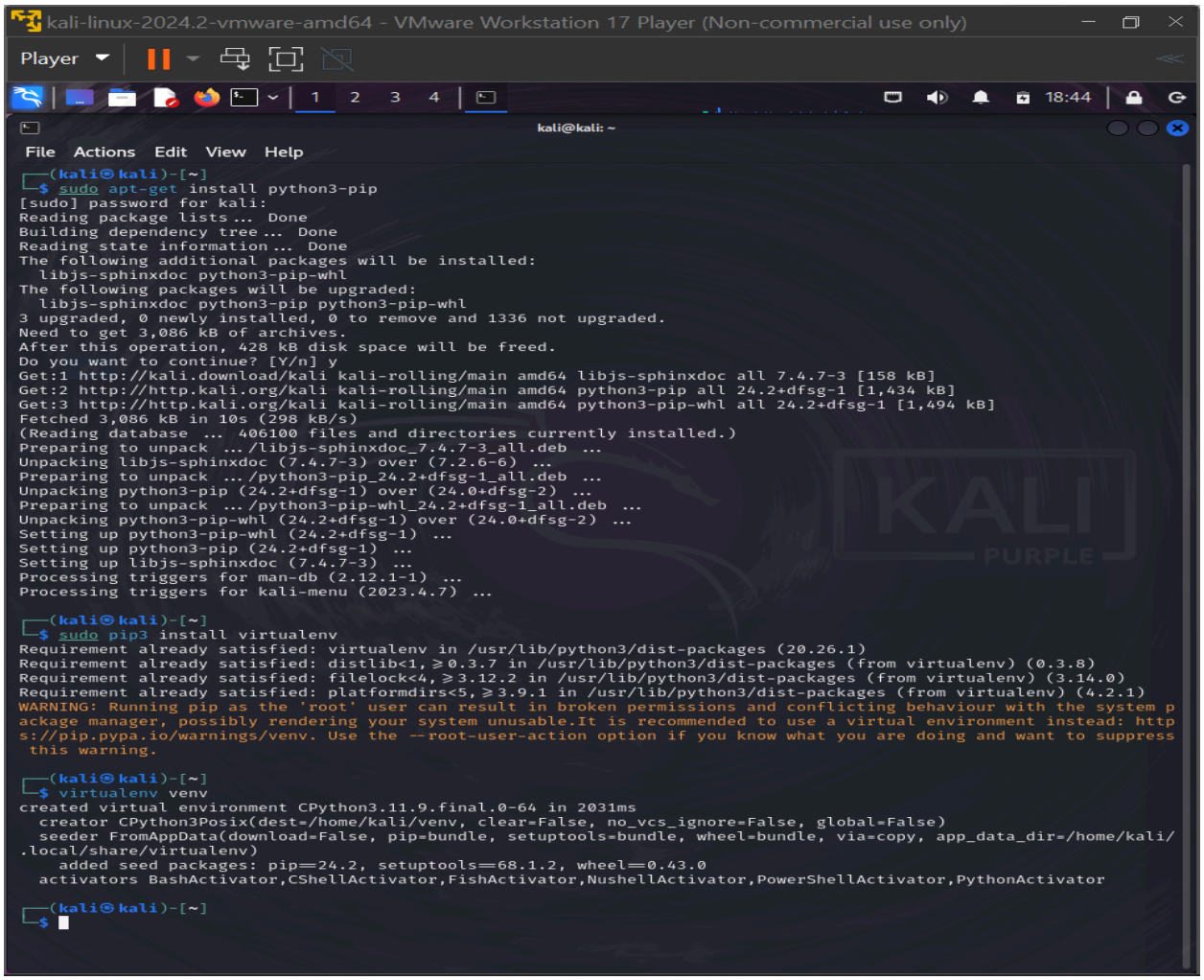
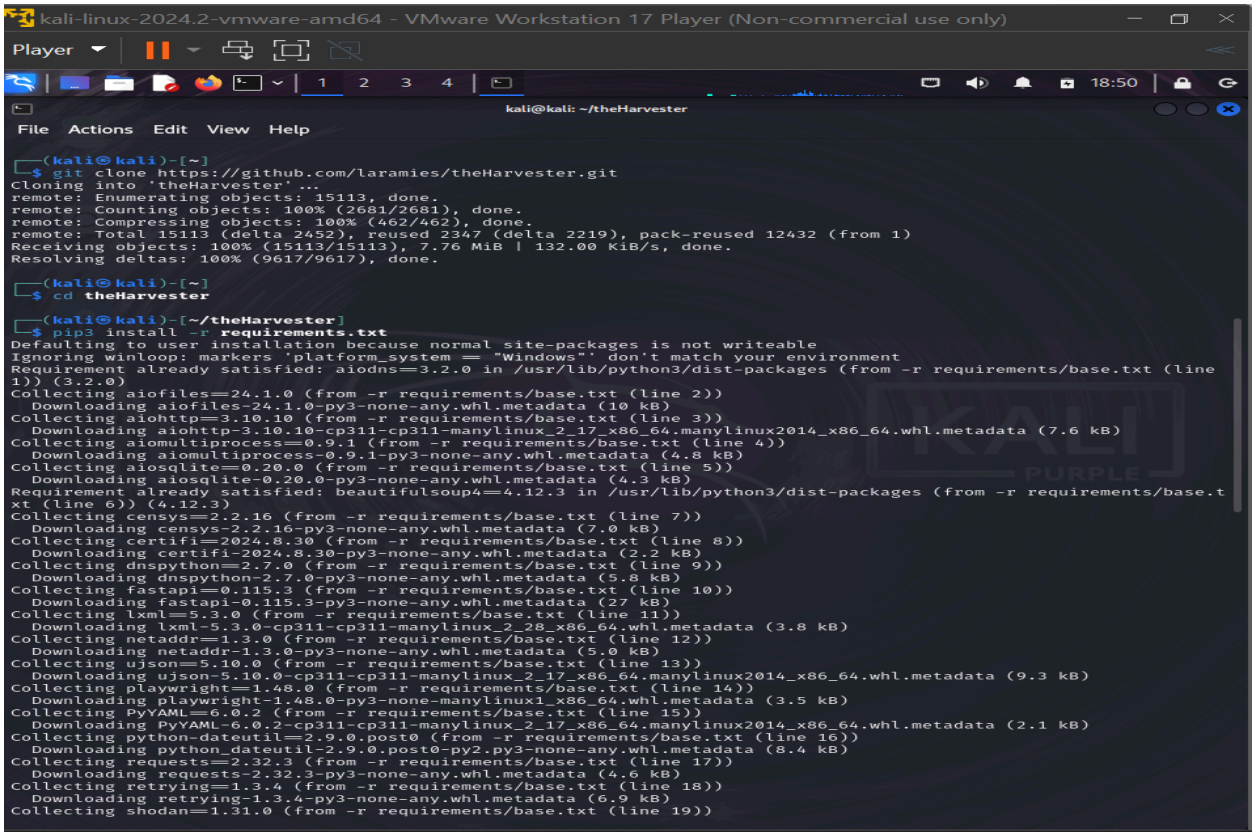
GATHERING OF INFORMATION USING THEHARVESTER

