EXPERMINT: 02

● **Aim:** Using OSINT tool such as (Harverster) you can gather information like emails, subdomains, hosts, employee names, open ports and banners from different public sources like search engines, PGP key server.

● Theory:

TheHarvester

theHarvester is an open-source OSINT (Open-Source Intelligence) tool used for gathering information about email addresses, subdomains, hosts, employee names, open ports, and more from various public sources like search engines, PGP key servers, and social media sites. It is primarily used for reconnaissance and information gathering in the field of cybersecurity and penetration testing.

Here's a breakdown of the key features and uses of theHarvester:

- **Email Enumeration**: theHarvester can be used to search for email addresses associated with a specific domain. This is useful for identifying valid email addresses within an organization, which can be valuable for security assessments.
- **Subdomain Discovery**: It can discover subdomains associated with a target domain. This information can be helpful for understanding a target's web infrastructure and potential attack surfaces.
- **Host Discovery**: theHarvester can find information about hosts and servers associated with a domain, helping in network reconnaissance and vulnerability assessments.
- **Employee Name Gathering**: It can assist in finding employee names associated with a target domain, which can be valuable for social engineering or profiling.
- **Open Port Scanning:** theHarvester can check for open ports on the discovered hosts, which can be important for identifying potential entry points for a penetration test.
- **Integration with Multiple Data Sources**: theHarvester supports integration with various data sources such as search engines (Google, Bing), PGP key servers, and social media platforms. This provides a broad range of information sources for reconnaissance.
- **Customizable and Extensible**: Users can customize theHarvester's search parameters to tailor it to their specific needs. It is also extensible, allowing you to add your data sources and plugins.

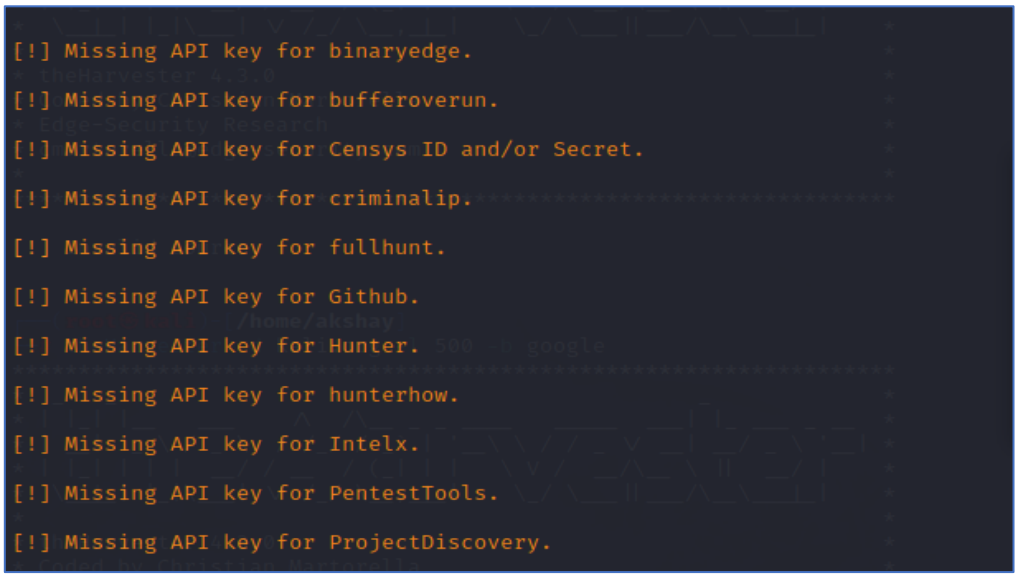
How to install theHarvester:

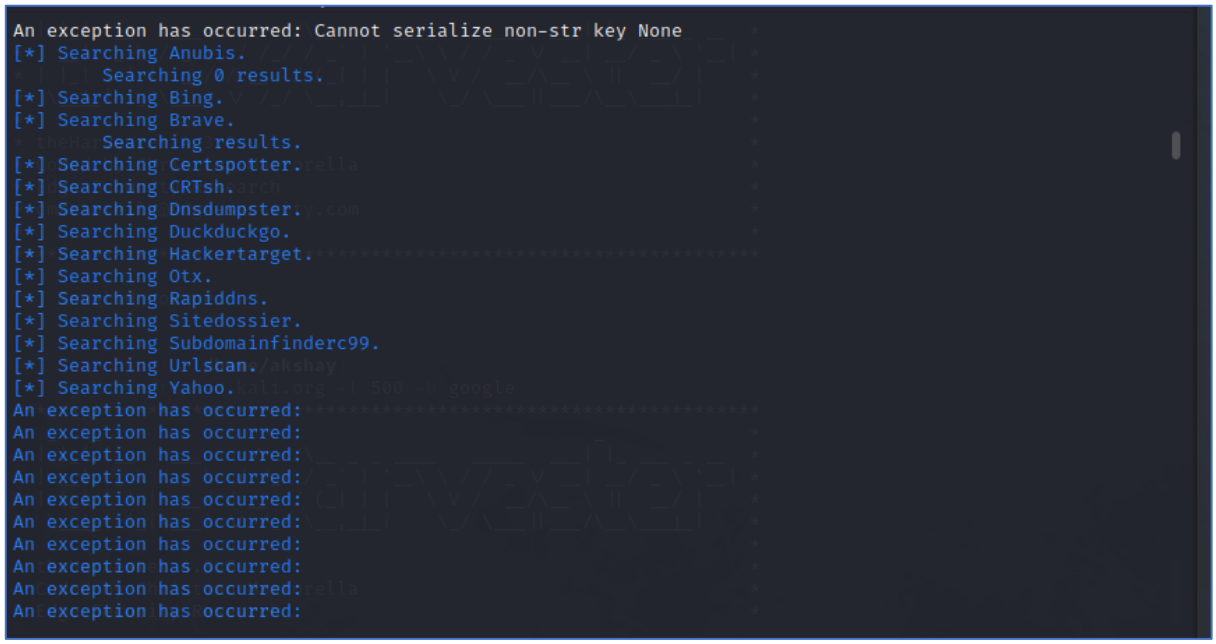
1 If you are using a Kali Linux machine then this tool is already installed in it, just type the command

