

---

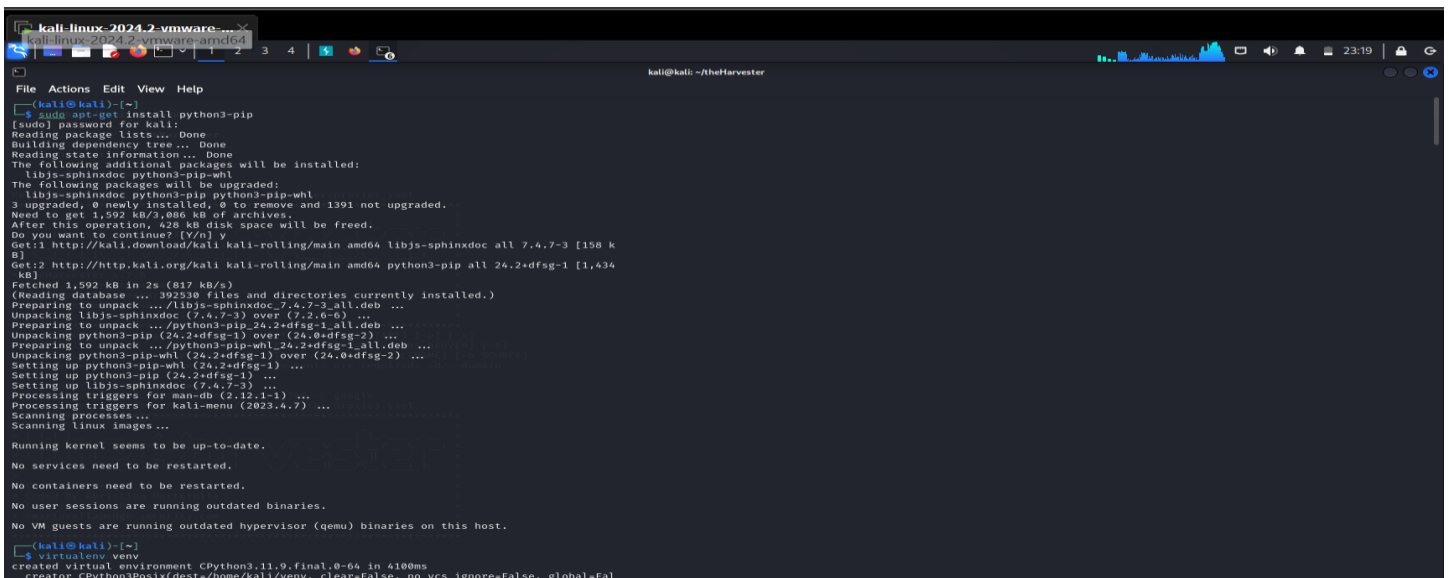
## INFORMATION GATHERING USING THE HARVESTER

---

Information gathering is often the first step of any penetration test. theHarvester is a very powerful OSINT (Open-Source Intelligence Tool) for finding information on a target URL. It searches multiple sites for information about the target URL and displays all the information it finds. It is particularly useful for finding names of people and their email addresses as well as subdomains of the target site.

