



Department of
Bachelor of Computer Applications

Ethical Hacking Fundamentals
Lab File – CA 03b

Subject Code: 19BCA4C02L
Class: IInd Year IInd Semester

Prepared By:
Suman Garai
20BCAR0246

Aim :

To explore and learn Recon-ng (an open-source intelligence tool) for reconnaissance.

Requirements :

- Virtualisation Software
- Kali Linux 2021.4a
- Basics of Maltego
- Administrator privileges
- Internet Connection

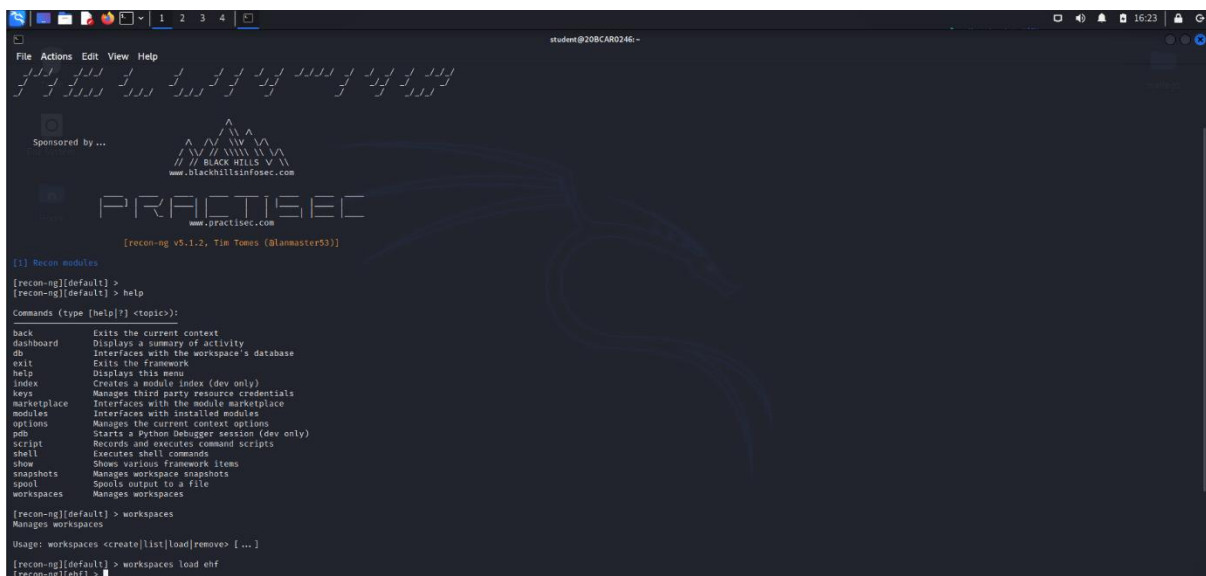
Objectives :

To Install & Run any module (with keys and dependencies) any obtain desired information using it. Also, generate report for the same.

Procedure :

