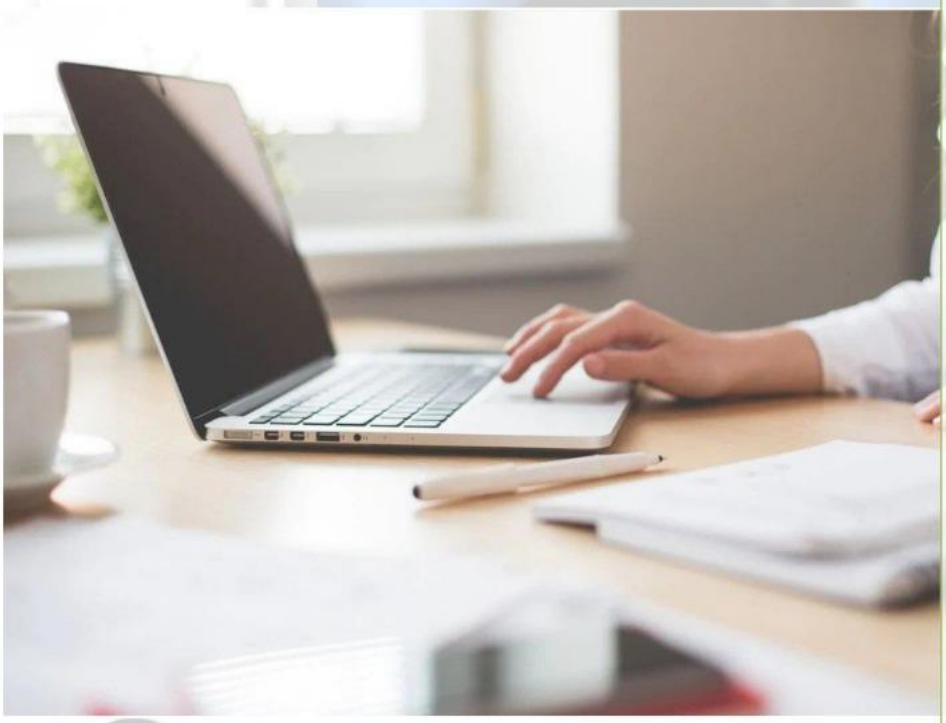
CRYPTUS CYBER
SECURITY PVT. LTD.

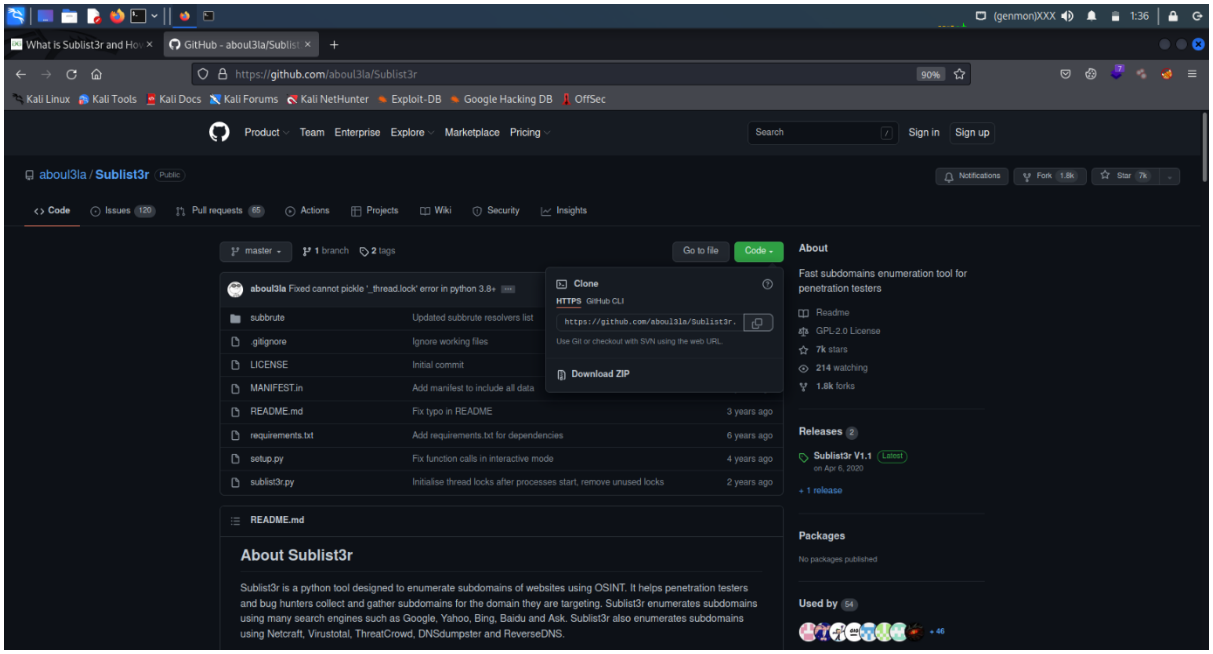


Enumeration (Tools)

What is Sublist3r and How to Use it?

