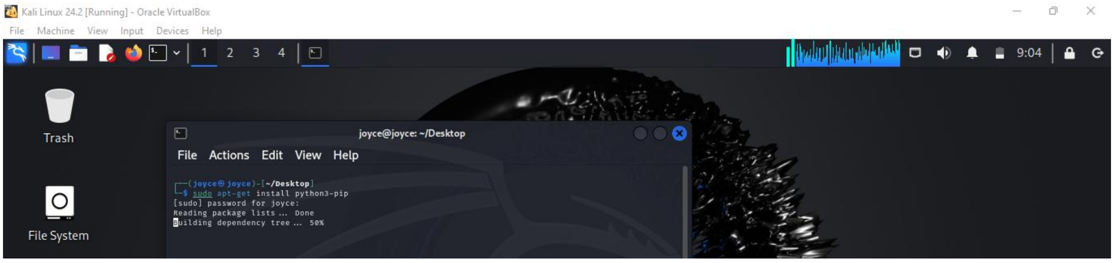
RESEARCH ON INFORMATION GATHERING USING THEHARVESTER

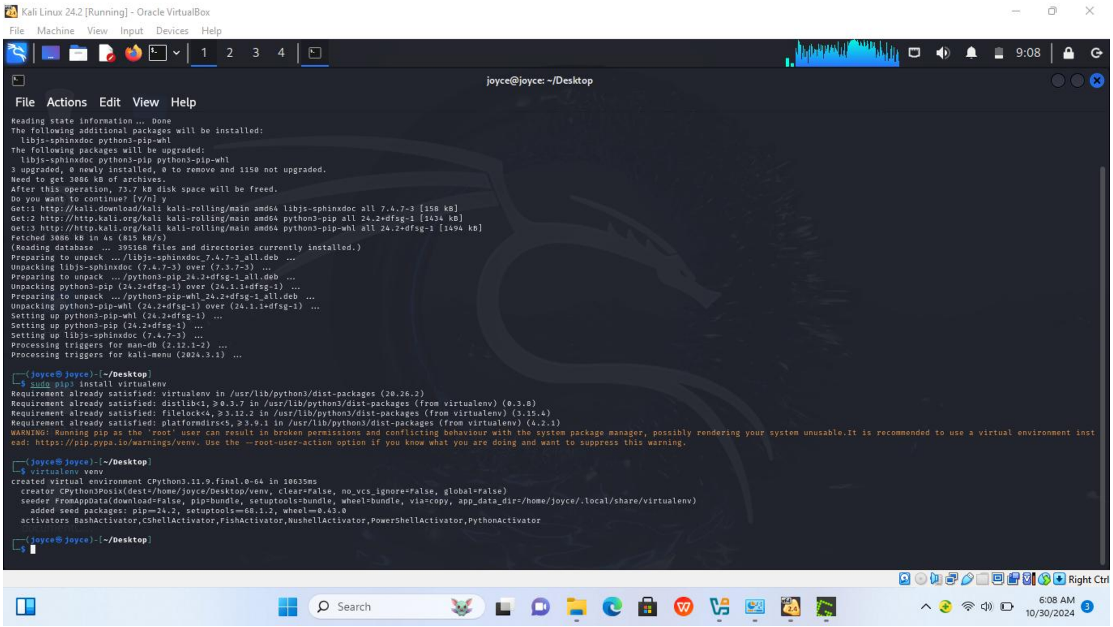
Project Objective: Learn how to gather information on a target site using theHarvester.

Information Gathering is usually the first step of any penetration test. theHarvester is an OSINT (Open-Source Intelligence Tool) for finding information on a target URL. It searches multiple sites for information about the URL. It is useful for finding names of people and their email addresses as well as subdomains of the site.

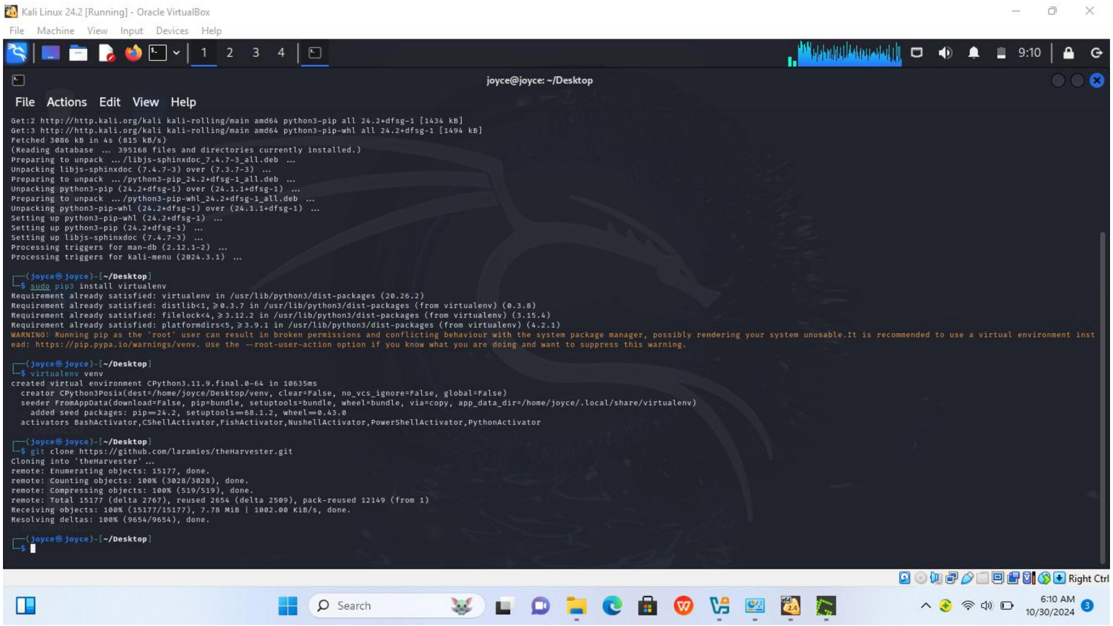
Project Tool: Kali Linux(theHarvester)


