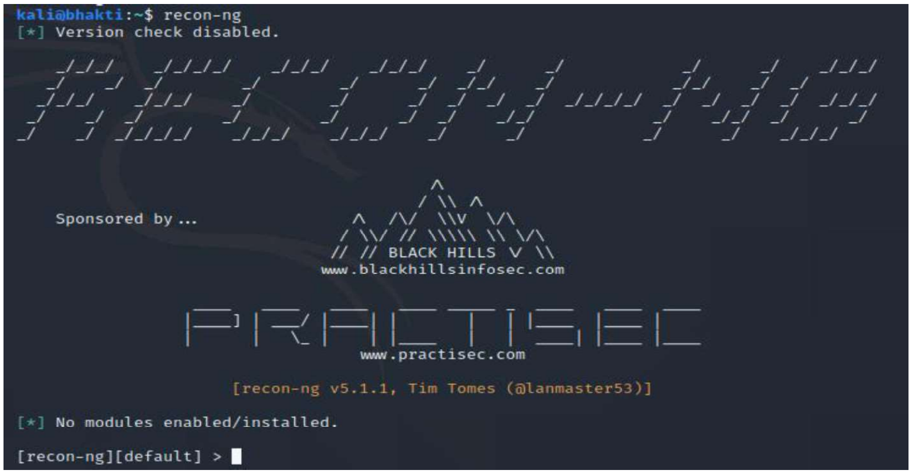
Practical

A. **Recon-ng** in Kali Linux.

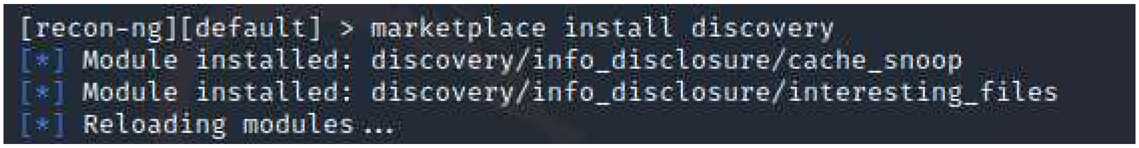
- **Recon-ng** is a full-featured Web Reconnaissance framework written in Python. Complete with independent modules, database interaction, built in convenience functions, interactive help, and command completion, Recon-ng provides a powerful environment in which open-source web-based reconnaissance can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

