

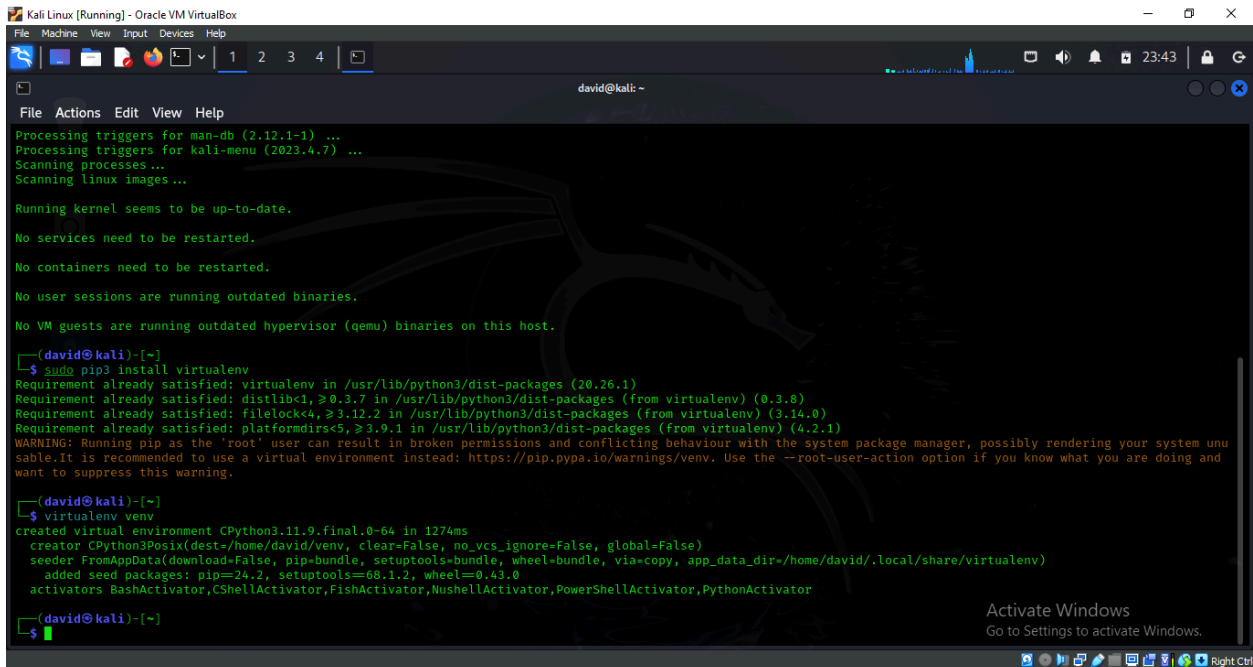
LAB 8:

Gathering information on a target site using theHarvester.

Tool: Kali Linux

Task 1: To begin, boot up Kali Linux in your VM and open a terminal. Follow the steps below:

```
sudo apt-get install python3-pip
sudo pip3 install virtualenv
virtualenv venv
```



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
david@kali: ~
File Actions Edit View Help
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No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
(david@kali)-[~]
└─$ sudo pip3 install virtualenv
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 virtualenv) (0.3.8)
Requirement already satisfied: filelock<4, >=3.12.2 in /usr/lib/python3/dist-packages (from virtualenv) (3.14.0)
Requirement already satisfied: platformdirs<5, >=3.9.1 in /usr/lib/python3/dist-packages (from virtualenv) (4.2.1)
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system package manager, possibly rendering your system unusable. It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv. Use the --root-user-action option if you know what you are doing and want to suppress this warning.
(david@kali)-[~]
└─$ virtualenv venv
created virtual environment CPython3.11.9.final.0-64 in 1274ms
creator CPython3Posix(dest=/home/david/venv, clear=False, no_vcs_ignore=False, global=False)
seeder FromAppData(download=False, pip=bundle, setuptools=bundle, wheel=bundle, via=copy, app_data_dir=/home/david/.local/share/virtualenv)
added seed packages: pip==24.2, setuptools==68.1.2, wheel==0.43.0
activators BashActivator,CShellActivator,FishActivator,NushellActivator,PowerShellActivator,PythonActivator
(david@kali)-[~]
└─$
```

Task 2: Clone the git repo:

```
git clone https://github.com/laramies/theHarvester.git
cd theHarvester
```

```
pip3 install -r requirements.txt
```

Kali Linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

david@kali: ~/theHarvester

File Actions Edit View Help