Sublister is a tool designed in python and uses OSINT in order to enumerate subdomains of websites. It helps pen-testers in collecting and gathering subdomains for a domain which is their target. In order to fetch the accurate results, sublilster uses many search engines like Google, Yahoo, etc. and even tools like Netcraft, Virustotal, etc.

How we install sublist3r in kali linux

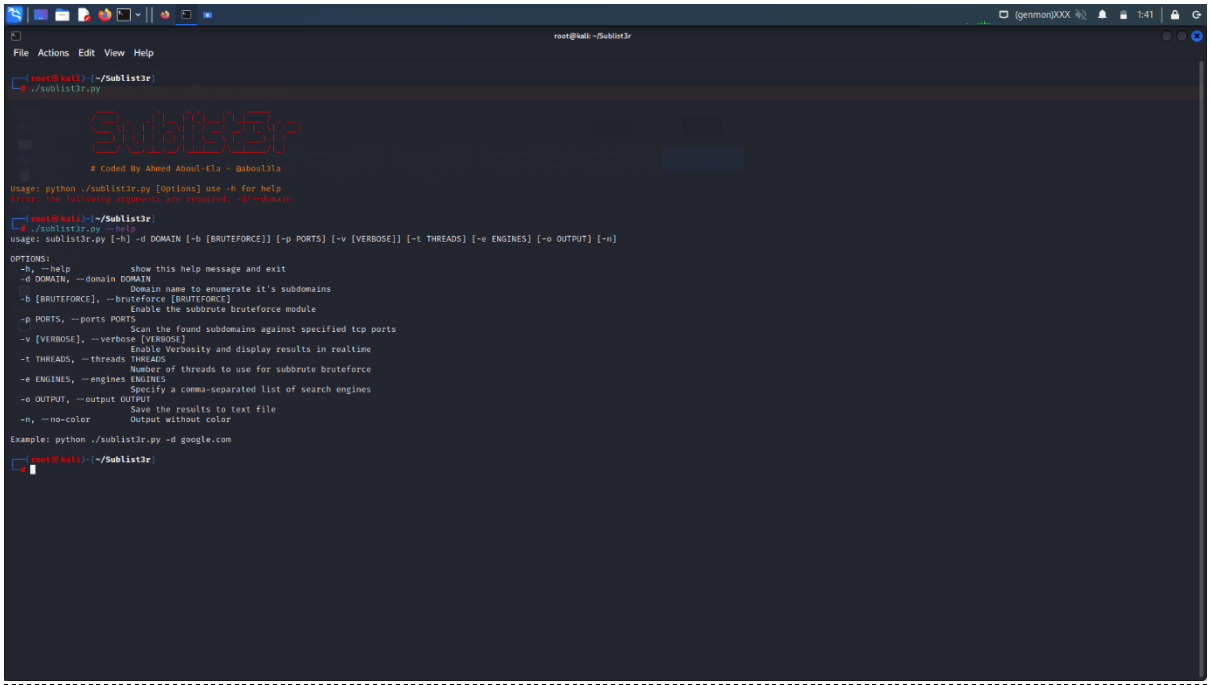


Git clone https://github.com/aboul3la/Sublist3r.git

Python3 sublist3r.py

4. To run the tool, Enter the following command in the terminal.

```
./sublist3r.py
```



./sublist3r.py –help (help manual)

OPTIONS:

-h, --help show this help message and exit

-d DOMAIN, --domain DOMAIN

Domain name to enumerate it's subdomains

-b [BRUTEFORCE], --bruteforce [BRUTEFORCE]

Enable the subbrute bruteforce module

-p PORTS, --ports PORTS

Scan the found subdomains against specified tcp ports

-v [VERBOSE], --verbose [VERBOSE]