Running Module with Keys

- 1> Open root terminal in kali linux, and run the command `recon-ng` to run recon-ng. Type `Help` for getting the list of working commands in recon-ng.
- 2> Type workspaces `load ehf` to begin working.



```
student@208CAR0246:~$ recon-ng
[recon-ng v5.1.2, Tim Tomus (@lanmaster53)]

[!] Recon modules
[recon-ng][default] >
[recon-ng][default] > 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
help          Displays this menu
index         Creates a module index (dev only)
keys          Manages third party resource credentials
marketplace   Interfaces with the module marketplace
modules       Interfaces with installed modules
options       Manages the current context options
pdb           Starts a Python Debugger session (dev only)
script        Records and executes command scripts
shell         Executes shell commands
show          Shows various framework items
snapshots     Manages workspace snapshots
spool         Spools output to a file
workspaces    Manages workspaces

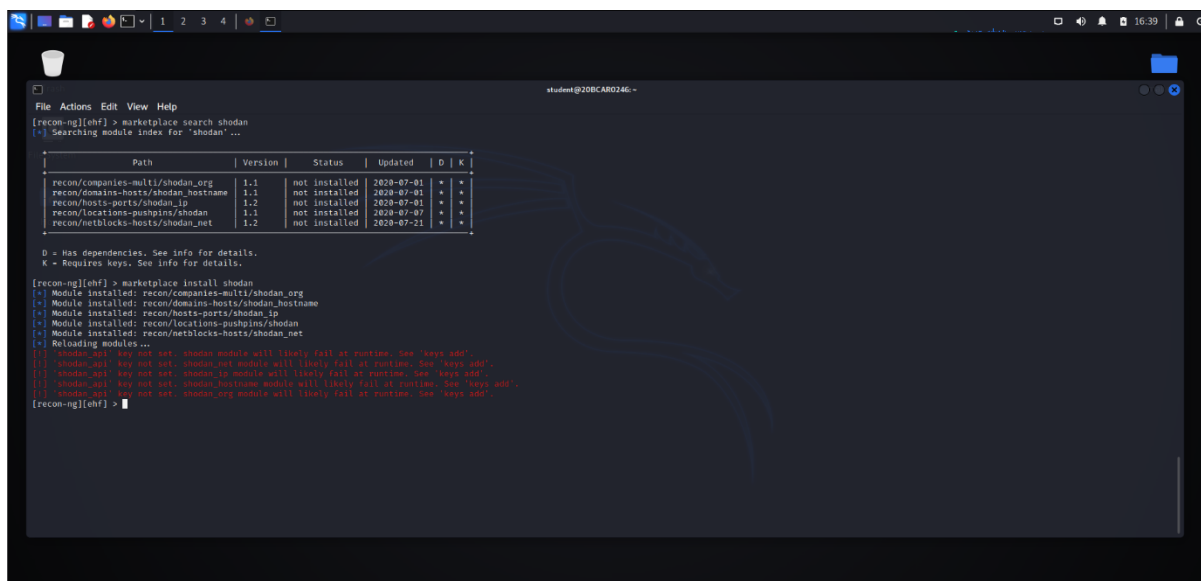
[recon-ng][default] > workspaces
Manages workspaces

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

[recon-ng][default] > workspaces load ehf
[recon-ng][ehf] >
```

As we can see, we are inside the workspace. For this lab, we are going to be using shodan modules.

Now, we will continue with installing required modules using workspaces install shodan.



```
[recon-ng][ehf] > marketplace search shodan
[+] Searching module index for 'shodan' ...

  Path | Version | Status | Updated | D | K |
-----|-----|-----|-----|---|---|
recon/companies-multi/shodan_org | 1.1 | not installed | 2020-07-01 | * | * |
recon/domains-hosts/shodan_hostname | 1.1 | not installed | 2020-07-01 | * | * |
recon/hosts-ports/shodan_ip | 1.2 | not installed | 2020-07-01 | * | * |
recon/locations-pushpins/shodan | 1.1 | not installed | 2020-07-07 | * | * |
recon/netblocks-hosts/shodan_net | 1.2 | not installed | 2020-07-21 | * | * |

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

[recon-ng][ehf] > marketplace install shodan
[+] Module installed: recon/companies-multi/shodan_org
[+] Module installed: recon/domains-hosts/shodan_hostname
[+] Module installed: recon/hosts-ports/shodan_ip
[+] Module installed: recon/locations-pushpins/shodan
[+] Module installed: recon/netblocks-hosts/shodan_net
[+] Reloading modules...
[+] shodan_net: key not set. shodan module will likely fail at runtime. See 'keys add'.
[+] shodan_ip: key not set. shodan_ip module will likely fail at runtime. See 'keys add'.
[+] shodan_hostname: key not set. shodan_hostname module will likely fail at runtime. See 'keys add'.
[+] shodan_net: key not set. shodan_net module will likely fail at runtime. See 'keys add'.
[+] shodan_org: key not set. shodan_org module will likely fail at runtime. See 'keys add'.
[recon-ng][ehf] >
```

To work with shodan, as mentioned in the screenshot, we will need keys and dependencies.

Therefore, we are now going to add keys to work with shodan. For that we are going to create a shodan account, after which we will use the api's of that account, as follows.