Kali Linux 24.2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
9:04
Trash
File System
joyce@joyce: ~/Desktop
File Actions Edit View Help

```
┌──(joyce㉿joyce)-[~/Desktop]
└─$ sudo apt-get install python3-pip
[sudo] password for joyce:
Reading package lists ... Done
Building dependency tree ... 50%
```

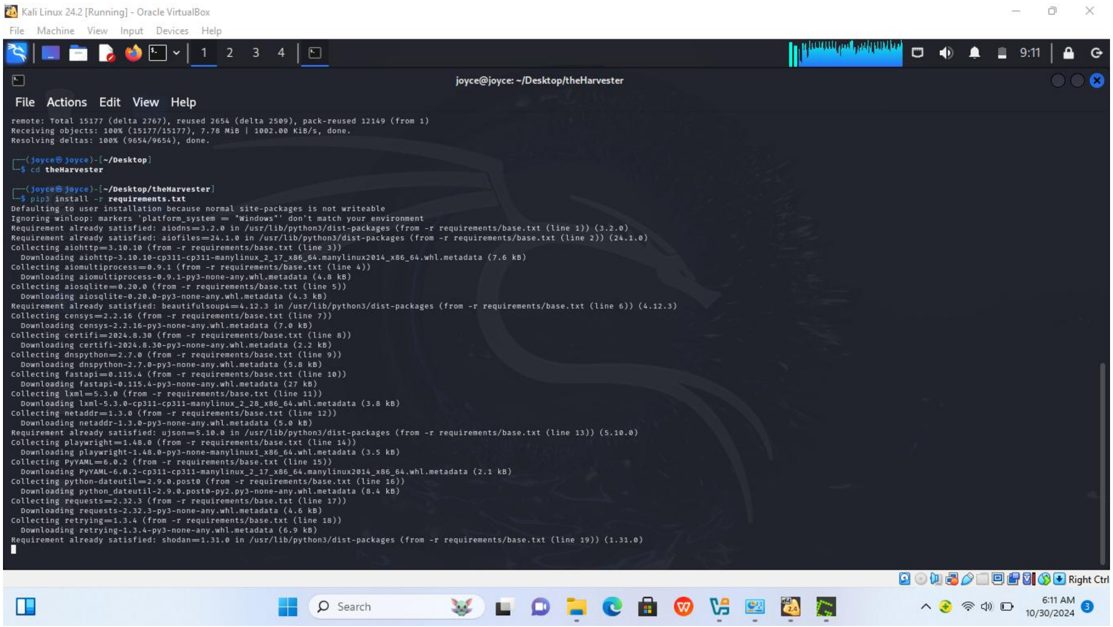

Kali Linux 24.2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
9:08
joyce@joyce: ~/Desktop
File Actions Edit View Help
Right Ctrl
Search
6:08 AM
10/30/2024

```
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 1150 not upgraded.
Need to get 3086 kB of archives.
After this operation, 73.7 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 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 python3-pip all 24.2+dfsg-1 [1434 kB]
Get:3 http://http.kali.org/kali kali-rolling/main amd64 python3-pip-whl all 24.2+dfsg-1 [1494 kB]
Fetched 3086 kB in 4s (815 kB/s)
(Reading database ... 395168 files and directories currently installed.)
Preparing to unpack .../libjs-sphinxdoc_7.4.7-3_all.deb ...
Unpacking libjs-sphinxdoc (7.4.7-3) over (7.3.7-3) ...
Preparing to unpack .../python3-pip_24.2+dfsg-1_all.deb ...
Unpacking python3-pip (24.2+dfsg-1) over (24.1.1+dfsg-1) ...
Preparing to unpack .../python3-pip-whl_24.2+dfsg-1_all.deb ...
Unpacking python3-pip-whl (24.2+dfsg-1) over (24.1.1+dfsg-1) ...
Setting up python3-pip-whl (24.2+dfsg-1) ...
Setting up python3-pip (24.2+dfsg-1) ...
Setting up libjs-sphinxdoc (7.4.7-3) ...
Processing triggers for man-db (2.12.1-2) ...
Processing triggers for kali-menu (2024.3.1) ...

┌──(joyce㉿joyce)-[~/Desktop]
└─$ sudo pip3 install virtualenv
Requirement already satisfied: virtualenv in /usr/lib/python3/dist-packages (20.26.2)
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) (3.15.4)
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 inst
ead: 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.

┌──(joyce㉿joyce)-[~/Desktop]
└─$ virtualenv venv
created virtual environment CPython3.11.9.final.0-64 in 10635ms
  creator CPython3Posix(dest=/home/joyce/Desktop/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/joyce/.local/share/virtualenv)
    added seed packages: pip==24.2, setuptools==68.1.2, wheel==0.43.0
  activators BashActivator,CShellActivator,FishActivator,NushellActivator,PowerShellActivator,PythonActivator

┌──(joyce㉿joyce)-[~/Desktop]
└─$
```


