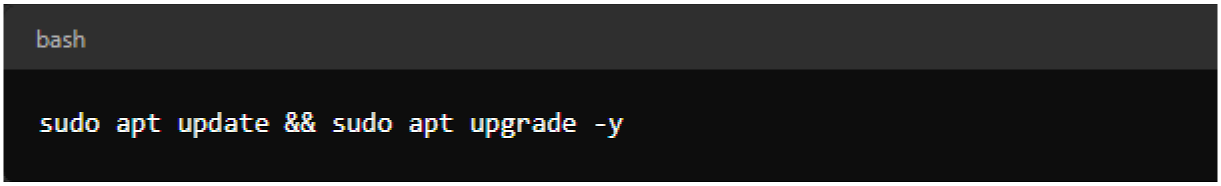
To set up and configure Kali Linux for OSINT (Open-Source Intelligence) and personal information (PI) reviews, you can use a variety of tools that are pre-installed or easily installable on Kali Linux. Below is a detailed guide on how to do this.

Step 1: Install Kali Linux

Ensure that you have Kali Linux installed on your machine. You can either install it on a physical machine, run it in a virtual machine, or use it as a live boot.

Step 2: Update and Upgrade Kali Linux

Before starting, make sure your system is updated:

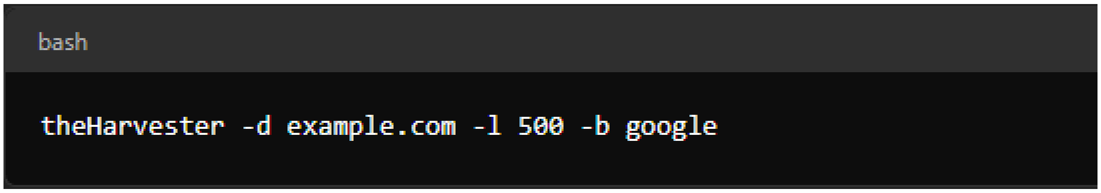


```bash
sudo apt update && sudo apt upgrade -y
```

Step 3: Install Required OSINT Tools

Some essential OSINT tools are either pre-installed or can be installed using Kali's package manager. Here are some of the most useful tools for OSINT and PI reviews:

1. **theHarvester**
   - **Purpose**: Gathers emails, subdomains, hosts, and more using public sources such as search engines, PGP key servers, and more.
   - **Installation**: Pre-installed on Kali.
   - **Usage**:

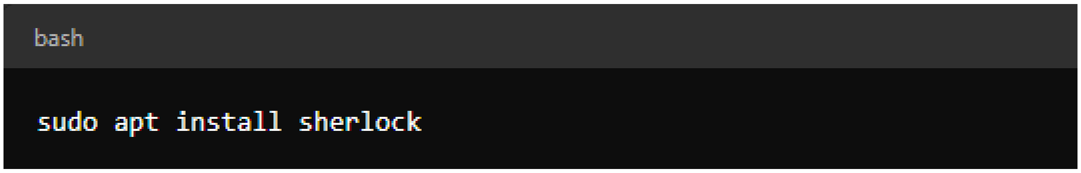
     

     ```bash
     theHarvester -d example.com -l 500 -b google
     ```

   - Replace example.com with the domain name you are investigating. The -b option specifies the data source, e.g., Google, Bing, etc.
2. **Maltego**
   - **Purpose**: A graphical tool that provides a visual link analysis for gathering and connecting information for investigative tasks.
   - **Installation**: Pre-installed on Kali.
   - **Usage**:
     - Start Maltego from the applications menu or by typing “maltego” in the terminal.

        - Use the transforms to search for information based on emails, names, phone numbers, etc.
        - Build relationships and visualize data.

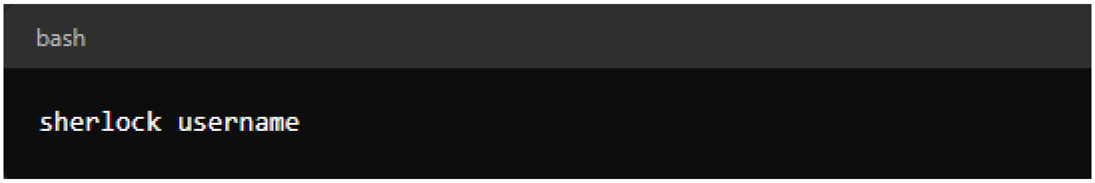
3. **Sherlock**
    - **Purpose**: Finds usernames across many social networks.
    - **Installation**:



bash

```bash
sudo apt install sherlock
```

    - **Usage**:

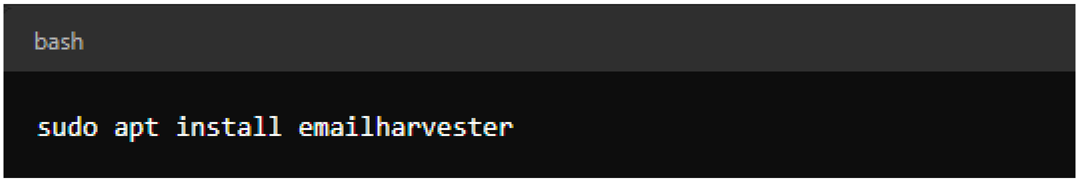


bash

```bash
sherlock username
```

    - Replace username with the actual username you are searching for across social networks.