1. Open Kali Linux Virtual Machine. And Open terminal.
2. Type **Recon-ng** to enter the console.



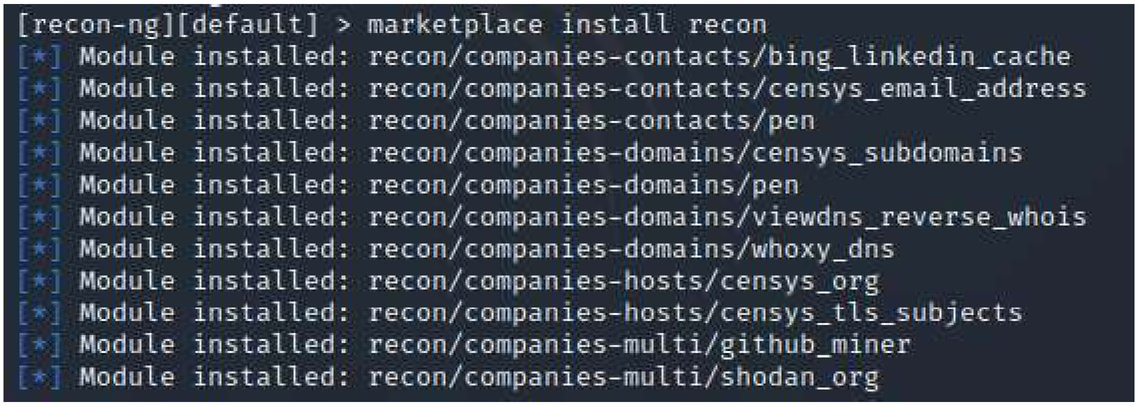
```
kali@bhakti:~$ recon-ng
[*] Version check disabled.

    Sponsored by ...
                                  BLACK HILLS
                          www.blackhillsinfosec.com

                             www.practisec.com

                [recon-ng v5.1.1, Tim Tomes (@lanmaster53)]

[*] No modules enabled/installed.

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

3. Initially there are no modules installed. To install the modules, we need to use the following commands.
    a. Discovery module



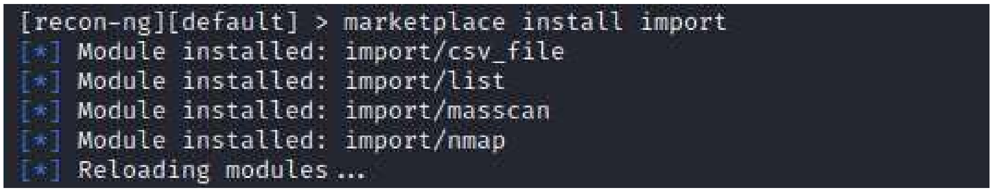
```
[recon-ng][default] > marketplace install discovery
[*] Module installed: discovery/info_disclosure/cache_snoop
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Reloading modules ...
```

    b. Recon module



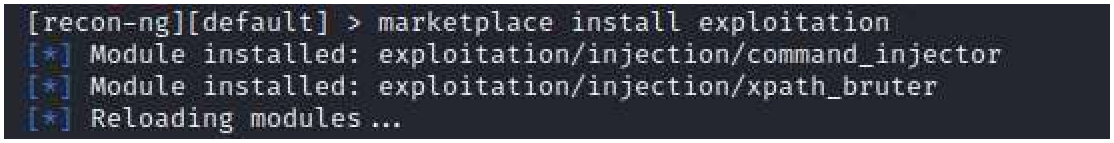
```
[recon-ng][default] > marketplace install recon
[*] Module installed: recon/companies-contacts/bing_linkedin_cache
[*] Module installed: recon/companies-contacts/censys_email_address
[*] Module installed: recon/companies-contacts/pen
[*] Module installed: recon/companies-domains/censys_subdomains
[*] 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
```

c. Importing module



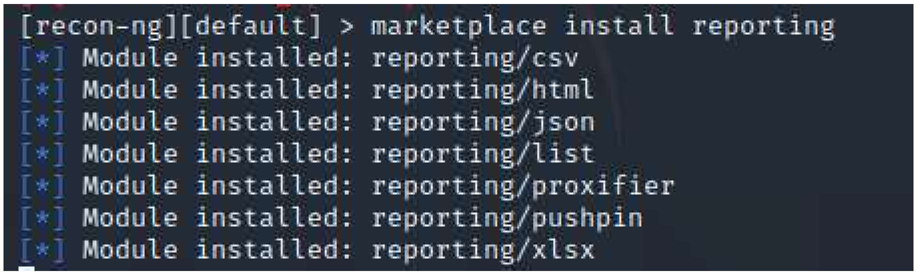
```
[recon-ng][default] > marketplace install import
[*] Module installed: import/csv_file
[*] Module installed: import/list
[*] Module installed: import/masscan
[*] Module installed: import/nmap
[*] Reloading modules ...
```

d. Exploitation module



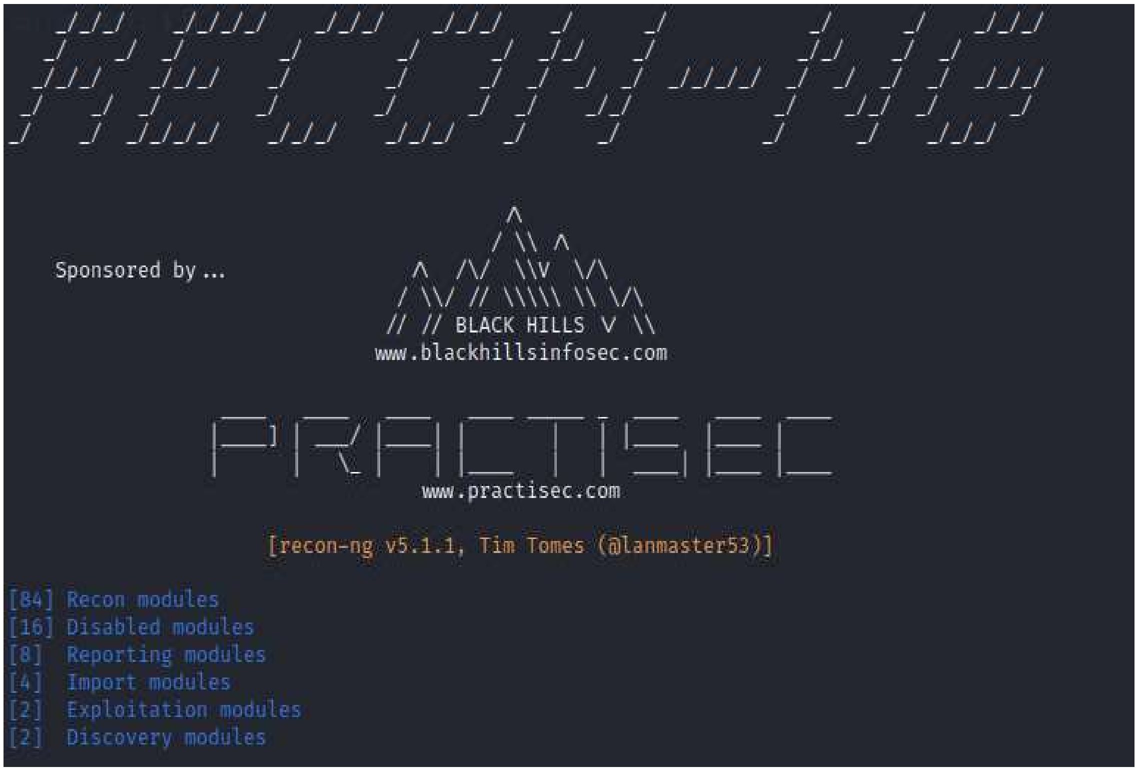
```
[recon-ng][default] > marketplace install exploitation
[*] Module installed: exploitation/injection/command_injector
[*] Module installed: exploitation/injection/xpath_bruter
[*] Reloading modules ...
```

e. Reporting module



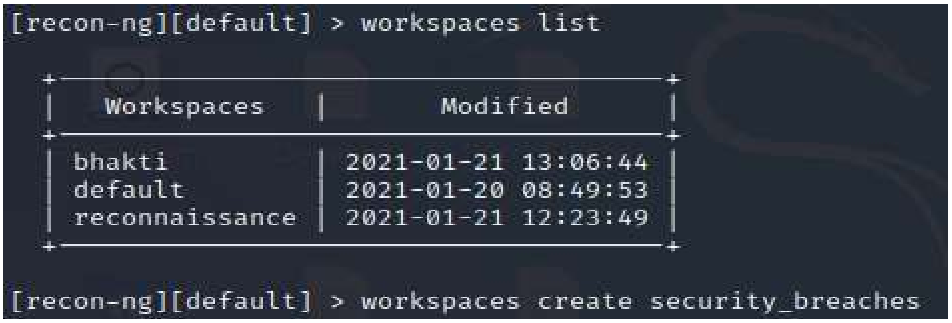
```
[recon-ng][default] > marketplace install reporting
[*] Module installed: reporting/csv
[*] Module installed: reporting/html
[*] Module installed: reporting/json
[*] Module installed: reporting/list
[*] Module installed: reporting/proxifier
[*] Module installed: reporting/pushpin
[*] Module installed: reporting/xlsx
```

Now the required modules are installed.

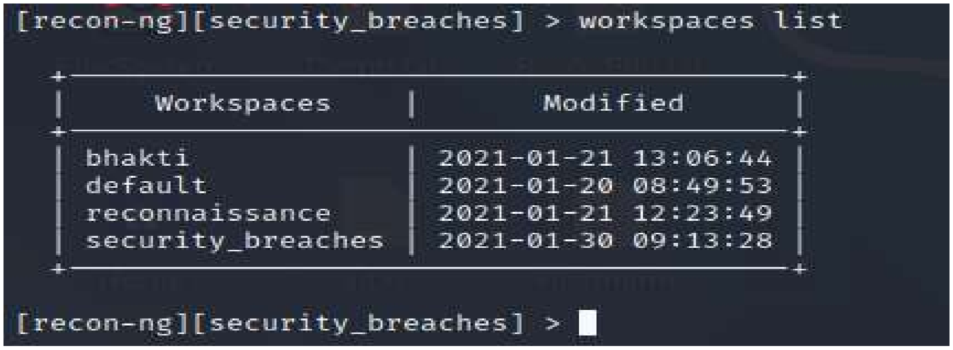


