Nasarul Naseer

Cybersecurity Analyst
nasarulnaseer.career@gmail.com | +91-77368-82643 | Kochi, Kerala
Linkedin: linkedin.com/in/nasarulnaseer | Github: github.com/nasarul10

EXPERIENCE

HASHROOT | Linux Server Admin Intern
Apr 2025 – Jun 2025 | Kochi, Kerala

- Administered Linux servers (AlmaLinux, Ubuntu) across 15+ lab setups, deploying Apache/NGINX, SSL, virtual hosts, and firewalls in test environments.
- Migrated 10+ WordPress sites in test scenarios with DNS setup, database management (MySQL/MariaDB), backup restoration, and basic CMS hardening.
- Managed 25+ domain environments via WHM, cPanel, and Plesk, configuring AutoSSL, PHP settings, cron jobs, and resolving issues like 404s and mail/database errors.

CYBERCELL KOCHI CITY | Intern
Jan 2025 – Feb 2025 | Kochi, Kerala

- Assisted in disk imaging, log analysis, and malware investigation during cybercrime case evaluations.
- Supported incident response efforts by gathering and analyzing digital evidence related to real-world threats.

FREELANCE | Video Editor/ Content Creation
Aug 2019 – Oct 2025 | Kochi, Kerala

- Produced high-performing content for Instagram (800K+ followers) and YouTube (100K+ subscribers).
- Managed editing workflows and file security, ensuring timely and confidential content delivery.
- Implemented remote collaboration tools and resolved technical issues to maintain workflow uptime.

PROJECTS

CLOUD BASED SOC OPERATIONS & THREAT DETECTION
Tools used: VMware, Sliver C2, Windows 10, Ubuntu, Sysmon, LimaCharlie, YARA

- Designed and deployed a SOC Analyst home lab simulating real-world attacks using Sliver C2, with endpoint telemetry collection via Sysmon and LimaCharlie EDR.
- Developed and tested custom detection rules and YARA signatures for threat behaviors like LSASS dumping and shadow copy deletion.

SPLUNK DEPLOYMENT AND LOG MONITORING LAB
Tools used: Splunk Enterprise, Universal Forwarder, FortiGate VM, Apache2, VMware, SPL

- Built a log monitoring lab using Splunk Enterprise to ingest and analyze logs from Apache2 and FortiGate via Universal Forwarder and Syslog.
- Created custom indexes, field extractions, interactive dashboards, and scheduled alerts using SPL for real-time log analysis and anomaly detection.

EDUCATION

MG UNIVERSITY
Bachelor of Science in Cyber Forensics
Sep 2021 - Oct 2024 | Kochi, Kerala

DHSE
Higher Secondary in Computer Science
Jun 2019 - Mar 2021 | Kochi, Kerala

SKILLS

TOOLS
Splunk • LimaCharlie • Wireshark • Qualys • Nessus • VirusTotal • Docker • VMware

TECHNOLOGIES
Log Analysis • Threat Detection • Incident Response • Network Monitoring • Security Monitoring • SIEM & EDR Operations • Vulnerability Management • Automation • Server Management • System Hardening • Cloud Security • MITRE ATT&CK Framework

PLATFORMS
Linux • Windows • AWS EC2

SOFT SKILLS
Clear Communication • Analytical Thinking • Calm Under Pressure • Time Management • Attention to Detail • Team Collaboration • Adaptability & Learning

CERTIFICATIONS

- Certified SOC Analyst v1
- ISO/IEC 27001:2022 Lead Auditor
- Qualys Vulnerability Management
- Intro to Threat Hunting
- Google Cloud Cybersecurity (Expected 08/25)

INTERESTS

Home Lab Building • Internet Browsing • Music • Traveling