1. Project Overview

Short Description:

This project aims to develop a comprehensive Ransomware Analysis and Defense System that identifies, analyzes, and mitigates various types of ransomware threats. The system will utilize multiple methodologies to simulate ransomware attacks, analyze their behavior, and implement defense mechanisms. The project will provide insights into the working mechanisms of ransomware while equipping users with tools to protect against these threats.

Working Method and Usage:

The project will involve setting up a controlled environment where different types of ransomwares can be executed safely for analysis. Users will be able to observe the behavior of ransomware, understand its encryption methods, and evaluate defense strategies. The system will also include educational components to inform users about ransomware threats and best practices for prevention.

2. Methodology

A. Attack Simulation

Sample Example: Crypto Ransomware Simulation

- **Description**: A controlled execution of a crypto ransomware variant (e.g., WannaCry) in a virtual environment to observe its file encryption process.
- **Objective**: To analyze how the ransomware encrypts files and demands ransom.

B. Defense Mechanism Implementation

Sample Example: Antivirus Software Deployment

- **Description**: Implementing an antivirus solution that detects and quarantines ransomware before it can execute.
- **Objective**: To demonstrate effective defense strategies against ransomware attacks.

C. Behavior Analysis

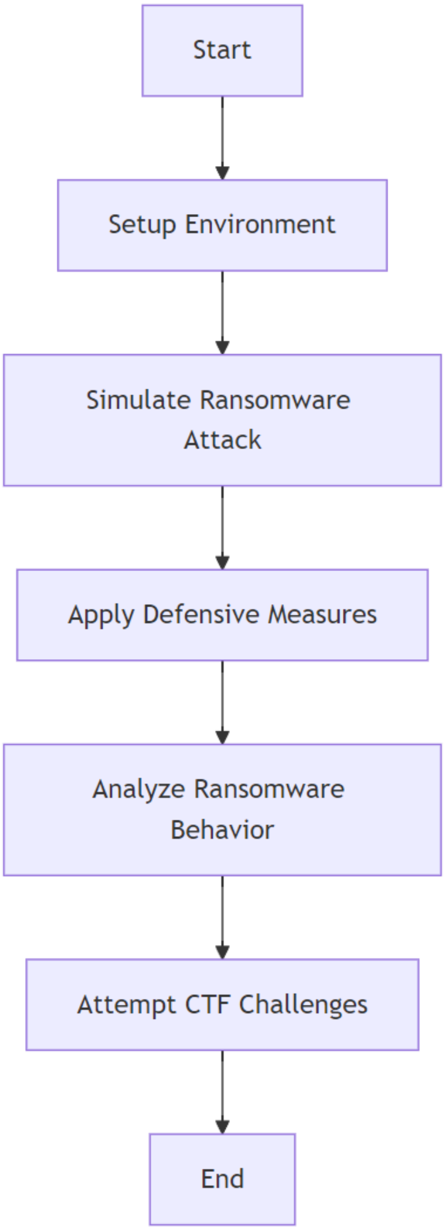
Sample Example: Network Traffic Monitoring

- **Description**: Utilizing tools like Wireshark to capture and analyze network traffic generated by the ransomware during its execution.
- **Objective**: To understand the communication patterns of ransomware with command-and-control servers.

3. Project Working Model

Workflow Steps:

1. **Setup and Initialization**:
   - Install the OS on a virtual machine.
   - Configure an isolated environment to prevent real-world risks.
2. **Attack Simulation**:
   - Execute ransomware samples to understand attack vectors.
3. **Defense and Mitigation**:
   - Use tools for detection, prevention, and recovery.
4. **Analysis**:
   - Perform static, dynamic, and network analysis on ransomware payloads.
5. **CTF Challenges**:
   - Solve challenges to identify infections, reverse encryption, and recover files


Start
Setup Environment
Simulate Ransomware Attack
Apply Defensive Measures
Analyze Ransomware Behavior
Attempt CTF Challenges
End

3. System and Hardware Requirements

Development Environment Requirements:

- **Operating System:** Ubuntu 22.04 or Debian-based distribution.

Recommended Hardware:

  - CPU: Quad-core processor or higher
  - RAM: 16 GB or higher
  - Storage: 100 GB SSD
  - Network: Stable internet connection for testing tools

User Requirements (Virtual Machine):

- **Minimum Requirements:**
  - VirtualBox or VMware installed
  - CPU: 2 cores assigned to VM
  - RAM: 4 GB allocated to VM
  - Storage: 20 GB allocated to VM
- **Maximum Requirements:**
  - CPU: 4 cores assigned to VM
  - RAM: 8 GB allocated to VM
  - Storage: 50 GB allocated to VM