SUPRIT KESTE

Nasalapur 591213 | suprithkeste111@gmail.com | 9164201070 | LinkedIn

OBJECTIVE

Passionate Computer Science student with hands on experience in SIEM, incident response, and vulnerability assessment. And currently engaged in Bug Bounty programs And Eager to contribute my cybersecurity Knowledge to a dedicated Security Team to solve real world problems.

SKILLS

Security Operations: Security Monitoring, Incident Response, Threat & Vulnerability Assessment, Log Analysis.
Tools & Technologies: Microsoft Sentinel, Burp Suite, Nmap, Wireshark, Metasploit, Nessus.
Programming: SQL, KQL, Python.
Security Concepts: CIA Triad, IDS/IPS, IAM, Network Security.
Operating Systems: Windows, Kali Linux.
Soft Skills: Communication, Problem-solving, Team collaboration, Documentation.

INTERNSHIP

Xencia Technology Solutions Pvt Ltd (**Link**) — BANGLORE, INDIA

Role: **Security Engineer Intern**
Feb 2025 – June 2025

- Worked with Microsoft Sentinel to manage SIEM/SOAR operations across client environments.
- Monitored and analyzed security alerts, logs, and incidents to identify threats.
- Used Kusto Query Language (KQL) to enhance detection capabilities and create analytics rules.
- Assisted in integrating log data connectors and developing automation playbooks for faster incident response.

PROJECTS

Network Anomaly Detection using Machine Learning — November 2024

Tools: Python, Flask, Jupyter Notebook, GridSearchCV, DB Scan, Isolation Forest
A system identifies abnormal network behaviour using ML, designed for real-time detection and analysis of anomalies.
Responsibilities: Implemented DB Scan and Isolation Forest algorithms, optimizing performance with GridSearchCV. Pre-processed and analysed the CICIDS2017 dataset to ensure data quality for model training. Designed and developed a Flask-based web interface for real-time anomaly alerts and monitoring. Conducted model testing and validation using different scenarios to enhance detection accuracy. Utilized Jupyter Notebook for iterative development and visualization of insights.

Network Vulnerability Scanner — August 2024

Tools: Python, Nmap, Flask, SQLite, Bootstrap
A lightweight web application for scanning and reporting vulnerabilities in network systems.
Responsibilities: Developed a Flask-based interface for initiating and managing network scans. Integrated Nmap for vulnerability detection and real-time scanning of network hosts. Created a database using SQLite to store scan results and provide historical analysis. Designed an intuitive Bootstrap-based dashboard for visualizing scan results and vulnerability metrics. Implemented logging and reporting features to generate actionable insights for users.

EDUCATION

Bachelor of Engineering in Computer Science and Engineering — Chikodi, Belagavi
KLE COLLEGE OF ENGINEERING AND TECHNOLOGY CHIKODI — Dec 2021 to May 2025
CGPA (aggregate): 7.1/10

CERTIFICATES

- ➢ SC-200 Microsoft Security Operations Analyst (Pursuing)
- ➢ Google Cybersecurity Certificate (Google Certificate by Coursera) Link
- ➢ Cyber Threat Intelligence 101 (ARCx) Link
- ➢ Introduction_to_Cybersecurity_Badge2023 (CISCO Networking Academy) Link

Other Achievements

Orchestrated all logistical aspects for Praxis-2K24, a national tech fest hosting 500+ participants, securing venue, managing vendor relationships, resulting in 95% positive feedback from attendees regarding event organization.