Kali Linux 24.2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
9:10
joyce@joyce: ~/Desktop
File Actions Edit View Help
Right Ctrl
Search
6:10 AM
10/30/2024

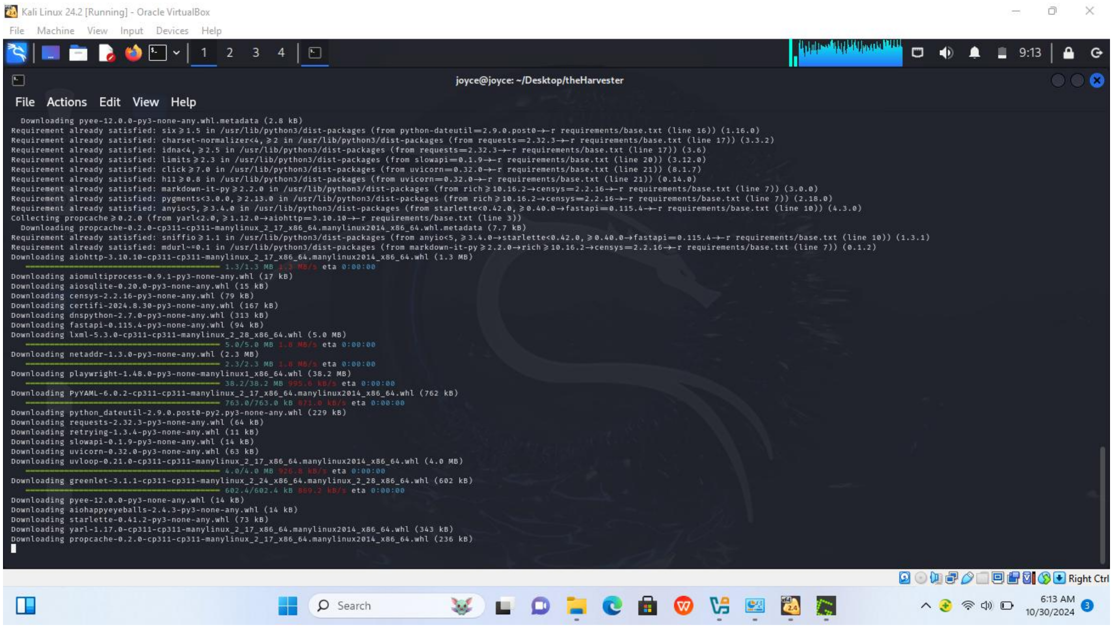
```
Get:2 http://http.kali.org/kali kali-rolling/main amd64 python3-pip all 24.2+dfsg-1 [1434 kB]
Get:3 http://http.kali.org/kali kali-rolling/main amd64 python3-pip-whl all 24.2+dfsg-1 [1494 kB]
Fetched 3086 kB in 4s (815 kB/s)
(Reading database ... 395168 files and directories currently installed.)
Preparing to unpack .../libjs-sphinxdoc_7.4.7-3_all.deb ...
Unpacking libjs-sphinxdoc (7.4.7-3) over (7.3.7-3) ...
Preparing to unpack .../python3-pip_24.2+dfsg-1_all.deb ...
Unpacking python3-pip (24.2+dfsg-1) over (24.1.1+dfsg-1) ...
Preparing to unpack .../python3-pip-whl_24.2+dfsg-1_all.deb ...
Unpacking python3-pip-whl (24.2+dfsg-1) over (24.1.1+dfsg-1) ...
Setting up python3-pip-whl (24.2+dfsg-1) ...
Setting up python3-pip (24.2+dfsg-1) ...
Setting up libjs-sphinxdoc (7.4.7-3) ...
Processing triggers for man-db (2.12.1-2) ...
Processing triggers for kali-menu (2024.3.1) ...

┌──(joyce㉿joyce)-[~/Desktop]
└─$ sudo pip3 install virtualenv
Requirement already satisfied: virtualenv in /usr/lib/python3/dist-packages (20.26.2)
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) (3.15.4)
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 inst
ead: 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.

┌──(joyce㉿joyce)-[~/Desktop]
└─$ virtualenv venv
created virtual environment CPython3.11.9.final.0-64 in 10635ms
  creator CPython3Posix(dest=/home/joyce/Desktop/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/joyce/.local/share/virtualenv)
    added seed packages: pip==24.2, setuptools==68.1.2, wheel==0.43.0
  activators BashActivator,CShellActivator,FishActivator,NushellActivator,PowerShellActivator,PythonActivator

┌──(joyce㉿joyce)-[~/Desktop]
└─$ git clone https://github.com/laramies/theHarvester.git
Cloning into 'theHarvester'...
remote: Enumerating objects: 15177, done.
remote: Counting objects: 100% (3028/3028), done.
remote: Compressing objects: 100% (519/519), done.
remote: Total 15177 (delta 2767), reused 2654 (delta 2509), pack-reused 12149 (from 1)
Receiving objects: 100% (15177/15177), 7.78 MiB | 1002.00 KiB/s, done.
Resolving deltas: 100% (9654/9654), done.

┌──(joyce㉿joyce)-[~/Desktop]
└─$ 
```

