InSkill-3

Step 1: Install King Phisher

1. **System Requirements**:
   - King Phisher is compatible with Linux distributions such as Kali Linux, Ubuntu, or Debian.
   - Ensure that you have `Python 3.7+` and `PostgreSQL` installed.
2. **Install Dependencies**:
   - Install required dependencies:

     ```
     sudo apt update
     sudo apt install python3 python3-pip python3-venv libpq-dev
     postgresql
     ```

3. **Clone the King Phisher Repository**:
   - Download the King Phisher source code from GitHub:

     ```
     git clone https://github.com/securestate/king-phisher.git
     cd king-phisher
     ```

4. **Set Up a Python Virtual Environment**:
   - Create and activate a Python virtual environment:

     ```
     python3 -m venv venv
     source venv/bin/activate
     ```

5. **Install King Phisher**:
   - Install King Phisher and its dependencies:

     ```
     python3 -m pip install -r requirements.txt
     ```

6. **Set Up the Database**:
   - King Phisher uses PostgreSQL. Set it up with:

     ```
     sudo -u postgres createuser king_phisher
     sudo -u postgres createdb king_phisher
     sudo -u postgres psql
     ```

   - In the PostgreSQL prompt, set the password:

     ```
     sql
     Copy code
     ALTER USER king_phisher WITH ENCRYPTED PASSWORD 'yourpassword';
     GRANT ALL PRIVILEGES ON DATABASE king_phisher TO king_phisher;
     \q
     ```

7. **Configure King Phisher**:
   - Copy the example configuration and edit it:

     ```
     cp server_config.yml.sample server_config.yml
     nano server_config.yml
     ```

     o   Edit the PostgreSQL section with the database name, user, and password.

Step 2: Running King Phisher

1. **Start the Server**:
   - o Launch the King Phisher server:

     ```
     ./KingPhisher
     ```

   - o The server will start and listen for connections. You should see output indicating the server is running.
2. **Access the King Phisher Client**:
   - o Open the King Phisher client (either from the terminal or the applications menu, depending on your setup):

     ```
     ./KingPhisherClient
     ```

   - o Connect to the server by entering the server IP and port (by default, it's `localhost` and port `80`).

Step 3: Configuring a Phishing Campaign

1. **Create a New Campaign**:
   - o Once logged in, you can create a new phishing campaign by going to **Campaigns -> New Campaign**.
   - o Fill in the details, including the campaign name, target domain, and other necessary information.
2. **Set Up Email Template**:
   - o Choose an email template or create your own. Templates are available in the **Templates -> Email Templates** section.
   - o Customize the email content to fit the scenario.
3. **Select a Landing Page**:
   - o If your phishing email includes a link, configure a landing page. King Phisher allows you to clone a website or create a custom landing page.
   - o Landing pages can be configured under **Templates -> Web Cloner**.
4. **Sending the Phishing Email**:
   - o After setting up the email and landing page, go back to the campaign screen and click **Send Messages**.
   - o Configure the sending options (such as sender email, SMTP server, etc.) and click **Send**.

Step 4: Monitoring and Analyzing the Campaign

1. **View Campaign Metrics**:
   - o Once the emails are sent, King Phisher tracks metrics such as email opens, clicks on links, and data submissions.
   - o Go to the **Campaigns** section to monitor these metrics.
2. **Analyze the Results**:

- o King Phisher provides detailed reports on the effectiveness of the phishing campaign. Use these to analyze how many users interacted with the email and what actions they took.

Step 5: Ethical Considerations and Cleanup

1. **Legal Usage**:
   - o Ensure that the phishing campaign is conducted ethically and legally. Only target systems and individuals for which you have explicit permission to test.
2. **Stopping the Server**:
   - o When done, stop the King Phisher server by pressing `Ctrl + C` in the terminal where it's running.
3. **Clean Up**:
   - o Remove any test data and configurations you no longer need.