### Lab Tool: Kali Linux

**STEP 1:** Instal python3-pip and virtualnv on kali linux using the following command: “**sudo apt-get install python3-pip**” “**sudo pip3 install virtualenv**”



```
kali@kali: ~$ sudo apt-get install python3-pip
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libjs-sphinxdoc python3-pip-whl
The following packages will be upgraded:
  libjs-sphinxdoc python3-pip python3-pip-whl
3 upgraded, 0 newly installed, 0 to remove and 1391 not upgraded.
Need to get 1,592 kB/2,086 kB of archives.
After this operation, 428 kB disk space will be freed.
Do you want to continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 libjs-sphinxdoc all 7.4.7-3 [158 k
B]
Get:2 http://kali.org/kali kali-rolling/main amd64 python3-pip all 24.2+dfsg-1 [1,434
kB]
Fetched 1,592 kB in 2s (817 kB/s)
(Reading database ... 29230 files and directories currently installed.)
Preparing to unpack .../libjs-sphinxdoc_7.4.7-3_all.deb ...
Unpacking libjs-sphinxdoc (7.4.7-3) over (7.2.0-6) ...
Preparing to unpack .../python3-pip_24.2+dfsg-1_all.deb ...
Unpacking python3-pip (24.2+dfsg-1) over (24.0+dfsg-2) ...
Preparing to unpack .../python3-pip-whl_24.2+dfsg-1_all.deb ...
Unpacking python3-pip-whl (24.2+dfsg-1) over (24.0+dfsg-2) ...
Setting up python3-pip (24.2+dfsg-1) ...
Setting up libjs-sphinxdoc (7.4.7-3) ...
Processing triggers for man-db (2.12.1-1) ...
Processing triggers for kali-menu (2023.4.7) ...
Scanning processes ...
Scanning linux images ...

Running kernel seems to be up-to-date.

No services need to be restarted.

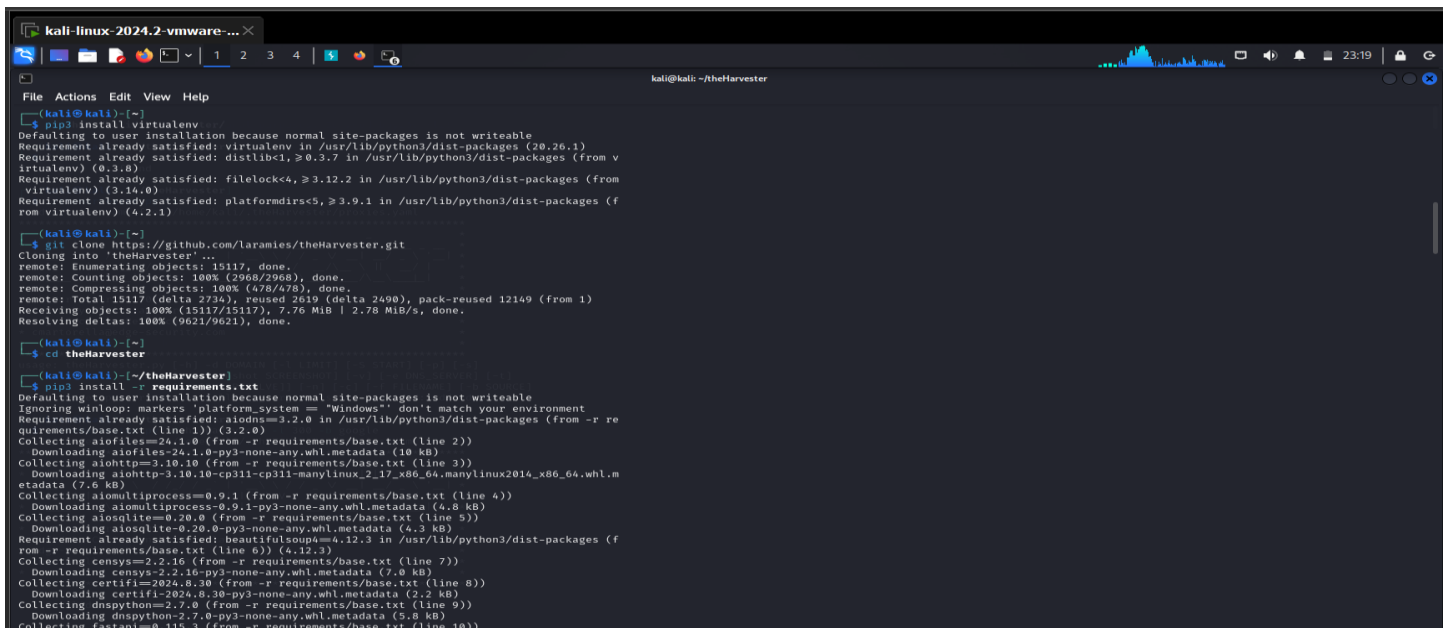
No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.

kali@kali: ~$ sudo pip3 install virtualenv
created virtual environment CPython3.11.9.final.0-64 in 410ms
creator CPython3Posix(dest=/home/kali/.venv, clear=False, no_vcs_ignore=False, global=False)
```