Install virtualvenv
Install gitclone of theHarvester


Kali Linux 24.2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
9:11
joyce@joyce: ~/Desktop/theHarvester
File Actions Edit View Help
Right Ctrl
Search
6:11 AM
10/30/2024

```
remote: Total 15177 (delta 2767), reused 2654 (delta 2509), pack-reused 12149 (from 1)
Receiving objects: 100% (15177/15177), 7.78 MiB | 1002.00 KiB/s, done.
Resolving deltas: 100% (9654/9654), done.

┌──(joyce㉿joyce)-[~/Desktop]
└─$ cd theHarvester

┌──(joyce㉿joyce)-[~/Desktop/theHarvester]
└─$ pip3 install -r requirements.txt
Defaulting to user installation because normal site-packages is not writeable
Ignoring winloop: markers 'platform_system == "Windows"' don't match your environment
Requirement already satisfied: aiodns==3.2.0 in /usr/lib/python3/dist-packages (from -r requirements/base.txt (line 1)) (3.2.0)
Requirement already satisfied: aiofiles==24.1.0 in /usr/lib/python3/dist-packages (from -r requirements/base.txt (line 2)) (24.1.0)
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.metadata (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 (from -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==0.115.4 (from -r requirements/base.txt (line 10))
  Downloading fastapi-0.115.4-py3-none-any.whl.metadata (27 kB)
Collecting lxml==5.3.0 (from -r requirements/base.txt (line 11))
  Downloading lxml-5.3.0-cp311-cp311-manylinux_2_28_x86_64.whl.metadata (3.8 kB)
Collecting netaddr==1.3.0 (from -r requirements/base.txt (line 12))
  Downloading netaddr-1.3.0-py3-none-any.whl.metadata (5.0 kB)
Requirement already satisfied: ujson==5.10.0 in /usr/lib/python3/dist-packages (from -r requirements/base.txt (line 13)) (5.10.0)
Collecting playwright==1.48.0 (from -r requirements/base.txt (line 14))
  Downloading playwright-1.48.0-py3-none-manylinux1_x86_64.whl.metadata (3.5 kB)
Collecting PyYAML==6.0.2 (from -r requirements/base.txt (line 15))
  Downloading PyYAML-6.0.2-cp311-cp311-manylinux_2_17_x86_64.manylinux2014_x86_64.whl.metadata (2.1 kB)
Collecting python-dateutil==2.9.0.post0 (from -r requirements/base.txt (line 16))
  Downloading python_dateutil-2.9.0.post0-py2.py3-none-any.whl.metadata (8.4 kB)
Collecting requests==2.32.3 (from -r requirements/base.txt (line 17))
  Downloading requests-2.32.3-py3-none-any.whl.metadata (4.6 kB)
Collecting retrying==1.3.4 (from -r requirements/base.txt (line 18))
  Downloading retrying-1.3.4-py3-none-any.whl.metadata (6.9 kB)
Requirement already satisfied: shodan==1.31.0 in /usr/lib/python3/dist-packages (from -r requirements/base.txt (line 19)) (1.31.0)
```