Enable Verbosity and display results in realtime

-t THREADS, --threads THREADS

Number of threads to use for subbrute bruteforce

-e ENGINES, --engines ENGINES

Specify a comma-separated list of search engines

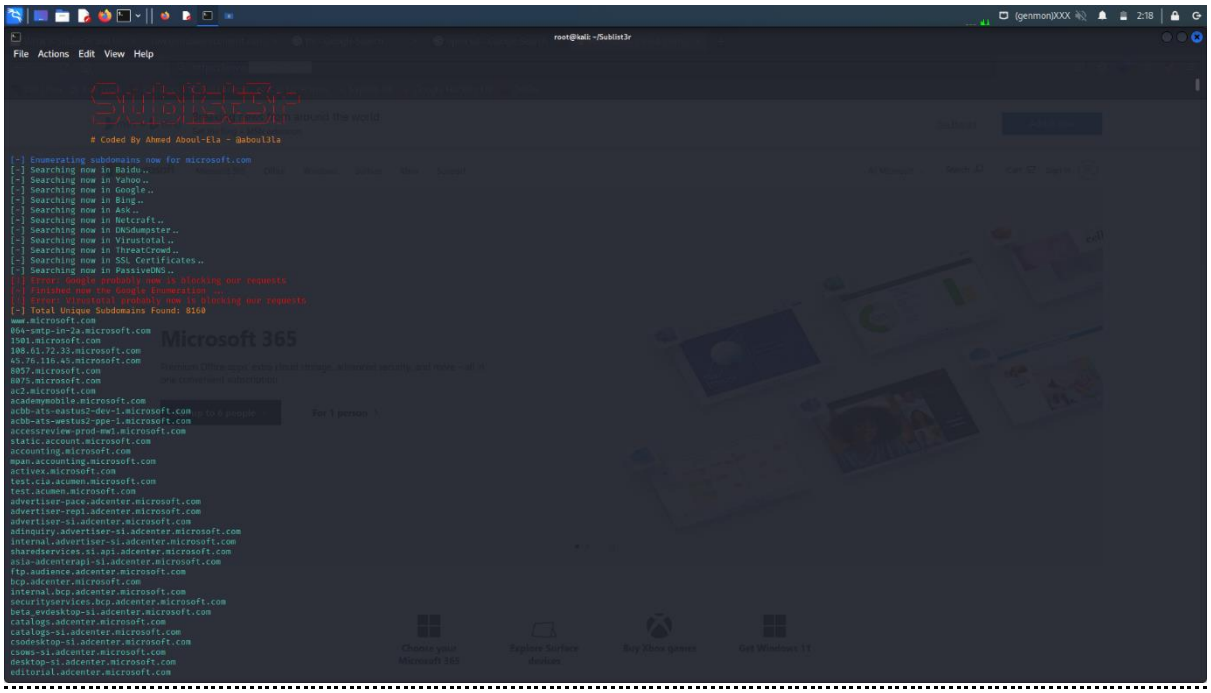
-o OUTPUT, --output OUTPUT

Save the results to text file

-n, --no-color Output without color

Let do practical

Simple scan to find subdomain :-



Commands:- python sublist3r.py -d microsoft.com

-o –output

python sublist3r.py -d microsoft.com -o (name of file)

-e –engines

python sublist3r.py -d microsoft.com -e (name of engines like google, yahoo, Bing , etc)

-v –verbose (real time output)

-p –ports (specific port)

Dnsenum Tool

Dnsenum is a tool for DNS enumeration, which is the process of locating all DNS servers and DNS entries for an organization.

DNS enumeration will allow us to gather critical information about the organization such as usernames, computer names, IP addresses, and so on.

DNSENUM OPTIONS

```
--dnsserver     <server> Use this DNS server for A, NS and MX
queries.



--enum          Shortcut option equivalent to --threads 5 -s 15 -
w.



-h, --help      Print this help message.



--noreverse          Skip the reverse lookup operations.



--nocolor       Disable ANSIColor output.



--private       Show and save private ips at the end of the file
domain_ips.txt.
```

