Hands on Practice on Reconnaissance Tool

theHarvester

Submitted by :   Khizar ul Islam

Submitted to: Mr Imran

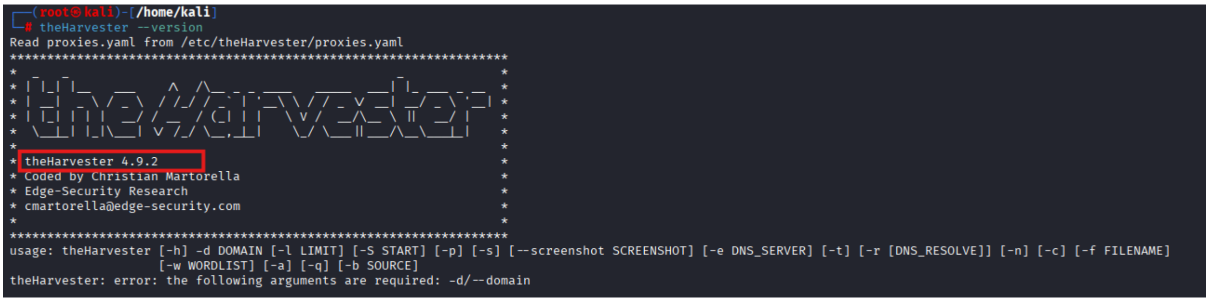
Task #1 :

Verify the tool

Command:

theHarvester --version

Screen Shot:



```
┌──(root㉿kali)-[/home/kali]
└─# theHarvester --version
Read proxies.yaml from /etc/theHarvester/proxies.yaml
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.9.2                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************
usage: theHarvester [-h] -d DOMAIN [-l LIMIT] [-S START] [-p] [-s] [--screenshot SCREENSHOT] [-e DNS_SERVER] [-t] [-r [DNS_RESOLVE]] [-n] [-c] [-f FILENAME]
                    [-w WORDLIST] [-a] [-q] [-b SOURCE]
theHarvester: error: the following arguments are required: -d/--domain
```

Explanation:

We can check the Version of the harvester if it is install it will show the current version of the harvester if it is not install then use (sudo apt install theHarvester –y) to install it.

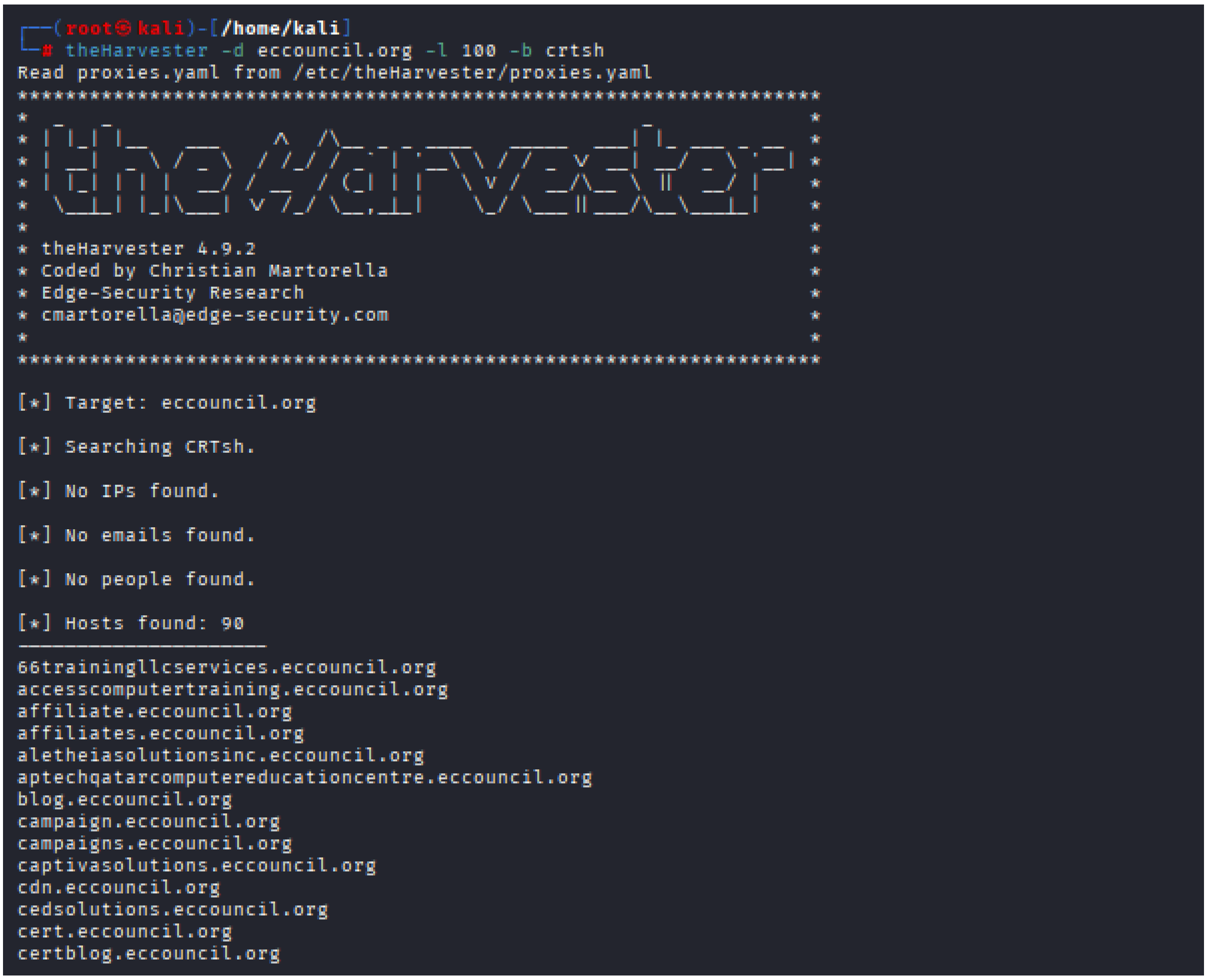
Task#2:

Discover Subdomains from Certificate Logs

Command:

theHarvester -d eccouncil.org -l 100 -b crtsh

Screenshot:



```
┌──(root㉿kali)-[/home/kali]
└─# theHarvester -d eccouncil.org -l 100 -b crtsh
Read proxies.yaml from /etc/theHarvester/proxies.yaml
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.9.2                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: eccouncil.org

[*] Searching CRTsh.

[*] No IPs found.

[*] No emails found.

[*] No people found.

[*] Hosts found: 90
---------------------
66trainingllcservices.eccouncil.org
accesscomputertraining.eccouncil.org
affiliate.eccouncil.org
affiliates.eccouncil.org
aletheiasolutionsinc.eccouncil.org
aptechqatarcomputereducationcentre.eccouncil.org
blog.eccouncil.org
campaign.eccouncil.org
campaigns.eccouncil.org
captivasolutions.eccouncil.org
cdn.eccouncil.org
cedsolutions.eccouncil.org
cert.eccouncil.org
certblog.eccouncil.org
```

Explanation:

By using command of crtsh we can discover the subdomains of the target

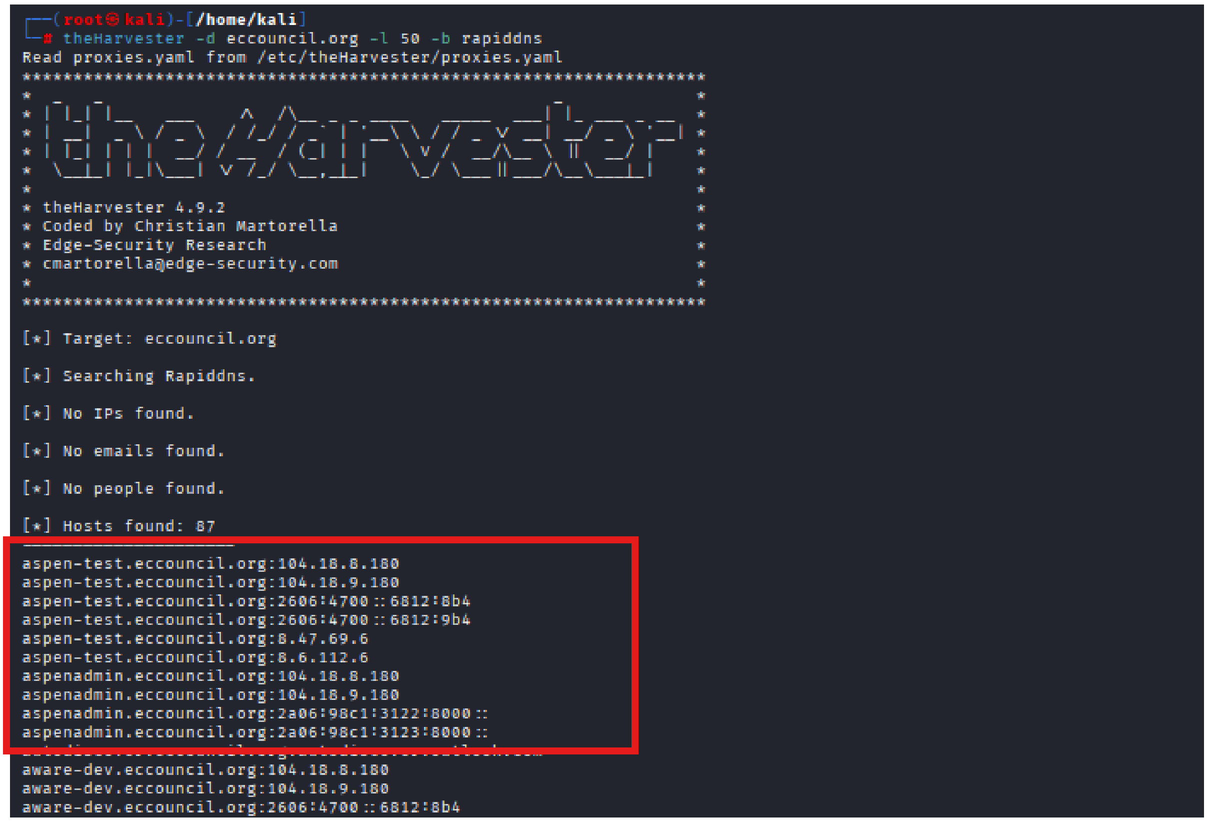
Task#3:

Gather Passive DNS Information

Command:

theHarvester -d eccouncil.org -l 50 -b rapiddns

Screenshot:



```
┌──(root㉿kali)-[/home/kali]
└─# theHarvester -d eccouncil.org -l 50 -b rapiddns
Read proxies.yaml from /etc/theHarvester/proxies.yaml