theharvester

use theharvester tool feature by giving a domain name in the command python3

theHarvester.py -d -l 500 -b





```
An exception has occurred:
[*] Searching Baidu.
[*] Searching Threatminer.
[!] Invalid source.
[*] ASNS found: 34
--------------------
AS13335
AS14061
AS14618
AS15169
AS15318
AS16509
AS16625
AS19527
AS19551
AS198371
AS19871
AS209242
AS20940
AS213120
AS22612
AS30148
AS32934
AS36666
AS393802
AS396982
AS43541
```

```
[*] Interesting Urls found: 4
--------------------------
https://www.facebook.com/SignUpGenius/
https://www.facebook.com/WeInspireWe
https://www.facebook.com/biolase/
https://www.facebook.com/login/?next=https%3A%2F%2Fwww.facebook.com%2FintrinsiQ-160203274033832
[*] LinkedIn Links found: 0
---------------------------

[*] IPs found: 831
------------------
1.0.0.5
1.0.0.30
1.0.0.37
1.0.0.72
1.0.0.106
1.0.0.120
2.23.196.80
3.69.136.55
5.100.254.187
5.129.103.53
5.254.65.16
13.107.246.45
13.224.189.39
```

```
31.13.64.1
31.13.64.17
31.13.64.32
31.13.64.35
31.13.64.48
31.13.64.65
31.13.64.81
31.13.64.97
31.13.64.113
31.13.65.1
31.13.65.7
31.13.65.17
31.13.65.23
31.13.65.36
31.13.66.1
31.13.66.7
31.13.66.17
31.13.66.23
```

```
2620:3e:a000:40::6
2620:12a:8000::2
2a02:26f0:480:5a0::1e62
2a02:26f0:480:5ac::f1e
2a02:26f0:480:5b3::f1e
2a02:26f0:480:9ad::b58
2a02:26f0:1700:181::1dc5
2a03:2880:f176:84:face:b00c:0:25de
2a03:2880:f177:83:face:b00c:0:25de
2a03:2880:f177:185:face:b00c:0:25de
2a03:2880:f276:e8:face:b00c:0:4420
2a03:b0c0:1:d0::1057:1
2a06:98c1:3120::3
2a06:98c1:3121::3

[*] No emails found.

[*] Hosts found: 5
---------------------
facebook.com
foundation.facebook.com
m.facebook.com
mx.facebook.com
static.ak.facebook.com
```

```
File  Edit  View  Search  Terminal  Help
204.79.197.200  platform.bing.com
204.79.197.200  speech.platform.bing.com
204.79.197.200  www4.bing.com
204.79.197.200  hk.bing.com
204.79.197.200  de.bing.com
204.79.197.200  mx.bing.com
204.79.197.200  be.bing.com
204.79.197.200  wp.m.bing.com
204.79.197.200  it.bing.com
204.79.197.200  websockets.platform.bing.com
23.77.57.144    hs.windows.microsoft.com
204.79.197.219  <strong>www.myhomemsn.com<
204.79.197.219  msdl.microsoft.com
204.79.197.219  ambassadors.<strong>xbox<
root@P4ND4:~# theharvester -d microsoft.com -b linkedin

*******************************************************************
*                                                                 *
*  _   _                                            _             *
*  | | | |                                          | |            *
*  | |_| |__   ___ /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
*  | __| '_ \ / _ \ \/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__|  *
*  | |_| | | |  __/ /\ \ (_| | |   \ V /  __/\__ \ ||  __/ |     *
*   \__|_| |_|\___|/  \/\__,_|_|    \_/ \___||___/\__\___|_|     *
*                                                                 *
* TheHarvester Ver. 2.6                                           *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


[-] Searching in Linkedin..
        Searching 100 results..
Users from Linkedin:
====================
Chirmoy Joshi - Pre Sales Consultant - Sunnex Australia
```

● Conclusion:

Using OSINT tools like theHarvester, you can effectively gather a wide range of information from public sources, including emails, subdomains, hosts, employee names, open ports, and banners. This information can be invaluable for various purposes such as reconnaissance, security assessments, and penetration testing. However, it's essential to use these tools responsibly, following legal and ethical guidelines, and ensuring that your activities are conducted within the bounds of the law.