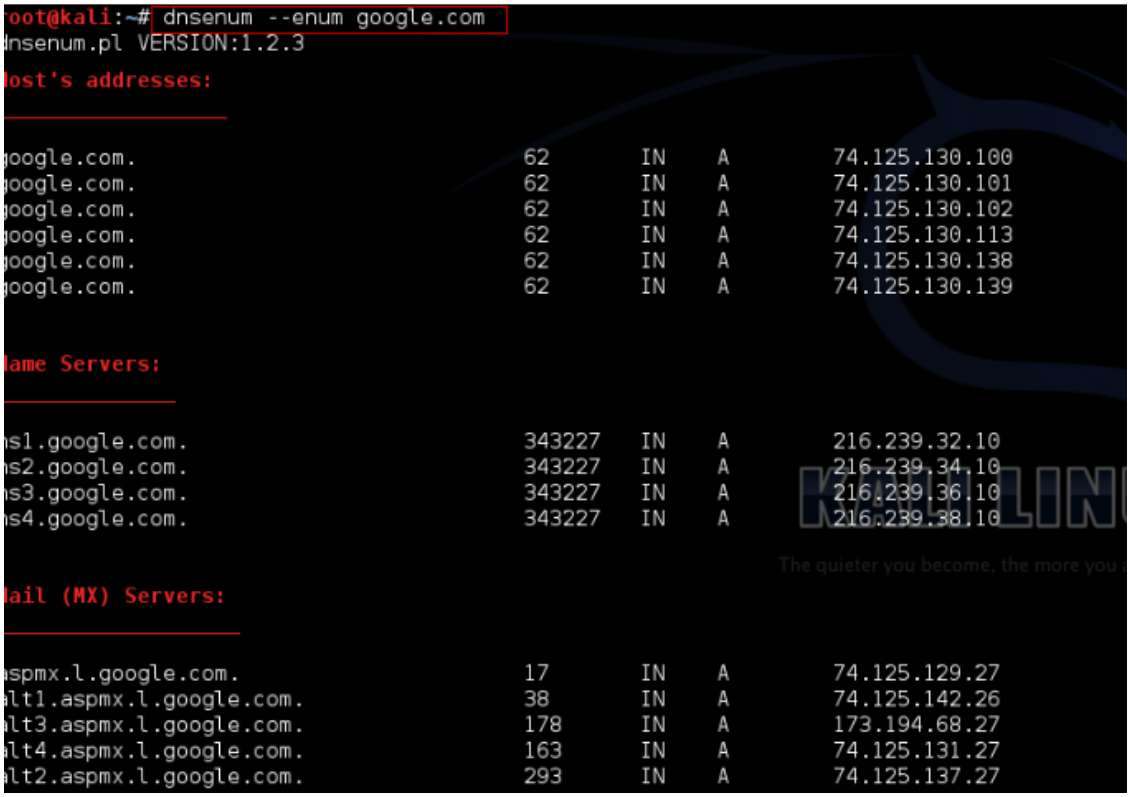
```
--subfile <file>     Write all valid subdomains to this file.



-t, --timeout <value> The tcp and udp timeout values in seconds
(default: 10s).



--threads <value>    The number of threads that will perform
different queries.



-v, --verbose        Be verbose: show all the progress and all
the error messages.



GOOGLE SCRAPING OPTIONS:



-p, --pages <value>  The number of google search pages to process
when scraping names, the default is 5 pages, the -s switch must
be specified.



-s, --scrap <value>  The maximum number of subdomains that will
be scraped from Google (default 15).



BRUTE FORCE OPTIONS:
```

```
-f, --file <file>    Read subdomains from this file to perform
brute force.



-u, --update    <a|g|r|z> Update the file specified with the -f
switch with valid subdomains.





a (all)    Update using all results.

g          Update using only google scraping results.

r          Update using only reverse lookup results.

z          Update using only zonetransfer results.



-r, --recursion Recursion on subdomains, brute force all
discovred subdomains that have an NS record.



WHOIS NETRANGE OPTIONS:



-d, --delay <value>  The maximum value of seconds to wait between
whois queries, the value is defined randomly, default: 3s.

-w, --whois          Perform the whois queries on c class network
ranges.



REVERSE LOOKUP OPTIONS:



-e, --exclude   <regexp> Exclude PTR records that match the
regexp expression from reverse lookup results, useful on invalid
hostnames.
```

```
OUTPUT OPTIONS:



-o --output <file>   Output in XML format. Can be imported in
MagicTree
```