Installing pip requirements -r

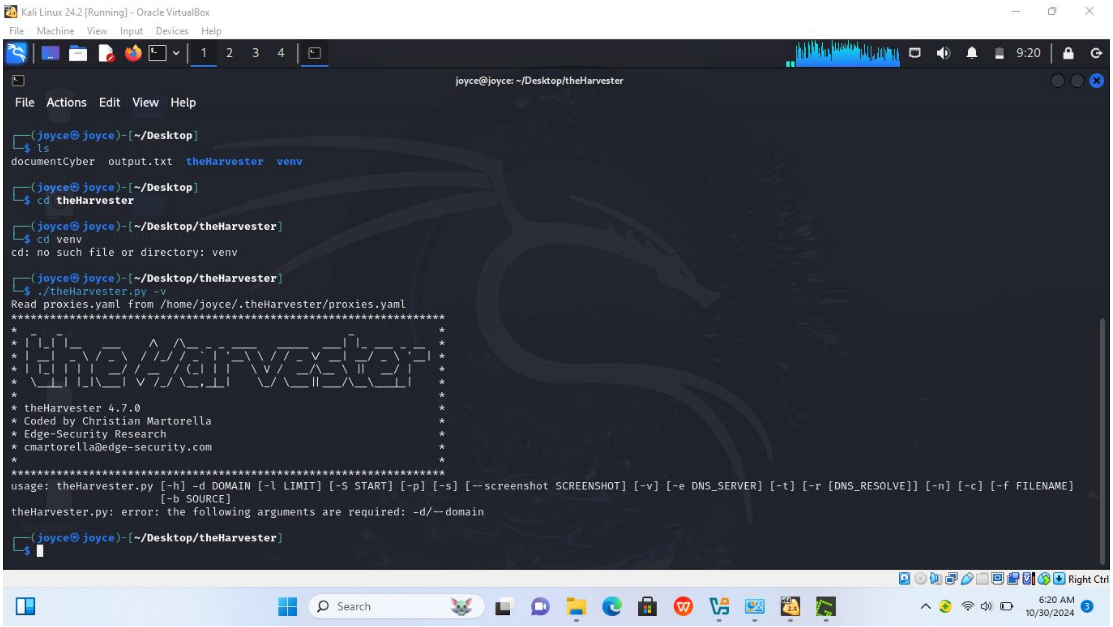


Kali Linux 24.2 [Running] - Oracle VirtualBox

joyce@joyce: ~/Desktop/theHarvester

```
  Downloading pyee-12.0.0-py3-none-any.whl.metadata (2.8 kB)
Requirement already satisfied: six≥1.5 in /usr/lib/python3/dist-packages (from python-dateutil==2.9.0.post0→-r requirements/base.txt (line 16)) (1.16.0)
Requirement already satisfied: charset-normalizer<4,≥2 in /usr/lib/python3/dist-packages (from requests==2.32.3→-r requirements/base.txt (line 17)) (3.3.2)
Requirement already satisfied: idna<4,≥2.5 in /usr/lib/python3/dist-packages (from requests==2.32.3→-r requirements/base.txt (line 17)) (3.6)
Requirement already satisfied: limits≥2.3 in /usr/lib/python3/dist-packages (from slowapi==0.1.9→-r requirements/base.txt (line 20)) (3.12.0)
Requirement already satisfied: click≥7.0 in /usr/lib/python3/dist-packages (from uvicorn==0.32.0→-r requirements/base.txt (line 21)) (8.1.7)
Requirement already satisfied: h11≥0.8 in /usr/lib/python3/dist-packages (from uvicorn==0.32.0→-r requirements/base.txt (line 21)) (0.14.0)
Requirement already satisfied: markdown-it-py≥2.2.0 in /usr/lib/python3/dist-packages (from rich≥10.16.2→censys==2.2.16→-r requirements/base.txt (line 7)) (3.0.0)
Requirement already satisfied: pygments<3.0.0,≥2.13.0 in /usr/lib/python3/dist-packages (from rich≥10.16.2→censys==2.2.16→-r requirements/base.txt (line 7)) (2.18.0)
Requirement already satisfied: anyio<5,≥3.4.0 in /usr/lib/python3/dist-packages (from starlette<0.42.0,≥0.40.0→fastapi==0.115.4→-r requirements/base.txt (line 10)) (4.3.0)
Collecting propcache≥0.2.0 (from yarl<2.0,≥1.12.0→aiohttp==3.10.10→-r requirements/base.txt (line 3))
  Downloading propcache-0.2.0-cp311-cp311-manylinux_2_17_x86_64.manylinux2014_x86_64.whl.metadata (7.7 kB)
Requirement already satisfied: sniffio≥1.1 in /usr/lib/python3/dist-packages (from anyio<5,≥3.4.0→starlette<0.42.0,≥0.40.0→fastapi==0.115.4→-r requirements/base.txt (line 10)) (1.3.1)
Requirement already satisfied: mdurl~=0.1 in /usr/lib/python3/dist-packages (from markdown-it-py≥2.2.0→rich≥10.16.2→censys==2.2.16→-r requirements/base.txt (line 7)) (0.1.2)
Downloading aiohttp-3.10.10-cp311-cp311-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (1.3 MB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 1.3/1.3 MB 1.3 MB/s eta 0:00:00
Downloading aiomultiprocess-0.9.1-py3-none-any.whl (17 kB)
Downloading aiosqlite-0.20.0-py3-none-any.whl (15 kB)
Downloading censys-2.2.16-py3-none-any.whl (79 kB)
Downloading certifi-2024.8.30-py3-none-any.whl (167 kB)
Downloading dnspython-2.7.0-py3-none-any.whl (313 kB)
Downloading fastapi-0.115.4-py3-none-any.whl (94 kB)
Downloading lxml-5.3.0-cp311-cp311-manylinux_2_28_x86_64.whl (5.0 MB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 5.0/5.0 MB 1.8 MB/s eta 0:00:00
Downloading netaddr-1.3.0-py3-none-any.whl (2.3 MB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 2.3/2.3 MB 1.8 MB/s eta 0:00:00
Downloading playwright-1.48.0-py3-none-manylinux1_x86_64.whl (38.2 MB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 38.2/38.2 MB 995.0 kB/s eta 0:00:00
Downloading PyYAML-6.0.2-cp311-cp311-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (762 kB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 763.0/763.0 kB 871.0 kB/s eta 0:00:00
Downloading python_dateutil-2.9.0.post0-py2.py3-none-any.whl (229 kB)
Downloading requests-2.32.3-py3-none-any.whl (64 kB)
Downloading retrying-1.3.4-py3-none-any.whl (11 kB)
Downloading slowapi-0.1.9-py3-none-any.whl (14 kB)
Downloading uvicorn-0.32.0-py3-none-any.whl (63 kB)
Downloading uvloop-0.21.0-cp311-cp311-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (4.0 MB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 4.0/4.0 MB 920.8 kB/s eta 0:00:00
Downloading greenlet-3.1.1-cp311-cp311-manylinux_2_24_x86_64.manylinux_2_28_x86_64.whl (602 kB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 602.4/602.4 kB 869.2 kB/s eta 0:00:00
Downloading pyee-12.0.0-py3-none-any.whl (14 kB)
Downloading aiohappyeyeballs-2.4.3-py3-none-any.whl (14 kB)
Downloading starlette-0.41.2-py3-none-any.whl (73 kB)
Downloading yarl-1.17.0-cp311-cp311-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (343 kB)
Downloading propcache-0.2.0-cp311-cp311-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (236 kB)
```