```
                                        ^
                                       / \\ ^
    Sponsored by ...              ^  /\/  \\v  \/\
                                 / \\/ // \\\\\ \\ \/\
                                // // BLACK HILLS \/ \\
                               www.blackhillsinfosec.com

                                   www.practisec.com

                        [recon-ng v5.1.1, Tim Tomes (@lanmaster53)]

[84] Recon modules
[16] Disabled modules
[8]  Reporting modules
[4]  Import modules
[2]  Exploitation modules
[2]  Discovery modules
```

4. To create a **new workspace**.

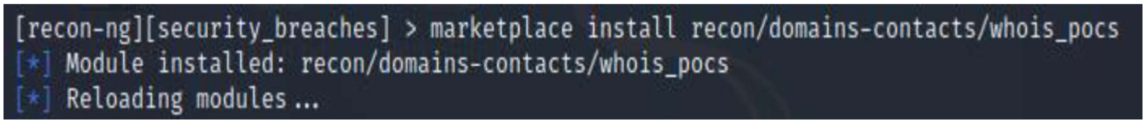


```
[recon-ng][default] > workspaces list

  +-------------------------------------------+
  |   Workspaces    |        Modified         |
  +-------------------------------------------+
  | bhakti          | 2021-01-21 13:06:44     |
  | default         | 2021-01-20 08:49:53     |
  | reconnaissance  | 2021-01-21 12:23:49     |
  +-------------------------------------------+

[recon-ng][default] > workspaces create security_breaches
```

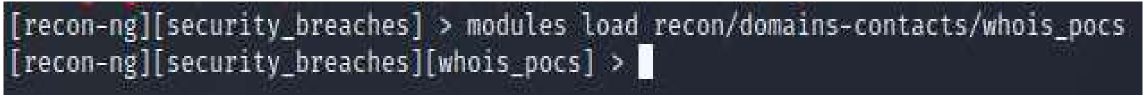


```
[recon-ng][security_breaches] > workspaces list

  +----------------------------------------------+
  |      Workspaces      |       Modified        |
  +----------------------------------------------+
  | bhakti               | 2021-01-21 13:06:44   |
  | default              | 2021-01-20 08:49:53   |
  | reconnaissance       | 2021-01-21 12:23:49   |
  | security_breaches    | 2021-01-30 09:13:28   |
  +----------------------------------------------+

[recon-ng][security_breaches] > 
```

5. Install the **module recon/domains-contacts/whois_pocs** and load the installed module.

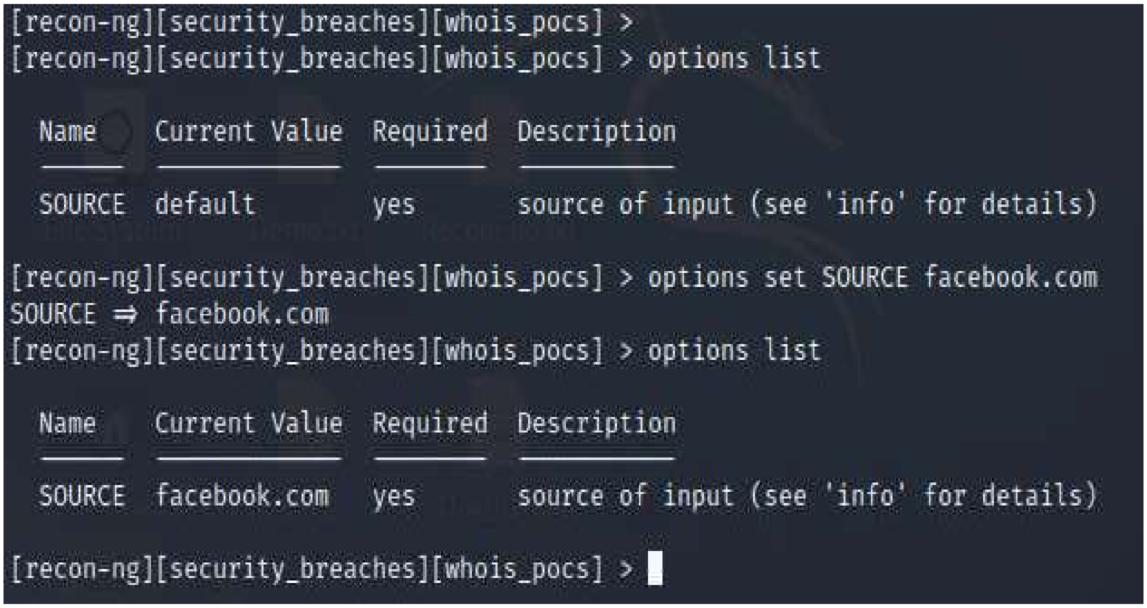