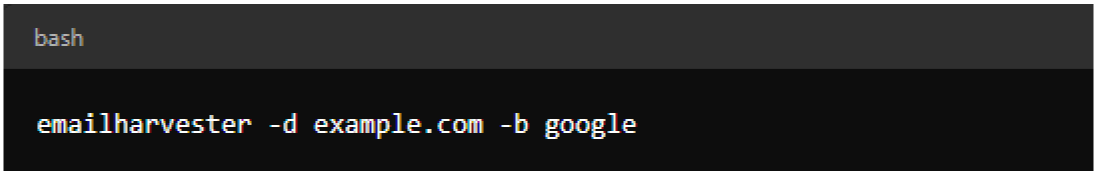
4. **EmailHarvester**
    - **Purpose**: Harvests email addresses by searching through various search engines.
    - **Installation**:



bash

```bash
sudo apt install emailharvester
```

    - **Usage**:



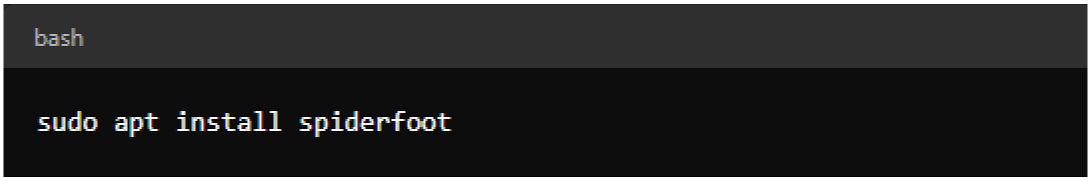
bash

```bash
emailharvester -d example.com -b google
```

    - Replace example.com with the domain you want to search.

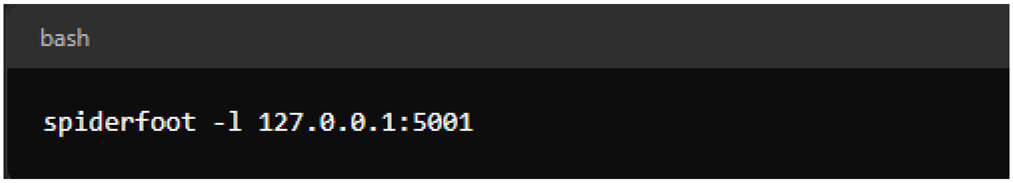
5. **SpiderFoot**

- **Purpose**: Automates the process of gathering OSINT on a given target, whether it's an IP address, domain name, email address, or other.
- **Installation**:



```bash
sudo apt install spiderfoot
```

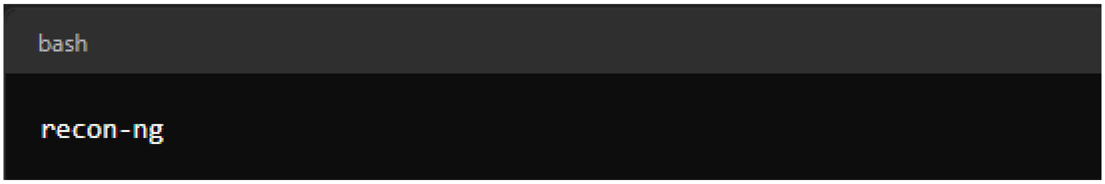
- **Usage**:



```bash
spiderfoot -l 127.0.0.1:5001
```

  - Access the web interface at http://127.0.0.1:5001 and create a new scan using an email, name, or domain.

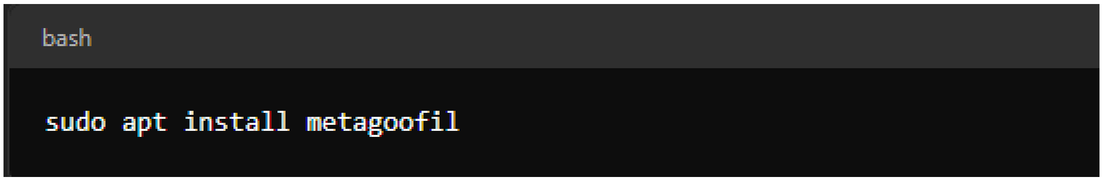
6. **Recon-ng**
   - **Purpose**: A powerful framework for web-based reconnaissance and OSINT gathering.
   - **Installation**: Pre-installed on Kali.
   - **Usage**:



```bash
recon-ng
```

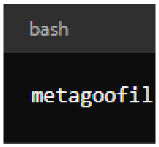
  - Within the Recon-ng console, use modules like recon/domains-hosts/google_site_web, recon/profiles-profiles/namechk, or recon/contacts-contacts/email_hunter to search based on different criteria.

