Mridul Gharami

+918972202991 | Email | Linkedin | Github | Portfolio | Twitter

SUMMARY:

Aspiring cybersecurity engineer with a passion for building secure systems, analyzing threats, and turning code into real-world protection.

TECHNICAL SKILLS:

- **Programming Languages:** C, Python, Java, Bash, Batch, PowerShell, HTML/CSS
- **Frameworks:** NIST CSF, MITRE ATT&CK, ISO/IEC 27001, Zero Trust, CIS Controls, GDPR, PCI-DSS
- **Operating Systems:** Windows System, Linux
- **Tools & Libraries:** Npcap, WinPcap, Git, Visual Studio, MinGW, Crypt32, ws2_32, Vim, Burp Suite, Metasploit, Nessus, John the Ripper, Nikto, Aircrack-ng, Hydra, Splunk, Snort.
- **Cloud:** AWS(VPC, Subnets, EC2, Security Groups, Internet Gateway, Route Table)
- **Other Skills:** CLI Tools Development, Secure File Management, Malware Analysis

EXPERIENCE:

Intern - Academy of Skill Development | April 2025 – June 2025

- Participated in hands-on cybersecurity training sessions covering ethical hacking, system hardening, and network security fundamentals.
- Assisted in analyzing simulated malware samples and identifying vulnerabilities in test environments.
- Collaborated with mentors to build beginner-level Capture The Flag (CTF) challenges for workshops.

PROJECTS:

[Link] SENTINAL_OS

Tech Stack: C, WinAPI, Npcap, SHA-256, Windows internals

- SENTINAL_OS is a lightweight, Windows-based Network Intrusion Detection and Process Monitoring System. Designed for cybersecurity enthusiasts and professionals, it combines real-time network packet sniffing with advanced process monitoring to help detect and mitigate threats on Windows systems. The system features a modular design with components for packet capture,

blacklist enforcement, SYN/UDP flood detection, port scan detection, and process integrity verification using SHA-256 hashes. It leverages Npcap for low-level packet capture and includes a thread-safe logging system for detailed event tracking.

[Link] AWS VPC & EC2 Deployment

Tech Stack: Cloud AWS

- This project demonstrates the setup of a secure, browser-accessible web server on AWS using a custom Virtual Private Cloud (VPC), Subnet, Internet Gateway, Route Table, and EC2 instance. The entire infrastructure was deployed using AWS Free Tier resources and configured with Apache and custom Security Groups. All steps are fully documented with screenshots and diagrams.

[Link] Blockchain-Backed Messaging

Tech Stack: Python, Socket Programming, SSL/TLS, Multithreading, Hashlib (SHA-256), JSON, OpenSSL

- A secure messaging system that leverages blockchain technology to ensure message integrity and prevent tampering. Each message is cryptographically signed and recorded on a blockchain ledger, providing a verifiable, immutable history of communication. The system is designed with end-to-end encryption, decentralized trust, and auditability in mind, making it ideal for sensitive or high-assurance environments.

EDUCATION:

University of Calcutta, kolkata | Bachelor's Degree in Computer Science | GPA - 7.6/10 (~76%) | July 2023 - Present