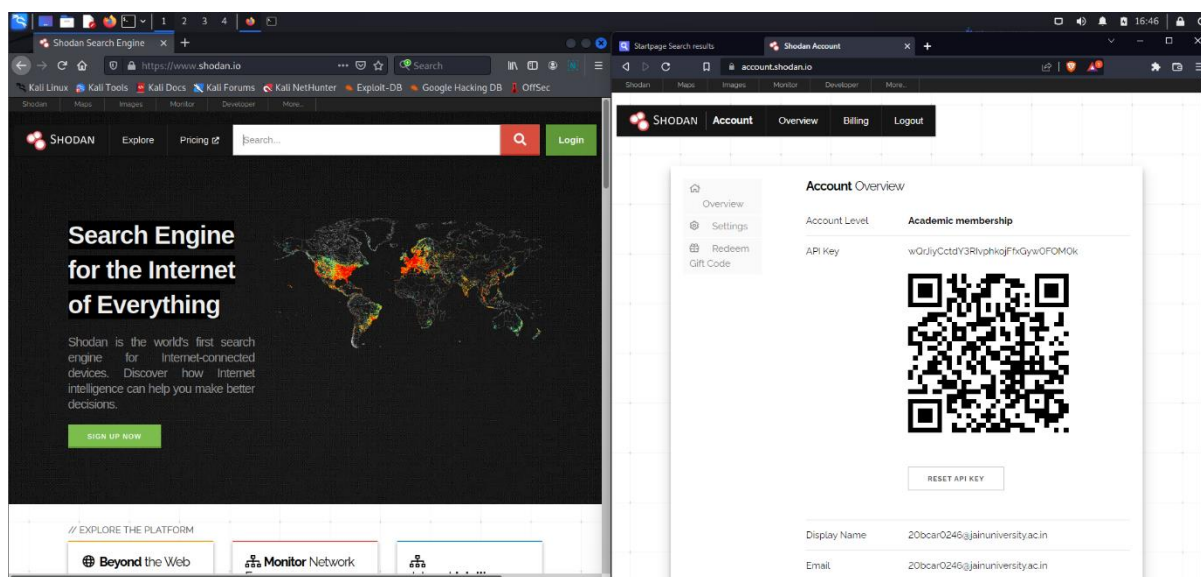


Figure: Obtained API keys

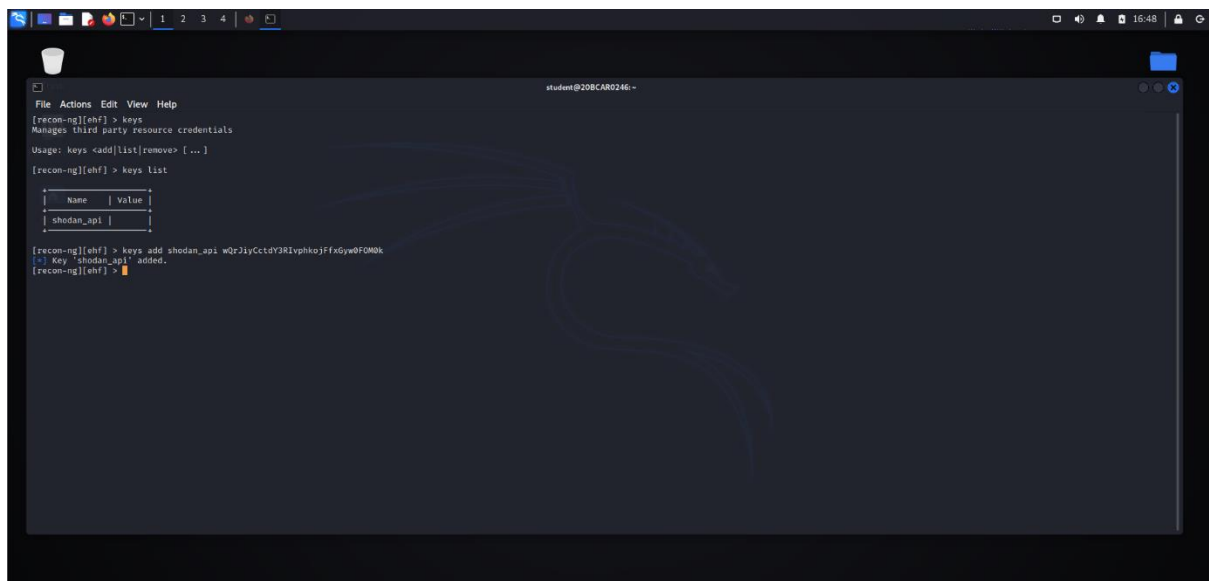
