NIHAL HASAIN C

Cybersecurity Intern | SOC Analyst

Bengaluru| +91 9048652406 |nihalcheer@gmail.com|linkedin.com/in/nihalhasain-c | Portfolio

PROFESSIONAL SUMMARY

Entry-level SOC Analyst with hands-on experience in log analysis, network traffic monitoring, phishing detection, VPN and DNS analysis, and endpoint security. Skilled in SIEM tools (Splunk), Wireshark, Nmap, Windows Defender Firewall, and email header analysis. Strong foundation in networking, Windows security, and incident investigation workflows. Actively seeking a SOC L1 role to contribute to real-time threat detection and response.

EDUCATION

Bachelor of Computer Applications (BCA) Bengaluru North University **2023 – 2026**

Higher Secondary Education GMHS Perinthalmanna **2021 – 2023**

TECHNICAL SKILLS

- **SOC & Security Operations**: Log analysis and alert triage, phishing detection and email header analysis, basic incident investigation and reporting, SIEM fundamentals and log correlation concepts.
- **Networking & OS Security**: TCP/IP, IPv4/IPv6, ports and common protocols, network connectivity testing and port analysis, Windows OS security fundamentals, basic Linux security exposure (Kali Linux).
- **Security Tools**: Splunk, Wireshark, Nmap, Netstat, Windows Defender Firewall, MXToolbox, DNS leak testing tools, VPN clients (Windscribe).

CERTIFICATIONS

- **Google Cybersecurity Professional Certificate**
- **IBM Cybersecurity Certificate**
- **Tata Cybersecurity Analyst Virtual Experience – Forage**
- **Mastercard Cybersecurity Virtual Experience – Forage**

EXPERIENCE

Cyber Security Intern | Elevate Labs **November 2025 – December 2025**

- Analyzed network traffic using Wireshark (DNS, TCP, TLS, HTTP).
- Performed basic network scanning and port analysis using Nmap.
- Conducted VPN and DNS leak testing to understand privacy and encryption.
- Analyzed phishing emails using header inspection and MXToolbox.
- Reviewed browser extensions to identify potential security risks.
- Worked with Windows Defender Firewall for basic system hardening.
- Used Splunk for basic log analysis and security event understanding.
- Developed a password security toolkit project.

SOC LABS & HANDS-ON PRACTICE

- Hands-on experience with Nmap, Wireshark, OWASP ZAP, Burp Suite, Nessus, and Splunk through structured labs.
- Performed manual web application testing including SQL injection authentication bypass and logic flaw analysis.
- Conducted SIEM-based log analysis using Splunk with SPL searches and dashboards.
- Analyzed Windows system and security logs to identify and classify security events.
- Practiced vulnerability scanning, network traffic analysis, and incident investigation workflows.

PROJECTS

PassIntel – Password Security Toolkit

- Built a password security tool that analyzes password strength, estimates crack time, demonstrates password-guessing techniques, and generates custom wordlists to highlight real-world attack methods.
- Designed for cybersecurity learning, the tool works offline and helps users understand and defend against common password attacks.