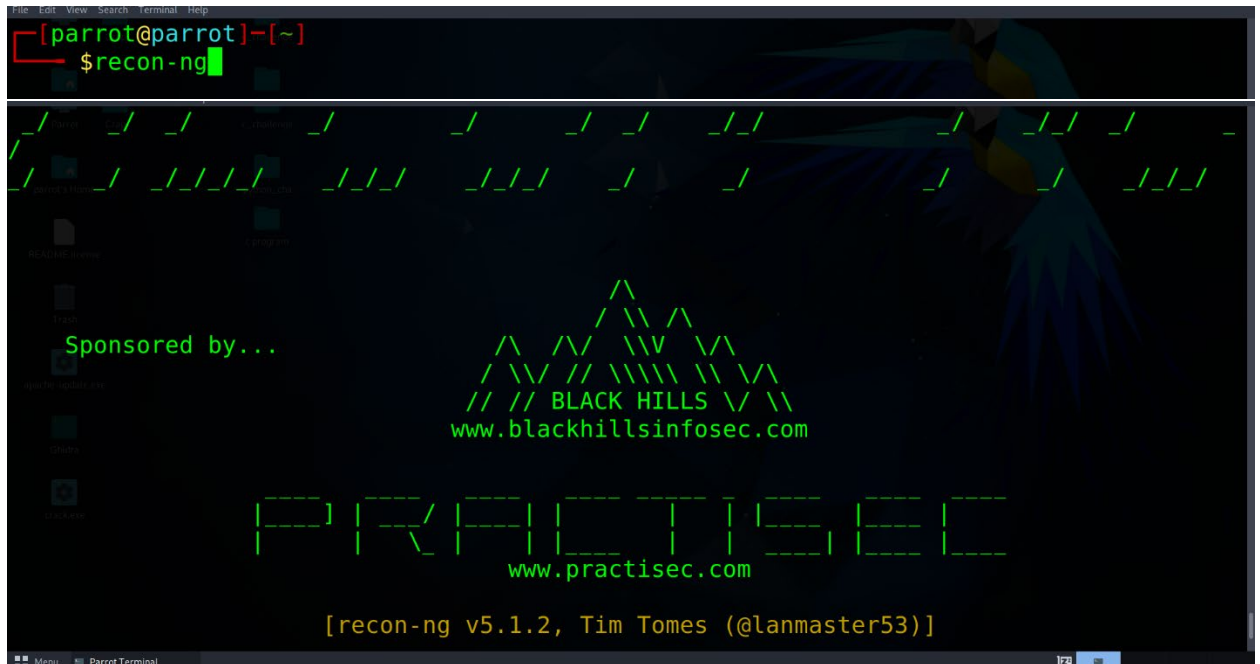
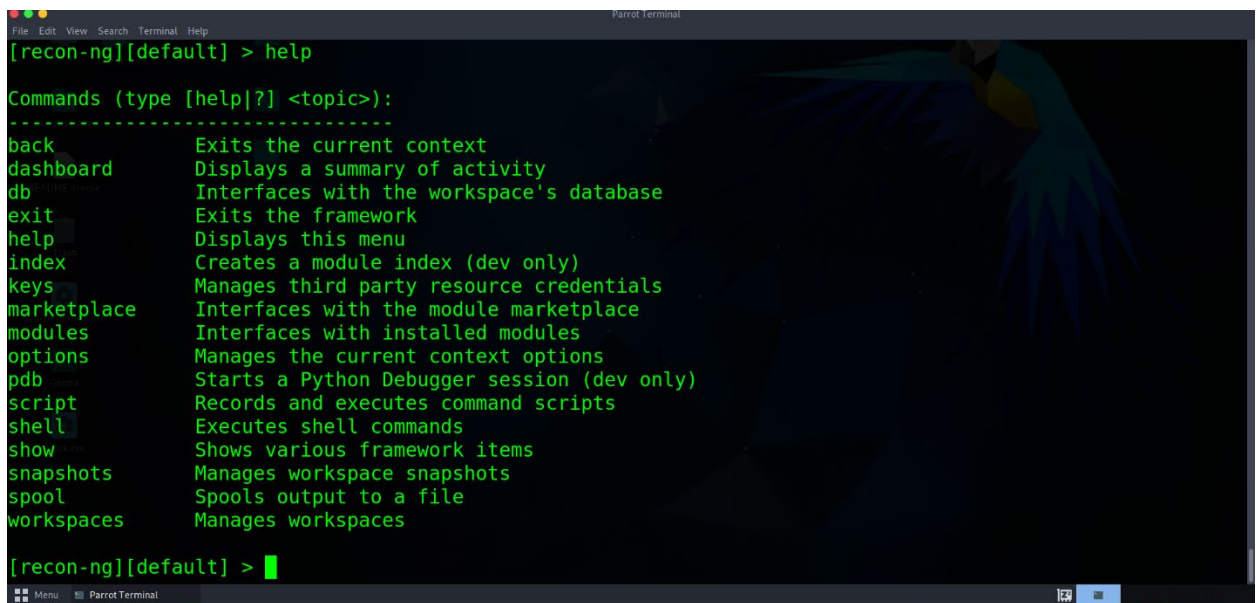