```
[recon-ng][security_breaches] > marketplace install recon/domains-contacts/whois_pocs
[*] Module installed: recon/domains-contacts/whois_pocs
[*] Reloading modules ...
```

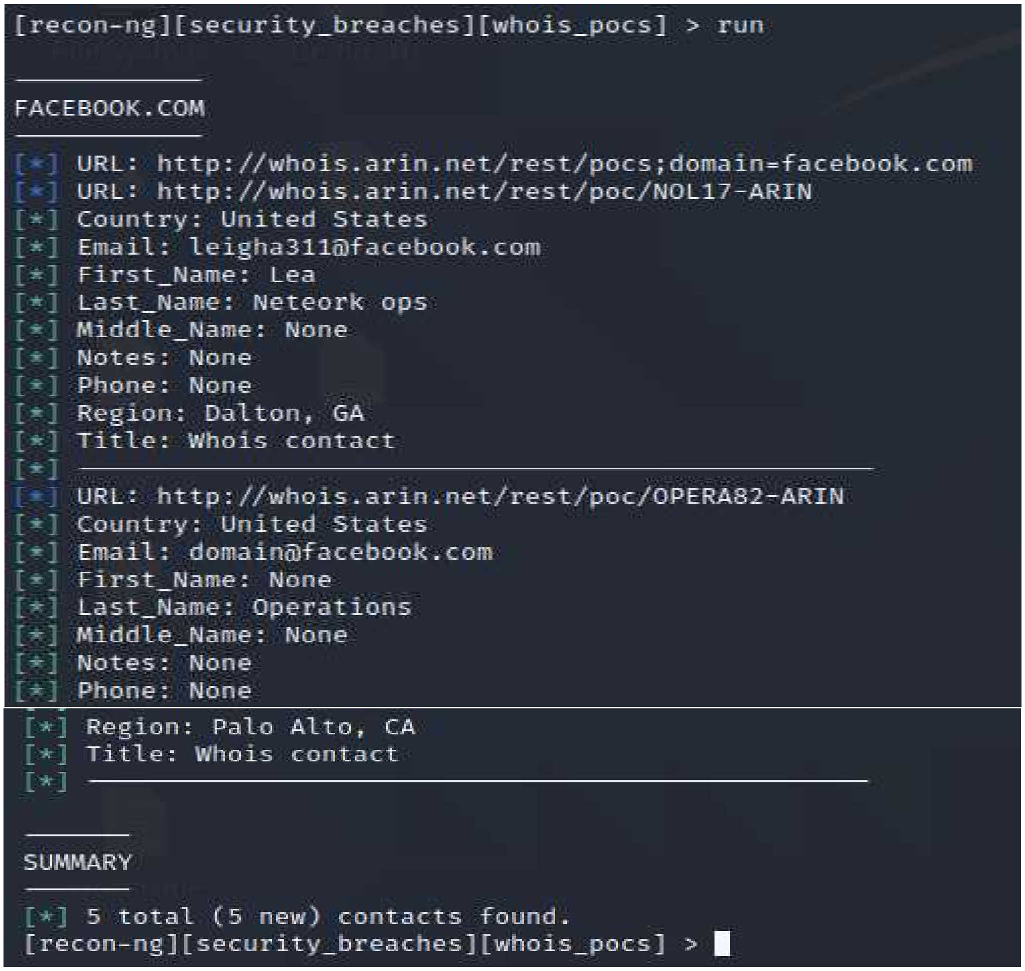


```
[recon-ng][security_breaches] > modules load recon/domains-contacts/whois_pocs
[recon-ng][security_breaches][whois_pocs] > 
```

6. Set the option and run the module.

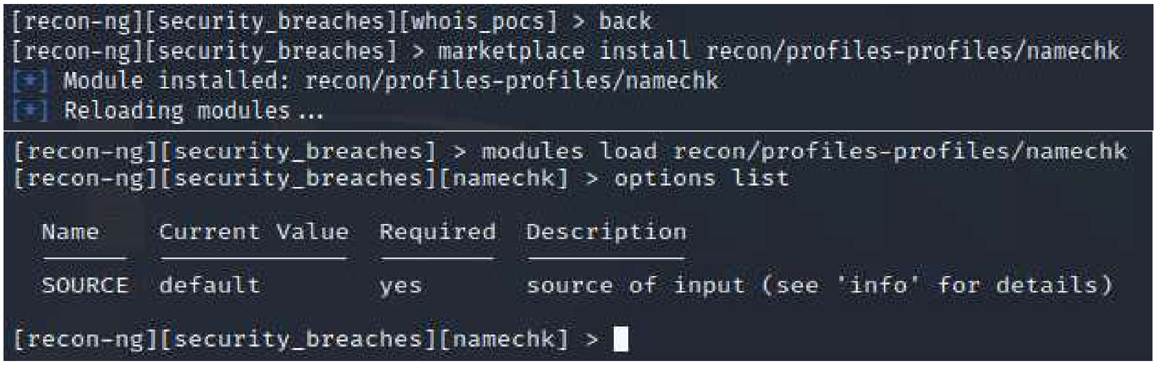