Lab 1: Enumeration With Default Settings

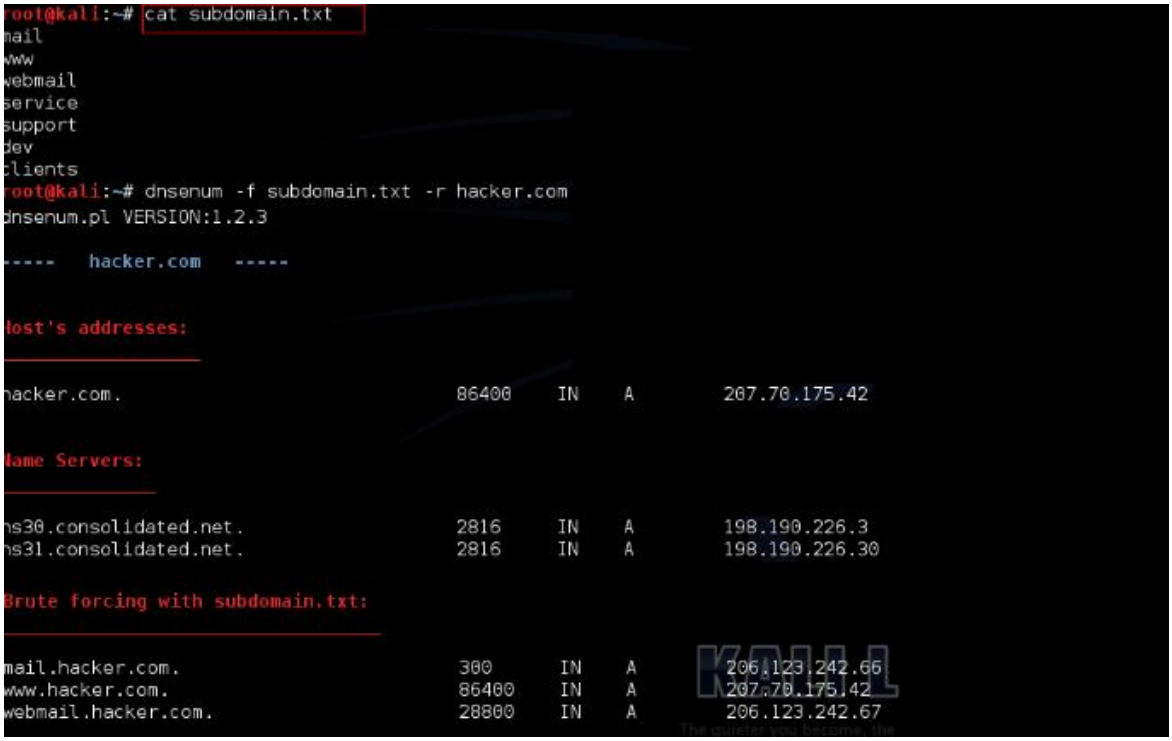
```
Syntax : dnsenum -enum <url>

Command : dnsenum -enum google.com
```



LAB 2: ENUMERATION OF SUBDOMAIN USING BRUTEFORCE AND FROM FILE

hen you run this command, it with perform brute force search on subdomains along with the custom file passed as an attribute.

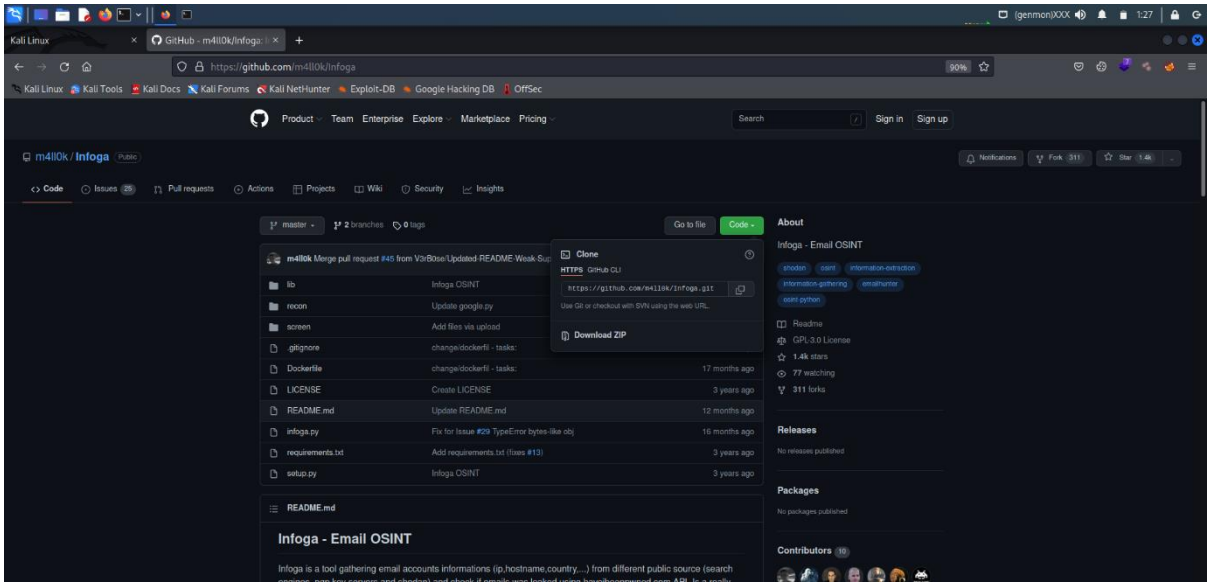
```
Syntax : dnsenum -f <file> -r <url>

Command : dnsenum -f subdomain.txt -r hacker.com
```