RECON-NG

1. Launching Recon-ng:



2. Help command:



DATABASE: help db

```
[recon-ng][206] > db schema
```

domains	
domain	TEXT
notes	TEXT
module	TEXT

companies	
company	TEXT
description	TEXT
notes	TEXT
module	TEXT

netblocks	
netblock	TEXT
notes	TEXT
module	TEXT

locations	
latitude	TEXT
longitude	TEXT
street_address	TEXT
notes	TEXT

notes	TEXT
module	TEXT

hosts	
host	TEXT
ip_address	TEXT
region	TEXT
country	TEXT
latitude	TEXT
longitude	TEXT
notes	TEXT
module	TEXT

contacts	
first_name	TEXT
middle_name	TEXT
last_name	TEXT
email	TEXT
title	TEXT
region	TEXT
country	TEXT
phone	TEXT
notes	TEXT
module	TEXT

credentials	
username	TEXT
password	TEXT
hash	TEXT
type	TEXT
leak	TEXT
notes	TEXT
module	TEXT

leaks	
leak_id	TEXT
description	TEXT
source_refs	TEXT
leak_type	TEXT
title	TEXT
import_date	TEXT
leak_date	TEXT
attackers	TEXT
num_entries	TEXT
score	TEXT
num_domains_affected	TEXT
attack_method	TEXT
target_industries	TEXT
password_hash	TEXT
password_type	TEXT
targets	TEXT
media_refs	TEXT
notes	TEXT
module	TEXT

```
[recon-ng][206] > db insert domains
domain (TEXT): testphp.com
notes (TEXT): For learning purpose.
[*] 1 rows affected.

[recon-ng][206] > show domains
+-----+-----+-----+-----+
| rowid | domain | notes | module |
+-----+-----+-----+-----+
| 1 | testphp.com | For learning purpose. | user_defined |
+-----+-----+-----+-----+

[*] 1 rows returned
```

```
[recon-ng][206] > db insert profiles
username (TEXT): a
resource (TEXT): a
url (TEXT): a
category (TEXT): aa
notes (TEXT): a
[*] 1 rows affected.
[recon-ng][206] > show profiles
+-----+-----+-----+-----+-----+-----+-----+
| rowid | username | resource | url | category | notes | module |
+-----+-----+-----+-----+-----+-----+-----+
| 1 | a | a | a | aa | a | user_defined |
+-----+-----+-----+-----+-----+-----+-----+

[*] 1 rows returned
[recon-ng][206] >
```

3. Workspaces :

```
Applications Places System Parrot Terminal Thu Sep 21 13:13
File Edit View Search Terminal Help

[recon-ng][default] > workspaces
Manages workspaces

Usage: workspaces <create|list|load|remove> [...]

[recon-ng][default] > workspaces create ITSC206
[!] 'bing_api' key not set. bing_linkedin_cache module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/companies-contacts/censys_email_address' disabled. Dependency required: 'censys'.
[!] Module 'recon/companies-domains/censys_subdomains' disabled. Dependency required: 'censys'.
[!] 'whoxy_api' key not set. whoxy_dns module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/companies-hosts/censys_org' disabled. Dependency required: 'censys'.
[!] Module 'recon/companies-hosts/censys_tls_subjects' disabled. Dependency required: 'censys'.
[!] 'github_api' key not set. github_miner module will likely fail at runtime. See 'keys add'.
[!] 'shodan_api' key not set. shodan_org module will likely fail at runtime. See 'keys add'.
[!] 'hibp_api' key not set. hibp_breach module will likely fail at runtime. See 'keys add'.
[!] 'hibp_api' key not set. hibp_paste module will likely fail at runtime. See 'keys add'.
[!] 'fullcontact_api' key not set. fullcontact module will likely fail at runtime. See 'keys add'.
[!] 'hashes_api' key not set. hashes_org module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/domains-companies/censys_companies' disabled. Dependency required: 'censys'.
[!] 'whoxy_api' key not set. whoxy_whois module will likely fail at runtime. See 'keys add'.
[!] 'hunter_io' key not set. hunter_io module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/domains-contacts/metacrawler' disabled. Dependency required: 'PyPDF3'.
```

```
[recon-ng][ITSC206] > workspaces list
```