```
[recon-ng][security_breaches][whois_pocs] >
[recon-ng][security_breaches][whois_pocs] > options list

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

[recon-ng][security_breaches][whois_pocs] > options set SOURCE facebook.com
SOURCE ⇒ facebook.com
[recon-ng][security_breaches][whois_pocs] > options list

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

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



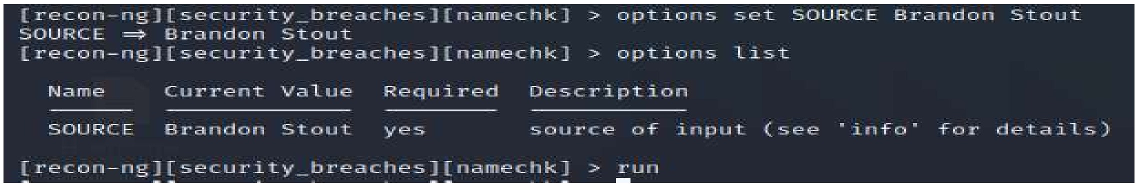
```
[recon-ng][security_breaches][whois_pocs] > run

────────────
FACEBOOK.COM
────────────
[*] URL: http://whois.arin.net/rest/pocs;domain=facebook.com
[*] URL: http://whois.arin.net/rest/poc/NOL17-ARIN
[*] Country: United States
[*] Email: leigha311@facebook.com
[*] First_Name: Lea
[*] Last_Name: Neteork ops
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Dalton, GA
[*] Title: Whois contact
[*] ──────────────────────────────────────────────────
[*] URL: http://whois.arin.net/rest/poc/OPERA82-ARIN
[*] Country: United States
[*] Email: domain@facebook.com
[*] First_Name: None
[*] Last_Name: Operations
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Palo Alto, CA
[*] Title: Whois contact
[*] ──────────────────────────────────────────────────

───────
SUMMARY
───────
[*] 5 total (5 new) contacts found.
[recon-ng][security_breaches][whois_pocs] >
```

7. Type **back** and enter the workspace. We will install another module **recon/profiles-profiles/namechk** and load the module to validate the user **Brandon Stout.**



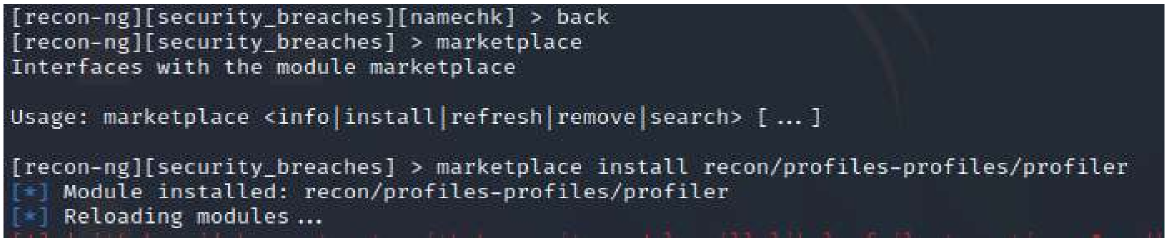
```
[recon-ng][security_breaches][whois_pocs] > back
[recon-ng][security_breaches] > marketplace install recon/profiles-profiles/namechk
[*] Module installed: recon/profiles-profiles/namechk
[*] Reloading modules ...
[recon-ng][security_breaches] > modules load recon/profiles-profiles/namechk
[recon-ng][security_breaches][namechk] > options list

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

[recon-ng][security_breaches][namechk] >
```

8. Set the option and run the module.

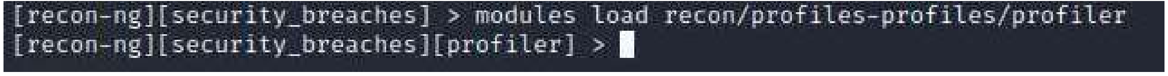


```
[recon-ng][security_breaches][namechk] > options set SOURCE Brandon Stout
SOURCE ⇒ Brandon Stout
[recon-ng][security_breaches][namechk] > options list

  Name    Current Value  Required  Description
  ──────  ─────────────  ────────  ───────────
  SOURCE  Brandon Stout  yes       source of input (see 'info' for details)

[recon-ng][security_breaches][namechk] > run
```

9. Type **back** and enter the workspace. We will install another module **recon/profiles-profiles/profiler** to check the existence of user **Brandon Stout**.