Infoga Tool

Infoga – Email Information Gathering Tool in Kali Linux

Infoga is a free and open-source tool available on GitHub, which is used for finding if emails were leaked using haveibeenpwned.com API. Infoga is used for scanning email addresses using different websites and search engines for information gathering and finding information about leaked information on websites and web apps. It is one of the **easiest and useful** tools for performing reconnaissance on websites and web apps for email analysis. The Infoga tool is also available for Linux operating systems. This tool can gather information such as ip, country of email and hostname also. This tool gets information from different public sources such as websites and search engines. For example, Google, **Shodan**, etc. This tool is very helpful for security researchers at early phases of penetration testing.



Downloads from GitHub :-

```
┌──(root㉿kali)-[~/Infoga]
└─# python infoga.py
_____________________________________
-=[ Infoga - Email OSINT
-=[ Momo (m4ll0k) Outaadi
-=[ https://github.com/m4ll0k
_____________________________________

Usage: infoga.py [OPTIONS]

        -d --domain     Target URL/Name
        -s --source     Source data, default "all":

                all     Use all search engine
                google  Use google search engine
                bing    Use bing search engine
                yahoo   Use yahoo search engine
                ask     Use ask search engine
                baidu   Use baidu search engine
                dogpile Use dogpile search engine
                exalead Use exalead search engine
                pgp     Use pgp search engine

        -b --breach     Check if email breached
        -i --info       Get email informations
        -r --report     Simple file text report
        -v --verbose    Verbosity level (1,2 or 3)
        -H --help       Show this help and exit

Example:
        infoga.py --domain site.gov -v 3
```

Python infoga.py (running commands)

```
_____________________________________
-=[ Infoga - Email OSINT
-=[ Momo (m4ll0k) Outaadi
-=[ https://github.com/m4ll0k
_____________________________________

Usage: infoga.py [OPTIONS]

        -d --domain     Target URL/Name
        -s --source     Source data, default "all":

                all     Use all search engine
                google  Use google search engine
                bing    Use bing search engine
                yahoo   Use yahoo search engine
                ask     Use ask search engine
                baidu   Use baidu search engine
                dogpile Use dogpile search engine
                exalead Use exalead search engine
                pgp     Use pgp search engine

        -b --breach     Check if email breached
        -i --info       Get email informations
        -r --report     Simple file text report
        -v --verbose    Verbosity level (1,2 or 3)
        -H --help       Show this help and exit

Example:
        infoga.py --domain site.gov -v 3
        infoga.py --info admin@site.gov -v 3
        infoga.py --domain site.gov --source pgp --breach -v 1
```

Help commands

-d --domain Target URL/Name

-s --source Source data, default "all":

all Use all search engine

google Use google search engine

bing Use bing search engine

yahoo Use yahoo search engine

ask Use ask search engine

baidu Use baidu search engine

dogpile Use dogpile search engine

exalead Use exalead search engine

pgp Use pgp search engine

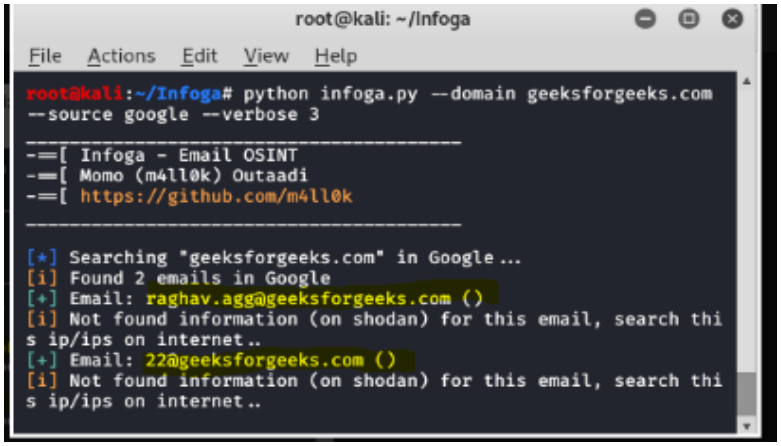
-b --breach Check if email breached

-i --info Get email informations

-r --report Simple file text report

-v --verbose Verbosity level (1,2 or 3)

