MANIPAL INSTITUTE OF TECHNOLOGY
MANIPAL
(A constituent unit of MAHE, Manipal)

Information Security Lab – ICT 3141

Project Synopsis – AI-Powered Penetration Testing Toolkit

Overview

This project aims to build an AI-assisted penetration testing platform that integrates open-source security tools with a locally running AI model. The AI acts as a virtual penetration tester, assisting in planning, executing, and interpreting security assessments. The platform will automate reconnaissance, scanning, exploitation, encryption of sensitive results, and reporting workflows.

Objectives

- Integrate AI with industry-standard penetration testing tools to enhance efficiency.
- Automate vulnerability identification, exploitation suggestions, and reporting.
- Enable offline/local AI processing for privacy and security.
- Secure all stored and transmitted results using AES-256 encryption.

Core Tools Used

1. **Kali Linux** – Primary penetration testing environment.
2. **OWASP ZAP** (Zed Attack Proxy) – Web application vulnerability scanning.
3. **Burp Suite** (Community Edition) – Manual and automated web security testing.
4. **Ettercap** – Network sniffing and man-in-the-middle attack simulations.
5. **Hydra** – Password cracking and brute-force attack tool.
6. **Nmap** – Network scanning and host discovery.
7. **SQLMap** – Automated SQL injection and database exploitation.
8. **MSFvenom** – Payload generation for penetration testing.

Key Features

AI & Automation

- **AI-Assisted Security Scanning** – Automatically generates optimal pentesting strategies.
- **Command Recommendation Engine** – AI suggests precise tool commands based on target and context.

- **Tool Output Analysis** – AI interprets results from scanners and suggests next actions.
- **Offline Local AI** – Powered by Llama 3, GPT4All, or PentestGPT for zero internet dependency.

Security & Data Handling

- **AES-256 Encryption** – All reports, logs, and sensitive outputs are encrypted before storage.

User Interface & Experience

- **Unified Dashboard** – Launch, control, and monitor all tools from one place.
- **Real-Time Log Viewer** – See live output from running tools without switching consoles.
- **Interactive Target Manager** – Easily add, configure, and switch between targets (e.g., DVWA, custom IPs).

Workflow & Integration

- **Built-in DVWA Integration** – Practice safely inside a controlled vulnerable environment.
- **Multi-Target Testing** – Scan multiple hosts or apps simultaneously.
- **Session Save & Resume** – Store current tests and continue later without re-scanning.
- **Auto-Generated Threat Models** – AI integrates Microsoft Threat Modeling for attack surface mapping.

Tech Stack

- **Backend** : Node + Express
- **Frontend** : Electron – User dashboard & visualization.
- **Database** : SQLite / PostgreSQL – Encrypted data storage using AES-256.
- **AI Engine** : Local LLM (Llama 3, GPT4All, PentestGPT).
- **Containerization** : Docker – Isolated environments for tools like DVWA or other targets.
- **OS** : Kali Linux – Base OS for pentesting tools.
- **Security Libraries** : pycryptodome (Python AES encryption), HTTPS-enabled communication.

Submitted by :-

• Aditanshu Sahu (230953444)
• Suniket Sen (230953372)
• Lakshya Agarwal (230953416)