

Md. Mahim Hossain

📍 Dhaka 📩 faaiz.mahim@gmail.com 📞 +880 18669-28533 💬 mahimsec 🌐 mahimsec

Professional Summary

I am a learner SOC Analyst Level 1, focusing on cybersecurity and basic networking for security. I am building my skills in threat detection, incident response, and security operations.

My goal is to grow as a SOC Analyst, work in Blue Team roles, and become a Security Engineer in the future. I am always learning and improving to stay prepared for new challenges in cybersecurity.

Education

BSc	Green University of Bangladesh , Computer Science Engineering	Feb 2022 – Feb 2026

30 Days SOC Challenge

Aug 2025

Completed a month-long SOC challenge covering practical modules:

- Linux Log Analysis — system log triage and anomaly detection.
- Wireshark — packet capture, protocol analysis, and traffic inspection.
- Wazuh SIEM — agent enrollment, alerting, and detection rule testing.
- Splunk SIEM — log ingestion, search queries, and dashboarding for threat detection.
- Phishing Analysis — email header analysis, link forensics, and IOC extraction.

Thesis

NeuroCrypt: A Secure Framework for Brain-Computer Interface Data Sharing

2025 – Present

Status: Ongoing

Description: Our research focused on developing a secure and privacy-preserving framework for sharing brain-computer interface (BCI) data.

Projects

Transaction System

Nov 26 , 2023

Shell-based transaction system for managing student payments.

Tools: Bash, Linux Terminal

Encryption and Decryption

Apr 17 , 2024

Implemented Caesar Cipher encryption/decryption in Assembly Language.

Tools: EMU8086

Student Admission Management System

Jun 28, 2024

Web system for managing student admissions including inquiry, application, and tracking.

Tools: HTML, CSS, Bootstrap, PHP, MySQL

Basic Network Sniffer

Sep 15, 2025

Developed a simple network sniffer for packet capture and analysis.

Tools: Python (Scapy/pcap), Wireshark

Wazuh SIEM Deployment

Sep 15, 2025

Successfully deployed and configured a Wazuh Server and Agent on a local host.

Implemented a robust security framework by configuring File Integrity Monitoring (FIM).

Tools: Wazuh,linux OS

Technical Skills and Interests

Languages: Python, C/C++, Java, Bash, JavaScript, HTML/CSS

Libraries/Packages: C++ STL, ReactJS

Frameworks/Platforms: Flask, Zero Trust, NIST, Cyber Kill Chain, ATT&CK, Docker

Cybersecurity Tools: Wazuh, Snort, Suricata, Wireshark, Nmap, Zeek, Maryam (OSINT), TryHackMe Labs, HTB Labs

Monitoring & Logging Stack: Elasticsearch, Filebeat

Cloud/Databases: Firebase, MySQL, SQLite

Development Tools: Git, GitHub, VSCode, Burp Suite, VMware, VirtualBox

Areas of Interest: SOC Operations, Defensive Security, Real-Time Anomaly Detection, Zero Trust Architecture

Soft Skills: Problem Solving, Self-Learning, Research, Teamwork, Adaptability