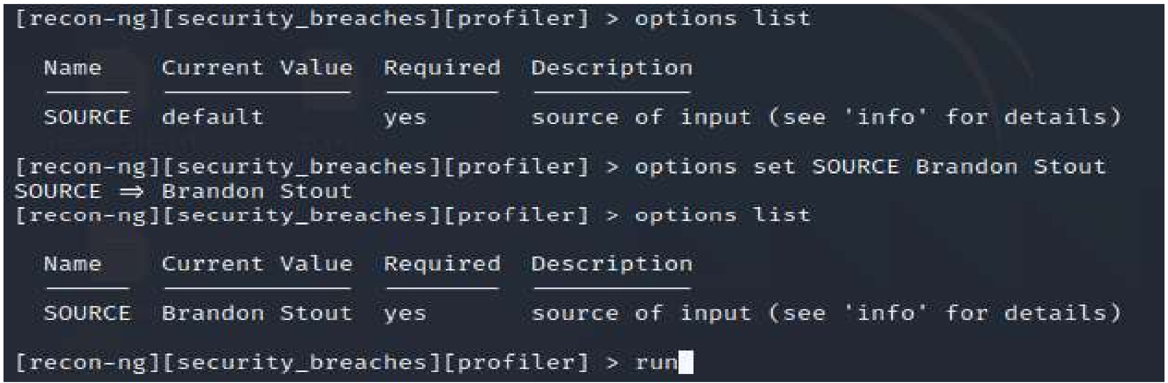


```
[recon-ng][security_breaches][namechk] > back
[recon-ng][security_breaches] > marketplace
Interfaces with the module marketplace

Usage: marketplace <info|install|refresh|remove|search> [ ... ]

[recon-ng][security_breaches] > marketplace install recon/profiles-profiles/profiler
[*] Module installed: recon/profiles-profiles/profiler
[*] Reloading modules ...
```

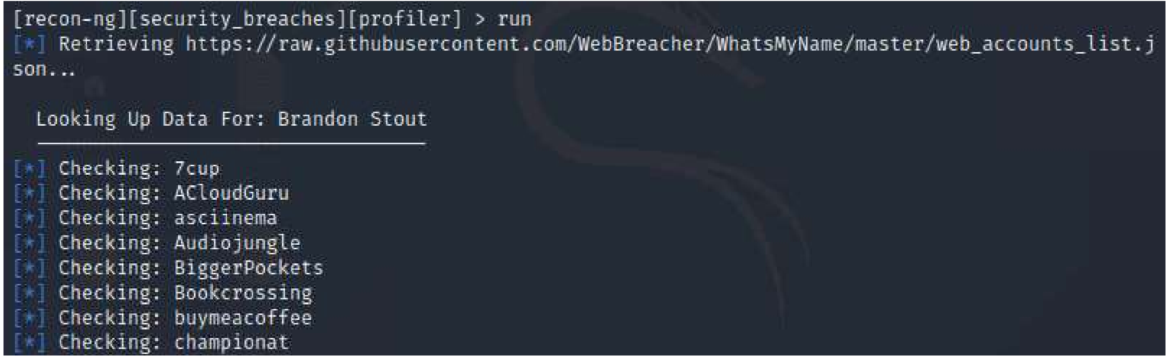


```
[recon-ng][security_breaches] > modules load recon/profiles-profiles/profiler
[recon-ng][security_breaches][profiler] >
```

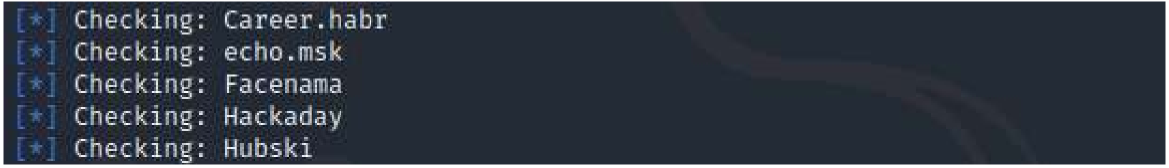
10. Set the option and **run** the module.



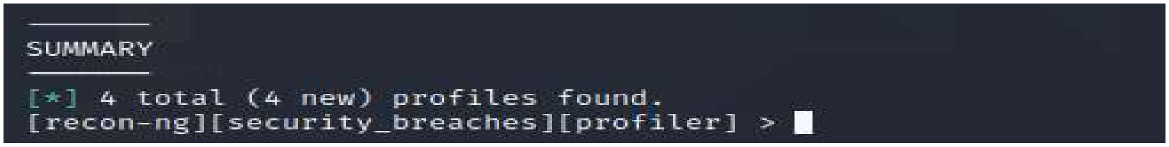
```
[recon-ng][security_breaches][profiler] > options list

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

[recon-ng][security_breaches][profiler] > options set SOURCE Brandon Stout
SOURCE => Brandon Stout
[recon-ng][security_breaches][profiler] > options list

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

[recon-ng][security_breaches][profiler] > run
```



```
[recon-ng][security_breaches][profiler] > run
[*] Retrieving https://raw.githubusercontent.com/WebBreacher/WhatsMyName/master/web_accounts_list.j
son...

  Looking Up Data For: Brandon Stout
  ----------------------------------

[*] Checking: 7cup
[*] Checking: ACloudGuru
[*] Checking: asciinema
[*] Checking: Audiojungle
[*] Checking: BiggerPockets
[*] Checking: Bookcrossing
[*] Checking: buymeacoffee
[*] Checking: championat
```

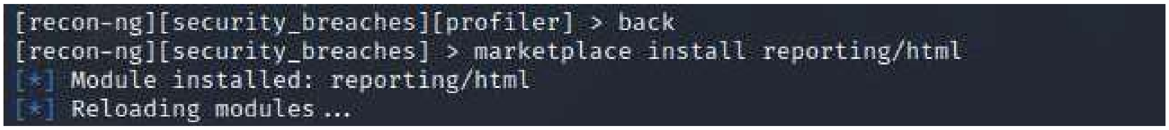


```
[*] Checking: Career.habr
[*] Checking: echo.msk
[*] Checking: Facenama
[*] Checking: Hackaday
[*] Checking: Hubski
```

