

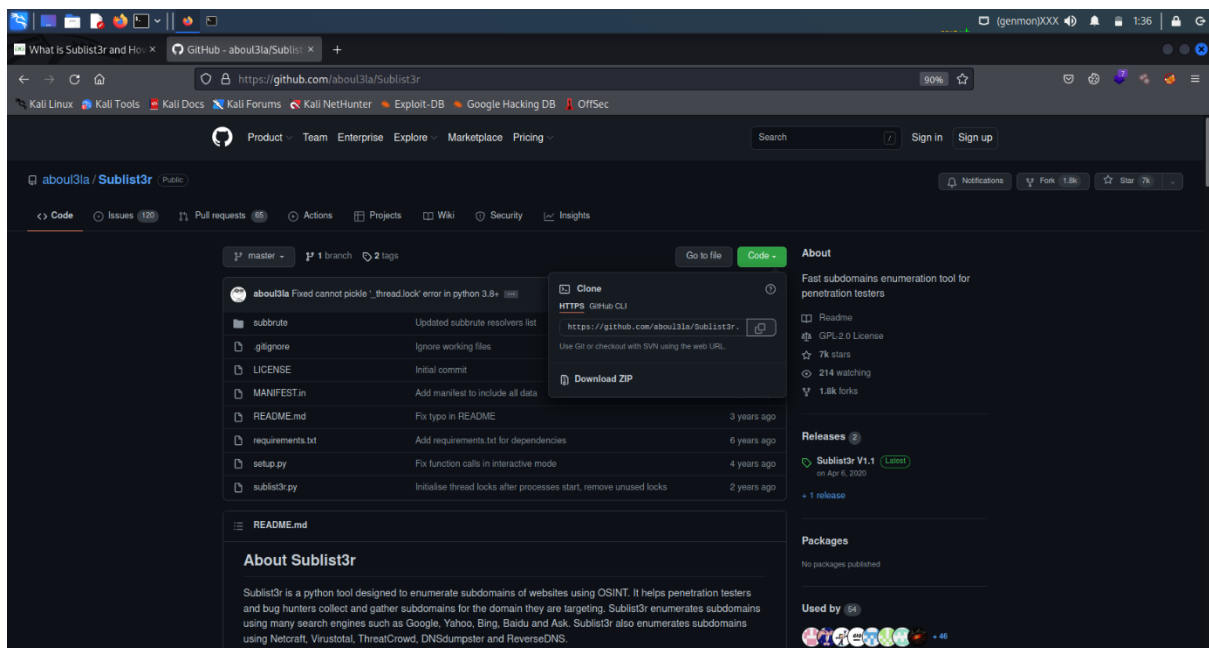


Enumeration (Tools)