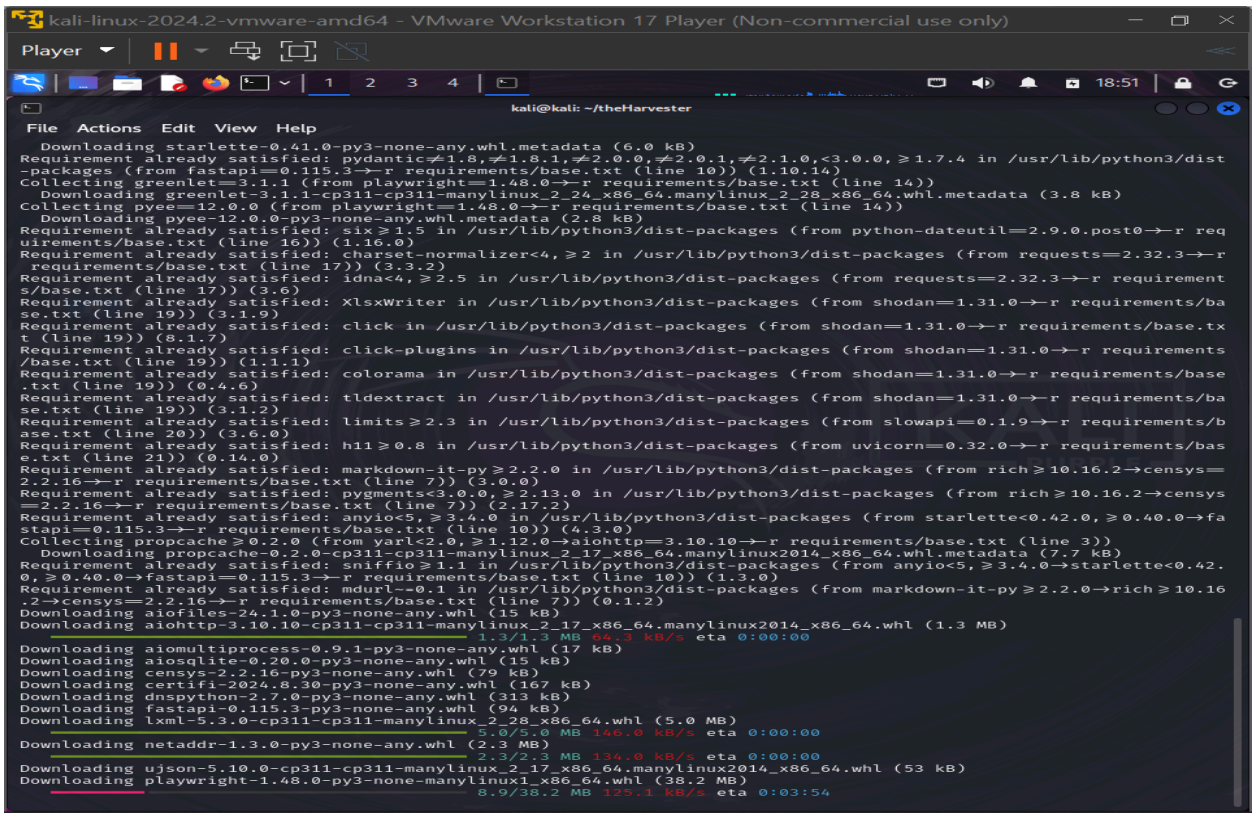
Tools : KALI LINUX [THEHARVESTER]
Project-Site : hackaday.com

