

Exercise No 5: Information gathering using theHarvester

Aim: To demonstrate information gathering using theHarvester

Procedure:

`-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 1: Open Terminal in the kali linux

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                                     Project: theHarvester
* 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 0x7f20df9acbc0 [None]
An exception has occurred: Cannot connect to host wappass.baidu.com:443 ssl:ssl.SSLContext object at 0x7f20df9ad0c0 [None]
An exception has occurred: Cannot connect to host wappass.baidu.com:443 ssl:ssl.SSLContext object at 0x7f20df9ac6c0 [None]
[*] Searching Anubis.
An exception has occurred: Cannot connect to host dns.bufferover.run:443 ssl:ssl.SSLContext object at 0x7f20dd34bb40 [Name or service not known]
[*] Searching Certspotter.
An exception has occurred: Cannot connect to host dns.bufferover.run:443 ssl:ssl.SSLContext object at 0x7f20dd34bb40 [Name or service not known]
[*] Searching Crtsh.
[*] Searching Dnsdumpster.
[*] Searching Hackertarget.
[*] Searching Otx.
[*] Searching Qnabu.
[*] Searching Rapid7.
An exception has occurred: 0, message='Attempt to decode JSon with unexpected mimetype: text/html; charset=utf-8', url-URL('https://sonar.omisint.io/all/arms.sse.saveetha.com?page=1')
[*] Searching Omsint.
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 Uriscan.
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: CERTIFICATE_VERIFY_FAILED])")]
[*] 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
AS56272
AS56272
AS56272
[*] Interesting Urls Found: 3
http://arms.sse.saveetha.com/
http://arms.sse.saveetha.com/404testpage4525d2fde
http://arms.sse.saveetha.com/Login.aspx?e=exp
[*] LinkedIn Links Found: 0
[*] IPs found: 5
16.199.487.237
151.191.65.195
108.235.121.242
[*] No emails found.
[*] Hosts Found: 2
www.arms.sse.saveetha.com:443 48 47 416
```

```
An exception has occurred: Cannot connect to host dns.bufferover.run:443 ssl:ssl.SSLContext object at 0x7f20dd34bb40 [Name or service not known]
[*] Searching Certspotter.
[*] Searching Crtsh.
[*] Searching Dnsdumpster.
[*] Searching Hackertarget.
[*] Searching Otx.
[*] Searching Qnabu.
[*] Searching Rapid7.
An exception has occurred: 0, message='Attempt to decode JSon with unexpected mimetype: text/html; charset=utf-8', url-URL('https://sonar.omisint.io/all/arms.sse.saveetha.com?page=1')
[*] Searching Omsint.
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 Uriscan.
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: CERTIFICATE_VERIFY_FAILED])")]
[*] 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
AS56272
AS56272
AS56272
[*] Interesting Urls Found: 3
http://arms.sse.saveetha.com/
http://arms.sse.saveetha.com/404testpage4525d2fde
http://arms.sse.saveetha.com/Login.aspx?e=exp
[*] LinkedIn Links Found: 0
[*] IPs found: 5
16.199.487.237
151.191.65.195
108.235.121.242
[*] No emails found.
[*] Hosts Found: 2
www.arms.sse.saveetha.com:443 48 47 416
```

```
* theHarvester -d www.zoho.com -l 300 -b all
*****
theHarvester
*****
* 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 0x7f419adf5dc0> [None]
[*] Searching Anubis.
An exception has occurred: Cannot connect to host dns.bufferover.run:443 ssl:<ssl.SSLContext object at 0x7f4198739a40> [Name or service not known]
    Searching 0 results.
[*] Searching Bing.
    Searching results.
[*] Searching Certspotter.
[*] Searching CRTsh.
[*] Searching Dnsdumpster.
[*] Searching Hackertarget.
```

```
[*] Searching Certificates...
[*] Searching CIRTsh...
[*] Searching Crtsh...
[*] Searching Dnsdumpster...
[*] Searching Hackettarget...
[*] Searching Duckduckgo...
[*] Searching Otx...
[*] Searching Owaynt...
[*] 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' (-1.c.9927)")]
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 Uriscan...
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
AS2039
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=X2Fmycalendar
https://www.zoho.com/campaigns/explainer/zcsend.html
https://www.zoho.com/campaigns/explainer/zcvg.html
https://www.zoho.com/creator/analyst/isp-provider-lens-next-gen-adm-solutions-2022-report.html?utm_source=footerbutm_medium=bannerbutm_campaign=ISG6promo-2022
https://www.zoho.com/creator/login.html?serviceurl=https%3A%2F%2Fbxchampion.zohocreator.com%3Dtks3A*Abxchampion.zohocreator.com%3Bportal%3Dprosystem-washingtontas
https://www.zoho.com/de/crm/
https://www.zoho.com/en-au/
https://www.zoho.com/en-uk/
https://www.zoho.com/en-us/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
```

```
https://www.zoho.com/nl/salesiq/  
https://www.zoho.com/people/?zsrc=fromproduct  
https://www.zoho.com/show/  
https://www.zoho.com/sites/?zsrc=fromproduct  
https://www.zoho.com/social/  
https://www.zoho.com/sprints/  
https://www.zoho.com/survey/?utm_source=Email-Distribution
```

```
[*] LinkedIn Links found: 0
```

```
[*] IPs found: 39
```

```
8.39.54.155  
8.40.222.155  
74.201.84.81  
74.201.112.101  
74.201.112.118  
74.201.113.118  
74.201.113.176  
74.201.113.203  
74.201.155.201  
89.36.170.52  
103.163.152.75  
104.16.11.213  
104.16.12.213  
104.16.13.213  
104.16.14.213  
104.16.15.213  
104.16.43.59  
104.16.44.59  
136.143.182.155  
136.143.190.79  
136.143.190.155  
136.143.191.204  
148.62.36.5  
165.173.187.32  
165.254.167.165  
165.254.168.165  
169.148.148.139  
185.20.209.52  
185.230.212.81  
204.141.32.155  
204.141.42.79  
204.141.42.155  
204.141.42.156  
204.141.43.204  
216.52.72.155  
2a06:98c1:3120::c
```

```
[*] No emails found.
```

Result

Information gathering using theHarvester is performed successfully.