7. **Metagoofil**
   - **Purpose**: Extracts metadata from public documents (PDF, DOC, XLS, PPT, etc.) found on websites.
   - **Installation**:

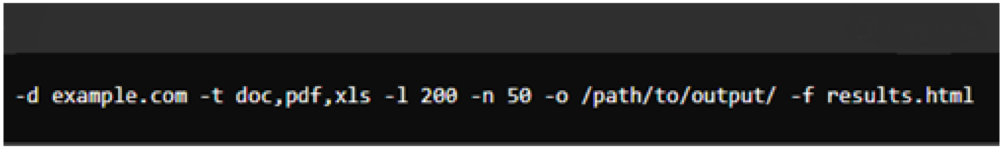


```bash
sudo apt install metagoofil
```

- **Usage**:

  ```bash
  metagoofil
  ```

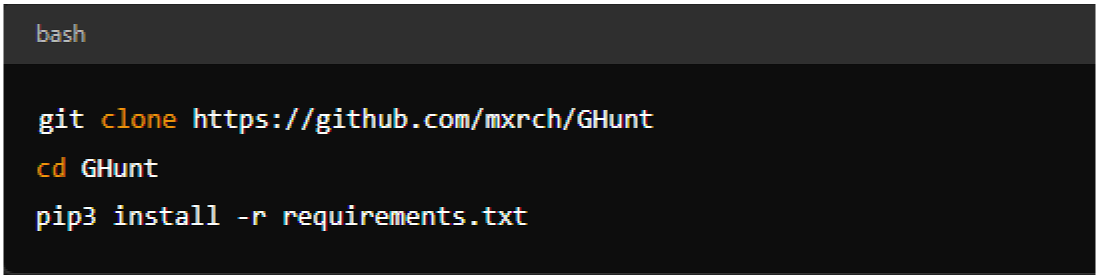
- 

  ```
  -d example.com -t doc,pdf,xls -l 200 -n 50 -o /path/to/output/ -f results.html
  ```

  - metagoofil -d example.com -t doc,pdf,xls -l 200 -n 50 -o /path/to/output/ -f results.html
  - Replace example.com with the target domain, and adjust the output path and filename as needed.

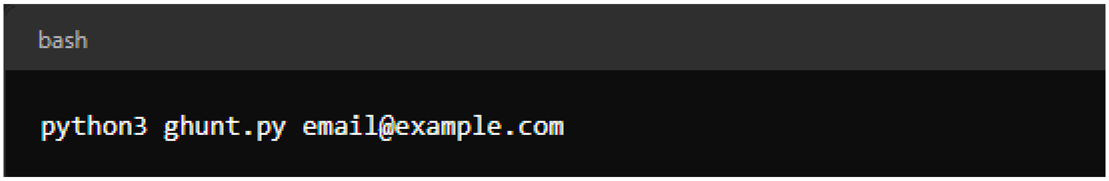
Step 4: Additional Tools for Email and Name Investigations

1. **Have I Been Pwned (HIBP)**
   - **Purpose**: Check if an email has been involved in any data breaches.
   - **Installation**: No installation required. You can use the website or integrate it with Recon-ng.
   - **Usage**:
     - Visit Have I Been Pwned and input the email address.
2. **Ghunt**
   - **Purpose**: OSINT framework to track the footprints of Google accounts.
   - **Installation**:

     ```bash
     git clone https://github.com/mxrch/GHunt
     cd GHunt
     pip3 install -r requirements.txt
     ```

   - **Usage**:

     ```bash
     python3 ghunt.py email@example.com
     ```

   - Replace email@example.com with the target email.

Step 5: Analyzing Results

After collecting data, you will need to analyze the information gathered. You can use:

- **Maltego** for visual link analysis.
- **Custom scripts** to parse and correlate data.
- **Manual investigation** for verifying and cross-referencing gathered intelligence.

Step 6: Ethical Considerations

Always ensure that your OSINT activities comply with legal and ethical guidelines. Unauthorized access to data, hacking, or intrusive methods can be illegal and unethical.

By following this setup, you should have a robust environment in Kali Linux for conducting OSINT and PI reviews based on email addresses, names, or other related information.