To launch “virtualenv” I typed the command: “**virtualenv venv**” and also cloning git via <https://github.com/laramies/theHarvester.git> . Then “**cd theHarvester**” to enter harvester directory. The following command is typed in order to install pip3 “**pip3 install -r requirements.txt**”



```
kali@kali: ~$ virtualenv venv
created virtual environment CPython3.11.9.final.0-64 in 410ms
creator CPython3Posix(dest=/home/kali/.venv, clear=False, no_vcs_ignore=False, global=False)

kali@kali: ~$ cd theHarvester

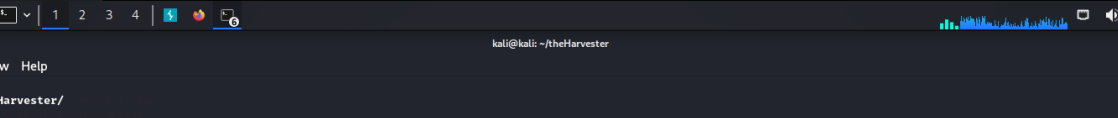
kali@kali: ~/theHarvester$ pip3 install -r requirements.txt
Defaulting to user installation because normal site-packages is not writeable
Ignoring winlogo: markers 'platform.system == "Windows"' don't match your environment
Requirement already satisfied: virtualenv in /usr/lib/python3/dist-packages (20.26.1)
Requirement already satisfied: distlib<1, >=0.3.7 in /usr/lib/python3/dist-packages (from v
irtualenv) (0.3.8)
Requirement already satisfied: filelock<4, >=3.12.2 in /usr/lib/python3/dist-packages (from
virtualenv) (3.16.0)
Requirement already satisfied: platformdirs<5, >=3.9.1 in /usr/lib/python3/dist-packages (f
rom virtualenv) (4.2.1)

kali@kali: ~/theHarvester$ git clone https://github.com/laramies/theHarvester.git
Cloning into 'theHarvester' ...
remote: Enumerating objects: 15117, done.
remote: Counting objects: 100% (2968/2968), done.
remote: Compressing objects: 100% (478/478), done.
remote: Total 15117 (delta 2736), reused 2619 (delta 2608), pack-reused 12149 (from 1)
Receiving objects: 100% (15117/15117), 7.76 MiB | 2.78 MiB/s, done.
Resolving deltas: 100% (9621/9621), done.

kali@kali: ~/theHarvester$ cd theHarvester

kali@kali: ~/theHarvester$ pip3 install -r requirements.txt
Defaulting to user installation because normal site-packages is not writeable
Ignoring winlogo: markers 'platform.system == "Windows"' don't match your environment
Requirement already satisfied: aiodns==3.2.0 in /usr/lib/python3/dist-packages (from -r re
quirements/base.txt (line 1)) (3.2.0)
Collecting aiofiles==24.1.0 (from -r requirements/base.txt (line 2))
  Downloading aiofiles-24.1.0-py3-none-any.whl.metadata (10 kB)
Collecting aiohttp==3.10.10 (from -r requirements/base.txt (line 3))
  Downloading aiohttp-3.10.10-cp311-cp311-manylinux_2_17_x86_64.manylinux2014_x86_64.whl.m
etadata (7.6 kB)
Collecting aiomultiprocess==0.9.1 (from -r requirements/base.txt (line 4))
  Downloading aiomultiprocess-0.9.1-py3-none-any.whl.metadata (4.8 kB)
Collecting aiosqlite==0.20.0 (from -r requirements/base.txt (line 5))
  Downloading aiosqlite-0.20.0-py3-none-any.whl.metadata (4.3 kB)
Requirement already satisfied: BeautifulSoup4==4.12.3 in /usr/lib/python3/dist-packages (f
rom -r requirements/base.txt (line 6)) (4.12.3)
Collecting censys==2.2.16 (from -r requirements/base.txt (line 7))
  Downloading censys-2.2.16-py3-none-any.whl.metadata (7.0 kB)
Collecting certifi==2024.8.30 (from -r requirements/base.txt (line 8))
  Downloading certifi-2024.8.30-py3-none-any.whl.metadata (2.2 kB)
Collecting dnspython==2.7.0 (from -r requirements/base.txt (line 9))
  Downloading dnspython-2.7.0-py3-none-any.whl.metadata (5.8 kB)
Collecting fastapi==0.115.3 (from -r requirements/base.txt (line 10))
```

