LEWIS (Linux Environment Working Intelligence System)

AI-Powered Cybersecurity Assistant for Ethical Hackers

Overview

LEWIS is an advanced, self-learning AI cybersecurity assistant built to automate, analyze, and enhance the ethical hacking workflow. Designed for use in Termux with Kali NetHunter, LEWIS integrates AI, Machine Learning, voice/command interfaces, and real-time tool execution with a beautiful, customizable web UI.

LEWIS acts as a hacker's digital partner, capable of understanding natural language queries, generating and executing scripts, analyzing security logs, and visualizing threats — all while constantly learning and improving itself.

Core Capabilities

Technical Features

AI Engine using transformers, openai, and NLP libraries

Real-time execution of system and network tools

Flask backend API and React frontend with a dark hacker UI

Voice recognition and TTS using SpeechRecognition + pyttsx3

Graph-based threat visualization via matplotlib

Custom commands and logs in SQLite

Configurable themes, permissions, and tool paths

Modular design — extend or replace any component easily

File Structure

```
/lewis/
├── core/               # AI Engine, Voice Control, Command Handler
├── web-ui/             # Web Frontend (React) + Flask API
├── security_tools/     # Wrappers for Nmap, Nikto, Metasploit
├── ml_models/          # ML models for threat detection
├── datasets/           # Training logs and pattern data
├── config/             # YAML config, command list, themes
├── database/           # SQLite DB and setup SQL
├── scripts/            # Setup for Termux and Kali
├── lewis-cli.py        # Terminal entry script
├── main.py             # Program entry point
├── requirements.txt    # Python dependencies
├── Dockerfile          # Containerized setup (optional)
```

Usage Examples

"Scan this IP and tell me open ports" → Translates to Nmap, runs scan, visualizes ports.

"Generate script to brute force FTP login" → Returns script with optional execution.

"What’s the summary of my last 10 logs?" → Analyzes logs and gives threat insights.

Voice Command: “Start Nikto scan on 192.168.0.1” → Executes tool and logs results.

Platform Compatibility

Primary: Termux + Kali NetHunter

Secondary: Linux Servers / Containers

Optional: Docker deployment for cross-platform use

Future Add-ons

Cloud sync with Zehra Sec backend

Real-time threat alert system

Integrated phishing kit detection

Chatbot deployment on Telegram/WhatsApp