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.9.2                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: eccouncil.org

[*] Searching Rapiddns.

[*] No IPs found.

[*] No emails found.

[*] No people found.

[*] Hosts found: 87
---------------------
aspen-test.eccouncil.org:104.18.8.180
aspen-test.eccouncil.org:104.18.9.180
aspen-test.eccouncil.org:2606:4700::6812:8b4
aspen-test.eccouncil.org:2606:4700::6812:9b4
aspen-test.eccouncil.org:8.47.69.6
aspen-test.eccouncil.org:8.6.112.6
aspenadmin.eccouncil.org:104.18.8.180
aspenadmin.eccouncil.org:104.18.9.180
aspenadmin.eccouncil.org:2a06:98c1:3122:8000::
aspenadmin.eccouncil.org:2a06:98c1:3123:8000::
aware-dev.eccouncil.org:104.18.8.180
aware-dev.eccouncil.org:104.18.9.180
aware-dev.eccouncil.org:2606:4700::6812:8b4
```

New Findings:

Comparing the result of task 3 with task 2 we manage to find the some new subdomains and Ip's as well.

aspen-test.eccouncil.org:104.18.8.180 aspen-test.eccouncil.org:104.18.9.180 aspen-test.eccouncil.org:2606:4700::6812:8b4 aspen-test.eccouncil.org:2606:4700::6812:9b4 aspen-test.eccouncil.org:8.47.69.6 aspen-test.eccouncil.org:8.6.112.6
aspenadmin.eccouncil.org:104.18.8.180
aspenadmin.eccouncil.org:104.18.9.180
aspenadmin.eccouncil.org:2a06:98c1:3122:8000::
aspenadmin.eccouncil.org:2a06:98c1:3123:8000::