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

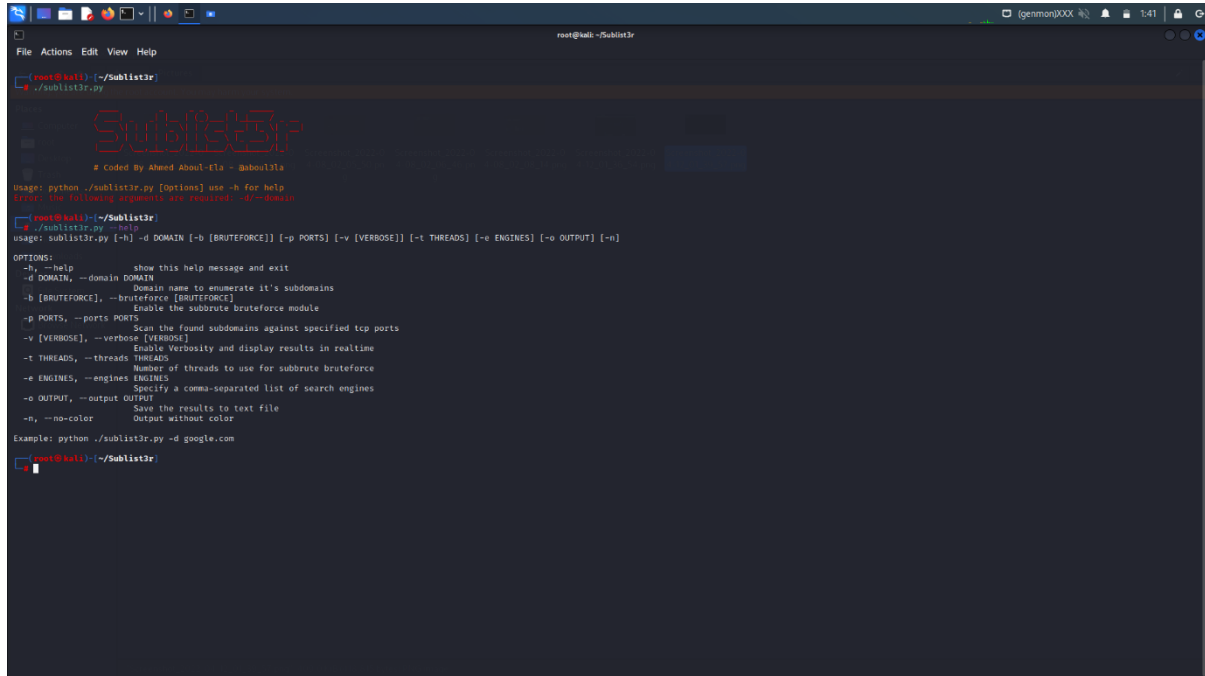


Git clone <https://github.com/about31a/Sublist3r.git>

Python3 sublist3r.py

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

```
./sublist3r.py
```



```
root@kali: ~/Sublist3r
[root@kali] ~/Sublist3r
# ./sublist3r.py

Sublist3r
# coded By Ahmed Aboul-El* - aahoul31a

usage: python ./sublist3r.py [Options] use -h for help
Error: too little arguments are required - (2 - 4 args)

[root@kali] ~/Sublist3r
# ./sublist3r.py --help
usage: sublist3r.py [-h] -d DOMAIN [-b [BRUTEFORCE]] [-p PORTS] [-v [VERBOSE]] [-t THREADS] [-e ENGINES] [-o OUTPUT] [-n]

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

Example: python ./sublist3r.py -d google.com

[root@kali] ~/Sublist3r
```

