sivadharani23/) | Github - <https://github.com/sivadharani-a>

Portfolio - <https://sivadharani-a.netlify.app/>

SUMMARY

Entry-level SOC Analyst with foundational knowledge in cybersecurity, system administration (Windows, Linux), and incident monitoring. Skilled in shell scripting, log analysis, and basic threat detection. Eager to support SOC operations, triage alerts, and contribute to secure enterprise environments. Adept at triaging alerts, performing root cause analysis, and supporting incident response processes.

EDUCATION

Master of Computer Applications

Anna University, Tiruchirappalli.

2023 - 2025

CGPA - 8.4

Bachelor of Computer Applications

AVC College(Autonomous), Mayiladuthurai.

2020 - 2023

CGPA - 8

SKILLS SUMMARY

- Security Tools: Kali Linux, Wireshark, Nmap, Burp Suite, Metasploit
- Threat Detection & Monitoring: Web traffic analysis, SIEM (basic, Splunk), IDS/IPS concepts
- Operating Systems: Windows, Linux
- Frameworks & Standards: NIST, ISO 27001, CIS Controls (basic understanding)
- Programming/Scripting: Python, Bash, Java, C, C++
- Networking Fundamentals: TCP/IP, Firewalls, Proxies

WORK EXPERIENCE

Cyber Security Intern | Shadowfox | October 2024 - November 2024

- Conducted vulnerability assessments with Nessus, identifying 50+ security gaps and mitigating threats.
- Enhanced network security using Wireshark, Nmap, reducing incident resolution time by 25%

Ethical Hacking and Penetration Testing Intern | C-DAC | December 2024 - January 2025

- Gained hands-on experience in ethical hacking and penetration testing, identifying vulnerabilities and security risks.
- Developed skills in exploit detection, threat analysis, and network security best practices.

PROJECTS

1. **WebDefender-X**: AI-Driven Web Application Firewall

Technologies: Python, Machine Learning, Scikit-learn, Linux.

- Developed an AI-powered Adaptive Web Application Firewall (AWAF) to detect and mitigate SQLi, XSS, and DDoS attacks in real time, with a dynamic threat monitoring dashboard.

2. **Secure File Transfer System**

Technologies: Python, AES Encryption, Sockets

- Built a fast, user-friendly network port scanner to identify open ports, analyze vulnerabilities, and generate actionable security reports.

3. **Network Topology – Packet Tracer**

Tools: Cisco Packet Tracer

- Designed and simulated a multi-subnet network with PCs, switches, and routers to understand IP addressing, routing, and LAN communication for security monitoring.

CERTIFICATIONS

- Tools of the Trade: Linux and SQL – Google
- Introduction to Cybersecurity Awareness – HP LIFE
- Cybersecurity Analyst Job Simulation – Forage
- Malware Analyst vs. Ransomware Defense – Simplilearn (Masterclass)