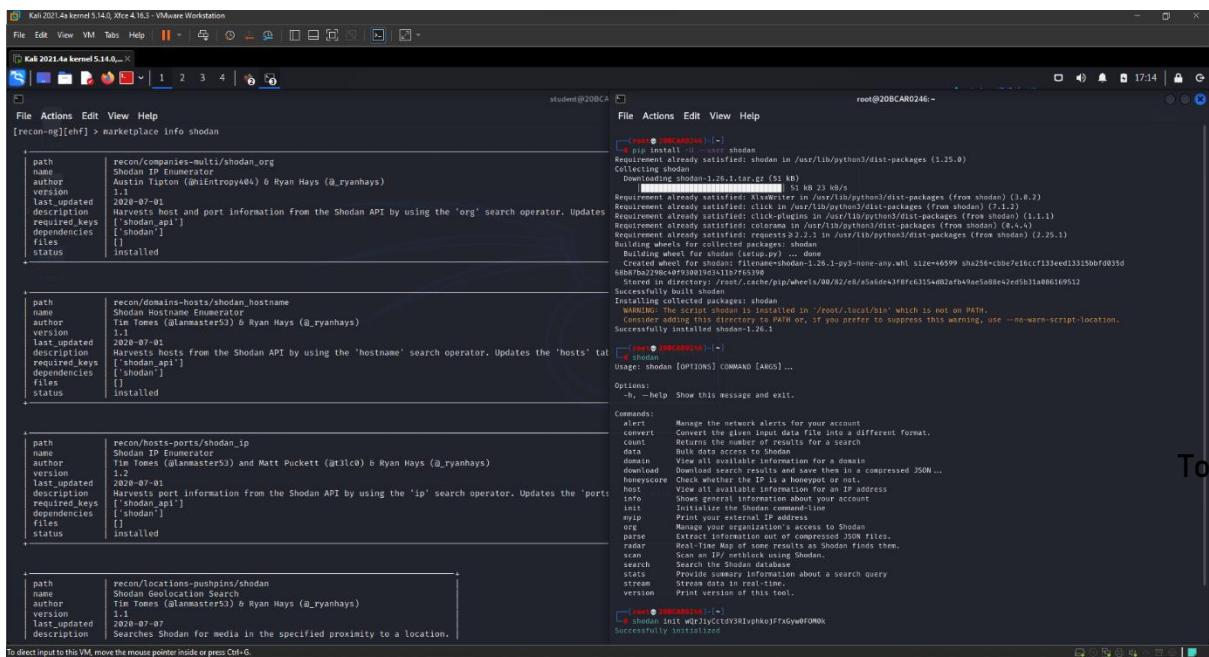


Figure: Setting API Keys

We, would also need to set dependencies before working on the module.