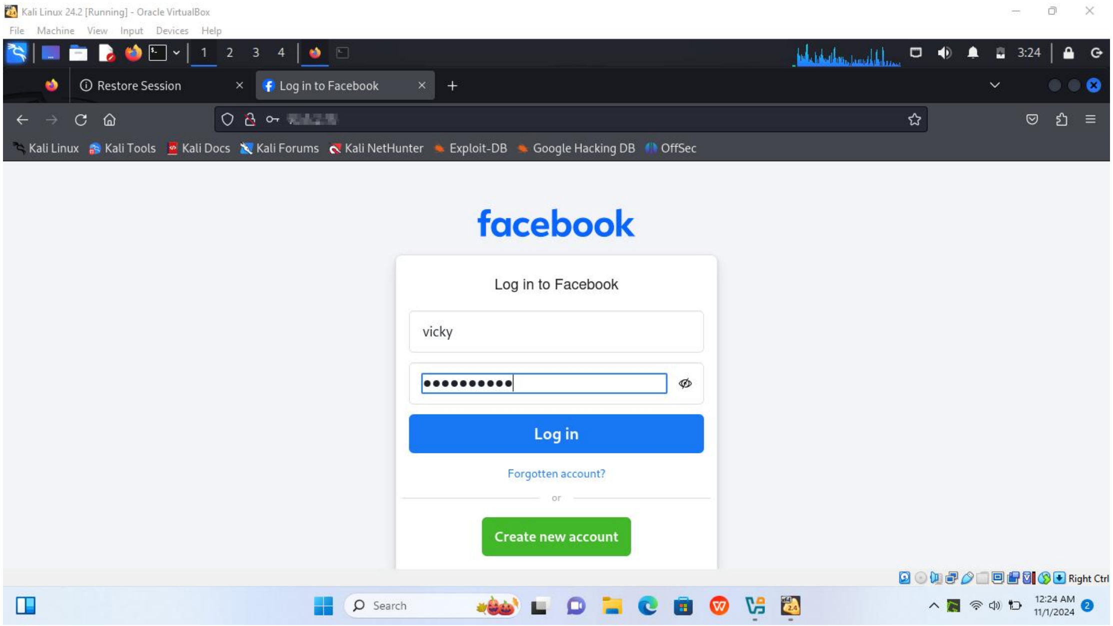
```
cd /home/kali/theHarvester/
./theHarvester.py -v
```



Kali Linux 24.2 [Running] - Oracle VirtualBox

joyce@joyce: ~/Desktop/theHarvester

```
┌──(joyce㉿joyce)-[~/Desktop]
└─$ ls
documentCyber  output.txt  theHarvester  venv

┌──(joyce㉿joyce)-[~/Desktop]
└─$ cd theHarvester

┌──(joyce㉿joyce)-[~/Desktop/theHarvester]
└─$ cd venv
cd: no such file or directory: venv

┌──(joyce㉿joyce)-[~/Desktop/theHarvester]
└─$ ./theHarvester.py -v
Read proxies.yaml from /home/joyce/.theHarvester/proxies.yaml
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* 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

┌──(joyce㉿joyce)-[~/Desktop/theHarvester]
└─$ 
```



Kali Linux 24.2 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Restore Session | Log in to Facebook

[redacted]

facebook

Log in to Facebook

vicky

●●●●●●●●●●

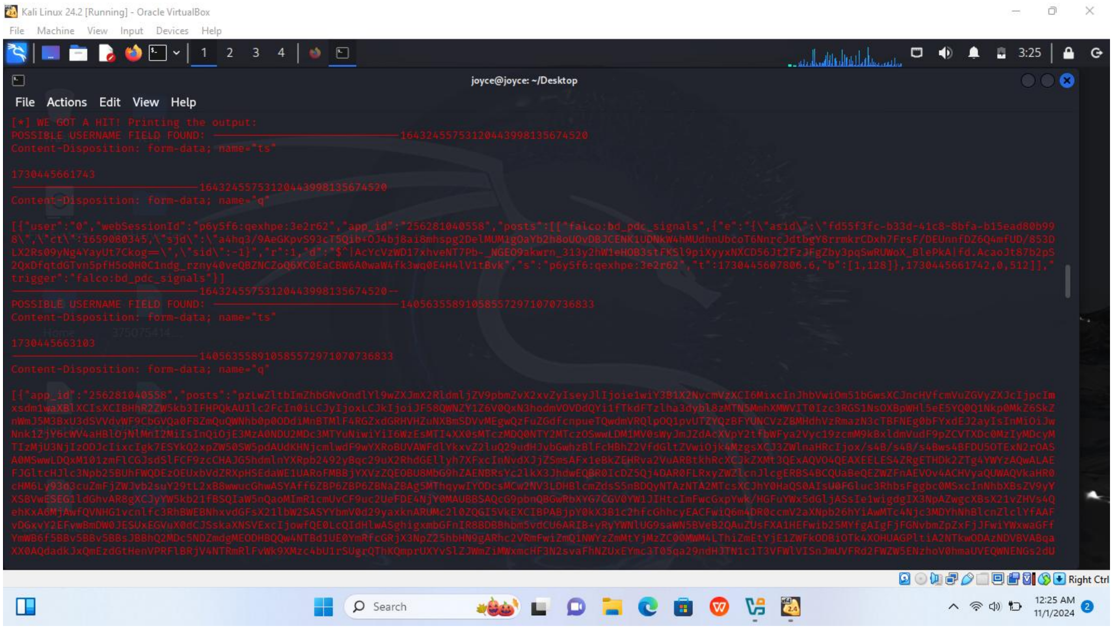
Log in

Forgotten account?

or

Create new account

Navigating the cloned facebook login form with local IP address. Inputing random username and password, and log in

