K.Gowtham
192011090

Exercise No 5: **Information gathering using theHarvester**

Aim: To demonstrate information gathering using theHarvester
Procedure:

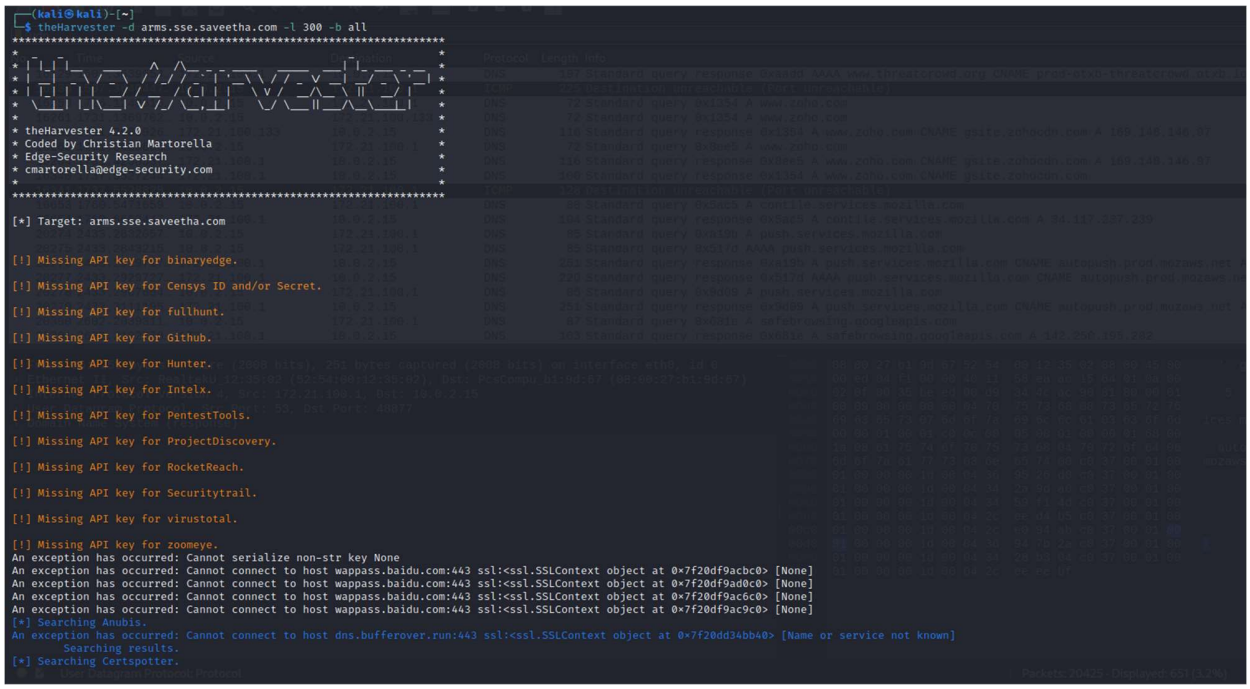
STEP 1: Open Terminal in the kali linux

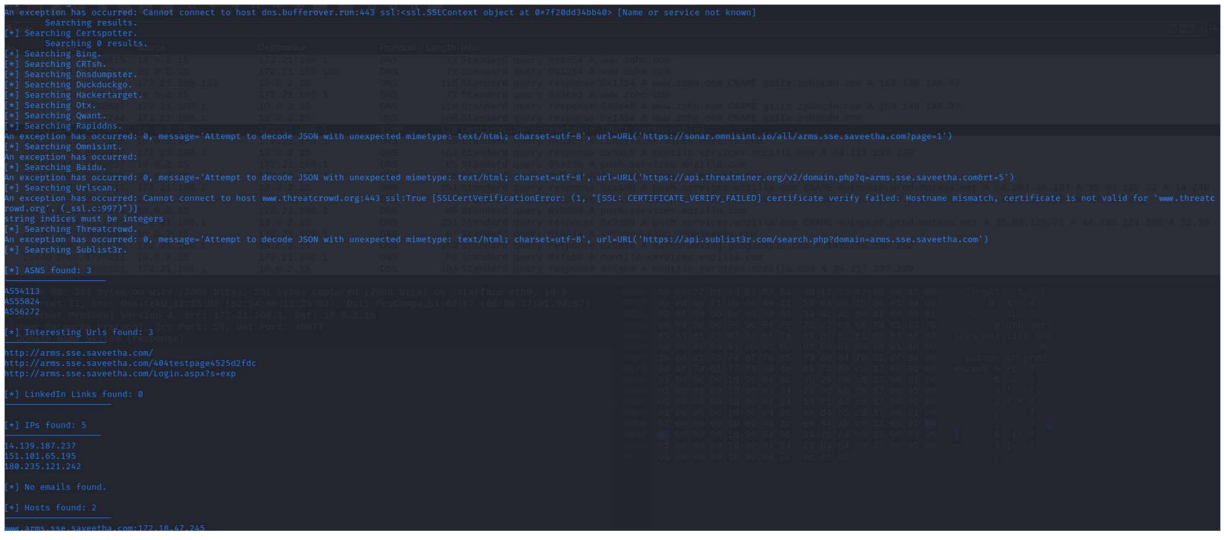
```
-d [url] will be the remote site from which you wants to fetch


-l will limit the search for specified number.

-b is used to specify search engine name.
```