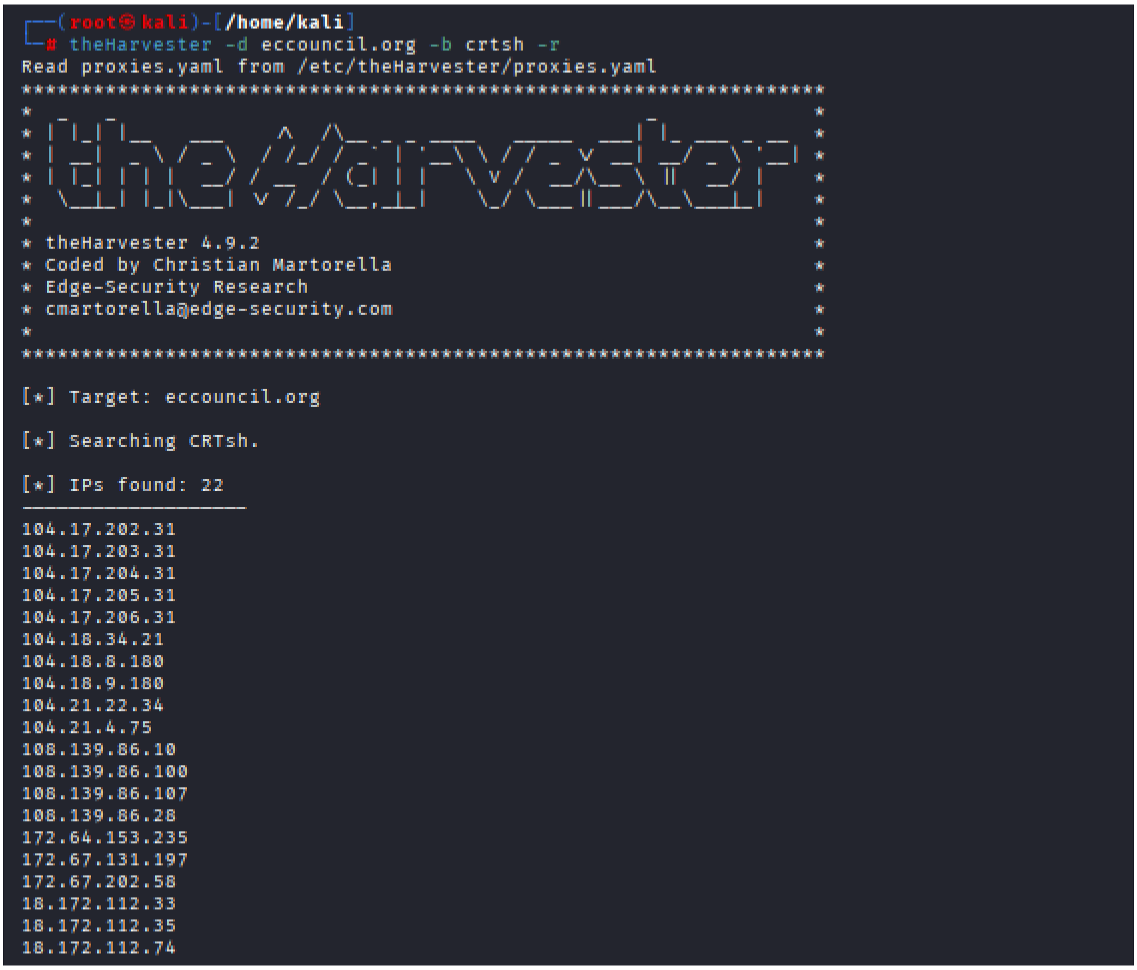
Task#4:

Resolve Discovered Hosts to IP Addresses

Command:

theHarvester -d eccouncil.org -b crtsh -r

Screenshot:



```
┌──(root㉿kali)-[/home/kali]
└─# theHarvester -d eccouncil.org -b crtsh -r
Read proxies.yaml from /etc/theHarvester/proxies.yaml
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.9.2                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: eccouncil.org

[*] Searching CRTsh.

[*] IPs found: 22
-------------------
104.17.202.31
104.17.203.31
104.17.204.31
104.17.205.31
104.17.206.31
104.18.34.21
104.18.8.180
104.18.9.180
104.21.22.34
104.21.4.75
108.139.86.10
108.139.86.100
108.139.86.107
108.139.86.28
172.64.153.235
172.67.131.197
172.67.202.58
18.172.112.33
18.172.112.35
18.172.112.74
```

Explanation:

We have discovered some hosts along with their Ip addresses.

