

INTRODUCTION

Recon-ng is a full-featured Web Reconnaissance framework written in Python. Complete with independent modules, database interaction, built in convenience functions, interactive help, and command completion, Recon-ng provides a powerful environment in which open source web-based reconnaissance can be conducted quickly and thoroughly.

Recon-ng has a look and feel similar to the Metasploit Framework, reducing the learning curve for leveraging the framework. However, it is quite different. Recon-ng is not intended to compete with existing frameworks, as it is designed exclusively for web-based open source reconnaissance. If you want to exploit, use the Metasploit Framework. If you want to Social Engineer, use the Social Engineer Toolkit. If you want to conduct reconnaissance, use Recon-ng! See the Usage Guide for more information.

Recon-ng is a completely modular framework and makes it easy for even the newest of Python developers to contribute. Each module is a subclass of the “module” class. The “module” class is a customized “cmd” interpreter equipped with built-in functionality that provides simple interfaces to common tasks such as standardizing output, interacting with the database, making web requests, and managing API keys. Therefore, all the hard work has been done. Building modules is simple and takes little more than a few minutes. See the Development Guide for more information.

There are five categories of Modules in RECON-NG tool :

1. Recon modules
2. Reporting modules
3. Import modules
4. Exploitation modules
5. Discovery modules



In this report I used the following

OS USED : Kali Linux

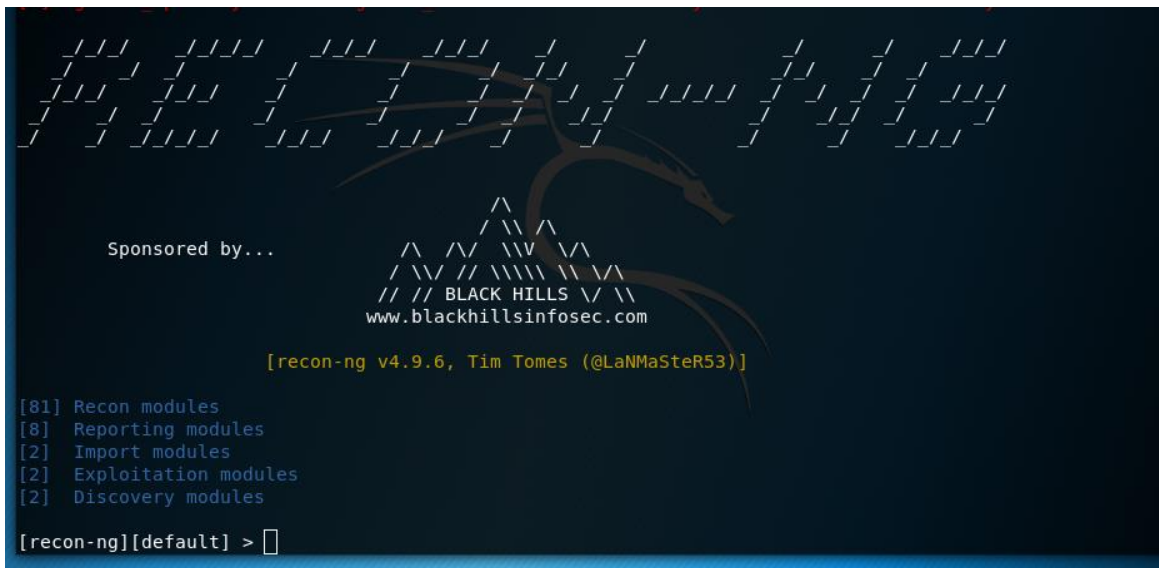
TARGET : [Yahoo.com](https://www.yahoo.com)

STARTING RECON-NG

For starting recon-ng, we have two options. First is to search for RECON-NG tool in applications, and second option is to start it from CLI by entering the following command :

COMMAND 1:

