V GREESHMA GOWDA

CYBER SHIELD

A Comprehensive Cyber Security Suite

LinkedIn: https://www.linkedin.com/in/greeshmagowda06

GitHub: https://github.com/greeshmagowda06/Cyber-Shield

Abstract

Cyber Shield is a consolidated collection of practical cybersecurity projects that progressively explore network defense, data protection, digital forensics, and AI-driven threat detection.

The suite is divided into Basic, Intermediate, and Advanced levels, each targeting specific areas such as encryption, steganography, intrusion detection, vulnerability scanning, and secure communication.

Objectives

- Understand the fundamentals of encryption, authentication, and secure communication.
- Implement and simulate real-world cybersecurity mechanisms.
- Detects and prevents potential cyber threats using AI and automation.
- Build practical, ethical cybersecurity tools for research and learning.

Project Structure

The **Cyber Shield** project is divided into four main sections — Basic, Intermediate, Advanced, and Hack Defense — each focusing on a different level of cybersecurity implementation.

The **Basic Projects** include the Firewall Log Analyzer, which reads and analyzes firewall logs to detect suspicious activity; the Password Strength Checker, which validates password security; the Phishing URL Detector, which identifies phishing links; and the Simple Port Scanner, which scans systems for open ports to assess network exposure.

The **Intermediate Projects** cover tools like the File Encryption & Decryption Tool for secure file storage, the Keylogger Detector for identifying unauthorized keylogging, the Malware Hash Checker for verifying files against known malware signatures, and the Network Packet Sniffer for capturing and analyzing live network data.

The **Advanced Projects** demonstrate higher-level cybersecurity mechanisms such as the Brute Force Attack Simulator, which safely mimics password attacks; the Intrusion Detection System (IDS), which monitors and flags network anomalies; the Secure Chat Application, which enables encrypted messaging using AES/RSA; and the Web Vulnerability Scanner, which detects common website vulnerabilities like SQL Injection and XSS.

Finally, the **Hack Defense (Research & Innovation)** section explores advanced and research-oriented tools, including the Blockchain-Based File Verifier for integrity tracking, the Dark Web Crawler for safe metadata collection via Tor, the Digital Forensics Analyzer for extracting file evidence, the AI Network Intrusion Detector and Phishing Email Classifier for machine learning–based threat detection, and the Password Vault, Sandbox Behavior Monitor, and Steganography Tool for encryption, behavioral analysis, and data hiding respectively.

Automated Recon Scanner

Performs automated reconnaissance on target domains by scanning ports, headers, sub-domains, and SSL info, producing structured reports in JSON/CSV format.

Technologies Used

- Language: Python 3
- Key Libraries: `cryptography`, `pillow`, `scikit-learn`, `pandas`, `psutil`, `requests`, `stem`, `exifread`, `flask`
- Tools & Environments: Visual Studio Code, Virtual Env, Tor, Git

Ethical Guidelines

All code is intended **strictly for educational and ethical research.** Do not deploy or test against external systems without authorization. Always comply with cybersecurity laws and responsible disclosure policies.