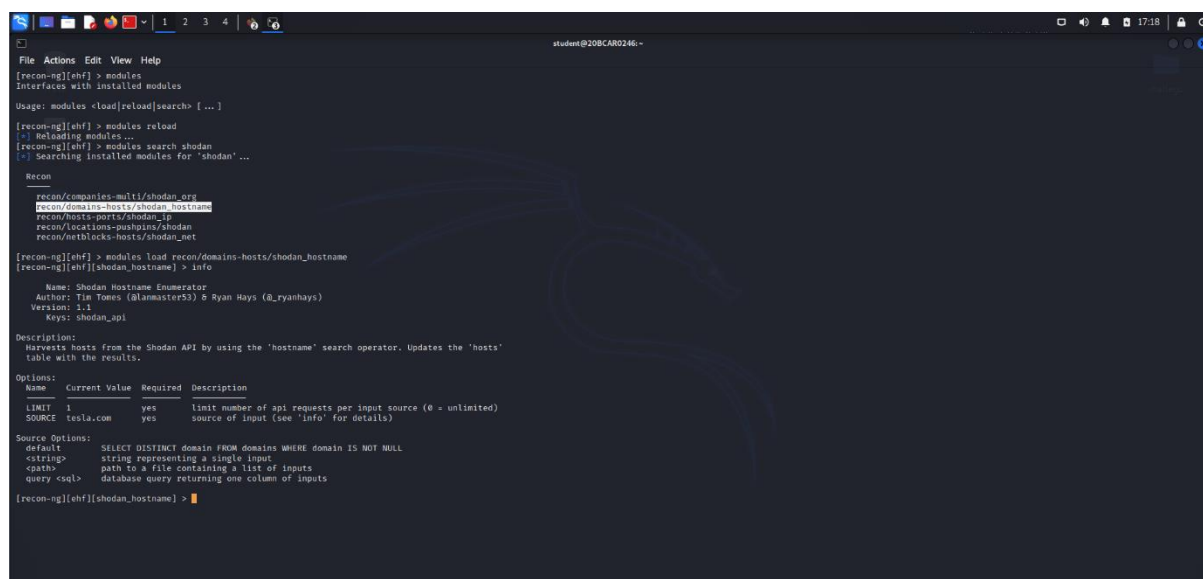
For that we are going to follow the steps mentioned here:

<https://help.shodan.io/command-line-interface/o-installation>



After being done with dependencies we will need to refresh the installed modules for once. Now, we being done with this, can continue with module configuration and running the same.

Well, there are a number of shodan modules present in the recon-ng. We need to select the desired, `shodan_hostname` in this case. Using the `options` command, we have changed the target server.



```
File Actions Edit View Help
[recon-ng][ehf] > modules
Interfaces with installed modules
Usage: modules <load|reload|search> [...]

[recon-ng][ehf] > modules reload
[?] Reloading modules ...
[recon-ng][ehf] > modules search shodan
[?] Searching installed modules for 'shodan' ...

Recon
-----
recon/companies-multi/shodan_org
recon/companies-multi/shodan_hostname
recon/hosts-ports/shodan_ip
recon/locations-pushpins/shodan
recon/webblocks-hosts/shodan_net

[recon-ng][ehf] > modules load recon/domains-hosts/shodan_hostname
[recon-ng][ehf][shodan_hostname] > info

Name: Shodan Hostname Enumerator
Author: Tim Tones (@lanmaster53) & Ryan Hays (@ryanhays)
Version: 1.1
Keys: shodan_api

Description:
Harvests hosts from the Shodan API by using the 'hostname' search operator. Updates the 'hosts'
table with the results.

Options:
Name      Current Value  Required  Description
LIMIT     1               yes       limit number of api requests per input source (0 = unlimited)
SOURCE     tesla.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>   database query returning one column of inputs

[recon-ng][ehf][shodan_hostname] >
```

Now, we run the module. Following are the results obtained.



```
File Actions Edit View Help
[recon-ng][ehf][shodan_hostname] > run

TESLA.COM

[?] Banner: None
[?] Host: events.tesla.com
[?] Ip Address: 13.111.47.195
[?] Notes: None
[?] Port: 443
[?] Protocol: tcp
[?]
[?] Country: None
[?] Host: events.tesla.com
[?] Ip Address: 13.111.47.195
[?] Latitude: None
[?] Longitude: None
[?] Notes: None
[?] Region: None
[?]
[?] Banner: None
[?] Host: events.tesla.com
[?] Ip Address: 13.111.47.195
[?] Notes: None
[?] Port: 80
[?] Protocol: tcp
[?]
[?] Country: None
[?] Host: events.tesla.com
[?] Ip Address: 13.111.47.195
[?] Latitude: None
[?] Longitude: None
[?] Notes: None
[?] Region: None
[?]
[?] Banner: None
[?] Host: pik-tesla.com.ua
[?] Ip Address: 91.239.232.36
[?] Notes: None
[?] Port: 993
[?] Protocol: tcp
[?]
[?] Country: None
[?] Host: pik-tesla.com.ua
[?] Ip Address: 91.239.232.36
[?] Latitude: None
[?] Longitude: None
[?] Notes: None
[?] Region: None
[?]
[?] Banner: None
```