>> Recon-ng

A terminal window showing the recon-ng v4.9.6 startup screen. The background is dark blue with a stylized dragon logo in the center. The text "Sponsored by..." is on the left, and "BLACK HILLS" with the website "www.blackhillsinfosec.com" is on the right. Below the logo, the version and author information "[recon-ng v4.9.6, Tim Tomes (@LaNMaSteR53)]" are displayed. A list of modules is shown: [81] Recon modules, [8] Reporting modules, [2] Import modules, [2] Exploitation modules, and [2] Discovery modules. The prompt "[recon-ng][default] >" is at the bottom.

```

Sponsored by...

      /\
     /\  /\
    /\  /\  /\
   /\  /\  /\  /\
  /\  /\  /\  /\  /\
 /\  /\  /\  /\  /\  /\
//  //  BLACK HILLS  \ \
//  //  www.blackhillsinfosec.com  \ \

[recon-ng v4.9.6, Tim Tomes (@LaNMaSteR53)]

[81] Recon modules
[8]  Reporting modules
[2]  Import modules
[2]  Exploitation modules
[2]  Discovery modules

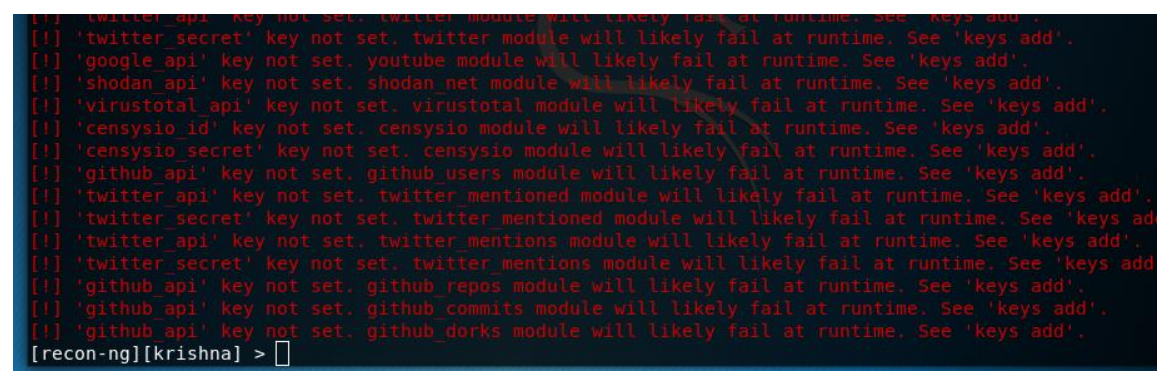
[recon-ng][default] >
```

CREATING WORKSPACES

Creating workspaces for every specific information gathering is very important as it provides a complete management and reporting of the information in a good manner. For creating the workspaces, we need to write the following command in the recon-ng module:

COMMAND 2:

>> workspaces add Krishna

A terminal window showing the output of the "workspaces add Krishna" command in recon-ng. The output consists of multiple lines of warnings indicating that various API keys are not set, which may cause modules to fail at runtime. The modules mentioned include twitter, google, youtube, shodan, virustotal, censysio, github_users, twitter_mentioned, twitter_mentions, github_repos, github_commits, and github_dorks. The prompt "[recon-ng][krishna] >" is at the bottom.

```

[!] 'twitter_api' key not set. twitter module will likely fail at runtime. See 'keys add'.
[!] 'twitter_secret' key not set. twitter module will likely fail at runtime. See 'keys add'.
[!] 'google_api' key not set. youtube module will likely fail at runtime. See 'keys add'.
[!] 'shodan_api' key not set. shodan net module will likely fail at runtime. See 'keys add'.
[!] 'virustotal_api' key not set. virustotal module will likely fail at runtime. See 'keys add'.
[!] 'censysio_id' key not set. censysio module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set. censysio module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set. github_users module will likely fail at runtime. See 'keys add'.
[!] 'twitter_api' key not set. twitter mentioned module will likely fail at runtime. See 'keys add'.
[!] 'twitter_secret' key not set. twitter_mentioned module will likely fail at runtime. See 'keys add'.
[!] 'twitter_api' key not set. twitter_mentions module will likely fail at runtime. See 'keys add'.
[!] 'twitter_secret' key not set. twitter_mentions module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set. github_repos module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set. github_commits module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set. github_dorks module will likely fail at runtime. See 'keys add'.
[recon-ng][krishna] >
```

ADDING DOMAIN

It is required to provide the specific target on which we have to perform the attack and gather the information. RECON-NG tool is very flexible, and it can accept multiple domains input as well and it performs operations on every domain individually. Below command is used to specify the domain:

COMMAND 3:

```
>> add domains
```

```
>> yahoo.com
```

```
[!]'virtuotal_api' key not set. virtuotal module will likely fail at runtime. See 'keys add'.
[!]'censysio_id' key not set. censysio module will likely fail at runtime. See 'keys add'.
[!]'censysio_secret' key not set. censysio module will likely fail at runtime. See 'keys add'.
[!]'github_api' key not set. github_users module will likely fail at runtime. See 'keys add'.
[!]'twitter_api' key not set. twitter_mentioned module will likely fail at runtime. See 'keys add'.
[!]'twitter_secret' key not set. twitter_mentioned module will likely fail at runtime. See 'keys add'.
[!]'twitter_api' key not set. twitter_mentions module will likely fail at runtime. See 'keys add'.
[!]'twitter_secret' key not set. twitter_mentions module will likely fail at runtime. See 'keys add'.
[!]'github_api' key not set. github_repos module will likely fail at runtime. See 'keys add'.
[!]'github_api' key not set. github_commits module will likely fail at runtime. See 'keys add'.
[!]'github_api' key not set. github_dorks module will likely fail at runtime. See 'keys add'.
[recon-ng][krishna] > add domains
domain (TEXT): yahoo.com
[recon-ng][krishna] > 
```

EXTRACT INFO

After adding the domain to the domain table, we need to specify which kind of operation we must perform on the target. Here, I used the **recon/domains-contacts/whois_pocs** for extracting the available information related to my target **yahoo.com**. This module provides the first, middle & last name, email addresses, region and country of the targeted domain users.

COMMAND 4:

```
>> use recon/domains-contacts/whois_pocs
```

After entering the above command, we need to look at the options related to this module and accordingly we need to set the parameters/options.

COMMAND 5:

```
>> show options
```

```
[!]'twitter_secret' key not set. twitter_mentions module will likely fail at runtime. See 'keys add'.
[!]'github_api' key not set. github_repos module will likely fail at runtime. See 'keys add'.
[!]'github_api' key not set. github_commits module will likely fail at runtime. See 'keys add'.
[!]'github_api' key not set. github_dorks module will likely fail at runtime. See 'keys add'.
[recon-ng][krishna] > add domains
domain (TEXT): yahoo.com
[recon-ng][krishna] > use recon/domains-contacts/whois_pocs
[recon-ng][krishna][whois_pocs] > show options

  Name      Current Value  Required  Description
  -----
SOURCE      default        yes       source of input (see 'show info' for details)

[recon-ng][krishna][whois_pocs] > 
```

Here, in options there is a parameter SOURCE, we need to specify the source because source is responsible for getting the vital information. But, here by default, the default source points to the domain table. For verification one may run the following command :

COMMAND 6 :

