GANESH KUMAR M

Email : theganeshkumar00@gmail.com | Phone No : 8525806498 | Portfolio | Linkedin | Skillrack | LeetCode

CAREER OBJECTIVE

Enthusiastic and quick-learning fresher with a strong interest in networking, Linux, SOC operations, SQL, and malware analysis. Eager to apply foundational knowledge and hands-on lab experience to support cybersecurity and infrastructure teams, while continuously learning and growing in a dynamic tech environment.

EDUCATIONEDUCATION

B.Tech IT - Kamaraj College of Engineering & Technology	2021 – 2025	**7.67**
HSC – Kalaimagal. HR.SEC School	2021	**86.0%**
SSLC – Kalaimagal. HR.SEC School	2019	**77.6%**

PROJECTS AND INNOVATION

SIEM TOOL (WAZUH) :

- The Wazuh Security Monitoring project implements key security features including File Integrity Monitoring (FIM), Vulnerability Detection, and Brute Force Attack Detection to ensure robust threat detection and system protection. It is integrated with IDS/IPS tools such as Suricata to monitor network traffic and detect intrusions in real time, forming a comprehensive SIEM solution

.

- The setup includes the deployment of two Wazuh agents — one on a Linux machine and another on Windows — to provide cross-platform visibility. With real-time alerts, centralized logging, and correlation capabilities, this project demonstrates how Wazuh can be effectively used to monitor, analyze, and respond to security events across different operating systems. (LINK)

NESSUS VULNURABILITY SCANNER :

- The Nessus Vulnerability Scanning project focuses on identifying security weaknesses across networked systems using one of the industry's leading vulnerability assessment tools. Nessus was configured to perform comprehensive scans on both Linux and Windows systems, detecting outdated software, missing patches, misconfigurations, and exploitable services.

- Scan results were analyzed to prioritize vulnerabilities based on CVSS scores and potential impact. The project demonstrates effective use of Nessus for automated vulnerability management, helping enhance system hardening efforts and improve overall security posture through actionable remediation insights (LINK)

KEYLOGGER :

- The Python Keylogger project demonstrates how simple keystroke logging mechanisms can be implemented for educational and ethical testing purposes. A lightweight Python script was developed to record keyboard inputs and save them to a hidden log file. The script was then converted into a standalone .exe file using tools like PyInstaller, enabling easy execution on Windows systems.
-
- For testing purposes, the executable was transferred to a USB drive, simulating a scenario where the keylogger activates upon manual execution when the drive is plugged into a target system. This project highlights the importance of endpoint protection, USB monitoring, and user awareness to prevent unauthorized or malicious code execution (LINK)

CERTIFICATION

- Google Cybersecurity Professional Certificate
- LAHTP
- Certified Ethical Hacking (Nativeva)
- SOC Analyst learning path (letsdefend)
- Cybersecurity Thread Hunting
- Linux
- SQL

INTERNSHIP

- Priga solution (DevOps Intern) - **Sep 2023 – April 2024**
- The red users (Cyber security intern) – Oct 2024 – Nov 2024
- Future intern (Cyber security intern) – Oct 2024 – Nov 2024

TECHNICAL SKILLS:

- **Networking:** OSI model | TCP/IP | VLAN | Routing | Switching | Firewall | Load Balancer | VPN
- **SOC :** SIME tool | Wazuh | Malware Analysis | IDS/IPS | Wireshark | Log Analysis | CTI
- **WEB Security :** Nmap | Nessus | Metasploit | OWASP TOP 10 | Burp Suite
- **Programming Skills:** Java | SQL | Python

AREA OF INTEREST

- Networking
- Penetration Testing
- Security Operation Center
- Endpoint Detection

ACHIEVEMENTS

- NCC Cadet at College days
- Pentathon 2024 CTF Competition
- Yukthy CTF Competition
- Ideathon 2024
- NSS Volunter
