# Ethical Hacking Educational Tool Documentation

## Introduction

This script provides an educational tool for ethical hacking, enabling users to perform various tasks such as port scanning, file encryption and decryption, XDR analysis, and remote code execution (RCE). It utilizes the Tkinter library to create a graphical user interface (GUI).

## Installation

Ensure that Python 3.x is installed on your system along with the cryptography library. The cryptography library can be installed using the following command:  
 pip install cryptography

## Features

### XDR Analysis

The script includes a simulated XDR (Extended Detection and Response) capability, which performs basic analysis by displaying a message about network traffic and server logs.  
Function: xdr\_analysis()

### Port Scanner

The port scanner checks common ports on a target IP address to determine which ones are open. It uses the socket library to perform connection attempts.  
Function: scan\_ports()

### File Encryption

This feature allows the user to encrypt a file using symmetric encryption provided by the cryptography library. An encryption key is generated at runtime.  
Function: encrypt\_file()

### File Decryption

The file decryption feature decrypts files that were encrypted using the encryption function. The decryption process uses the same encryption key.  
Function: decrypt\_file()

### Remote Code Execution (RCE)

The RCE feature allows the user to execute shell commands on the local machine. It uses the subprocess library to run commands and capture the output.  
Function: remote\_code\_execution()

## GUI Layout

The GUI is built using Tkinter. It features input fields for target IP address, file path, and RCE command, as well as buttons to trigger each function. The output of each function is displayed in a scrolled text box.

## Usage

To use the tool, run the script. Enter the necessary inputs in the respective fields and click the appropriate button to execute the desired function. The results will be displayed in the output text box.

## Security Considerations

Since this tool includes functionalities like remote code execution and file encryption/decryption, it should be used responsibly and only in controlled environments. Unauthorized use may result in security risks.

## Additional Features

### Dark Theme GUI

The GUI of the tool uses a dark theme with a black background and lime green text. This enhances readability and reduces eye strain during extended use.

### Scrolled Text Output

The tool uses a scrolled text widget to display the output of each function. This ensures that large outputs can be easily viewed and scrolled through by the user.

### File Dialog Integration

The file encryption and decryption functions include a file dialog feature. If the user does not provide a file path, they can use the file dialog to select a file.

## Use Cases with Step-by-Step Instructions

### 1. Port Scanning

Port scanning is used to check for open ports on a target machine.  
Steps:  
1. Enter the target IP address in the 'Target IP Address' field.  
2. Click the 'Scan Ports' button.  
3. The output will display the open ports or a message indicating no open ports.

### 2. File Encryption

File encryption secures a file by converting its contents into an unreadable format.  
Steps:  
1. Enter the file path in the 'File Path' field or click the 'Encrypt File' button to open a file dialog.  
2. Select the file to be encrypted.  
3. The output will display a message indicating the file has been encrypted and saved.

### 3. File Decryption

File decryption restores an encrypted file to its original readable format.  
Steps:  
1. Enter the file path in the 'File Path' field or click the 'Decrypt File' button to open a file dialog.  
2. Select the encrypted file (must have the '.encrypted' extension).  
3. The output will display a message indicating the file has been decrypted and saved.

### 4. XDR Analysis

XDR analysis simulates an extended detection and response process.  
Steps:  
1. Enter the target IP address in the 'Target IP Address' field.  
2. Click the 'XDR Analysis' button.  
3. The output will display a message simulating the XDR process.

### 5. Remote Code Execution (RCE)

RCE allows the user to execute shell commands on the local machine.  
Steps:  
1. Enter the target IP address in the 'Target IP Address' field.  
2. Enter the command to be executed in the 'Command for RCE' field.  
3. Click the 'Execute Command (RCE)' button.  
4. The output will display the result of the command execution.