```
crackmapexec 5.4.0 requires minikerberos=0.3.3, but you have minikerberos 0.4.4 which is incompatible.
crackmapexec 5.4.0 requires neo4j<5.0.0, >=4.1.1, but you have neo4j 5.2.dev0 which is incompatible.
crackmapexec 5.4.0 requires paramiko<3.0.0, >=2.7.2, but you have paramiko 3.4.0 which is incompatible.
crackmapexec 5.4.0 requires pypsrp<0.8.0, >=0.7.0, but you have pypsrp 0.8.1 which is incompatible.
crackmapexec 5.4.0 requires termcolor<2.0.0, >=1.1.0, but you have termcolor 2.4.0 which is incompatible.
crackmapexec 5.4.0 requires xmldict<0.13.0, >=0.12.0, but you have xmldict 0.13.0 which is incompatible.
theharvester 4.6.0 requires aiodns=3.1.1, but you have aiodns 3.2.0 which is incompatible.
theharvester 4.6.0 requires aiofiles=23.2.1, but you have aiofiles 24.1.0 which is incompatible.
theharvester 4.6.0 requires aiohttp=3.9.3, but you have aiohttp 3.10.10 which is incompatible.
theharvester 4.6.0 requires aiomultiprocess=0.9.0, but you have aiomultiprocess 0.9.1 which is incompatible.
theharvester 4.6.0 requires censys=2.2.11, but you have censys 2.2.16 which is incompatible.
theharvester 4.6.0 requires certifi=2024.2.2, but you have certifi 2024.8.30 which is incompatible.
theharvester 4.6.0 requires dnspython=2.6.1, but you have dnspython 2.7.0 which is incompatible.
theharvester 4.6.0 requires fastapi=0.110.0, but you have fastapi 0.115.4 which is incompatible.
theharvester 4.6.0 requires lxml=5.1.0, but you have lxml 5.3.0 which is incompatible.
theharvester 4.6.0 requires netaddr=1.2.1, but you have netaddr 1.3.0 which is incompatible.
theharvester 4.6.0 requires playwright=1.42.0, but you have playwright 1.48.0 which is incompatible.
theharvester 4.6.0 requires PyYAML=6.0.1, but you have pyyaml 6.0.2 which is incompatible.