STEP 2: Run the following command
Command: theHarvester -d arms.sse.saveetha.com**-l 300 -b all**

Step 4: run this command "theHarvester -d arms.sse.saveetha.com -l 300 -b all -f test" and hit enter to export the result as html file and xml file
Step 5: now close the terminal and navigate the home folder and search

OUTPUT


┌──(kali㉿kali)-[~]
└─$ theHarvester -d arms.sse.saveetha.com -l 300 -b all
* theHarvester 4.2.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
[*] Target: arms.sse.saveetha.com
[!] Missing API key for binaryedge.
[!] Missing API key for Censys ID and/or Secret.
[!] Missing API key for fullhunt.
[!] Missing API key for Github.
[!] Missing API key for Hunter.
[!] Missing API key for Intelx.
[!] Missing API key for PentestTools.
[!] Missing API key for ProjectDiscovery.
[!] Missing API key for RocketReach.
[!] Missing API key for Securitytrail.
[!] Missing API key for virustotal.
[!] Missing API key for zoomeye.
An exception has occurred: Cannot serialize non-str key None
An exception has occurred: Cannot connect to host wappass.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f20df9acbc0> [None]
An exception has occurred: Cannot connect to host wappass.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f20df9ad0c0> [None]
An exception has occurred: Cannot connect to host wappass.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f20df9ac6c0> [None]
An exception has occurred: Cannot connect to host wappass.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f20df9ac9c0> [None]
[*] Searching Anubis.
An exception has occurred: Cannot connect to host dns.bufferover.run:443 ssl:<ssl.SSLContext object at 0×7f20dd34bb40> [Name or service not known]
Searching results.
[*] Searching Certspotter.