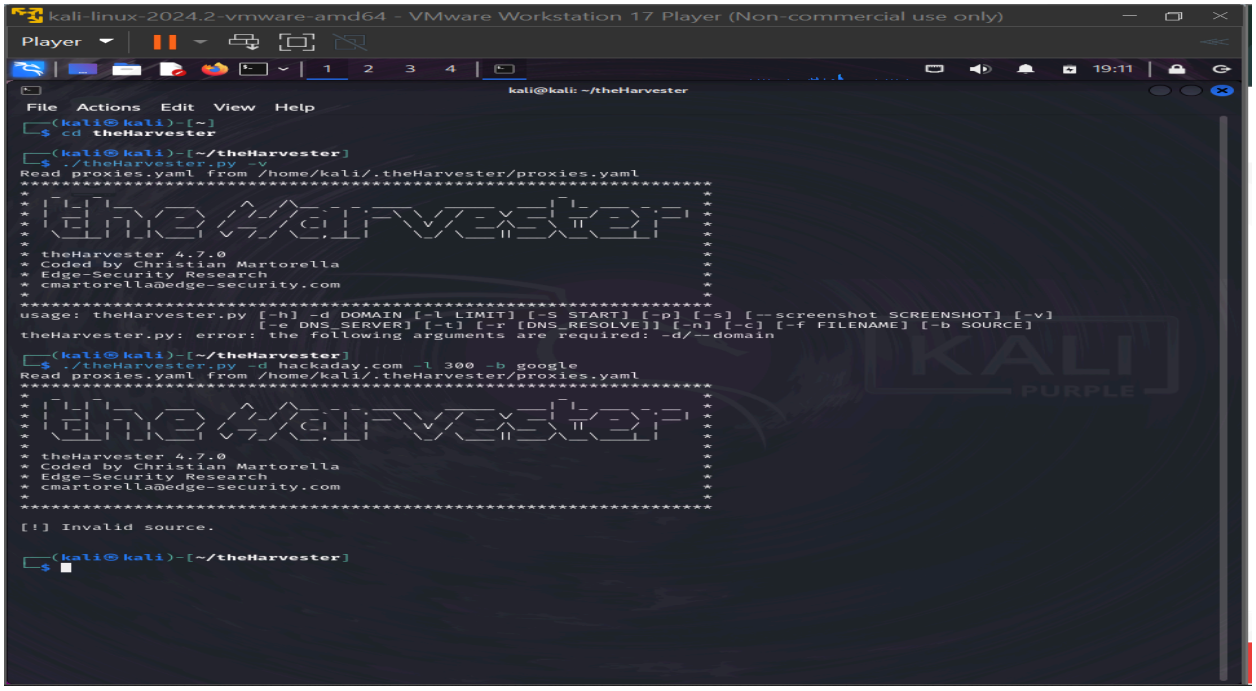
TheHarvester is an open-source intelligence (OSINT) tool used for gathering information about a target. It can collect email addresses, subdomains, and other data from various public sources, including search engines and social media. It's often used in security assessments and penetration testing to help identify potential vulnerabilities.

