**Lockphish: Phishing Attack Tool Documentation**

**Aim**

The aim of this project is to explore and understand the functionality of **Lockphish**, a phishing attack tool designed to simulate phishing scenarios and demonstrate the risks associated with credential theft through social engineering.

**Introduction**

Lockphish is a widely known phishing tool that enables the creation of fake login pages to trick users into revealing their credentials. The tool is often used for educational purposes to simulate phishing attacks and raise awareness about cybersecurity threats. Lockphish supports phishing simulations for lock-screen credentials on platforms like Windows, macOS, and Linux.

**Key Features**

1. **Phishing Simulation**: Generates fake lock-screen credential pages to simulate phishing attacks.
2. **Cross-Platform**: Simulates phishing pages for Windows, macOS, and Linux systems.
3. **Easy Setup**: Minimal configuration required to deploy fake credential pages.
4. **Cloud Integration**: Uses Ngrok or Serveo to make the phishing pages accessible over the internet.
5. **Credential Capture**: Captures and displays login credentials entered by the victim.

**Setup Instructions**

1. **Install Prerequisites**:
   * Update your system: sudo apt update && sudo apt upgrade
   * Install Git: sudo apt install git
   * Install Python 3: sudo apt install python3
   * Install Ngrok: Download from the [official site](https://ngrok.com/).
2. **Clone Lockphish Repository**:
   * git clone https://github.com/thelinuxchoice/lockphish.git
3. **Navigate to Lockphish Directory**:
   * cd lockphish
4. **Run Lockphish**:
   * bash lockphish.sh
5. **Provide Ngrok Token**:
   * If required, authenticate your Ngrok account and provide the token.

**Working Principle**

1. **Generating Fake Pages**:
   * Lockphish creates a fake lock-screen page mimicking legitimate platforms (Windows, macOS, Linux).
2. **Hosting via Ngrok or Serveo**:
   * The tool uses Ngrok or Serveo to expose the phishing page to the victim over the internet.
3. **Capturing Credentials**:
   * When victims enter their credentials on the fake page, Lockphish captures and displays them in real-time.
4. **Credential Storage**:
   * Credentials are logged for analysis and reporting purposes.

**Steps to Use Lockphish**

1. **Run the Script**:
   * Execute the lockphish.sh script from the cloned directory.
2. **Select Options**:
   * Choose the lock-screen platform to simulate (Windows, macOS, or Linux).
3. **Share the URL**:
   * Copy and share the Ngrok-generated link with the target (for educational purposes only).
4. **Monitor Activity**:
   * Observe captured credentials in the terminal as victims interact with the page.

**Applications**

1. **Educational Awareness**: Simulates phishing attacks to educate users on identifying phishing attempts.
2. **Security Training**: Helps organizations train employees on social engineering attacks.
3. **Research**: Allows researchers to study the effectiveness of phishing techniques.
4. **Ethical Hacking Demonstrations**: Demonstrates phishing attack vectors in controlled environments.

**Sample Use Case**

**Scenario**: Demonstrating a phishing attack for educational purposes.

1. Clone the Lockphish repository.
2. Generate a fake lock-screen page mimicking a Windows login.
3. Share the phishing link with test users in a controlled lab environment.
4. Capture credentials entered by test users and highlight vulnerabilities.

**Ethical Guidelines**

* Obtain **explicit permission** before testing Lockphish in any environment.
* Use only for **educational** or **authorized penetration testing** purposes.
* Do not deploy on public networks or target individuals without consent.

**Conclusion**

**Lockphish** is a powerful tool for understanding the risks of phishing attacks. By simulating realistic phishing scenarios, it helps raise awareness about credential theft and reinforces the importance of cybersecurity practices. It serves as a valuable resource for security professionals, researchers, and educators working to combat phishing threats.