ANANDHU GIREESH

CYBER SECURITY ANALYST

anandhu45gireesh@gmail.com | www.linkedin.com/in/anandhu-gireesh-b39332322
Kerala,Kochil +91 8606636056

SUMMARY

Passionate Cybersecurity Analyst with foundational knowledge in SOC operations, malware analysis, and network security. Basic proficiency in ELK Stack, Splunk, and Sysmon. Strong understanding of Mitre Framework, OWASP Top 10, and network data flows. Adept at penetration testing, vulnerability assessment, and phishing email analysis. Known for analytical skills, adaptability, and excellent communication. Open to rotational shifts and working independently or as a team player.

TECHNICAL SKILLS

- Security Operations & Analysis- Malware Analysis, Phishing Email Analysis
- Tools- Basic knowledge of ELK Stack, Splunk, Wireshark, Tcpdump, Nmap, Metasploit, Burp Suite, Snort, Suricata, Lima Charlie ,FTK Imager,Yara,MISP Threat intelligence
- Network & Protocols- Understanding of network data flows, ports, and protocols
- Linux Fundamentals
- Frameworks & Standards- Mitre Framework, OWASP Top 10, GRC, Cloud Security, Active Directory (theoretical knowledge)

EDUCATION

MG University

BSc Cyber Forensics 2021-2024

CERTIFICATION

- Certified Ethical Hacker (EC Council) 2024-2027
- Certified Penetration Tester (RedTeam Hacker Academy)
- Certified Cyber Warrior (Hackingflix Academy)

SOFT SKILLS

- **Problem-Solving** - Ability to identify issues and develop effective solutions.
- **Adaptability** - Ability to quickly adapt to new technologies and changing environments.
- **Critical Thinking** - Skilled in analyzing situations and making informed decisions
- **Creativity** - Innovative in finding unique solutions to complex problems.
- **Empathy** - Understanding and addressing the needs and concerns of others.

ADDITIONAL INFORMATION

- **Languages:** English, Malayalam
- **Services:** National Service Scheme (NSS)
  Actively participated in community service activities and social initiatives under the National Service Scheme.Developed leadership,teamwork skills

PROJECTS

IDS/IPS Lab with Snort

- Implemented IDS/IPS: Successfully set up Snort in an Ubuntu environment,
- Configured and managed custom rules.
- Learned and applied actions such as drop, reject, log, and alert

Splunk Home Lab Setup

- Designed and implemented a basic Splunk home lab for monitoring and analyzing events.

ELK Home Lab Setup

- Developed an ELK stack home lab to gain hands-on experience with log analysis.

Phishing Email Analysis Lab

- Conducted analysis of phishing emails to identify and mitigate threats.

Lima Charlie EDR Setup

- Set up and configured Lima Charlie for endpoint detection and response