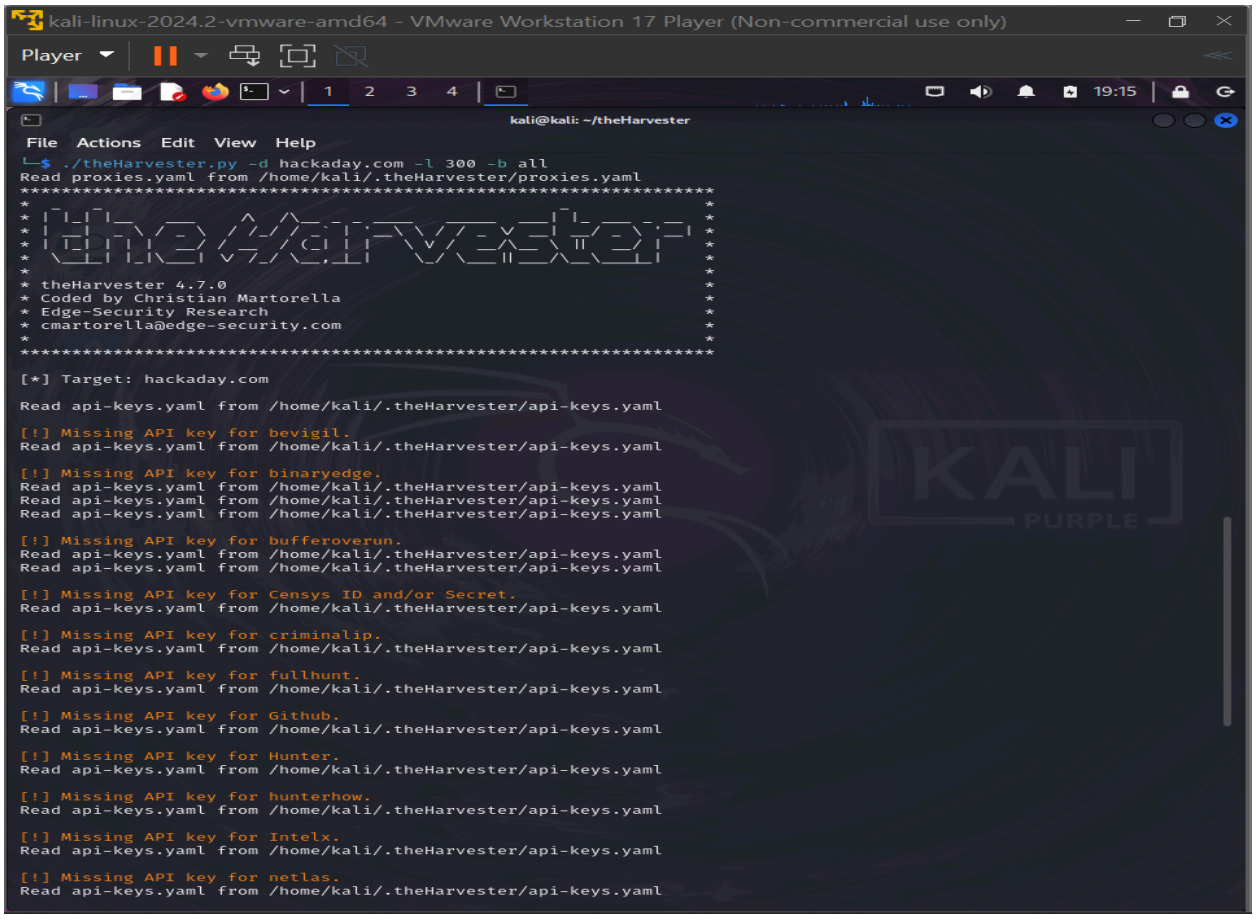
Input from Kali : theHarvester

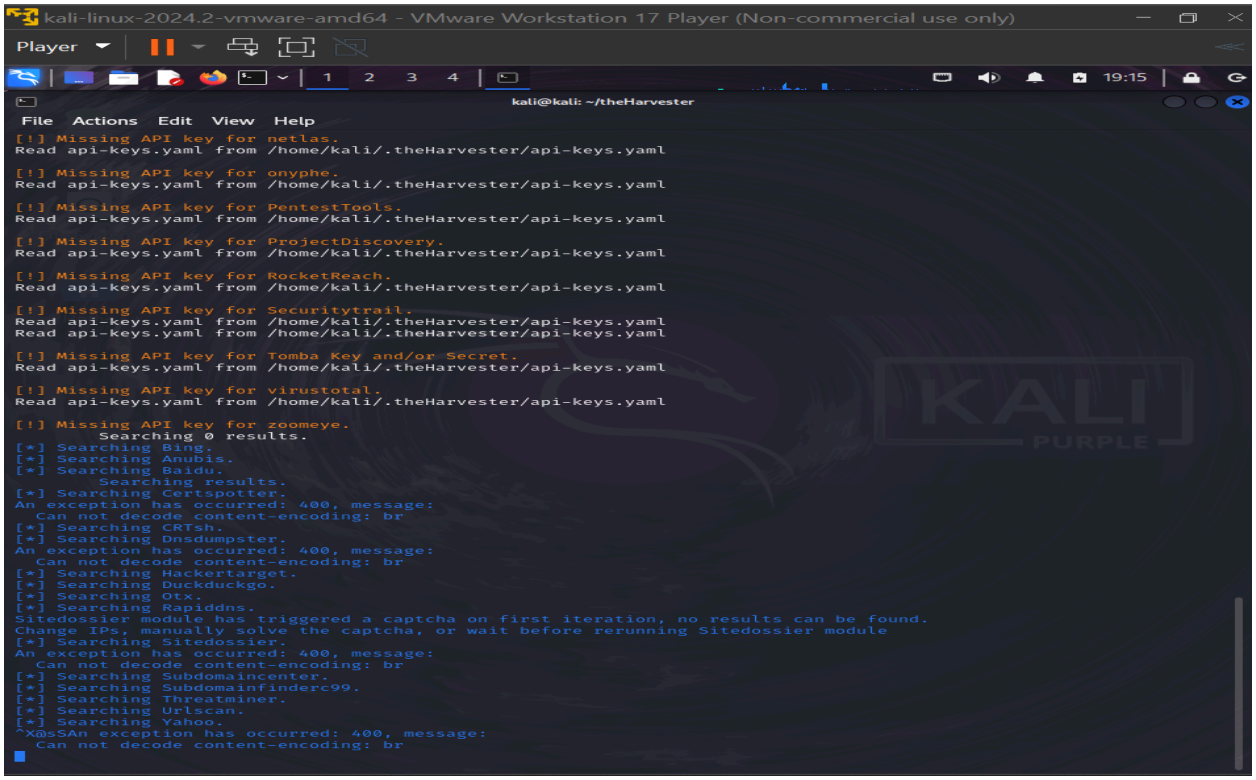


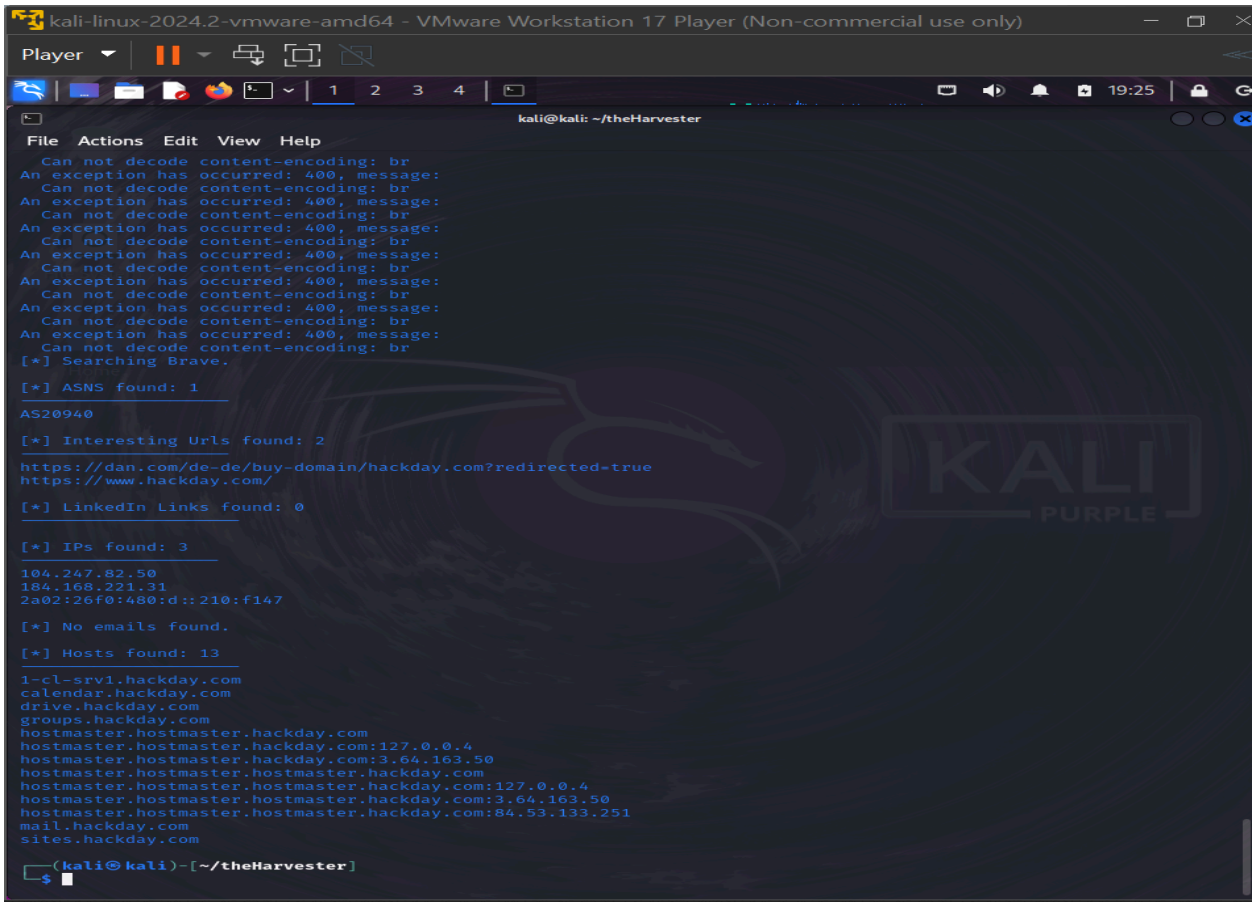

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
18:50
kali@kali: ~/theHarvester
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/laramies/theHarvester.git
Cloning into 'theHarvester'...
remote: Enumerating objects: 15113, done.
remote: Counting objects: 100% (2681/2681), done.
remote: Compressing objects: 100% (462/462), done.
remote: Total 15113 (delta 2452), reused 2347 (delta 2219), pack-reused 12432 (from 1)
Receiving objects: 100% (15113/15113), 7.76 MiB | 132.00 KiB/s, done.
Resolving deltas: 100% (9617/9617), done.
┌──(kali㉿kali)-[~]
└─$ cd theHarvester
┌──(kali㉿kali)-[~/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)
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.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==0.115.3 (from -r requirements/base.txt (line 10))
Downloading fastapi-0.115.3-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)
Collecting ujson==5.10.0 (from -r requirements/base.txt (line 13))
Downloading ujson-5.10.0-cp311-cp311-manylinux_2_17_x86_64.manylinux2014_x86_64.whl.metadata (9.3 kB)
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)
Collecting shodan==1.31.0 (from -r requirements/base.txt (line 19))