theharvester 4.6.0 requires requests=2.31.0, but you have requests 2.32.3 which is incompatible.
theharvester 4.6.0 requires setuptools=69.2.0, but you have setuptools 68.1.2 which is incompatible.
theharvester 4.6.0 requires ujson=5.9.0, but you have ujson 5.10.0 which is incompatible.
theharvester 4.6.0 requires uvicorn=0.28.0, but you have uvicorn 0.32.0 which is incompatible.
theharvester 4.6.0 requires uvloop=0.19.0; platform_system != "Windows", but you have uvloop 0.21.0 which is incompatible.
mitmproxy 10.2.3 requires aioquic<0.10, >=0.9.24, but you have aioquic 1.0.0 which is incompatible.
mitmproxy 10.2.3 requires asgiref<3.8, >=3.2.10, but you have asgiref 3.8.1 which is incompatible.
mitmproxy 10.2.3 requires pyOpenSSL<24.1, >=22.1, but you have pyopenssl 24.1.0 which is incompatible.
osdp-openvas 22.7.1 requires redis>=4.5.0, but you have redis 4.3.4 which is incompatible.
lsassy 3.1.10 requires netaddr<0.9.0, >=0.8.0, but you have netaddr 1.3.0 which is incompatible.
lsassy 3.1.10 requires rich<11.0.0, >=10.6.0, but you have rich 13.7.1 which is incompatible.
Successfully installed PyYAML-6.0.2 aiofiles-24.1.0 aiohappyeyeballs-2.4.3 aiohttp-3.10.10 aiomultiprocess-0.9.1 aiosqlite-0.20.0 censys-2.2.16 certifi-2024.8.30 dnsp
ython-2.7.0 fastapi-0.115.4 greenlet-3.1.1 lxml-5.3.0 netaddr-1.3.0 playwright-1.48.0 propcache-0.2.0 pyee-12.0.0 python-dateutil-2.9.0.post0 requests-2.32.3 retrying
-1.3.4 shodan-1.31.0 slowapi-0.1.9 starlette-0.41.2 ujson-5.10.0 uvicorn-0.32.0 uvloop-0.21.0 yarll-1.17.1
```

(david@kali) [~/theHarvester]

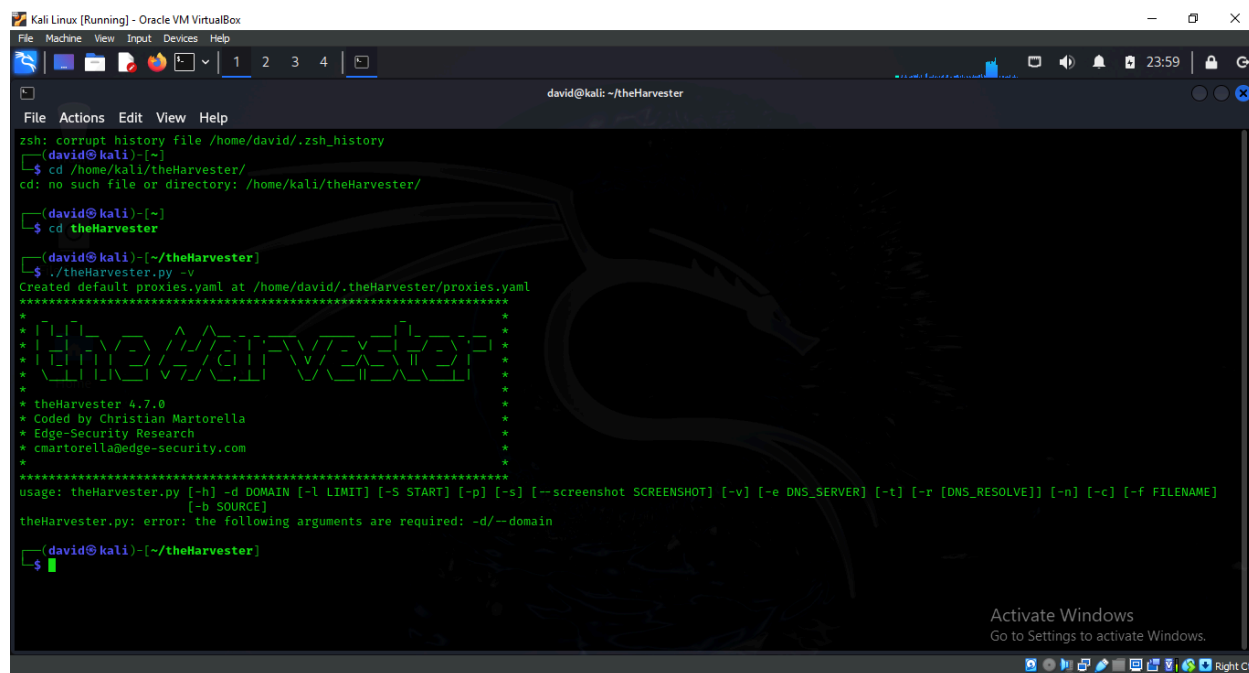
\$

Activate Windows
Go to Settings to activate Windows.

Right Ctrl

Close this terminal and open a new one. Now, we are ready to use “theHarvester.py” in “kali” user’s home directory. Type:

```
cd /home/kali/theHarvester/  
./theHarvester.py -v
```



The screenshot shows a Kali Linux terminal window titled "Kali Linux [Running] - Oracle VM VirtualBox". The terminal output is as follows:

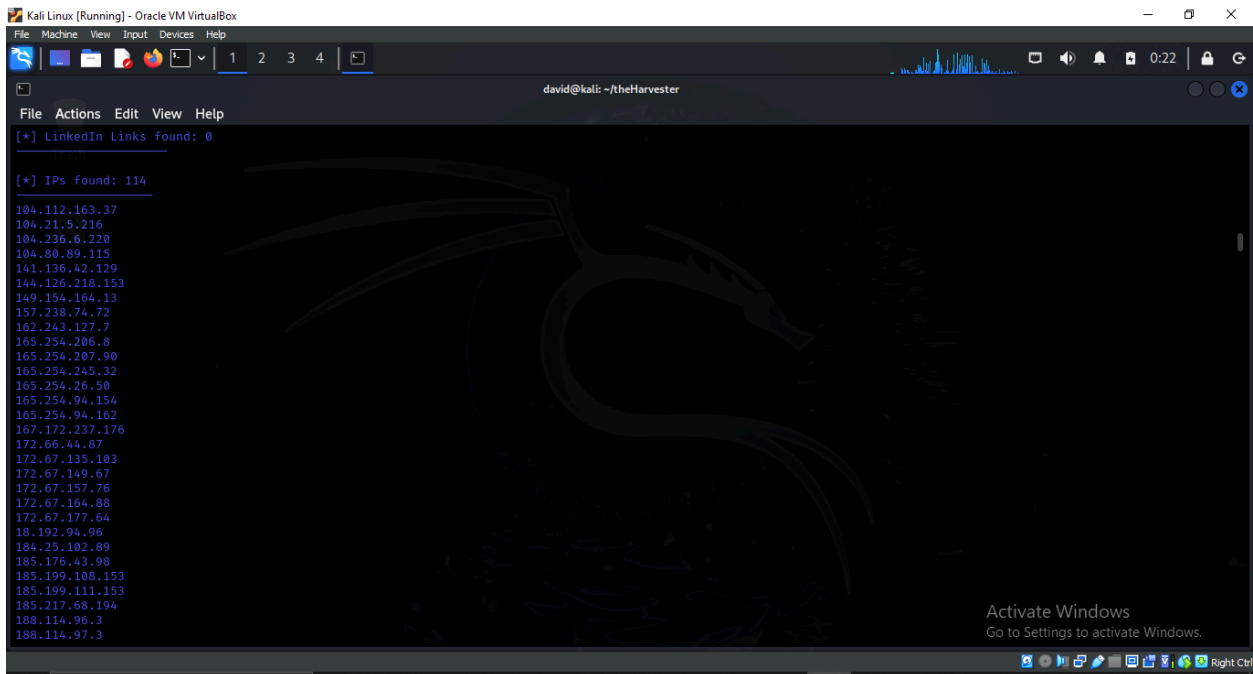
```
zsh: corrupt history file /home/david/.zsh_history  
(david@kali)~  
$ cd /home/kali/theHarvester/  
cd: no such file or directory: /home/kali/theHarvester/  
(david@kali)~  
$ cd theHarvester  
(david@kali)~/theHarvester  
$ ./theHarvester.py -v  
Created default proxies.yaml at /home/david/.theHarvester/proxies.yaml  
*****  
* THE HARVESTER *  
* THE HARVESTER *  
* THE HARVESTER *  
* THE HARVESTER *  
* 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/--domain  
(david@kali)~/theHarvester  
$
```

An "Activate Windows" watermark is visible in the bottom right corner of the terminal window.

Task 3: To launch an information gathering campaign on a target, type the following:
./theHarvester.py -d hackaday.com -l 300 -b google

If we want to gather even more information about our target, we can specify the following:

./theHarvester.py -d hackaday.com
-l 300 -b all

A screenshot of a Kali Linux terminal window titled "Kali Linux [Running] - Oracle VM VirtualBox". The terminal shows the output of the command `./theHarvester.py -d hackaday.com -l 300 -b all`. The output displays a list of 114 IP addresses found, starting with `104.112.163.37` and ending with `188.114.97.3`. The terminal also shows a message `[*] LinkedIn Links found: 0`. The background of the terminal window features a large, stylized dragon logo. The terminal window is running on a Kali Linux desktop environment, with a taskbar at the bottom showing various application icons and a system tray on the right. The desktop background is dark with a large, stylized dragon logo. The terminal window is titled "Kali Linux [Running] - Oracle VM VirtualBox". The terminal shows the output of the command `./theHarvester.py -d hackaday.com -l 300 -b all`. The output displays a list of 114 IP addresses found, starting with `104.112.163.37` and ending with `188.114.97.3`. The terminal also shows a message `[*] LinkedIn Links found: 0`. The background of the terminal window features a large, stylized dragon logo. The terminal window is running on a Kali Linux desktop environment, with a taskbar at the bottom showing various application icons and a system tray on the right. The desktop background is dark with a large, stylized dragon logo. The terminal window is titled "Kali Linux [Running] - Oracle VM VirtualBox".

```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
david@kali: ~/theHarvester
File Actions Edit View Help
[*] LinkedIn Links found: 0

[*] IPs found: 114
104.112.163.37
104.21.5.216
104.236.6.220
104.80.89.115
141.136.42.129
144.126.218.153
149.154.164.13
157.238.74.72
162.243.127.7
165.254.206.8
165.254.207.90
165.254.245.32
165.254.26.50
165.254.94.154
165.254.94.162
167.172.237.176
172.66.44.87
172.67.135.103
172.67.149.67
172.67.157.76
172.67.164.88
172.67.177.64
18.192.94.96
184.25.102.89
185.176.43.98
185.199.108.153
185.199.111.153
185.217.68.194
188.114.96.3
188.114.97.3

Activate Windows
Go to Settings to activate Windows.
```