NISHOK KUMAR S

SOC Analyst

CONTACT

6382422061

nishokkumarsrm@gmail.com

No:1/105 Gandhi Nagar, Periya Mathur, Chennai - 68

git\NISHOKKUMAR

PROFILE SUMMARY

I'm a driven professional looking for a workplace where I can **keep growing**, contribute to the organization's success, and work alongside **talented people**. I'm eager to **learn new skills**, share my ideas, and take on **challenges** that help me **explore more** in my field. My goal is to make a **real impact** and help the team achieve success

EDUCATION

2024 - 2026

PANIMALAR ENGINEERING COLLEGE

- M.E CSE 8.8

2020 - 2024

SRM VALLIAMMAI ENGINEERING COLLEGE

- B.E CSE 8.3

2018 - 2020

SKNS PMC Vivekananda Vidyalaya

- 12th 92%

SKILLS

- Red Hat (RHEL) | Ubuntu
- Network
- ELK Stack (SIEM)
- MITRE ATT&CK Framework
- Low-level Programming
- Forensic (The Sleuth Kit)
- Programming Language : C++, PHP, Python, Bash

LANGUAGES

- Tamil
- English
- Korean

PROJECT EXPERIENCE

Elastic SIEM Deployment & Secure Log Ingestion (ELK Stack | Ubuntu | Windows | SSL/TLS)

- Configured and deployed Elastic SIEM (ELK stack) on Ubuntu with Winlogbeat integration on Windows endpoints.
- Implemented two-way SSL/TLS between ELK and endpoints, ensuring encrypted and authenticated log transmission.
- Optimized log pipeline for centralized security monitoring, incident detection, and SIEM rule tuning.

Phishing Incident Analysis & Blue Team Reporting (Wireshark | IOC Enrichment | SANS Framework)

- Investigated a phishing email credential theft attack by analyzing malicious traffic in PCAP files using Wireshark.
- Extracted and enriched Indicators of Compromise (IOCs) with threat intel platforms (VirusTotal, AbuseIPDB, etc.) to assess impact.
- Authored a comprehensive Blue Team Incident Report aligned with SANS Incident Handler's Handbook, strengthening skills in Incident Response, Threat Hunting, and Forensics.

Malware Keylogger Development (C++ | Windows API Hooking | Obfuscation)

- Designed and implemented a custom Windows malware keylogger using API hooking techniques with advanced code obfuscation for evasion.
- Logged keystrokes securely into local files, leveraging multithreading and mutex synchronization to ensure stability.
- Enhanced expertise in Malware Analysis, Threat Simulation, Windows Internals, and secure coding practices.

Bash Automation Scripts Github