Sahil Kumar

8591104707 | sahilkumarsws@gmail.com | LinkedIn

Education

Ramrao Adik Institute of Technology — Nerul, Navi Mumbai
B.Tech in Information Technology — *Aug. 2022 – Present*

Greenfingers Global School — Kharghar, Navi Mumbai
Central Board of Secondary Education — *Aug. 2010 – Mar 2022*

Technical Skills

Languages: Python, Javascript, Bash, Typescript
Technologies: Git, AWS, Azure, Docker, Jenkins
Frameworks: React, Node.js, Flask
Cybersecurity Tools: Splunk, Nessus, Tenable One, Burpsuite, Metasploit

Projects

Security Lab SIEM with Cloud Environment | *Wazuh, Graylog, AWS EC2* June 2024 – Aug 2024

- Set up a SOC environment using Wazuh and Graylog to simulate log collection, threat detection, and alerting workflows across Windows and Linux virtual machines.
- Analyzed logs from multiple sources including Windows Event Logs, Sysmon and Zeek network monitoring logs to practice triage common attack patterns like brute-force attempts and suspicious process executions.
- Deployed a simple HTML application on AWS EC2 and a local virtual server to simulate cloud environments, monitored using CloudTrail, VPC Flow Logs, and sys logs for suspicious activity.
- Built a foundational understanding of how log pipelines, detection logic and cloud monitoring work into day-to-day SOC analyst tasks.

Network Intrusion Detection System | *Wireshark,* tcpdump, Snort, Python, Mint OS Nov 2024 – Jan 2025

- Implemented a basic NIDS to monitor network traffic and detect suspicious activities such as port scanning, unusual traffic spikes and known malicious IP addresses.
- Developed detection logic for common intrusion patterns like DDoS, SYN flood and triggered alerts on matching signatures.
- Gained hands-on experience with network forensics, intrusion detection concepts and traffic analysis—core skills for SOC and Blue Team roles.

AI-Based Chatbot for Privacy Literacy | *Python, Flask, NLTK, Vercel* Jan 2025 – Feb 2025

- Developed an interactive chatbot using Python to educate users on digital privacy topics such as data protection, password hygiene and online tracking.
- Integrated privacy best practices content sourced from reputable organizations to ensure accurate and up-to-date educational material.
- Designed a simple frontend using HTML/CSS and deployed the chatbot on a local web server (Ubuntu server) using Flask, simulating a real-world user-facing privacy assistant.
- Focused on user education and awareness in cybersecurity, demonstrating an interest in ethical tech and digital safety.

Achievements

- Conducted extensive monitoring on LetsDefend. Published blogs on Medium regarding the findings of labs on LetsDefend.
- Created various walkthrough tutorials for CTFs and challenges on THM, Portswigger and LetsDefend.

Certifications and Courses

- CCNA - Enterprise Networking, Security, and Automation
- ISC2 Certified in Cybersecurity – ISC2
- AWS Academy Cloud Architecting – AWS Academy