Ashit Mallick

+91-9555217020| airdevil2003@gmail.com | linkedin.com/in/ashit-mallick-a7a386250 | github.com/Wingedarrows03 |

TECHNICAL SKILLS

- **Programming & Scripting Languages:** C++, Python3, Bash
- **Security Tools & Technologies:** Linux, , Git, GitHub, Burp Suite, Nmap, SQL-map, Sherlock, Recon - ng, Wireshark, AWS (EC2, IAM, S3), MySQL, DynamoDB
- **Core Knowledge:** Pentesting, Cryptography, OWASPTop 10, Vulnerability Management, Malware Analysis, Incident response, Networks

PROJECTS

RakshaChakra— User Authentication , ML based anamoly detection, AWS, Docker — [GitHub] **Jul 2025**

- Engineered a secure authentication protocol leveraging Firebase Realtime Database, ensuring robust (MFA) multi-factor user verification and strict data privacy.
- Enforced a strict data privacy model by implementing robust encryption-at-rest for all sensitive PII (Personally Identifiable Information), both within the backend database and in the application's local storage, ensuring data is cryptographically secured and inaccessible to unauthorized parties.
- Deployed and managed a scalable machine learning pipeline on AWS Elastic Beanstalk , enabling real-time, behavior-based fraud detection to secure financial transactions.
- Hardened the application's security posture by integrating an ML-driven anomaly detection engine that analyzes real-time phone sensor data (e.g., accelerometer, gyroscope) to generate a dynamic security score and flag potentially compromised sessions.

TIFA (**Threat Intelligence Feed Aggregator**)— Python, Security Dashboard , Gradio , SQLite— [GitHub] **Aug 2025**

- Developed an AI-driven Threat Intelligence Platform using the Google Gemini API to aggregate, de-duplicate, and unify over 5 real-time threat feeds (including US-CERT and SANS) onto a centralized dashboard. This system provides 95% accurate threat classification , delivering high-fidelity, actionable intelligence to support Security Operations Center (SOC) analysts.
- Engineered a high-throughput, regex-based automation system to parse unstructured threat data, successfully extracting and categorizing more than 8 distinct types of Indicators of Compromise (IoCs), such as IP addresses, domains, and file hashes. .
- Implemented a configurable analysis engine designed for automated severity assessment of incoming threats, allowing analysts to prioritize high-risk alerts efficiently.
- Built a scalable backend architecture using Python and SQLite to manage the continuous influx of threat data, powering a responsive Gradio web dashboard that enables real-time threat visualization, interactive analysis, and automated data refresh cycles.

ACHIEVEMENTS & CERTIFICATIONS

- **Canara Bank Hackathon '25:** Achieved Top 105 placement nationally out of more than 4,000 participants, showcasing competitiveness and technical proficiency.
- **Societet General Hackathon:** Secured 4th place and achieved a finalist position among competing teams, demonstrating strong problem-solving and development skills in a high-pressure environment.
- **Cyber Shakti CTF (Indian Army):** Successfully captured 3 out of 4 flags in the national-level cybersecurity competition, demonstrating practical offensive security and penetration testing skills.
- **Technical Writing:** Authored a high-impact technical blog post detailing malware analysis, including classifications (e.g., viruses, worms, ransomware), infection vectors, and operational mechanics.

EDUCATION

Vellore Institute of Technology, Bhopal **Aug 2022 – Jun 2026**

Bachelor of Technology (B.Tech), Computer Science and Engineering *CGPA: 8.2/10.0*