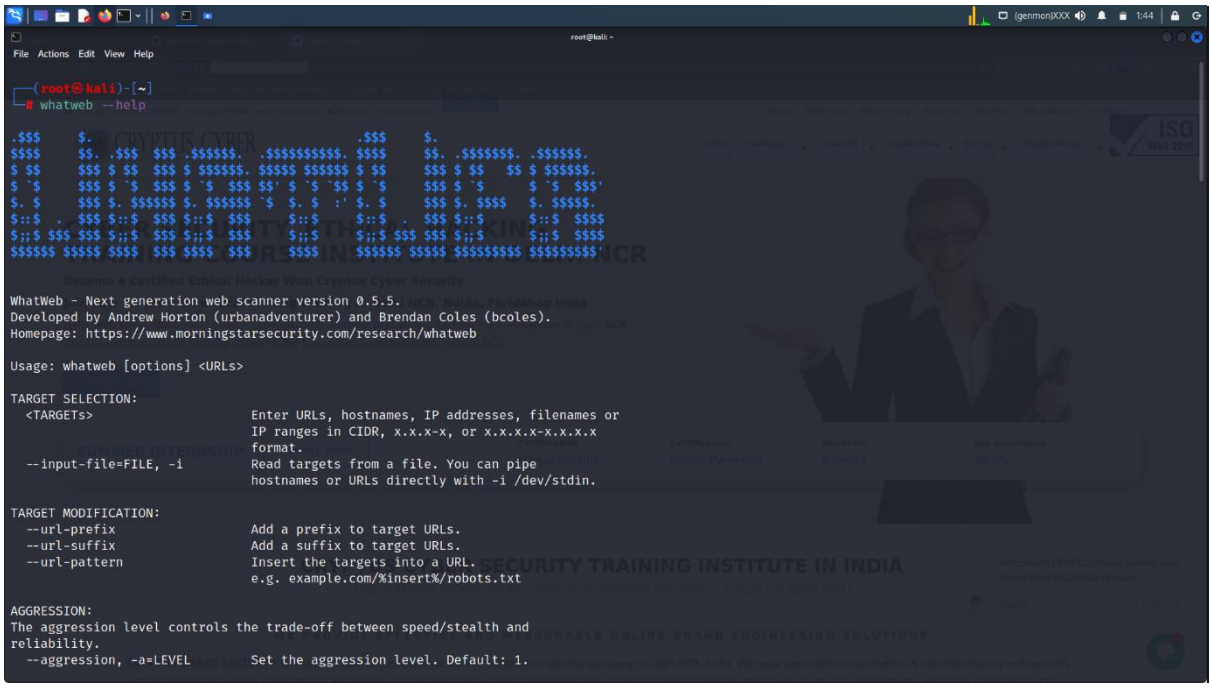
-H --help Show this help and exit



python infoga.py –domain fbi.gov –source google –verbose 3

What Web Tool

Whatweb is a free and open-source tool available on GitHub. Whatweb is a scanner written in the Ruby language. This tool can identify and recognize all the web technologies available on the target website. This tool can identify technologies used by websites such as blogging, content management system, all JavaScript libraries. Whatweb contains more than 180 modules. each module is responsible for grabbing particular information from the target website. Whatweb works as an information-gathering tool and can identify all the email addresses, SQL errors, technology used in the website.



Whatweb –help

Whatweb (url)

Like : - https://www.cryptus.in/

EXAMPLE USAGE:

* Scan example.com.

./whatweb example.com

* Scan reddit.com slashdot.org with verbose plugin descriptions.

./whatweb -v reddit.com slashdot.org

* An aggressive scan of wired.com detects the exact version of WordPress.