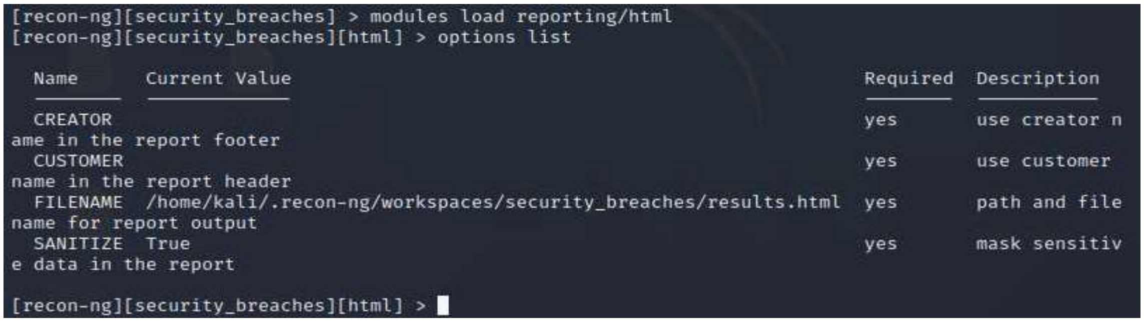


```
 -------
 SUMMARY
 -------
 [*] 4 total (4 new) profiles found.
 [recon-ng][security_breaches][profiler] >
```

11. Generate a **Report**. We will install another **module reporting/html** and load the module to generate a report in html file.

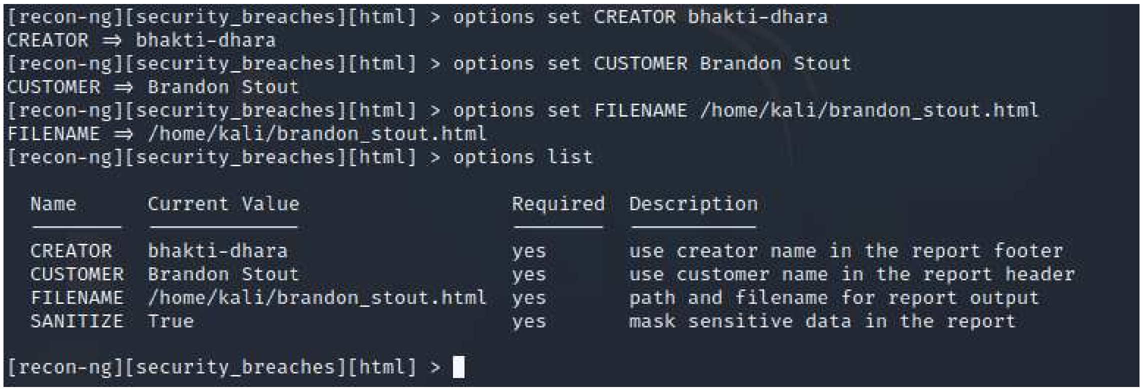


```
[recon-ng][security_breaches][profiler] > back
[recon-ng][security_breaches] > marketplace install reporting/html
[*] Module installed: reporting/html
[*] Reloading modules ...
```



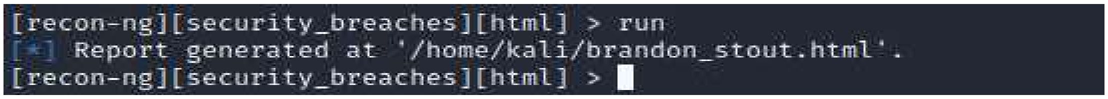
```
[recon-ng][security_breaches] > modules load reporting/html
[recon-ng][security_breaches][html] > options list

  Name      Current Value                                                  Required  Description
  --------  -------------                                                  --------  -----------
  CREATOR                                                                  yes       use creator n
ame in the report footer
  CUSTOMER                                                                 yes       use customer
name in the report header
  FILENAME  /home/kali/.recon-ng/workspaces/security_breaches/results.html yes       path and file
name for report output
  SANITIZE  True                                                           yes       mask sensitiv
e data in the report

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

Set all the options.



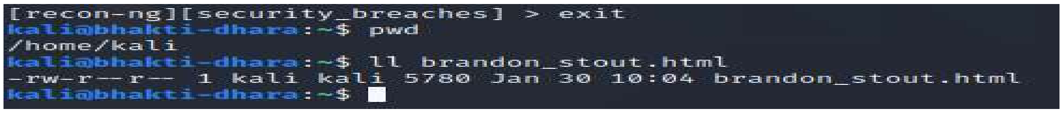
```
[recon-ng][security_breaches][html] > options set CREATOR bhakti-dhara
CREATOR => bhakti-dhara
[recon-ng][security_breaches][html] > options set CUSTOMER Brandon Stout
CUSTOMER => Brandon Stout
[recon-ng][security_breaches][html] > options set FILENAME /home/kali/brandon_stout.html
FILENAME => /home/kali/brandon_stout.html
[recon-ng][security_breaches][html] > options list

  Name      Current Value                  Required  Description
  --------  -------------                  --------  -----------
  CREATOR   bhakti-dhara                   yes       use creator name in the report footer
  CUSTOMER  Brandon Stout                  yes       use customer name in the report header
  FILENAME  /home/kali/brandon_stout.html  yes       path and filename for report output
  SANITIZE  True                           yes       mask sensitive data in the report

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

Run the module.