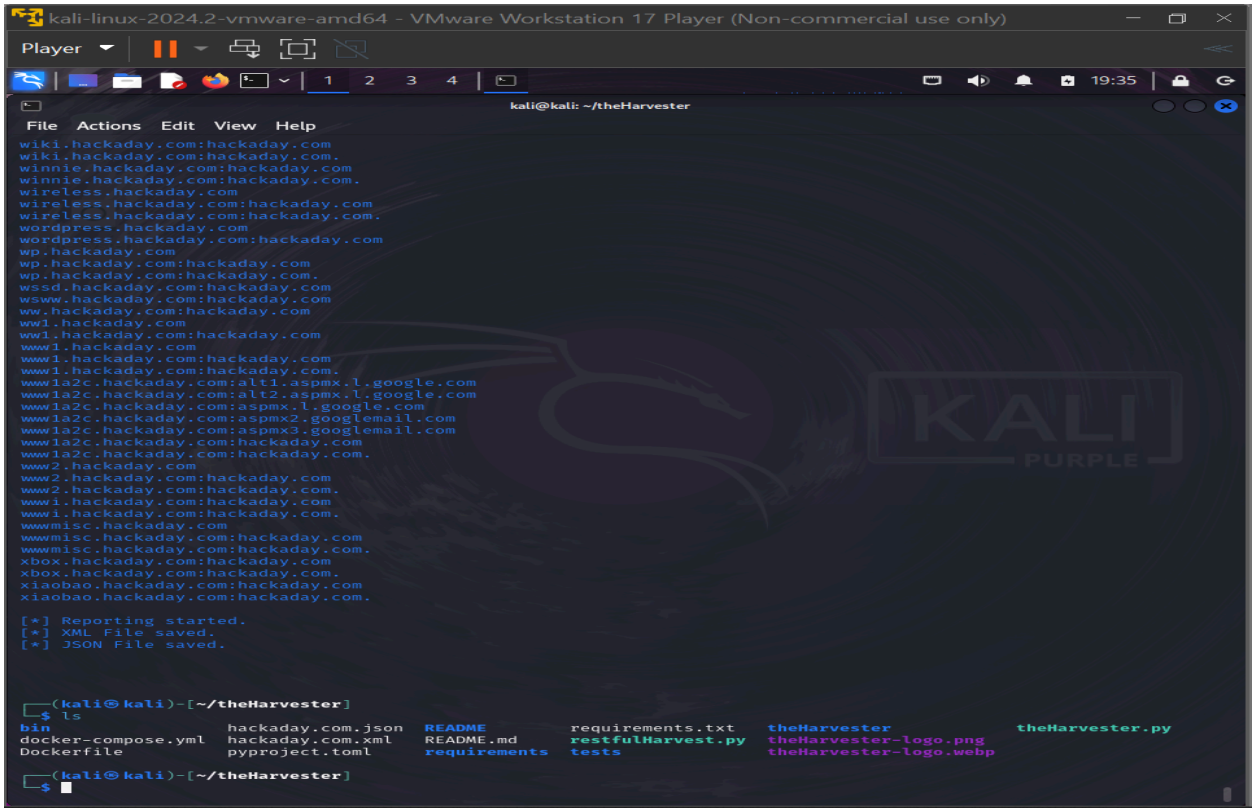

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
18:51
kali@kali: ~/theHarvester
File Actions Edit View Help
Downloading starlette-0.41.0-py3-none-any.whl.metadata (6.0 kB)
Requirement already satisfied: pydantic≠1.8,≠1.8.1,≠2.0.0,≠2.0.1,≠2.1.0,<3.0.0,≥1.7.4 in /usr/lib/python3/dist-packages (from fastapi==0.115.3→-r requirements/base.txt (line 10)) (1.10.14)
Collecting greenlet==3.1.1 (from playwright==1.48.0→-r requirements/base.txt (line 14))
Downloading greenlet-3.1.1-cp311-cp311-manylinux_2_24_x86_64.manylinux_2_28_x86_64.whl.metadata (3.8 kB)
Collecting pyee==12.0.0 (from playwright==1.48.0→-r requirements/base.txt (line 14))
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: XlsxWriter in /usr/lib/python3/dist-packages (from shodan==1.31.0→-r requirements/base.txt (line 19)) (3.1.9)
Requirement already satisfied: click in /usr/lib/python3/dist-packages (from shodan==1.31.0→-r requirements/base.txt (line 19)) (8.1.7)
Requirement already satisfied: click-plugins in /usr/lib/python3/dist-packages (from shodan==1.31.0→-r requirements/base.txt (line 19)) (1.1.1)
Requirement already satisfied: colorama in /usr/lib/python3/dist-packages (from shodan==1.31.0→-r requirements/base.txt (line 19)) (0.4.6)
Requirement already satisfied: tldextract in /usr/lib/python3/dist-packages (from shodan==1.31.0→-r requirements/base.txt (line 19)) (3.1.2)
Requirement already satisfied: limits≥2.3 in /usr/lib/python3/dist-packages (from slowapi==0.1.9→-r requirements/base.txt (line 20)) (3.6.0)
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)) (2.17.2)
Requirement already satisfied: anyio<5,≥3.4.0 in /usr/lib/python3/dist-packages (from starlette<0.42.0,≥0.40.0→fastapi==0.115.3→-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==0.115.3→-r requirements/base.txt (line 10)) (1.3.0)
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 aiofiles-24.1.0-py3-none-any.whl (15 kB)
Downloading aiohttp-3.10.10-cp311-cp311-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (1.3 MB)
1.3/1.3 MB 64.3 kB/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-0.115.3-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 146.0 kB/s eta 0:00:00
Downloading netaddr-1.3.0-py3-none-any.whl (2.3 MB)
2.3/2.3 MB 134.0 kB/s eta 0:00:00
Downloading ujson-5.10.0-cp311-cp311-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (53 kB)
Downloading playwright-1.48.0-py3-none-manylinux1_x86_64.whl (38.2 MB)
8.9/38.2 MB 125.1 kB/s eta 0:03:54