>> show info

Now, after verification we need to hit the run command to get the results

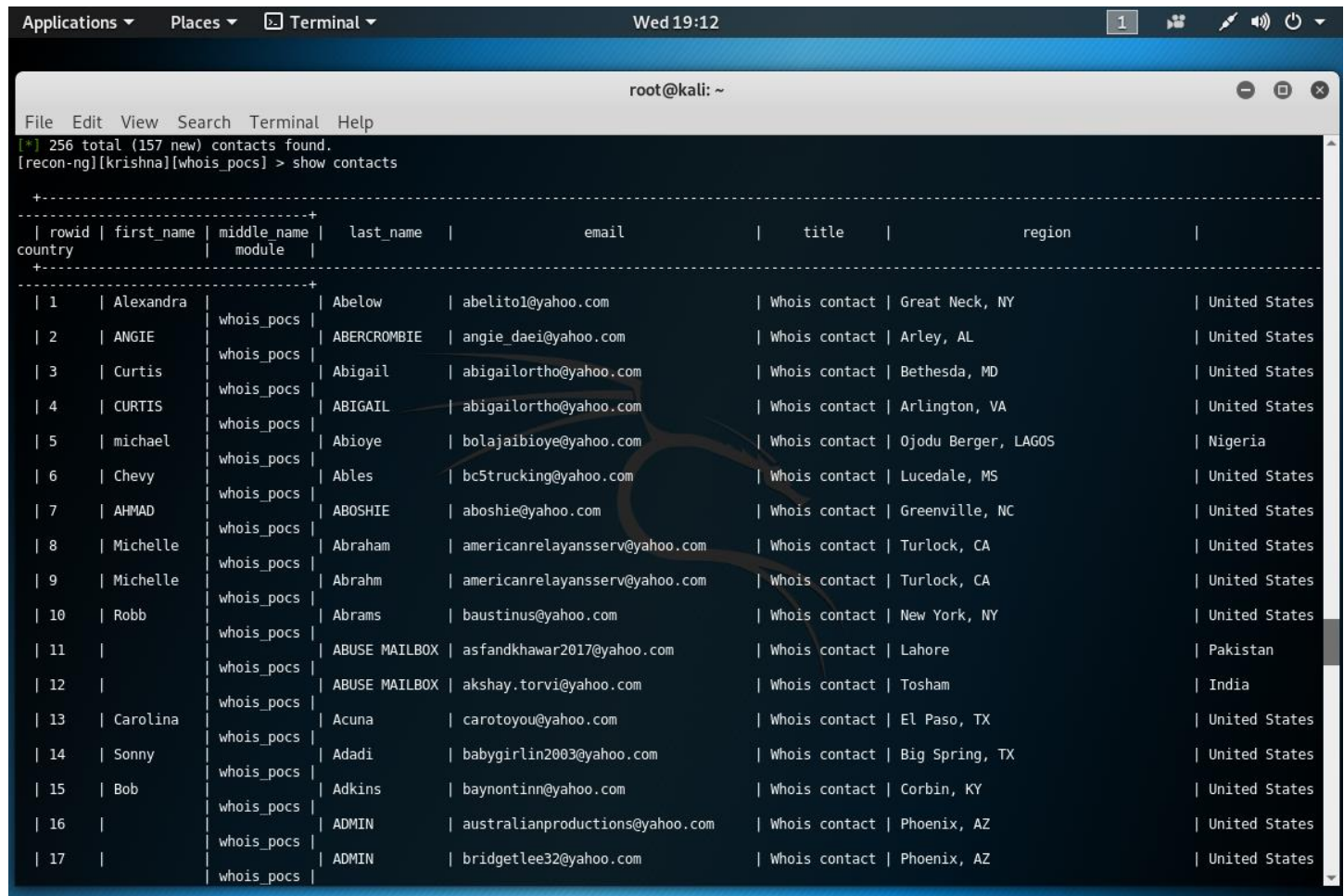
COMMAND 7 :

>> run

After, the completion of the operation, we get some results in an improper format and to show the output in a proper format we need to specify the following command:

COMMAND 7 :

>> show contacts



```
File Edit View Search Terminal Help
[*] 256 total (157 new) contacts found.
[recon-ng][krishna][whois_pocs] > show contacts
```

rowid	first_name	middle name	last_name	email	title	region	country
1	Alexandra		Abelow	abelitol@yahoo.com	Whois contact	Great Neck, NY	United States
2	ANGIE	whois_pocs	ABERCROMBIE	angie daei@yahoo.com	Whois contact	Arley, AL	United States
3	Curtis	whois_pocs	Abigail	abigailortho@yahoo.com	Whois contact	Bethesda, MD	United States
4	CURTIS	whois_pocs	ABIGAIL	abigailortho@yahoo.com	Whois contact	Arlington, VA	United States
5	michael	whois_pocs	Abioye	bolajaibioye@yahoo.com	Whois contact	Ojodu Berger, LAGOS	Nigeria
6	Chevy	whois_pocs	Ables	bc5trucking@yahoo.com	Whois contact	Lucedale, MS	United States
7	AHMAD	whois_pocs	ABOSHIE	aboshie@yahoo.com	Whois contact	Greenville, NC	United States
8	Michelle	whois_pocs	Abraham	americanrelayansserv@yahoo.com	Whois contact	Turlock, CA	United States
9	Michelle	whois_pocs	Abrahm	americanrelayansserv@yahoo.com	Whois contact	Turlock, CA	United States
10	Robb	whois_pocs	Abrams	baustinus@yahoo.com	Whois contact	New York, NY	United States
11		whois_pocs	ABUSE MAILBOX	asfandkhawar2017@yahoo.com	Whois contact	Lahore	Pakistan
12		whois_pocs	ABUSE MAILBOX	akshay.torvi@yahoo.com	Whois contact	Tosham	India
13	Carolina	whois_pocs	Acuna	carotoyou@yahoo.com	Whois contact	El Paso, TX	United States
14	Sonny	whois_pocs	Adadi	babygirlin2003@yahoo.com	Whois contact	Big Spring, TX	United States
15	Bob	whois_pocs	Adkins	baynontinn@yahoo.com	Whois contact	Corbin, KY	United States
16		whois_pocs	ADMIN	australianproductions@yahoo.com	Whois contact	Phoenix, AZ	United States
17		whois_pocs	ADMIN	bridgetlee32@yahoo.com	Whois contact	Phoenix, AZ	United States