Workspaces	Modified
ITSC206	2023-09-21 13:50:54
carlover	2023-09-20 22:54:12
default	2023-09-20 22:40:26

```
[recon-ng][ITSC206] > workspaces remove carlover
[recon-ng][ITSC206] > workspaces list
```

Workspaces	Modified
ITSC206	2023-09-21 13:50:54
default	2023-09-20 22:40:26

```
[recon-ng][ITSC206] >
```

You can load an existing workspace by the following command:

```
File Edit View Search Terminal Help
[recon-ng][default] > workspaces load ITSC206
```

Opening up the directory directly for a particular workspace.


```

File Actions Edit View Help

+-----+
| Path | Version | Status | Updated | D | K |
+-----+
| discovery/info_disclosure/cache_snoop | 1.1 | not installed | 2020-10-13 | | |
| discovery/info_disclosure/interesting_files | 1.2 | not installed | 2021-10-04 | | |
| exploitation/injection/command_injector | 1.0 | not installed | 2019-06-24 | | |
| exploitation/injection/xpath_bruter | 1.2 | not installed | 2019-10-08 | | |
| import/csv_file | 1.1 | not installed | 2019-08-09 | | |
| import/list | 1.1 | not installed | 2019-06-24 | | |
| import/masscan | 1.0 | not installed | 2020-04-07 | | |
| import/nmap | 1.1 | not installed | 2020-10-06 | | |
| recon/companies-contacts/bing_linkedin_cache | 1.0 | not installed | 2019-06-24 | | * |
| recon/companies-contacts/censys_email_address | 2.0 | not installed | 2021-05-11 | * | * |
| recon/companies-contacts/pen | 1.1 | not installed | 2019-10-15 | | |
| recon/companies-domains/censys_subdomains | 2.0 | not installed | 2021-05-10 | * | * |
| recon/companies-domains/pen | 1.1 | not installed | 2019-10-15 | | |
| recon/companies-domains/viewdns_reverse_whois | 1.1 | not installed | 2021-08-24 | | |
| recon/companies-domains/whoxy_dns | 1.1 | not installed | 2020-06-17 | | * |
| recon/companies-hosts/censys_org | 2.0 | not installed | 2021-05-11 | * | * |
| recon/companies-hosts/censys_tls_subjects | 2.0 | not installed | 2021-05-11 | * | * |
| recon/companies-multi/github_miner | 1.1 | not installed | 2020-05-15 | | * |
| recon/companies-multi/shodan_org | 1.1 | not installed | 2020-07-01 | * | * |
| recon/companies-multi/whois_miner | 1.1 | not installed | 2019-10-15 | | |
| recon/contacts-contacts/abc | 1.0 | not installed | 2019-10-11 | * | |
| recon/contacts-contacts/mailtester | 1.0 | not installed | 2019-06-24 | | |
| recon/contacts-contacts/mangle | 1.0 | not installed | 2019-06-24 | | |
| recon/contacts-contacts/unmangle | 1.1 | not installed | 2019-10-27 | | |

+-----+

recon/netblocks-ports/censysio | 1.0 | not installed | 2019-06-24 | | * |
recon/ports-hosts/migrate_ports | 1.0 | not installed | 2019-06-24 | | * |
recon/ports-hosts/ssl_scan | 1.1 | not installed | 2021-08-24 | | |
recon/profiles-contacts/bing_linkedin_contacts | 1.2 | not installed | 2021-08-24 | | * |
recon/profiles-contacts/dev_diver | 1.1 | not installed | 2020-05-15 | | |
recon/profiles-contacts/github_users | 1.0 | not installed | 2019-06-24 | | * |
recon/profiles-profiles/namechk | 1.0 | not installed | 2019-06-24 | | * |
recon/profiles-profiles/profiler | 1.1 | not installed | 2019-10-16 | | |
recon/profiles-profiles/twitter_mentioned | 1.0 | not installed | 2019-06-24 | | * |
recon/profiles-profiles/twitter_mentions | 1.0 | not installed | 2019-06-24 | | * |
recon/profiles-repositories/github_repos | 1.1 | not installed | 2020-05-15 | | * |
recon/repositories-profiles/github_commits | 1.0 | not installed | 2019-06-24 | | * |
recon/repositories-vulnerabilities/gists_search | 1.0 | not installed | 2019-06-24 | | |
recon/repositories-vulnerabilities/github_dorks | 1.0 | not installed | 2019-06-24 | | * |
reporting/csv | 1.0 | not installed | 2019-06-24 | | |
reporting/html | 1.0 | not installed | 2019-06-24 | | |
reporting/json | 1.0 | not installed | 2019-06-24 | | |
reporting/list | 1.0 | not installed | 2019-06-24 | | |
reporting/proxifier | 1.0 | not installed | 2019-06-24 | | |
reporting/pushpin | 1.0 | not installed | 2019-06-24 | | * |
reporting/xlsx | 1.0 | not installed | 2019-06-24 | | |
reporting/xml | 1.1 | not installed | 2019-06-24 | | |

+-----+

D = Has dependencies. See info for details.
K = Requires keys. See info for details.

[recon-ng][default] >

