MONISHA M R

+91 9148105876 ◇ monishamr27@gmail.com ◇ linkedin.com/in/monisha-m-r ◇ GitHub

OBJECTIVE

Seeking to join a dynamic SOC team where I can apply my knowledge of network protocols, SIEM tools, and incident response processes to detect, analyze, and contain cyber threats in real time.

EDUCATION

Dayananda Sagar College of Engineering, Bengaluru 2021 - 2025
Bachelor of Engineering in Electronics and Telecommunication, **CGPA: 8.88**

TECHNICAL SKILLS

- **Networking & Security:** TCP/IP, DNS, DHCP, Firewalls, VPN, IDS/IPS
- **SOC Processes:** Monitoring, Log Analysis, Incident Playbooks, Reporting
- **Frameworks:** MITRE ATT&CK, Cyber Kill Chain
- **Tools:** Splunk, Microsoft Defender, Any.run, Barracuda, Zscaler, ServiceNow, Code42, Nessus, AWS

INTERNSHIP & TRAINING

Cybersecurity & Ethical Hacking Intern Jan 2025 – Apr 2025
Robomanthan Pvt Ltd *Remote*

- Conducted reconnaissance and threat intelligence gathering using **Whois, VirusTotal, and OSINT tools**.
- Executed phishing simulations with **SET** and analyzed malicious email indicators for detection insights.
- Performed system hacking simulations using **Kali Linux** and **Metasploit**, including exploitation of **MS17-010 (EternalBlue)**.

Security Analyst Trainee May 2025 – Jul 2025
SOC Experts Training Institute Bengaluru, India

- Monitored and analyzed simulated alerts in **Splunk** to detect and respond to security incidents.
- Investigated phishing and malware threats using **Barracuda Email Gateway** and **Any.run sandbox**.
- Applied **Code42 DLP** for data exfiltration prevention and conducted vulnerability assessments using **Nessus**.
- Monitored cloud security events and threats in **AWS** environments.
- Gained knowledge of various cyberattack types, including malware, brute force attacks, and other common threat techniques.

PROJECTS

Phishing Email Simulation using SET 2025

- Simulated phishing attacks using the **Social Engineering Toolkit (SET)** in Kali Linux within a controlled lab setup.
- Crafted phishing emails with spoofed senders and malicious links to study delivery methods and detection points.
- Identified phishing indicators such as suspicious headers, attachments, and redirect links.
- Analyzed detection methods of security tools to prevent phishing attacks.

System Hacking using Kali Linux and Metasploit Framework 2025

- Conducted system hacking simulation on a Windows 7 VM using **Kali Linux** and **Metasploit Framework**.
- Performed **Nmap scanning** to identify open ports and fingerprint the target operating system.
- Exploited the **MS17-010 (EternalBlue)** vulnerability to gain unauthorized access.
- Demonstrated understanding of **penetration testing lifecycle** – reconnaissance, exploitation, and post-exploitation.

CERTIFICATIONS

- Certified Ethical Hacking Fundamentals – Coursera, 2025
- SOC Analyst Training – SOC Experts Training Institute, 2025