RESOLVING SUB-DOMAINS & IPs

For getting the complete sub-domain lists and their IP addresses, we need to use other modules to complete the task. Here the brute force method is used to resolve the sub-domains and IP address of the target. The module which is used too resolve the sub-domains and IPs is **recon/domains-hosts/brute_force**.

COMMAND 8 :

```
>> use recon/domains-hosts/brute_force
```

```
>> run
```

```
-----+
[*] 157 rows returned
[recon-ng][krishna][whois_pocs] > use recon/domains-hosts/brute_hosts
[recon-ng][krishna][brute_hosts] >
[recon-ng][krishna] > use recon/domains-hosts/brute_hosts
[recon-ng][krishna][brute_hosts] > run
```

```
root@kali: ~
File Edit View Search Terminal Help
[recon-ng][krishna][brute_hosts] > run

-----
YAHOO.COM
-----
[*] No Wildcard DNS entry found.
[*] 0.yahoo.com => No record found.
[*] 11.yahoo.com => No record found.
[*] 14.yahoo.com => No record found.
[*] 13.yahoo.com => No record found.
[*] 12.yahoo.com => No record found.
[*] 01.yahoo.com => No record found.
[*] 10.yahoo.com => No record found.
[*] 2.yahoo.com => No record found.
[*] 17.yahoo.com => No record found.
[*] 3.yahoo.com => No record found.
[*] 02.yahoo.com => No record found.
[*] 4.yahoo.com => No record found.
[*] 15.yahoo.com => No record found.
[*] 1.yahoo.com => No record found.
[*] 6.yahoo.com => No record found.
[*] 20.yahoo.com => No record found.
[*] 16.yahoo.com => No record found.
[*] 18.yahoo.com => No record found.
[*] 9.yahoo.com => No record found.
[*] ILMI.yahoo.com => No record found.
[*] a.yahoo.com => No record found.
[*] a02.yahoo.com => No record found.
[*] 3com.yahoo.com => No record found.
[*] abc.yahoo.com => No record found.
[*] 03.yahoo.com => No record found.
[*] 19.yahoo.com => No record found.
[*] ac.yahoo.com => No record found.
[*] 7.yahoo.com => No record found.
```

Again, the desired output is not aligned. So, we need to write one specific command to get output in proper format

COMMAND 9 :

```
>> show hosts
```

```

root@kali: ~
File Edit View Search Terminal Help
[*] 1445 total (604 new) hosts found.
[recon-ng][krishna][brute_hosts] > show hosts