```

- To install all modules in one go, give the command : marketplace install all

```
[recon-ng][ISA] > marketplace install all
[*] Module installed: discovery/info_disclosure/cache_snoop
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Module installed: exploitation/injection/command_injector
[*] Module installed: exploitation/injection/xpath_bruter
[*] Module installed: import/csv_file
[*] Module installed: import/list
[*] Module installed: import/masscan
[*] Module installed: import/nmap
[*] Module installed: recon/companies-contacts/bing_linkedin_cache
[*] Module installed: recon/companies-contacts/censys_email_address
[*] Module installed: recon/companies-contacts/pen
[*] Module installed: recon/companies-domains/censys_subdomains
[*] Module installed: recon/companies-domains/pen
[*] Module installed: recon/companies-domains/viewdns_reverse_whois
[*] Module installed: recon/companies-domains/whoxy_dns
[*] Module installed: recon/companies-hosts/censys_org
[*] Module installed: recon/companies-hosts/censys_tls_subjects
[*] Module installed: recon/companies-multi/github_miner
[*] Module installed: recon/companies-multi/shodan_org
[*] Module installed: recon/companies-multi/whois_miner
[*] Module installed: recon/contacts-contacts/abc
[*] Module installed: recon/contacts-contacts/mailtester
[*] Module installed: recon/contacts-contacts/mangle
[*] Module installed: recon/contacts-contacts/unmangle
[*] Module installed: recon/contacts-credentials/hibp_breach
[*] Module installed: recon/contacts-credentials/hibp_paste
```

