**Infoga – Email Information Gathering Tool**

**Infoga Overview:**

Infoga is a free and open-source tool accessible on GitHub, designed to identify whether email addresses have been compromised using the haveibeenpwned.com API. It excels in scanning email addresses through various websites and search engines, collecting information and detecting leaked data on websites and web applications. Known for its user-friendliness, Infoga is one of the most effective tools for performing reconnaissance on websites and web applications specifically for email analysis.

The tool is compatible with Linux operating systems and can gather detailed information such as IP addresses, countries of origin, and hostnames associated with email addresses. Infoga retrieves data from a variety of public sources, including popular websites and search engines like Google and Shodan. This makes it particularly valuable for security researchers in the initial stages of penetration testing.

**Features and Uses of Infoga:**

**Free and Open Source**: Infoga is available at no cost, and you can download and use it freely.

**Comprehensive Information Gathering**: It's a full package with various modules designed to check if an email has been leaked.

**API Tool**: Infoga functions using APIs to gather information.

**Acts as a Scanner**: It operates as a scanner for reconnaissance on public sources.

**Python-Based**: Infoga is written in the Python programming language.

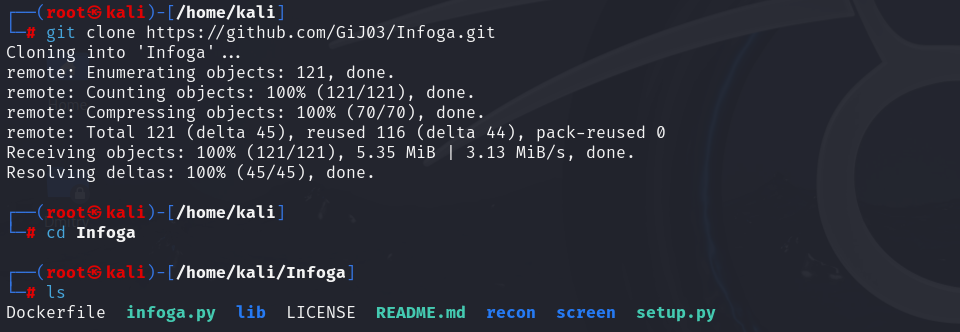
**User-Friendly Interface**: Its interface is similar to Metasploit 1 and Metasploit 2, making it easy for users familiar with those tools.

**Interactive Console**: Infoga’s interactive console offers several helpful features to streamline the information gathering process.

**Installation:**

**Step 1:**Open your Kali Linux operating system and install the tool using the following command.

Command: git clone https://github.com/GiJ03/Infoga.git



**Step 2:**The tool has been downloaded into your system use the following command to run the tool.

Command: python3 infoga.py

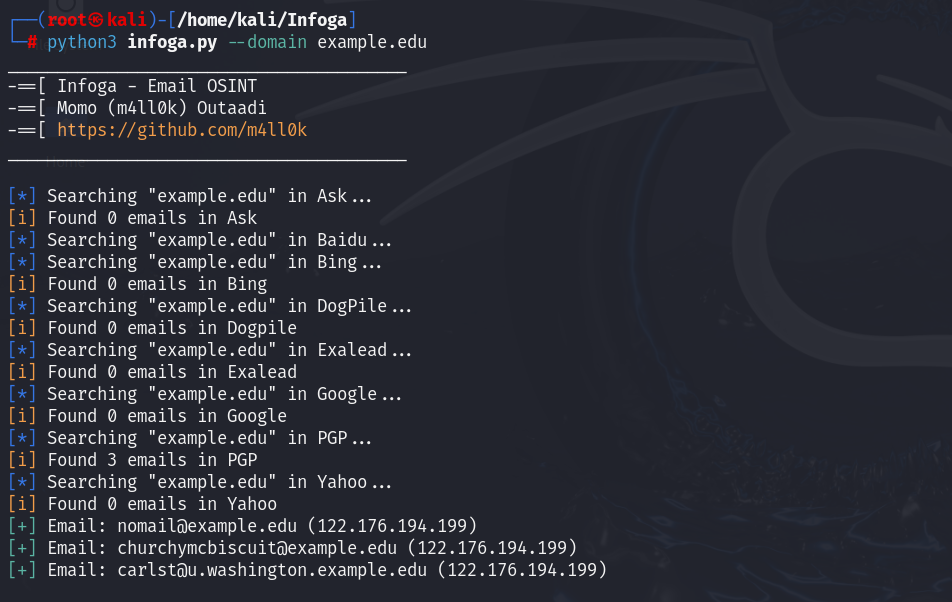


**Usage:**

**Basic Domain Search:**

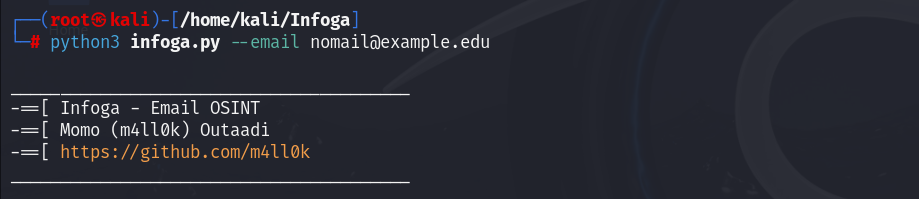
Use the Infoga tool to scan example.edu by using the following command

Command: python3 infoga.py –-domain example.edu

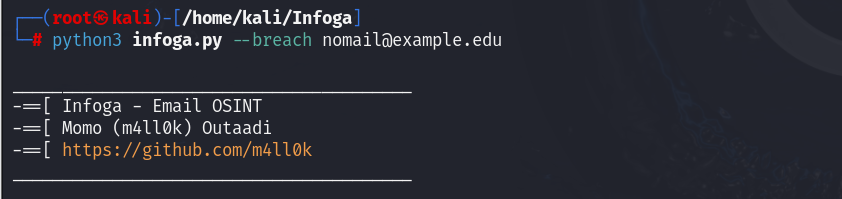


You can see that 3 emails have been found by this tool which got leaked in any data breach. This is how you can use the tool for our target also.

**Verify an Email Address:**



**Search for Breached Data:**



We can specify the search engine by **–-source** (search engine name) and can get information about email by using **–-info .**