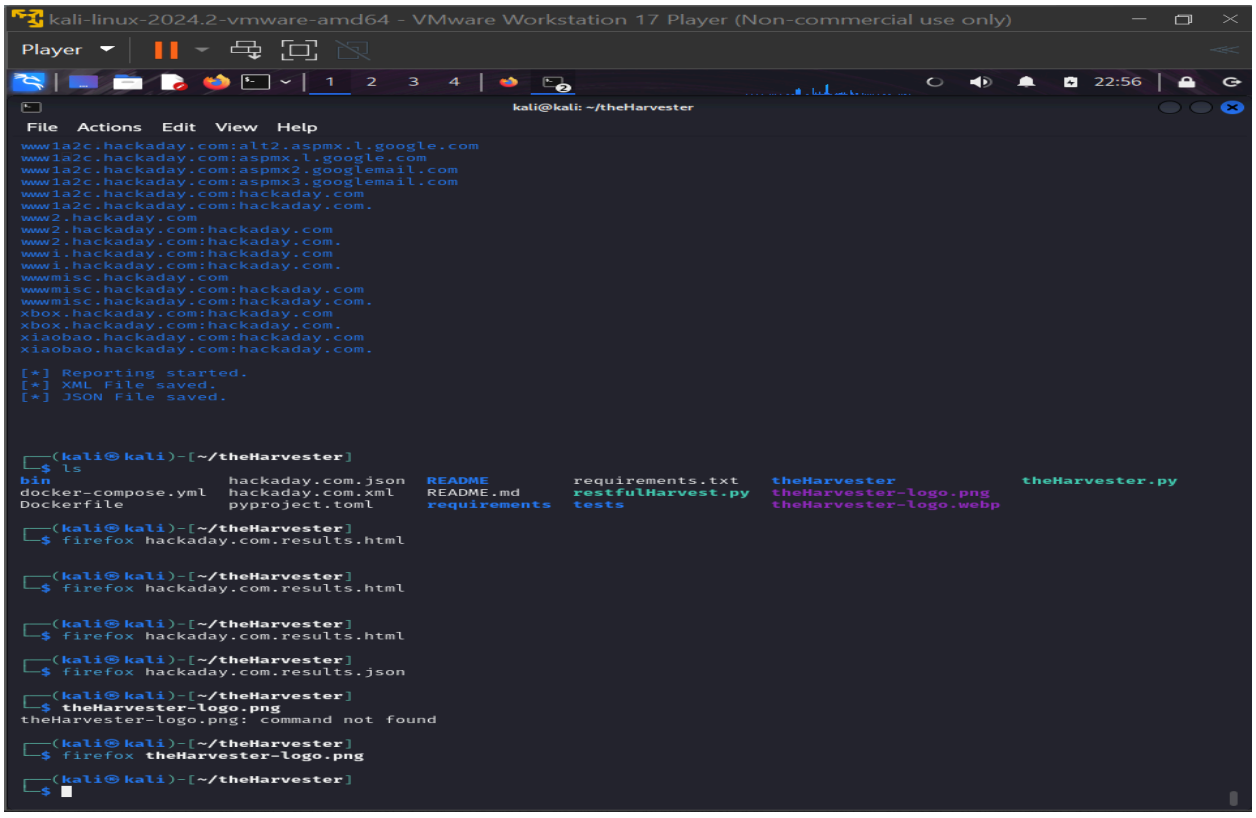

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
19:11
kali@kali: ~/theHarvester
File Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ cd theHarvester
┌──(kali㉿kali)-[~/theHarvester]
└─$ ./theHarvester.py -v
Read proxies.yaml from /home/kali/.theHarvester/proxies.yaml
* 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
┌──(kali㉿kali)-[~/theHarvester]
└─$ ./theHarvester.py -d hackaday.com -l 300 -b google
Read proxies.yaml from /home/kali/.theHarvester/proxies.yaml
* theHarvester 4.7.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
[!] Invalid source.
┌──(kali㉿kali)-[~/theHarvester]
└─$


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
19:15
kali@kali: ~/theHarvester
File Actions Edit View Help
└─$ ./theHarvester.py -d hackaday.com -l 300 -b all
Read proxies.yaml from /home/kali/.theHarvester/proxies.yaml
* theHarvester 4.7.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
[*] Target: hackaday.com
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for bevigil.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for binaryedge.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for bufferoverun.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for Censys ID and/or Secret.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for criminalip.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for fullhunt.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for Github.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for Hunter.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for hunterhow.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for Intelx.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for netlas.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
19:15
kali@kali: ~/theHarvester
File Actions Edit View Help
[!] Missing API key for netlas.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for onyphe.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for PentestTools.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for ProjectDiscovery.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for RocketReach.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for Securitytrail.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for Tomba Key and/or Secret.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for virustotal.
Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
[!] Missing API key for zoomeye.
Searching 0 results.
[*] Searching Bing.
[*] Searching Anubis.
[*] Searching Baidu.
Searching results.
[*] Searching Certspotter.
An exception has occurred: 400, message:
Can not decode content-encoding: br
[*] Searching CRTsh.
[*] Searching Dnsdumpster.
An exception has occurred: 400, message:
Can not decode content-encoding: br
[*] Searching Hackertarget.
[*] Searching Duckduckgo.
[*] Searching Otx.
[*] Searching Rapiddns.
Sitedossier module has triggered a captcha on first iteration, no results can be found.
Change IPs, manually solve the captcha, or wait before rerunning Sitedossier module
[*] Searching Sitedossier.
An exception has occurred: 400, message:
Can not decode content-encoding: br
[*] Searching Subdomaincenter.
[*] Searching Subdomainfinderc99.
[*] Searching Threatminer.
[*] Searching Urlscan.
[*] Searching Yahoo.
^X@sSAn exception has occurred: 400, message:
Can not decode content-encoding: br


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
19:25
kali@kali: ~/theHarvester
File Actions Edit View Help
Can not decode content-encoding: br
An exception has occurred: 400, message:
Can not decode content-encoding: br
An exception has occurred: 400, message:
Can not decode content-encoding: br
An exception has occurred: 400, message:
Can not decode content-encoding: br
An exception has occurred: 400, message:
Can not decode content-encoding: br
An exception has occurred: 400, message:
Can not decode content-encoding: br
An exception has occurred: 400, message:
Can not decode content-encoding: br
[*] Searching Brave.
[*] ASNS found: 1
AS20940
[*] Interesting Urls found: 2
https://dan.com/de-de/buy-domain/hackday.com?redirected=true
https://www.hackday.com/
[*] LinkedIn Links found: 0
[*] IPs found: 3
104.247.82.50
184.168.221.31
2a02:26f0:480:d::210:f147
[*] No emails found.
[*] Hosts found: 13
1-cl-srv1.hackday.com
calendar.hackday.com
drive.hackday.com
groups.hackday.com
hostmaster.hostmaster.hackday.com
hostmaster.hostmaster.hackday.com:127.0.0.4
hostmaster.hostmaster.hackday.com:3.64.163.50
hostmaster.hostmaster.hostmaster.hackday.com
hostmaster.hostmaster.hostmaster.hackday.com:127.0.0.4
hostmaster.hostmaster.hostmaster.hackday.com:3.64.163.50
hostmaster.hostmaster.hostmaster.hackday.com:84.53.133.251
mail.hackday.com
sites.hackday.com
(kali㉿kali)-[~/theHarvester]
$