```

rowid	host	ip_address	region	country	latitude	longitude	module
1	san2.src.yahoo.com						brute_hosts
2	about.yahoo.com						brute_hosts
3	any-src.san2.a01.yahoodns.net						brute_hosts
4	about.yahoo.com	212.82.100.152					brute_hosts
5	a5.yahoo.com						brute_hosts
6	ad.yahoo.com						brute_hosts
7	ad.yahoo.com	204.71.200.45					brute_hosts
8	src1.yahoo.com						brute_hosts
9	accounts.yahoo.com						brute_hosts
10	src.san1.g01.yahoodns.net						brute_hosts
11	any-src.san1.a01.yahoodns.net						brute_hosts
12	accounts.yahoo.com	98.136.103.24					brute_hosts
13	adspecs.yahoo.com						brute_hosts
14	adkit.yahoo.com						brute_hosts
15	adkit.yahoo.com	98.136.103.24					brute_hosts
16	ds-geoycpi-uno.gycpi.b.yahoodns.net						brute_hosts
17	ads.yahoo.com						brute_hosts
18	ads.yahoo.com	27.123.43.204					brute_hosts
19	ads.yahoo.com	27.123.43.205					brute_hosts
20	global1.adserver.gysm.yahoodns.net						brute_hosts
21	adserver.yahoo.com						brute_hosts
22	adserver.yahoo.com	106.10.193.24					brute_hosts
23	src.yahoo.com						brute_hosts
24	affiliates.yahoo.com						brute_hosts
25	src.g03.yahoodns.net						brute_hosts
26	any-src.a03.yahoodns.net						brute_hosts
27	affiliates.yahoo.com	98.136.103.23					brute_hosts
28	agenda.yahoo.com						brute_hosts
29	agenda.yahoo.com	98.136.103.23					brute_hosts
30	www.yahoo.com						brute_hosts
31	alerts.yahoo.com						brute_hosts
32	atsv2-fp-shed.wg1.b.yahoo.com						brute_hosts
33	alerts.yahoo.com	106.10.236.140					brute_hosts
34	ar.yahoo.com						brute_hosts
35	ar.yahoo.com	212.82.100.151					brute_hosts

REPORTING

Reporting is the essential part of the information gathering. A proper documentation is required for the better understanding of the results/output. In RECON-NG we also have some reporting modules which can provide a complete report of all the operations performed in the specific workspace. For this report, **reporting/html** module is used.

COMMAND 10 :

>> use reporting/html

Here, we need to specify few parameters to complete the reporting in a proper format. For setting all parameters, we need to look into all the required parameters by running the following command :

>> show options

```

[*] 604 rows returned
[recon-ng][krishna][brute_hosts] > use reporting/html
[recon-ng][krishna][html] >
[recon-ng][krishna] > use reporting/html
[recon-ng][krishna][html] > show options

```

Name	Current Value	Required	Description
CREATOR		yes	creator name for the report footer
CUSTOMER		yes	customer name for the report header
FILENAME	/root/.recon-ng/workspaces/krishna/results.html	yes	path and filename for report output
SANITIZE	True	yes	mask sensitive data in the report

Here, we have four different options and we need to set three of the options which is required:

Let's set the CREATOR

COMMAND 11 :

>> set CREATOR Krishna

Let's set the CUSTOMER

COMMAND 12 :

>> set CUSTOMER INT244

Let's set the FILENAME

COMMAND 13 :

>> set FILENAME report.html

>> run

```
[recon-ng][krishna][html] > set CREATOR Krishna
CREATOR => Krishna
[recon-ng][krishna][html] > set CUSTOMER INT244
CUSTOMER => INT244
[recon-ng][krishna][html] > set FILENAME /root/Desktop/report.html
FILENAME => /root/Desktop/report.html
[recon-ng][krishna][html] >
```

Now, browse the file **report.html** open it in browser and analyze the output :

The screenshot shows a Firefox ESR browser window with the title "Recon-ng Reconnaissance Report - Mozilla Firefox". The address bar shows the file path "file:///root/Desktop/report.html". The report content is as follows:

INT244

www.recon-ng.com

Recon-ng Reconnaissance Report

[+] Summary

[+] Domains

[+] Hosts

[+] Contacts

Created by: Krishna
Wed, Apr 08 2020 19:23:23

Let's Look at the SUMMARY

Recon-ng Reconnaissance Report - Mozilla Firefox

Recon-ng Reconnaissance R... Firefox Privacy Notice — x +

file:///root/Desktop/report.html

Most Visited Getting Started Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security

INT244

www.recon-ng.com

Recon-ng Reconnaissance Report

[-] Summary

table	count
domains	1
companies	0
netblocks	0
locations	0
vulnerabilities	0
ports	0
hosts	604
contacts	157
credentials	0
leaks	0
pushpins	0
profiles	0
repositories	0

[+] Domains

[+] Hosts

[+] Contacts

Created by: Krishna
Wed, Apr 08 2020 19:23:23

Here is the link for web view of the report :



THANK YOU !!