`./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

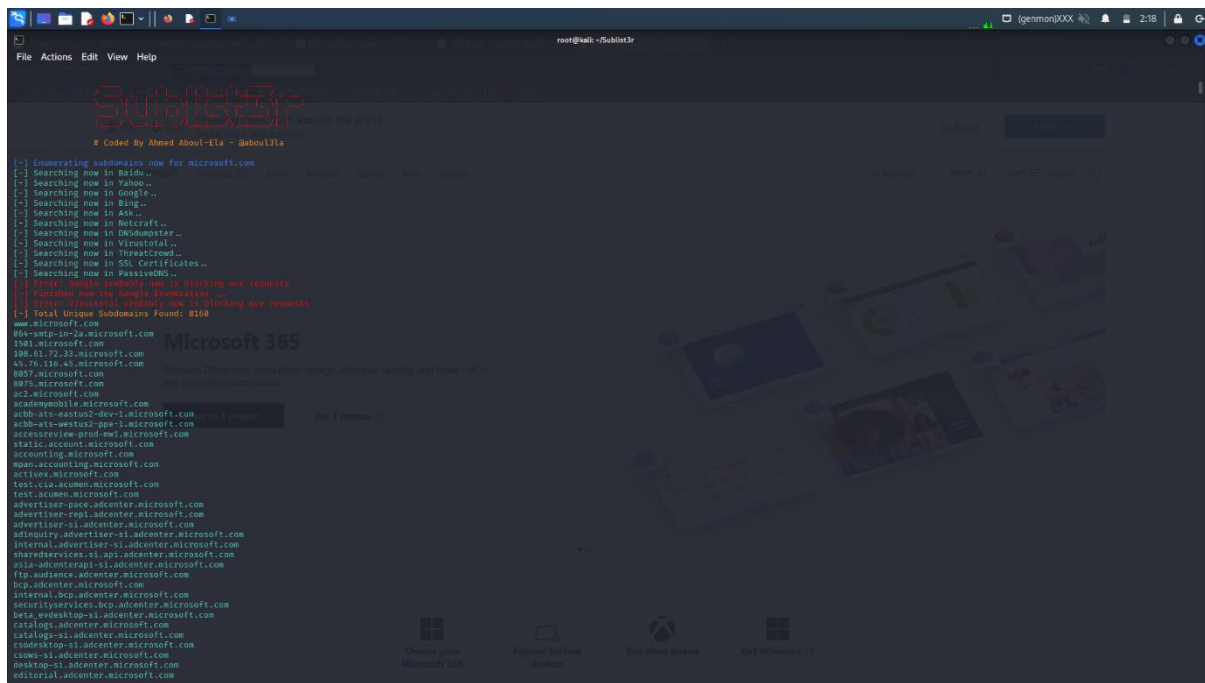
-o OUTPUT, --output OUTPUT

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 discovered 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

```
root@kali:~# dnsenum --enum google.com
dnsenum.pl VERSION:1.2.3

Host's addresses:
-----
google.com.          62      IN      A       74.125.130.100
google.com.          62      IN      A       74.125.130.101
google.com.          62      IN      A       74.125.130.102
google.com.          62      IN      A       74.125.130.113
google.com.          62      IN      A       74.125.130.138
google.com.          62      IN      A       74.125.130.139

Name Servers:
-----
ns1.google.com.      343227  IN      A       216.239.32.10
ns2.google.com.      343227  IN      A       216.239.34.10
ns3.google.com.      343227  IN      A       216.239.36.10
ns4.google.com.      343227  IN      A       216.239.38.10

Mail (MX) Servers:
-----
aspmx.l.google.com.  17      IN      A       74.125.129.27
alt1.aspmx.l.google.com. 38      IN      A       74.125.142.26
alt3.aspmx.l.google.com. 178     IN      A       173.194.68.27
alt4.aspmx.l.google.com. 163     IN      A       74.125.131.27
alt2.aspmx.l.google.com. 293     IN      A       74.125.137.27
```


LAB 2: ENUMERATION OF SUBDOMAIN USING BRUTEFORCE AND FROM FILE

When you run this command, it will 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`

```
root@kali:~# cat subdomain.txt
mail
www
webmail
service
support
dev
clients
root@kali:~# dnsenum -f subdomain.txt -r hacker.com
dnsenum.pl VERSION:1.2.3

----- hacker.com -----

Host's addresses:
-----
hacker.com.                86400    IN      A       207.70.175.42

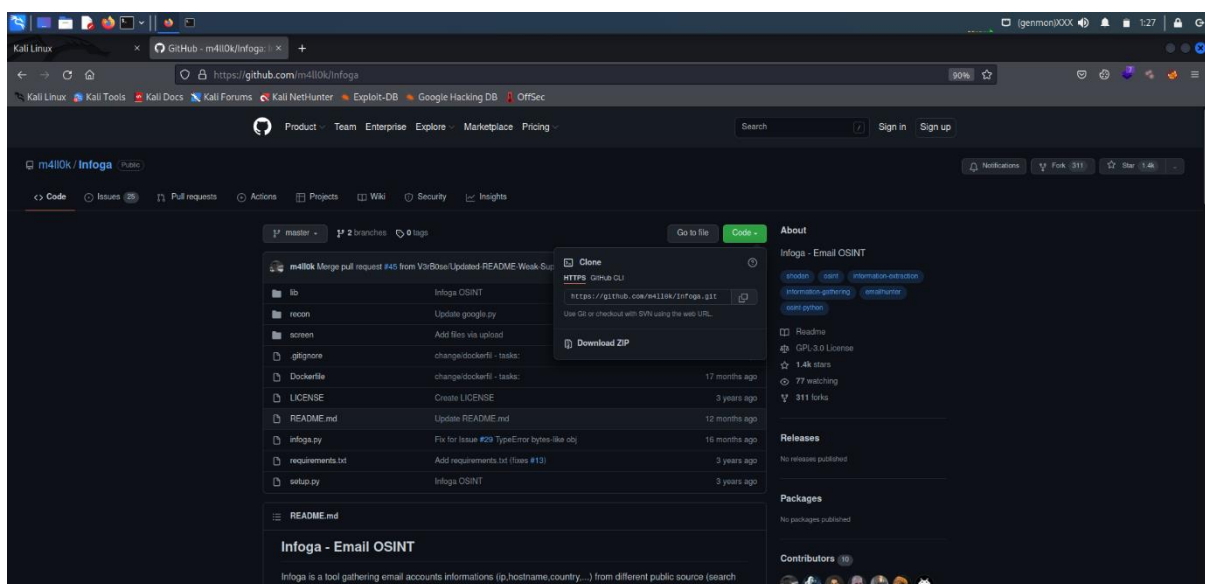
Name Servers:
-----
ns30.consolidated.net.    2816     IN      A       198.190.226.3
ns31.consolidated.net.    2816     IN      A       198.190.226.30

Brute forcing with subdomain.txt:
-----
mail.hacker.com.          300      IN      A       206.123.242.66
www.hacker.com.           86400    IN      A       207.70.175.42
webmail.hacker.com.       28800    IN      A       206.123.242.67
```