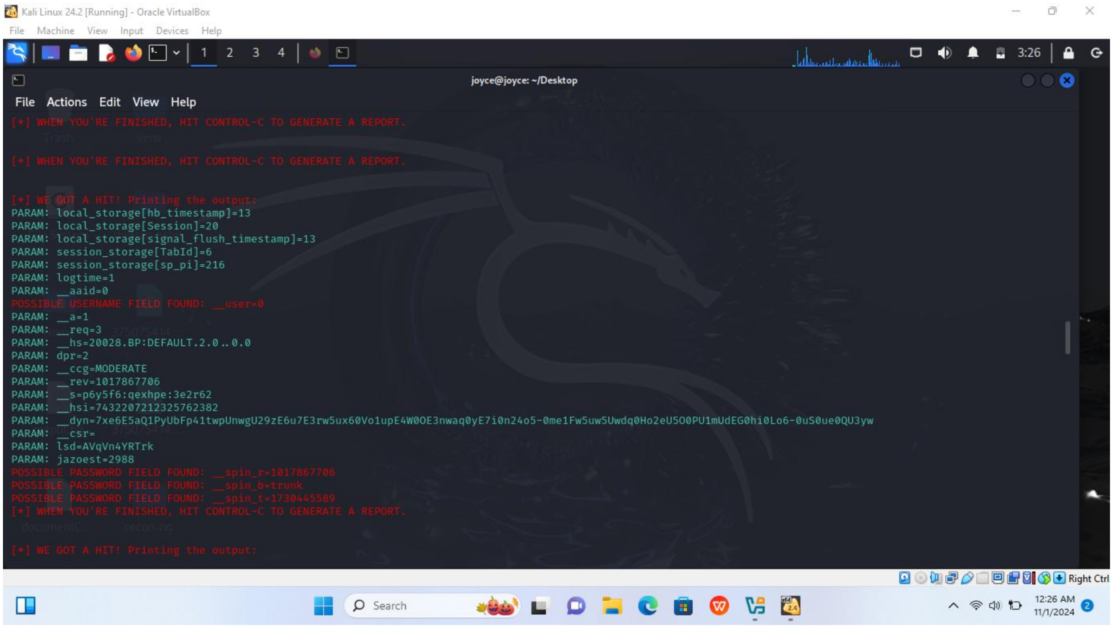


Kali Linux 24.2 [Running] - Oracle VirtualBox

joyce@joyce: ~/Desktop

```
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: ----------------------------164324557531204439981356745 20
Content-Disposition: form-data; name="ts"

1730445661743
-----------------------------164324557531204439981356745 20
Content-Disposition: form-data; name="q"

[{"user":"0","webSessionId":"p6y5f6:qexhpe:3e2r62","app_id":"256281040558","posts":[["falco:bd_pdc_signals",{"e":"{\"asid\":\"fd55f3fc-b33d-41c8-8bfa-b15ead80b99
8\",\"ct\":1659080345,\"sjd\":\"a4hq3/9AeGKpvS93cT5Qib+OJ4bj8ai8mhspg2DelMUM1gOaYb2h8oUOvDBJCENK1UDNkW4hMUdhnUbcoT6NnrcJdtbgY8rrmkrCDxh7FrsF/DEUnnfDZ6Q4mfUD/853D
LX2Rs09yNg4YayUt7Ckog==\",\"sid\":-1}","r":1,"d":"$^|AcYcVzWD17xhveNT7Pb-_NGEO9akwrn_313y2hW1eHOB3stFKSl9piXyyxNXCD56Jt2FzJFgZby3pqSwRUWoX_BlePkA|fd.AcaoJt87b2pS
2QxDfqtdGTvn5pfH5o0H0C1ndg_rzny40veQBZNCZoQ6XC0EaCBW6A0waW4fk3wq0E4H4lV1tBvk","s":"p6y5f6:qexhpe:3e2r62","t":1730445607806.6,"b":[1,128]},1730445661742,0,512]],"
trigger":"falco:bd_pdc_signals"}]
-----------------------------164324557531204439981356745 20--
POSSIBLE USERNAME FIELD FOUND: ----------------------------140563558910585572971070736833
Content-Disposition: form-data; name="ts"

1730445663103
-----------------------------140563558910585572971070736833
Content-Disposition: form-data; name="q"

[{"app_id":"256281040558","posts":"pzLwZltbImZhbGNvOndlYl9wZXJmX2RldmljZV9pbmZvX2xvZyIseyJlIjoie1wiY3B1X2NvcmVzXCI6MixcInJhbVwiOm51bGwsXCJncHVfcmVuZGVyZXJcIjpcIm
xsdm1waXBlXCIsXCIBHhR2ZW5kb3IFHPQkAU1lc2FcIn0iLCJyIjoxLCJkIjoiJF58QWNZY1Z6V0QxN3hodmVOVDdQYi1fTkdFTzlha3dybl8zMTN5MmhXMWVIT0Izc3RGS1NsOXBpWHl5eE5YQ0Q1Nkp0MkZ6SkZ
nWmJ5M3BxU3dSVVdvWF9CbGVQa0F8ZmQuQWNhb0p0ODdiMnBTMlF4RGZxdGRHVHZuNXBmSDVvMEgwQzFuZGdfcnpueTQwdmVRQlpOQ1pvUTZYQzBFYUNCVzZBMHdhVzRmazN3cTBFNEg0bFYxdEJ2ayIsInMiOiJw
Nnk1ZjY6cWV4aHBlOjNlMnI2MiIsInQiOjE3MzA0NDU2MDc3MTYuNiwiYiI6WzEsMTI4XX0sMTczMDQ0NTY2MTczOSwwLDM1MV0sWyJmJZdAcXVpY2tfbWFya2Vyc19zcmM9kBxldmVudF9pZCVTXDc0MzIyMDcyM
TIzMjU3NjIzODJcIixcIgk7ESYkQ2xpZW50SW5pdAUdKHNjcmlwdF9wYXRoBUVAWFdlYkxvZ2luQ29udHJvbGwhzBlFcHBhZ2VfdGltZVwiOjk4MzgsXCJ3ZWlnaHRcIjox/s4B/s4B/s4Bws4BFDU5OTExN2rOAS
A0MSwwLDQxM101zmFlCGJsdSlFCF9zcCHAJG5hdmlnYXRpb2492yBqc29uX2RhdGEllyh7XFxcInNvdXJjZSmsAFx1eBkZEHRva2VuARBtkhRcXCJkZXMt3QExAQVO4QEAXEELES4ZRgETHDk2ZTg4YWYzAQwALAE