I. connect.eccouncil.org → 104.17.202.31
II. cdn.eccouncil.org → 108.139.86.10
III. labs.eccouncil.org → 40.114.68.21

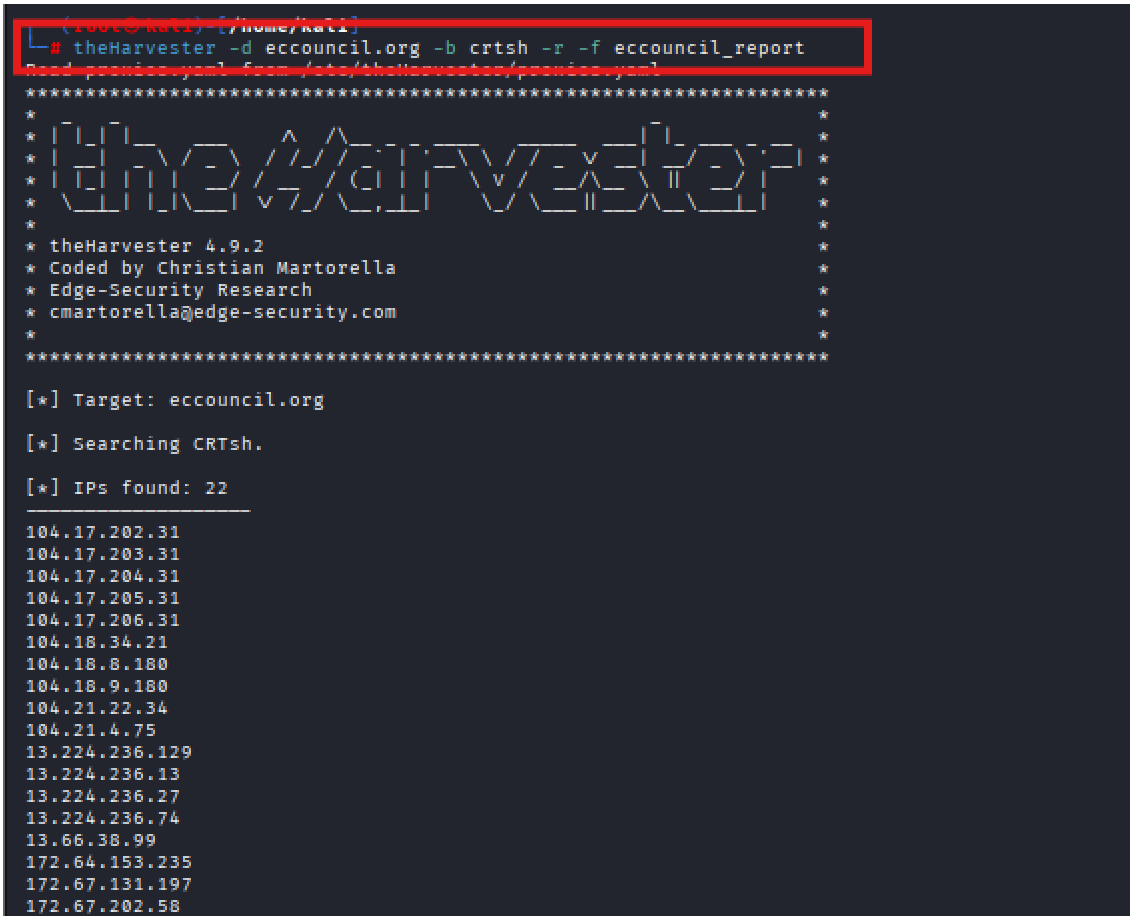
Task#5:

Export the Reconnaissance Report

Command:

theHarvester -d eccouncil.org -b crtsh -f eccouncil_report

Screenshot:



```
┌──(root㉿kali)-[/home/kali]
└─# theHarvester -d eccouncil.org -b crtsh -r -f eccouncil_report
Read proxies.yaml from /etc/theHarvester/proxies.yaml
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.9.2                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: eccouncil.org

[*] Searching CRTsh.

[*] IPs found: 22
-------------------
104.17.202.31
104.17.203.31
104.17.204.31
104.17.205.31
104.17.206.31
104.18.34.21
104.18.8.180
104.18.9.180
104.21.22.34
104.21.4.75
13.224.236.129
13.224.236.13
13.224.236.27
13.224.236.74
13.66.38.99
172.64.153.235
172.67.131.197
172.67.202.58
```

Explanation:

So by using –f command we can export all the subdomains and ips in just 1 Json file .

why passive reconnaissance is difficult to detect.

Passive reconnaissance is difficult to detect because it totally rely on the information available over the internet so attacker is not targeting any organization or individual just gather information over the internet and target remain unaware where someone is gathering information against them or not .