An exception has occurred: Cannot connect to host dns.bufferover.run:443 ssl:<ssl.SSLContext object at 0×7f20dd34bb40> [Name or service not known]
Searching results.
[*] Searching Certspotter.
Searching 0 results.
[*] Searching Bing.
[*] Searching CRTsh.
[*] Searching Dnsdumpster.
[*] Searching Duckduckgo.
[*] Searching Hackertarget.
[*] Searching Otx.
[*] Searching Qwant.
[*] Searching Rapiddns.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: text/html; charset=utf-8', url=URL('https://sonar.omnisint.io/all/arms.sse.saveetha.com?page=1')
[*] Searching Omnisint.
An exception has occurred:
[*] Searching Baidu.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: text/html; charset=utf-8', url=URL('https://api.threatminer.org/v2/domain.php?q=arms.sse.saveetha.com&rt=5')
[*] Searching Urlscan.
An exception has occurred: Cannot connect to host www.threatcrowd.org:443 ssl:True [SSLCertVerificationError: (1, "[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed: Hostname mismatch, certificate is not valid for 'www.threatcrowd.org'. (_ssl.c:997)")]
string indices must be integers
[*] Searching Threatcrowd.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: text/html; charset=utf-8', url=URL('https://api.sublist3r.com/search.php?domain=arms.sse.saveetha.com')
[*] Searching Sublist3r.
[*] ASNS found: 3
AS54113
AS55824
AS56272
[*] Interesting Urls found: 3
http://arms.sse.saveetha.com/
http://arms.sse.saveetha.com/404testpage4525d2fdc
http://arms.sse.saveetha.com/Login.aspx?s=exp
[*] LinkedIn Links found: 0
[*] IPs found: 5
34.139.187.237
151.101.65.195
180.235.121.242
[*] No emails found.
[*] Hosts found: 2
www.arms-sse.saveetha.com:172.18.47.205

```
┌──(root㉿kali)-[~]
└─# theHarvester -d  www.zoho.com -l 300 -b all
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \___|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.2.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: www.zoho.com


[!] Missing API key for binaryedge.

[!] Missing API key for Censys ID and/or Secret.

[!] Missing API key for fullhunt.

[!] Missing API key for Github.

[!] Missing API key for Hunter.

[!] Missing API key for Intelx.

[!] Missing API key for PentestTools.

[!] Missing API key for ProjectDiscovery.

[!] Missing API key for RocketReach.

[!] Missing API key for Securitytrail.

[!] Missing API key for virustotal.

[!] Missing API key for zoomeye.
An exception has occurred: Cannot serialize non-str key None
An exception has occurred: Cannot connect to host wappass.baidu.com:443 ssl:<ssl.SSLContext object at 0×7f419adf5dc0> [None]
[*] Searching Anubis.
An exception has occurred: Cannot connect to host dns.bufferover.run:443 ssl:<ssl.SSLContext object at 0×7f4198739a40> [Name or service not known]
       Searching 0 results.
[*] Searching Bing.
       Searching results.
[*] Searching Certspotter.
[*] Searching CRTsh.
[*] Searching Dnsdumpster.
[*] Searching Hackertarget.
```

```
[*] Searching Certspotter.
[*] Searching CRTsh.
[*] Searching Dnsdumpster.
[*] Searching Hackertarget.
[*] Searching Duckduckgo.
[*] Searching Otx.
[*] Searching Qwant.
[*] Searching Rapiddns.
An exception has occurred:
[*] Searching Baidu.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: text/html; charset=utf-8', url=URL('https://sonar.omnisint.io/all/www.zoho.com?page=1')
[*] Searching Omnisint.
An exception has occurred: Cannot connect to host www.threatcrowd.org:443 ssl:True [SSLCertVerificationError: (1, "[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed: Hostname mismatch, certificate is not valid for 'www.threatcrowd.org'. (_ssl.c:997)")]
string indices must be integers
[*] Searching Threatcrowd.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: text/html; charset=utf-8', url=URL('https://api.threatminer.org/v2/domain.php?q=www.zoho.com&rt=5')
[*] Searching Urlscan.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: text/html; charset=utf-8', url=URL('https://api.sublist3r.com/search.php?domain=www.zoho.com')
[*] Searching Sublist3r.

[*] ASNS found: 7
--------------------
AS13335
AS141757
AS205111
AS2639
AS33070
AS41913
AS56201

[*] Interesting Urls found: 28
----------------------------
https://www.zoho.com/
https://www.zoho.com/analytics/
https://www.zoho.com/ar/forms/
https://www.zoho.com/assist/
https://www.zoho.com/blog/payroll/strategies-for-remote-payroll-management-at-scale.html
https://www.zoho.com/calendar/?zsrc=fromproduct&serviceurl=%2Fmycalendar
https://www.zoho.com/campaigns/explainer/zcsend.html
https://www.zoho.com/campaigns/explainer/zcvg.html
https://www.zoho.com/creator/analyst/isg-provider-lens-next-gen-adm-solutions-2022-report.html?utm_source=footer&utm_medium=banner&utm_campaign=ISGpromo-2022
https://www.zoho.com/creator/login.html?serviceurl=https%3A%2F%2Fbxchampion.zohocreator.comhttps%3A**Abxchampion.zohocreator.com&portal=prosystem-washingtongas
https://www.zoho.com/de/crm/
https://www.zoho.com/en-au/
https://www.zoho.com/en-uk/
https://www.zoho.com/es-xl/creator/whatsnew/creator6.html
https://www.zoho.com/forms/
https://www.zoho.com/mail/
https://www.zoho.com/mail/?zsrc=fromproduct
https://www.zoho.com/mail/control-panel.html?zsrc=fromproduct
```

Result

Information gathering using theHarvester is performed successfully.