[recon-ng][default] > marketplace search

Module Name	Path	Version	Status	Updated	D	K
discovery/info_disclosure/cache_snoop		1.1	installed	2020-10-13		
discovery/info_disclosure/interesting_files		1.2	installed	2021-10-04		
exploitation/injection/command_injector		1.0	installed	2019-06-24		
exploitation/injection/xpath_bruter		1.2	installed	2019-10-08		
import/csv_file		1.1	installed	2019-08-09		
import/list		1.1	installed	2019-06-24		
import/masscan		1.0	installed	2020-04-07		
import/nmap		1.1	installed	2020-10-06		
recon/companies-contacts/bing_linkedin_cache		1.0	installed	2019-06-24		*
recon/companies-contacts/censys_email_address		2.0	disabled	2021-05-11	*	*
recon/companies-contacts/pen		1.1	installed	2019-10-15		
recon/companies-domains/censys_subdomains		2.0	disabled	2021-05-10	*	*
recon/companies-domains/pen		1.1	installed	2019-10-15		
recon/companies-domains/viewdns_reverse_whois		1.1	installed	2021-08-24		
recon/companies-domains/whoxy_dns		1.1	installed	2020-06-17		*
recon/companies-hosts/censys_org		2.0	disabled	2021-05-11	*	*
recon/companies-hosts/censys_tls_subjects		2.0	disabled	2021-05-11	*	*
recon/companies-multi/github_miner		1.1	installed	2020-05-15		*
recon/domains-hosts/censys_domain		2.0	disabled	2021-05-10	*	*
recon/domains-hosts/certificate_transparency		1.2	installed	2019-09-16		
recon/domains-hosts/google_site_web		1.0	installed	2019-06-24		
recon/domains-hosts/hackertarget		1.1	installed	2020-05-17		
recon/domains-hosts/mx_spf_ip		1.0	installed	2019-06-24		
recon/domains-hosts/netcraft		1.1	installed	2020-02-05		
recon/domains-hosts/shodan_hostname		1.1	installed	2020-07-01	*	*
recon/domains-hosts/spyse_subdomains		1.1	installed	2021-08-24		*
recon/domains-hosts/ssl_san		1.0	installed	2019-06-24		
recon/domains-hosts/threatcrowd		1.0	installed	2019-06-24		
recon/domains-hosts/threatminer		1.0	installed	2019-06-24		
recon/domains-vulnerabilities/ghdb		1.1	installed	2019-06-26		
recon/domains-vulnerabilities/xssed		1.1	installed	2020-10-18		
recon/hosts-domains/migrate_hosts		1.1	installed	2020-05-17		
recon/hosts-hosts/bing_ip		1.0	installed	2019-06-24		*
recon/hosts-hosts/censys_hostname		2.0	disabled	2021-05-10	*	*
recon/hosts-hosts/censys_ip		2.0	disabled	2021-05-10	*	*
recon/hosts-hosts/censys_query		2.0	disabled	2021-05-10	*	*
recon/hosts-hosts/ipinfodb		1.2	installed	2021-08-24		*
recon/hosts-hosts/ipstack		1.0	installed	2019-06-24		*
recon/hosts-hosts/resolve		1.0	installed	2019-06-24		
recon/hosts-hosts/reverse_resolve		1.0	installed	2019-06-24		
recon/hosts-hosts/ssltools		1.0	installed	2019-06-24		

6. Installing a module: modules install (module name)

7. Modules search: It will give you the list of installed modules in the framework.
8. Command: modules search.

```
File Edit View Search Terminal Help
import/nmap

Recon
-----
recon/companies-contacts/bing_linkedin_cache
recon/companies-contacts/pen
recon/companies-domains/pen
recon/companies-domains/viewdns_reverse_whois
recon/companies-domains/whoxy_dns
recon/companies-multi/github_miner
recon/companies-multi/shodan_org
recon/companies-multi/whois_miner
recon/contacts-contacts/abc
recon/contacts-contacts/mailtester
recon/contacts-contacts/mangle
recon/contacts-contacts/unmangle
recon/contacts-credentials/hibp_breach
recon/contacts-credentials/hibp_paste
recon/contacts-domains/migrate_contacts
recon/contacts-profiles/fullcontact
recon/credentials-credentials/adobe
recon/credentials-credentials/bozocrack
recon/credentials-credentials/hashe.org
recon/domains-vulnerabilities/xssed
recon/hosts-domains/migrate_hosts
recon/hosts-hosts/bing_ip
recon/hosts-hosts/ipinfodb
recon/hosts-hosts/ipstack
recon/hosts-hosts/resolve
recon/hosts-hosts/reverse_resolve
recon/hosts-hosts/ssltools
recon/hosts-hosts/virustotal
recon/hosts-locations/migrate_hosts
recon/hosts-ports/binaryedge
recon/hosts-ports/shodan_ip
recon/locations-locations/geocode
recon/locations-locations/reverse_geocode
recon/locations-pushpins/flickr
recon/locations-pushpins/shodan
recon/locations-pushpins/twitter
recon/locations-pushpins/youtube
recon/netblocks-companies/whois_orgs
recon/netblocks-hosts/reverse_resolve
recon/netblocks-hosts/shodan_net
recon/netblocks-hosts/virustotal
recon/netblocks-ports/census_2012
```

Modules are grouped together under various categories:

- Discovery
- Exploitation
- Import
- Recon
- Reporting

Back command:

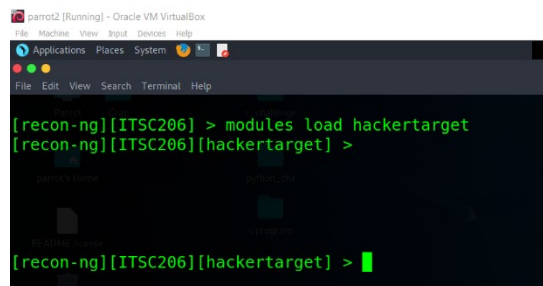

```
D = Has dependencies. See info for details.
K = Requires keys. See info for details.

[recon-ng][ITSC206] > marketplace info ssltools
+-----+
| path      | recon/hosts-hosts/ssltools |
| name      | SSLTools.com Host Name Lookups |
| author    | Tim Maletic (borrowing from the ssl_san module by Zach Graces) |
| version   | 1.0 |
| last_updated | 2019-06-24 |
| description | Uses the ssltools.com site to obtain host names from a site's SSL certificate metadata to update the 'hosts' table. Security issues with the certificate trust are pushed to the 'vulnerabilities' table. |
| required_keys | [] |
| dependencies | [] |
| files      | [] |
| status     | installed |
+-----+
```

RECON-NG EXAMPLE:

Gathering information about subdomains.

- Command to install the module: marketplace install hackertarget
- Load the module:



```
parrot2 [Running] - Oracle VM VirtualBox
File Machine View Host Devices Help

[recon-ng][ITSC206] > modules load hackertarget
[recon-ng][ITSC206][hackertarget] >

[recon-ng][ITSC206][hackertarget] >
```

- Module help:

```
[recon-ng][ITSC206][hackertarget] > help

Commands (type [help?] <topic>):
-----
back          Exits the current context
dashboard     Displays a summary of activity
db            Interfaces with the workspace's database
exit          Exits the framework
options       Manages the global context options
help          Displays this menu
info          Shows details about the loaded module
input         Shows inputs based on the source option
keys          Manages third party resource credentials
modules       Interfaces with installed modules
options       Manages the current context options
pdb           Starts a Python Debugger session (dev only)
reload        Reloads the loaded module
run           Runs the loaded module
script        Records and executes command scripts
shell         Executes shell commands
show          Shows various framework items
spool         Spools output to a file

[recon-ng][ITSC206][hackertarget] >
```

```
[recon-ng][ITSC206][hackertarget] > options list

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

[recon-ng][ITSC206][hackertarget] >
```

- Set source : options set SOURCE *yourtarget*

```
[recon-ng][ITSC206][hackertarget] > options list

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

[recon-ng][ITSC206][hackertarget] > options set SOURCE testphp.vulnweb.com
SOURCE => testphp.vulnweb.com
[recon-ng][ITSC206][hackertarget] > info

Name: HackerTarget Lookup
Author: Michael Henriksen (@michenriksen)
Version: 1.1

Description:
  Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the results.

Options:
Name      Current Value  Required  Description
-----
SOURCE     testphp.vulnweb.com yes       source of input (see 'info' for details)

Source Options:
default   SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
<string>  string representing a single input
<path>    path to a file containing a list of inputs
query <sql> database query returning one column of inputs
```

- Checking info and input:

```

SOURCE => testphp.vulnweb.com
[recon-ng][ITSC206][hackertarget] > info

Name: HackerTarget Lookup
Author: Michael Henriksen (@michenriksen)
Version: 1.1

Description:
  Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the results.

Options:
  Name      Current Value      Required  Description
  -----
  SOURCE    testphp.vulnweb.com      yes       source of input (see 'info' for details)

Source Options:
  default    SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>    string representing a single input
  <path>      path to a file containing a list of inputs
  query <sql> database query returning one column of inputs

[recon-ng][ITSC206][hackertarget] > input

+-----+
| Module Inputs |
+-----+
| testphp.vulnweb.com |
+-----+

[recon-ng][ITSC206][hackertarget] >

```

- Run:

```

[recon-ng][ITSC206][hackertarget] > run

TESTPHP.VULNWEB.COM
-----
[*] Country: None
[*] Host: testphp.vulnweb.com
[*] Ip Address: 44.228.249.3
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
Summary
-----
[*] 1 total (1 new) hosts found.

```

- Command: show hosts
- Command: show domains

```

[recon-ng][206][hackertarget] > show hosts

+-----+
| rowid | host           | ip_address | region | country | latitude | longitude | notes | module |
+-----+
| 1     |                |            |        |          |           |            |       |         |
| 2     |                |            |        |          |           |            |       |         |
| 3     | testphp.vulnweb.com | 44.228.249.3 |        |          |           |            |       | hackertarget |
+-----+

[*] 3 rows returned
[recon-ng][206][hackertarget] > show domains

+-----+
| rowid | domain | notes           | module |
+-----+
| 1     | testphp.com | For learning purpose. | user_defined |
+-----+

```

What if we want to create a report ?