./whatweb -a 3 www.wired.com

* Scan the local network quickly and suppress errors.

whatweb --no-errors 192.168.0.0/24

* Scan the local network for https websites.

whatweb --no-errors --url-prefix https:// 192.168.0.0/24

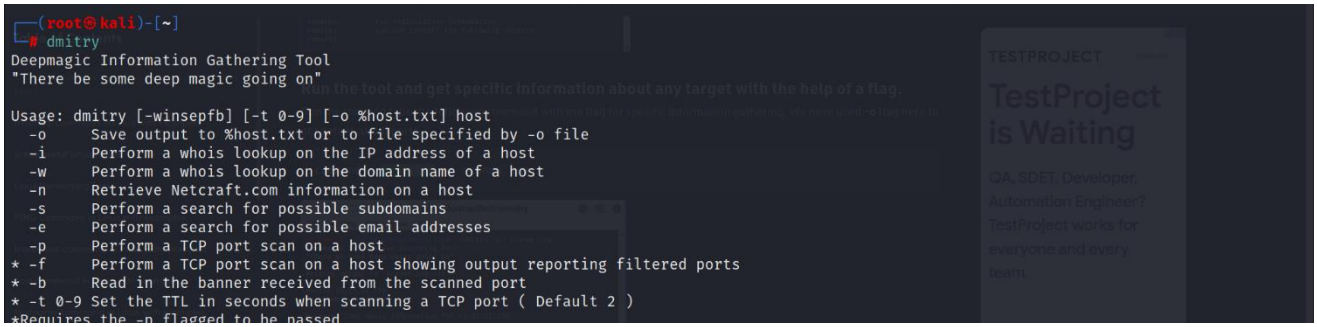
* Scan for crossdomain policies in the Alexa Top 1000.

./whatweb -i plugin-development/alexa-top-100.txt \

--url-suffix /crossdomain.xml -p crossdomain_xml

Dmitry Tool

Dmitry is a free and open-source tool available on GitHub. The tool is used for information gathering. You can download the tool and install in your Kali Linux. Dmitry stands for DeepMagic Information Gathering Tool. It's a command-line tool Using Dmitry tool You can collect information about the target, this information can be used for social engineering attacks. It can be used to gather a number of valuable pieces of information



Usages of Dmitry Tool :

- Dmitry Tool can be used to search **subdomains** of the target.
- Dmitry Tool can be used to find **open ports** of the target system.
- Dmitry Tool can be used to perform **TCP scan**.
- Dmitry Tool can be used with netcraft service to get the target information such as **operating system, web server details, web host details, hosting service details**, etc.
- Dmitry Tool can be used with whois service to get the target information such as **registered domain**, **name**, **address**, the **contact information** of the person who registered it.

- Dmitry Tool can be used to get **email addresses** that are associated with the domain of the target.

Dimitry –help

```
┌──(root㉿kali)-[~]
└─# dmitry --help
Deepmagic Information Gathering Tool
"There be some deep magic going on"

dmitry: invalid option -- '-'
Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host
  -o     Save output to %host.txt or to file specified by -o file
  -i     Perform a whois lookup on the IP address of a host
  -w     Perform a whois lookup on the domain name of a host
  -n     Retrieve Netcraft.com information on a host
  -s     Perform a search for possible subdomains
  -e     Perform a search for possible email addresses
  -p     Perform a TCP port scan on a host
* -f     Perform a TCP port scan on a host showing output reporting filtered ports
* -b     Read in the banner received from the scanned port
* -t 0-9 Set the TTL in seconds when scanning a TCP port ( Default 2 )
*Requires the -p flagged to be passed
```

-e (email information)

```
┌──(root㉿kali)-[~]
└─# dmitry https://www.cryptus.in/ -e
Deepmagic Information Gathering Tool
"There be some deep magic going on"

ERROR: Unable to locate Host IP addr. for https://www.cryptus.in/
Continuing with limited modules
HostIP:
HostName:https://www.cryptus.in/

Gathered E-Mail information for https://www.cryptus.in/
---------------------------------------
Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 E-Mail(s) for host https://www.cryptus.in/, Searched 0 pages containing 0 results

All scans completed, exiting
```

```
└─# dmitry cryptus.in
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:134.209.144.200
HostName:cryptus.in

Gathered Inet-whois information for 134.209.144.200
---------------------------------------


inetnum:        134.207.0.0 - 134.211.255.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        ------------------------------------------------------------
remarks:
remarks:        For registration information,
remarks:        you can consult the following sources:
remarks:
remarks:        IANA
remarks:        http://www.iana.org/assignments/ipv4-address-space
remarks:        http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:        http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:        AFRINIC (Africa)
remarks:        http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:        APNIC (Asia Pacific)
remarks:        http://www.apnic.net/ whois.apnic.net
remarks:
remarks:        ARIN (Northern America)
remarks:        http://www.arin.net/ whois.arin.net
remarks:
remarks:        LACNIC (Latin America and the Carribean)
remarks:        http://www.lacnic.net/ whois.lacnic.net
remarks:
```

Full scan: - dmitry cryptus.in

Fierce Tool