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
19:35
kali@kali: ~/theHarvester
File Actions Edit View Help
wiki.hackaday.com:hackaday.com
wiki.hackaday.com:hackaday.com.
winnie.hackaday.com:hackaday.com
winnie.hackaday.com:hackaday.com.
wireless.hackaday.com
wireless.hackaday.com:hackaday.com
wireless.hackaday.com:hackaday.com.
wordpress.hackaday.com
wordpress.hackaday.com:hackaday.com
wp.hackaday.com
wp.hackaday.com:hackaday.com
wp.hackaday.com:hackaday.com.
wssd.hackaday.com:hackaday.com
wsww.hackaday.com:hackaday.com
ww.hackaday.com:hackaday.com
ww1.hackaday.com
ww1.hackaday.com:hackaday.com
www1.hackaday.com
www1.hackaday.com:hackaday.com
www1.hackaday.com:hackaday.com.
www1a2c.hackaday.com:alt1.aspmx.l.google.com
www1a2c.hackaday.com:alt2.aspmx.l.google.com
www1a2c.hackaday.com:aspmx.l.google.com
www1a2c.hackaday.com:aspmx2.googlemail.com
www1a2c.hackaday.com:aspmx3.googlemail.com
www1a2c.hackaday.com:hackaday.com
www1a2c.hackaday.com:hackaday.com.
www2.hackaday.com
www2.hackaday.com:hackaday.com
www2.hackaday.com:hackaday.com.
wwwi.hackaday.com:hackaday.com
wwwi.hackaday.com:hackaday.com.
wwwmisc.hackaday.com
wwwmisc.hackaday.com:hackaday.com
wwwmisc.hackaday.com:hackaday.com.
xbox.hackaday.com:hackaday.com
xbox.hackaday.com:hackaday.com.
xiaobao.hackaday.com:hackaday.com
xiaobao.hackaday.com:hackaday.com.
[*] Reporting started.
[*] XML File saved.
[*] JSON File saved.
(kali㉿kali)-[~/theHarvester]
$ ls
bin hackaday.com.json README requirements.txt theHarvester theHarvester.py
docker-compose.yml hackaday.com.xml README.md restfulHarvest.py theHarvester-logo.png
Dockerfile pyproject.toml requirements tests theHarvester-logo.webp
(kali㉿kali)-[~/theHarvester]
$


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
22:56
kali@kali: ~/theHarvester
File Actions Edit View Help
www1a2c.hackaday.com:alt2.aspmx.l.google.com
www1a2c.hackaday.com:aspmx.l.google.com
www1a2c.hackaday.com:aspmx2.googlemail.com
www1a2c.hackaday.com:aspmx3.googlemail.com
www1a2c.hackaday.com:hackaday.com
www1a2c.hackaday.com:hackaday.com.
www2.hackaday.com
www2.hackaday.com:hackaday.com
www2.hackaday.com:hackaday.com.
wwwi.hackaday.com:hackaday.com
wwwi.hackaday.com:hackaday.com.
wwwmisc.hackaday.com
wwwmisc.hackaday.com:hackaday.com
wwwmisc.hackaday.com:hackaday.com.
xbox.hackaday.com:hackaday.com
xbox.hackaday.com:hackaday.com.
xiaobao.hackaday.com:hackaday.com
xiaobao.hackaday.com:hackaday.com.
[*] Reporting started.
[*] XML File saved.
[*] JSON File saved.
(kali㉿kali)-[~/theHarvester]
$ ls
bin hackaday.com.json README requirements.txt theHarvester theHarvester.py
docker-compose.yml hackaday.com.xml README.md restfulHarvest.py theHarvester-logo.png
Dockerfile pyproject.toml requirements tests theHarvester-logo.webp
(kali㉿kali)-[~/theHarvester]
$ firefox hackaday.com.results.html
(kali㉿kali)-[~/theHarvester]
$ firefox hackaday.com.results.html
(kali㉿kali)-[~/theHarvester]
$ firefox hackaday.com.results.html
(kali㉿kali)-[~/theHarvester]
$ firefox hackaday.com.results.json
(kali㉿kali)-[~/theHarvester]
$ theHarvester-logo.png
theHarvester-logo.png: command not found
(kali㉿kali)-[~/theHarvester]
$ firefox theHarvester-logo.png
(kali㉿kali)-[~/theHarvester]
$

RESULT AND PROCEDURE FOR GATHERING OF INFORMATION USING THEHARVESTER.

Here we used theHarvester to gather information on a target website. We first started by installing python3, then we installed virtualenv. Then we cloned the git repo [git clone https://github.com/laramies/theHarvester.git] then we changed the directory to theHarvester.

After that we then installed the requirements to carry out this operation, then we closed the terminal and opened a new one. Now we have set up theHarvester and we are ready to use it. We changed directory to theHarvester then we began our motive. Now we want to launch an information gathering campaign on a target, we began by typing the following [./theHarvester.py -d hackaday.com -l 300 -b google]. This command starts theHarvester. It will begin searching google for the top 300 results related to hackaday.com. We can see that we couldn't find any information on google so let's dig deeper. Now we want to gather more information about our target, we would specify the following: [./theHarvester.py -d hackaday.com -l 300 -b all] The “-b all” tag will search all search engines available to theHarvester for information regarding hackaday.com. As you can see, it is an extremely useful tool for discovering email addresses, names of people associated with the target, sub-domain names and IP addresses.

TheHarvester is important for:

1. **OSINT Gathering**: Collects publicly available information about targets.
2. **Identifying Attack Surface**: Maps vulnerabilities by finding email addresses and subdomains.
3. **Reconnaissance**: Aids in the initial phase of penetration testing.
4. **Social Engineering Prep**: Information can be used for social engineering tactics.

5. **Efficiency**: Automates data collection, saving time.
6. **Compliance**: Helps organizations assess their publicly exposed information.

In short, it’s a key tool for cybersecurity professionals to enhance security and identify potential threats.