Trojan Horse Simulation – Project Report

1. Overview

This project demonstrates simulated Trojan malware behavior in a safe laboratory environment.

It includes keylogging, DLL injection, and reverse shell execution, along with full defensive detection workflows.

2. Keylogging Module

The keylogger captures keystrokes using keyboard event hooks and stores them locally for analysis.

3. DLL Injection Simulation

Simulated DLL injection using Windows API functions such as VirtualAllocEx, WriteProcessMemory, and CreateRemoteThread.

4. Reverse Shell Simulation

A controlled local reverse shell environment that allows command execution strictly within the VM.

5. Detection Workflow

The project uses:

- Sysmon for event logging

- Process Explorer for DLL inspection

- Wireshark for traffic monitoring

- Windows Defender for behavioral alerts

6. Outcomes

This project provides hands-on experience in offensive security techniques and defensive monitoring, helpful for VAPT, SOC, and Incident Response roles.

7. Disclaimer

This simulation is for educational and research purposes only and must be run in a controlled VM environment.