NOTE: We can run multiple modules together as mentioned here:
<https://github.com/sharathunni/auto-recon-ng>

Using the show command we can from tables detailing the results we want to view.

```
student@20BCAR0246-
File Actions Edit View Help
[*] 20 total (20 new) parts found.
[*] 20 total (7 new) hosts found.
[recon-ng][ehf][shodan_hostname] > show
Shows various framework items
Usage: show <companies>|<contacts>|<credentials>|<domains>|<hosts>|<leaks>|<locations>|<netblocks>|<ports>|<profiles>|<pushpins>|<repositories>|<vulnerabilities>
[recon-ng][ehf][shodan_hostname] > show hosts ports

rowid | host | ip_address | region | country | latitude | longitude | notes | module
-----|-----|-----|-----|-----|-----|-----|-----|-----
1 | events.tesla.com | 13.111.47.195 | | | | | | shodan_hostname
2 | pik-tesla.com.ua | 91.239.232.36 | | | | | | shodan_hostname
3 | marketing.tesla.com | 13.111.47.196 | | | | | | shodan_hostname
4 | click.emails.tesla.com | 13.111.48.178 | | | | | | shodan_hostname
5 | view.emails.tesla.com | 13.111.49.179 | | | | | | shodan_hostname
6 | florian.sv.s-tesla.com | 116.203.43.190 | | | | | | shodan_hostname
7 | nam.sv.s-tesla.com | 94.130.79.104 | | | | | | shodan_hostname

[*] 7 rows returned
[recon-ng][ehf][shodan_hostname] >
[recon-ng][ehf][shodan_hostname] > show ports

rowid | ip_address | host | port | protocol | banner | notes | module
-----|-----|-----|-----|-----|-----|-----|-----
1 | 13.111.47.195 | events.tesla.com | 443 | tcp | | | shodan_hostname
2 | 13.111.47.195 | events.tesla.com | 80 | tcp | | | shodan_hostname
3 | 91.239.232.36 | pik-tesla.com.ua | 993 | tcp | | | shodan_hostname
4 | 13.111.47.196 | marketing.tesla.com | 80 | tcp | | | shodan_hostname
5 | 13.111.48.178 | click.emails.tesla.com | 443 | tcp | | | shodan_hostname
6 | 13.111.48.178 | click.emails.tesla.com | 80 | tcp | | | shodan_hostname
7 | 91.239.232.36 | pik-tesla.com.ua | 443 | tcp | | | shodan_hostname
8 | 91.239.232.36 | pik-tesla.com.ua | 587 | tcp | | | shodan_hostname
9 | 91.239.232.36 | pik-tesla.com.ua | 465 | tcp | | | shodan_hostname
10 | 91.239.232.36 | pik-tesla.com.ua | 2887 | tcp | | | shodan_hostname
11 | 91.239.232.36 | pik-tesla.com.ua | 2886 | tcp | | | shodan_hostname
12 | 13.111.49.179 | view.emails.tesla.com | 995 | tcp | | | shodan_hostname
13 | 91.239.232.36 | pik-tesla.com.ua | 995 | tcp | | | shodan_hostname
14 | 116.203.43.190 | florian.sv.s-tesla.com | 3000 | tcp | | | shodan_hostname
15 | 13.111.49.179 | view.emails.tesla.com | 443 | tcp | | | shodan_hostname
16 | 91.239.232.36 | pik-tesla.com.ua | 2883 | tcp | | | shodan_hostname
17 | 13.111.47.196 | marketing.tesla.com | 443 | tcp | | | shodan_hostname
18 | 91.239.232.36 | pik-tesla.com.ua | 110 | tcp | | | shodan_hostname
19 | 91.239.232.36 | pik-tesla.com.ua | 80 | tcp | | | shodan_hostname
20 | 94.130.79.104 | nam.sv.s-tesla.com | 3000 | tcp | | | shodan_hostname

[*] 20 rows returned
```