To use theHarvester.py in kali via user directory I typed "cd /home/kali/theHarvester/ and ./theHarvester.py -v"



```
kali@kali: ~/theHarvester
File Actions Edit View Help
kali@kali:~$ cd /home/kali/theHarvester/
kali@kali:~/theHarvester$ python3 theHarvester.py -v
Read proxies.yaml from /home/kali/theHarvester/proxies.yaml
*****
* theHarvester *
* theHarvester 4.7.0 *
* Coded by Christian Martorella *
* Edge-Security Research *
* cmartorella@edge-security.com *
*****
usage: theHarvester.py [-h] -d DOMAIN [-l LIMIT] [-s START] [-p] [-s]
                        [--screenshot SCREENSHOT] [-v] [-e DNS_SERVER] [-t]
                        [-r [DNS_RESOLVE]] [-n] [-c] [-f FILENAME] [-b SOURCE]
theHarvester.py: error: the following arguments are required: -d
```

**Step 2:** To start theHarvester I typed this command and also search google for the top 300 result related to hackaday.com `“./theHarvester.py -d hackaday.com -l 300 -b google”`. For this target, we could not find any information on Google. I decided to dig deeper.

A screenshot of a Kali Linux virtual machine window titled "kali-linux-2024.2-vmware...". The terminal shows the output of a command, likely from Burp Suite's HTTP history tab. It displays several error messages related to failed connections to host "search.yahoo.com:443" and "ssl.gstatic.com:443". Below these errors, it lists multiple instances of "An exception has occurred: 400, message: Can not decode content-encoding: br". At the bottom, it states "[+] Searching Brave." followed by "[+] ASN found: 17" and a partial IP address "AS19335". The system clock at the top right indicates 23:21.

**Step 3:** I decided to gather more information about the target by typing `“./theHarvester.py -d hackaday.com -l 300 -b all”`. The `“-b all”` means it would search all search engine available to theHarvester for information regarding hackaday.com

```
kali-linux-2024.2-vmware-...  
kali@kali: ~/TheHarvester  
[*] Interesting URLs found: 5  
https://hackaday.com/  
https://hackaday.com/2017/09/25/cuban-embassy-attacks-and-the-microwave-auditory-effect/  
https://hackaday.com/2021/02/06/hacking-hardware-bitcoin-wallets-extracting-the-cryptogram  
bit-sent-from-a-trojan/  
https://hackaday.com/2024/03/29/security-alert-potential-ssh-backdoor-via-liblza/  
https://hackaday.com/2024/07/13/the-naa-is-defeated-by-a-1950s-tape-recorder-can-you-help-  
them/  
[*] LinkedIn Links found: 0  
[*] IPs found: 111  
104.112.103.37  
104.21.5.216  
104.236.6.210  
104.80.89.115  
141.136.67.129  
146.120.210.153  
149.154.166.13  
157.240.76.72  
162.243.127.7  
163.254.286.8  
166.254.287.98  
169.254.245.32  
169.254.26.10  
169.254.96.134  
169.254.96.162  
169.172.232.176  
172.66.44.87  
172.67.235.103  
172.67.149.67  
172.67.152.96  
172.67.164.88  
172.67.177.66  
184.25.182.89  
185.176.43.98  
185.199.106.153  
185.199.111.153  
185.237.60.194  
188.134.95.3  
188.134.97.3  
192.0.66.96  
192.0.78.12
```