Kailas M K

Bengaluru | +91 8088200583 | kailasmk1@gmail.com | https://www.linkedin.com/in/kailas-m-k

EDUCATION

Presidency University **Bengaluru, Karnataka**

Bachelor of Technology - Cyber Security CGPA - 7.48 *Graduation Date: Nov 2024*

WORK EXPERIENCE

Remarkskill - Microsoft **Bengaluru, Karnataka**

Ethical Hacker Intern *Jan 2022 - Mar 2022*

- Researched various DoS and DDoS attack techniques, including SYN flooding, DNS amplification, and botnets.
- Analyzed the potential impact of these attacks on the organization's availability, reputation, and revenue.
- Assisted in the implementation of traffic filtering, rate limiting, and network segmentation strategies.
- Enhanced understanding of various DoS and DDoS attack vectors and their impact.

Swiftsafe **Bengaluru, Karnataka**

Security Research Intern *Jul 2024 - Dec 2024*

- Researched emerging threats and vulnerabilities, enabling proactive defenses that cut incident response time by 30%.
- Performed 50+ vulnerability assessments, reducing exploitable attack surfaces by 25%.
- Created detailed reports summarizing research results and recommending mitigation strategies.

PROJECT EXPERIENCE

Presidency University **Bengaluru, Karnataka**

Yarweb *Aug 2023 - Jan 2024*

- Developed YARWEB malware analysis platform using advanced algorithms for high-speed, accurate threat detection.
- Engineered analysis tools to identify multiple malware types, including viruses, Trojans, and ransomware.
- Implemented customizable detection rules for precise threat identification and mitigation.
- Designed an intuitive, user-friendly interface to enhance usability and navigation for security teams.

SIEM Setup and SOC Monitoring *Jan 2025 - Jan 2025*

- Built a virtual SOC lab using Splunk/Wazuh to ingest logs from Windows and Linux machines.
- Developed correlation rules to detect brute-force, privilege escalation, and malware events.
- Performed threat hunting exercises and documented findings aligned with the MITRE ATT&CK framework.
- Automated alert triaging and report generation to simulate Tier 1 SOC workflows.\

Endpoint Detection and Response (EDR) Simulation *Apr 2025 - May 2025*

- Configured Wazuh/OSSEC to monitor endpoint processes, registry changes, file integrity, and suspicious binaries.
- Developed custom detection rules to identify anomalous process behavior, and lateral movement indicators.
- Integrated threat intelligence feeds to enrich alerts with context on malicious IPs, domains, and file hashes.

SKILLS

Technical: Cybersecurity Fundamentals, Threat Detection and Analysis, Network Security Basics, Incident Response, Vulnerability Assessment, SIEM, Firewall and IDS/IPS Basics, Security Monitoring, NIST, ISO2007

CERTIFICATIONS

Google Cybersecurity Professional Certificate [https://shorturl.at/5RzDx]

Microsoft Security Fundamentals [https://shorturl.at/Omxho]