REPORTING MODULE:

```

[recon-ng][206][hackertarget] > modules search reporting
[*] Searching installed modules for 'reporting'...

Reporting
-----
reporting/csv
reporting/html
reporting/json
reporting/list
reporting/proxifier
reporting/pushpin
reporting/xlsx
reporting/xml

[recon-ng][206][hackertarget] >

```

Lets use the module reporting/html.


```
[recon-ng][206][hackertarget] > modules load reporting/html
[recon-ng][206][html] > info

Name: HTML Report Generator
Author: Tim Tomes (@lanmaster53)
Version: 1.0

Description:
Creates an HTML report.

Options:
  Name      Current Value      Required  Description
  -----
  CREATOR    yes                        use creator name in the report footer
  CUSTOMER   yes                        use customer name in the report header
  FILENAME   /root/.recon-ng/workspaces/206/results.html yes      path and filename for report output
  SANITIZE   True                       mask sensitive data in the report

[recon-ng][206][html] >
```

Setting creator & customer:

```
[recon-ng][206][html] > options set CREATOR Class206
CREATOR => Class206
[recon-ng][206][html] > options set CUSTOMER testphp
CUSTOMER => testphp
[recon-ng][206][html] >
```

Creating a file:

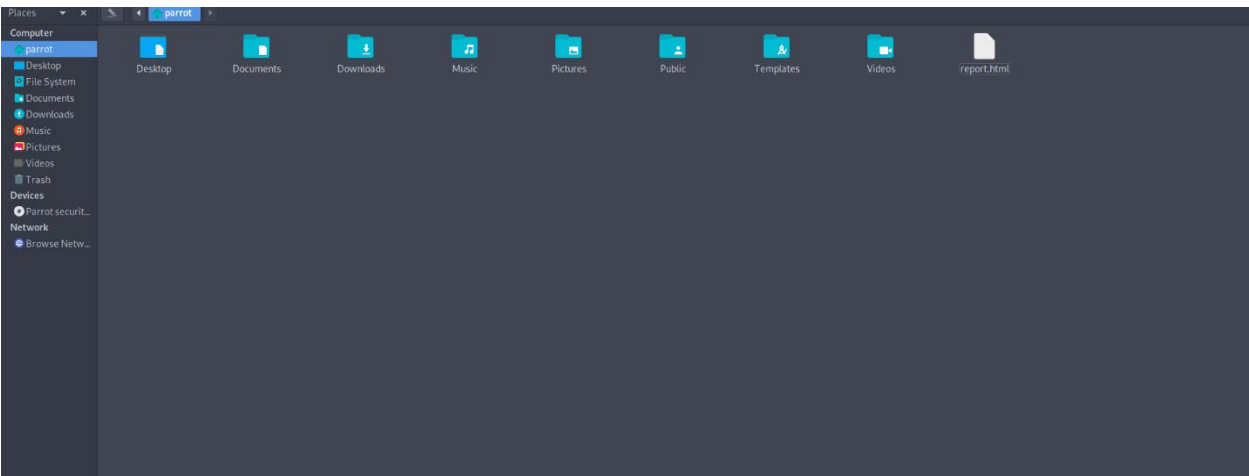
```
parrot@parrot:~$ touch report.html
parrot@parrot:~$ pwd
/home/parrot
parrot@parrot:~$
```

```
parrot [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places System

File Edit View Search Terminal Help
[recon-ng][206][html] > options set CREATOR Class206
CREATOR => Class206
[recon-ng][206][html] > options set CUSTOMER testphp
CUSTOMER => testphp
[recon-ng][206][html] > options set FILENAME /home/parrot/report.html
FILENAME => /home/parrot/report.html
[recon-ng][206][html] >
```

Lets run:

```
[recon-ng][206][html] > run
[*] Report generated at '/home/parrot/report.html'.
[recon-ng][206][html] >
```



testphp

Recon-ng Reconnaissance Report

Summary

table	count
domains	1
companies	0
networks	0
locations	0
vulnerabilities	0
ports	0
hosts	3
contacts	0
credentials	0
leaks	0
pushpins	0
profiles	1
repositories	0

Domains

Hosts

Profiles

Created by: Class206
Thu, Sep 21, 2023 23:18:59