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)

```
root@kali: ~/Infoga

==[ 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

```
root@kali: ~/Infoga
File Actions Edit View Help

root@kali:~/Infoga# python infoga.py --domain geeksforgeeks.com
--source google --verbose 3

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

[+] Searching "geeksforgeeks.com" in Google ...
[i] Found 2 emails in Google
[+] Email: raghav.agg@geeksforgeeks.com ()
[i] Not found information (on shodan) for this email, search this
ip/ips on internet..
[+] Email: 22@geeksforgeeks.com ()
[i] Not found information (on shodan) for this email, search this
ip/ips on internet..
```

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.

```
root@kali: ~
File Actions Edit View Help

root@kali:~# whatweb --help

.###.  $.  /CRYPTIC CYBER  .###.  $.
####.  $.  .###.  $.  .#####.  .###.  $.  .#####.  .#####.
$ $$.  $.  $.  $.  .#####.  .#####.  $.  $.  $.  $.  $.  .#####.
$ '$  $.  $.  '$  $.  '$  '$  '$  '$  '$  '$  '$  '$  '$  '$  '$  '$
$.  '$  $.  .#####.  $.  .#####.  '$  $.  '$  '$  '$  '$  '$  '$
$::$.  $.  $.  $::$.  $.  $.  $::$.  $.  $.  $::$.  $.  $.  $::$.  $.
$::$.  $.  $.  $::$.  $.  $.  $::$.  $.  $.  $::$.  $.  $.  $::$.  $.
#####.  #####.  #####.  #####.  #####.  #####.  #####.  #####.

Become a Certified Ethical Hacker With Cryptic Cyber Security

WhatWeb - Next generation web scanner version 0.5.5.
Developed by Andrew Horton (urbanadventurer) and Brendan Coles (bcoles).
Homepage: https://www.morningstarsecurity.com/research/whatweb

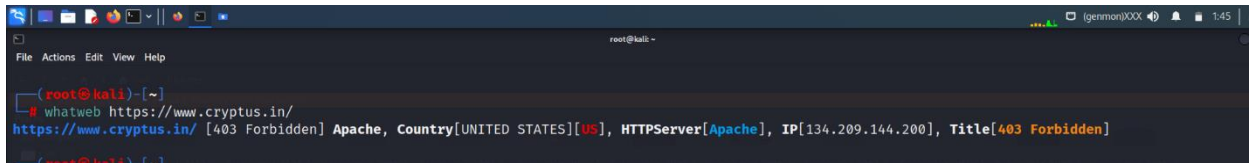
Usage: whatweb [options] <URLs>

TARGET SELECTION:
<TARGETS>      Enter URLs, hostnames, IP addresses, filenames or
                IP ranges in CIDR, x.x.x-x, or x.x.x.x-x.x.x.x
                format.
--input-file=FILE, -i  Read targets from a file. You can pipe
                hostnames or URLs directly with -i /dev/stdin.

TARGET MODIFICATION:
--url-prefix      Add a prefix to target URLs.
--url-suffix      Add a suffix to target URLs.
--url-pattern      Insert the targets into a URL.
                e.g. example.com/%insert%/robots.txt

AGGRESSION:
The aggression level controls the trade-off between speed/stealth and
reliability.
--aggression, -a=LEVEL  Set the aggression level. Default: 1.
```

Whatweb -help



```
root@kali: ~  
whatweb https://www.cryptus.in/  
https://www.cryptus.in/ [403 Forbidden] Apache, Country[UNITED STATES][US], HTTPServer[Apache], IP[134.209.144.200], Title[403 Forbidden]
```

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

```
(root@kali) - [~]
# dmitry
Deepmagic Information Gathering Tool
"There be some deep magic going on"
Use the tool and get specific information about any target with the help of a flag.

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
```

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

```

```

root@kali: ~
# 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:        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 Caribbean)
remarks:        http://www.lacnic.net/ whois.lacnic.net
remarks:

```


Full scan: - dmitry cryptus.in

Fierce Tool