Generating Reports

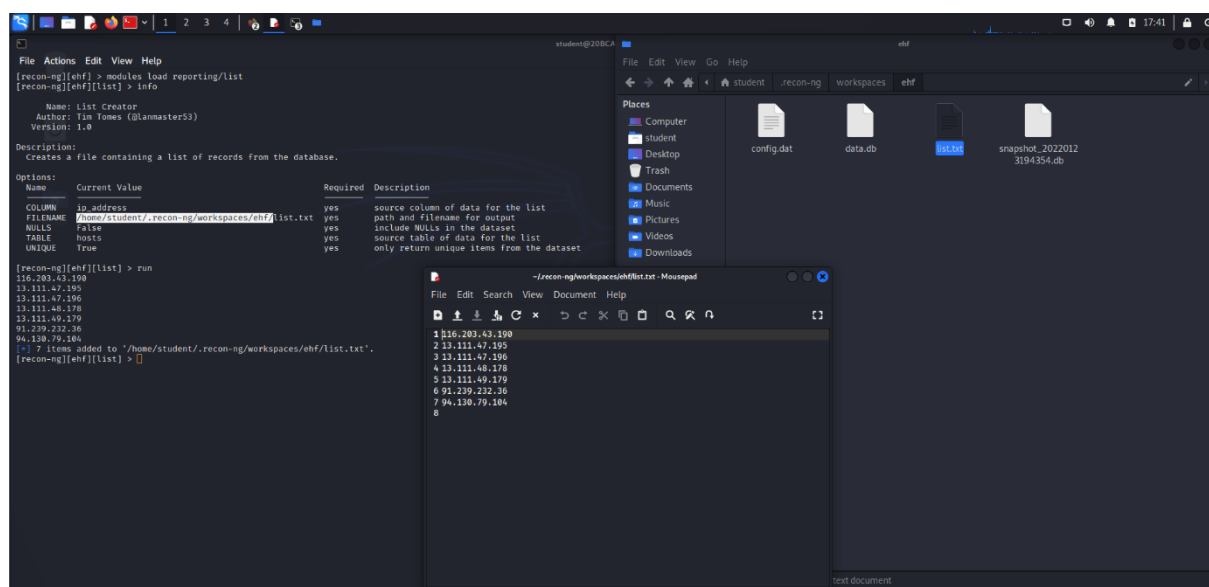
To begin with, we will need to install the respective modules for reporting from the marketplace.

```
student@20BCAR0246-
File Actions Edit View Help
[recon-ng][ehf] > marketplace search report
[*] Searching module index for 'report'...

Path | Version | Status | Updated | D | K
-----|-----|-----|-----|---|---
recon/hosts-hosts/virustotal | 1.0 | not installed | 2019-06-24 | * |
recon/netblocks-hosts/virustotal | 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/slix | 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][ehf] > marketplace install reporting
[*] Module installed: reporting/csv
[*] Module installed: reporting/html
[*] Module installed: reporting/json
[*] Module installed: reporting/list
[*] Module installed: reporting/proxifier
[*] Module installed: reporting/pushpin
[*] Module installed: reporting/slix
[*] Module installed: reporting/xml
[*] Reloading modules...
[*] not set, pushpin module will likely fail at runtime. See 'keys' and '
[recon-ng][ehf] >
```

Using `info` we can see the path the report is going to be saved. Now, after running the module if we go to the location, we can see the file generated, in this case a `.txt` file, noting the ip's, since using `reporting/list` module.



Conclusion :

Recon-ng is a powerful tool that can be further explored by looking through the list of modules. The help within the console is very clear and with a bit of playing around it won't take long to become an expert.

Once you start to become more familiar with the layout of the tool you will discover options such as workspaces that allow you to segment based on organization or network. The rise of bug bounties allows you to play with new tools and explore organizations internet-facing footprint. Have fun and don't break the rules.