FJGltcHJlc3Npb25BUhFWQDEzOEUxbVdZRXpHSEdaWE1UARoFMBBjYXVzZQEOBU8MbG9hZAENBRsYc2lkX3JhdwEQBR0IcDZ5Qj4DAR0FLRxyZWZlcnJlcgERBS4BCQUaBeQEZWZFnAEVOv4ACHVyaQUWAQVkaHR0
cHM6Ly93d3cuZmFjZWJvb2suY29tL2xB8wwucGhwASYAff6ZBP6ZBP6ZBNaZBAg5MThqywIYODcsMCw2NV3LDHBlcmZdsS5nBDQyNTAzNTA2MTcsXCJhY0HaQS0AIsU0FGluc3RhbsFggbc0MSxcInNhbXBsZV9yY
XSBVwESEG1ldGhvAR8gXCJyYW5kb21fBSQIaW5nQaoMImR1cmUvCF9uc2UeFDE4NjY0MAUBBSAQcG9pbnQBGwRbXYG7CGV0YW1JIHtcImFwcGxpYwk/HGFuYWx5dGljASsIe1wigdgIX3NpAZwgcXBsX21vZHVs4Q
ehKxAGMjAwfQVNHG1vcnlfc3RhBWEBNhxvdGFsX21lbW2SASYYbmV0d29yaxknARUMc2l0ZQGI5VkEXCIBPABjpY0kX3B1c2hfcGhhcyEACFwiQ6m4DR0ccmV2aXNpb26hYiAwMTc4Njc3MDYhNhBlcnZlclYfAAF
vDGxvY2EFvwBmDW0JESUxEGVuX0dCJSskaXNSVExcIjowfQE0LcQIdHlwASghigxmbGFnIR8BDBBhbm5vdCU6ARIB+yRyYWNlUG9saWN5BVeB2QAuZUsFXA1HEFwib25MYfgAIgFjFGNvbmZpZxFjJFwiYWxwaGFf
YmWB6f5BBv5BBv5BBsJBBhQ2MDc5NDZmdgMEODHBQQw4NTBd1UE0YmRfcGRjX3NpZ25hbHN9gARhc2VRmFwiZmQ1NWYzZmMtYjMzZC00MWM4LThiZmEtYjE1ZWFkODBiOTk4XOHUAGPltiA2NTkwODAzNDVBVABqa
XX0AQdadkJxQmEzdGtHenVPRFlBRjV4NTRmRlFvWk9XMzc4bU1rSUgrQThKQmprUXYvSlZJWmZiMWxmcHF3N2svaFhNZUxEYmc3T05qa29ndHJTN1c1T3VFWlVISnJmUVFRd2FWZW5ENzhoV0hmaUVEQWNENGs2dU
```

These are the username and password fields generated by the login form.



Kali Linux 24.2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
joyce@joyce: ~/Desktop
File Actions Edit View Help
3:26
Right Ctrl
Search
12:26 AM
11/1/2024

```
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


[*] WE GOT A HIT! Printing the output:
PARAM: local_storage[hb_timestamp]=13
PARAM: local_storage[Session]=20
PARAM: local_storage[signal_flush_timestamp]=13
PARAM: session_storage[TabId]=6
PARAM: session_storage[sp_pi]=216
PARAM: logtime=1
PARAM: __aaid=0
POSSIBLE USERNAME FIELD FOUND: __user=0
PARAM: __a=1
PARAM: __req=3
PARAM: __hs=20028.BP:DEFAULT.2.0..0.0
PARAM: dpr=2
PARAM: __ccg=MODERATE
PARAM: __rev=1017867706
PARAM: __s=p6y5f6:qexhpe:3e2r62
PARAM: __hsi=7432207212325762382
PARAM: __dyn=7xe6E5aQ1PyUbFp41twpUnwgU29zE6u7E3rw5ux60Vo1upE4W0OE3nwaq0yE7i0n24o5-0me1Fw5uw5Uwdq0Ho2eU5O0PU1mUdEG0hi0Lo6-0uS0ue0QU3yw
PARAM: __csr=
PARAM: lsd=AVqVn4YRTrk
PARAM: jazoest=2988
POSSIBLE PASSWORD FIELD FOUND: __spin_r=1017867706
POSSIBLE PASSWORD FIELD FOUND: __spin_b=trunk
POSSIBLE PASSWORD FIELD FOUND: __spin_t=1730445589
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

[*] WE GOT A HIT! Printing the output:
```