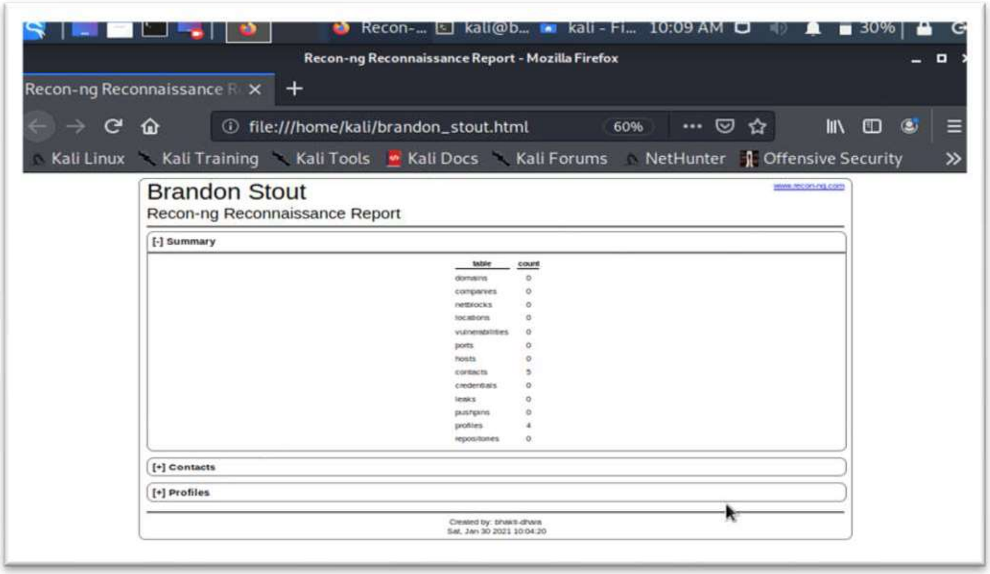


```
[recon-ng][security_breaches][html] > run
[*] Report generated at '/home/kali/brandon_stout.html'.
[recon-ng][security_breaches][html] >
```

12. Html file is generated in given location. Go to the location and double click on the file.



```
[recon-ng][security_breaches] > exit
kali@bhakti-dhara:~$ pwd
/home/kali
kali@bhakti-dhara:~$ ll brandon_stout.html
-rw-r--r-- 1 kali kali 5780 Jan 30 10:04 brandon_stout.html
kali@bhakti-dhara:~$
```



Brandon Stout
Recon-ng Reconnaissance Report

[-] Summary

table	count
domains	0
companies	0
netblocks	0
locations	0
vulnerabilities	0
ports	0
hosts	0
contacts	5
credentials	0
leaks	0
pushpins	0
profiles	4
repositories	0

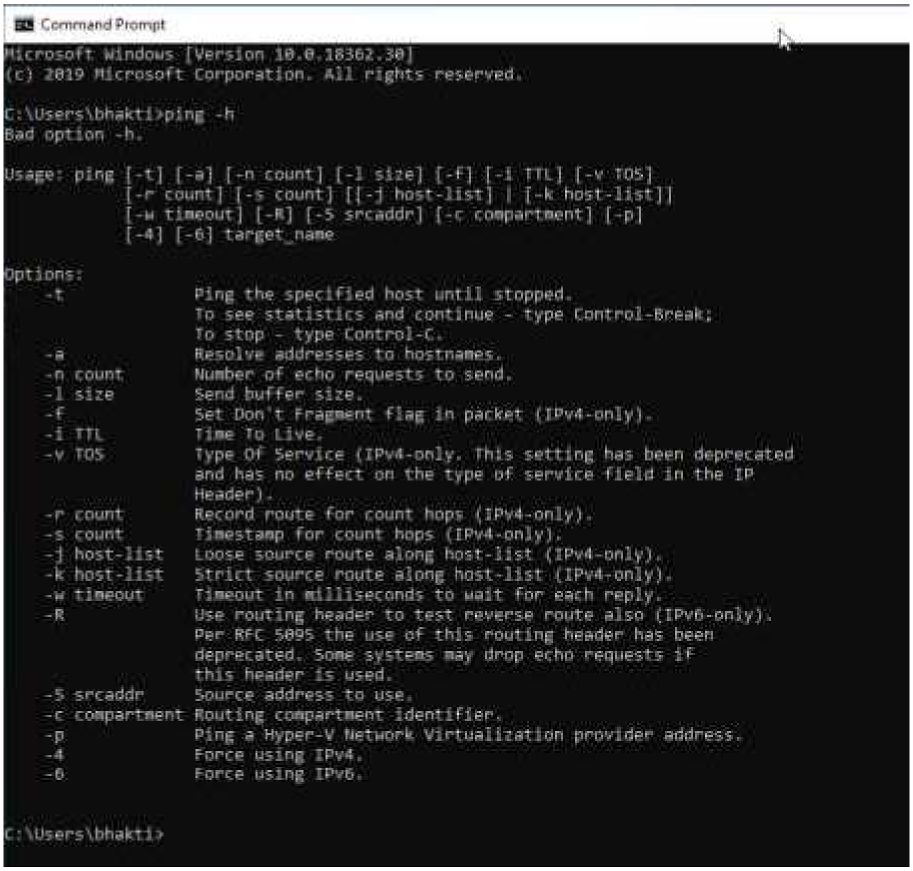
[+] Contacts

[+] Profiles

Created by: bhakti-dhara
Sat, Jan 30 2021 10:04:20

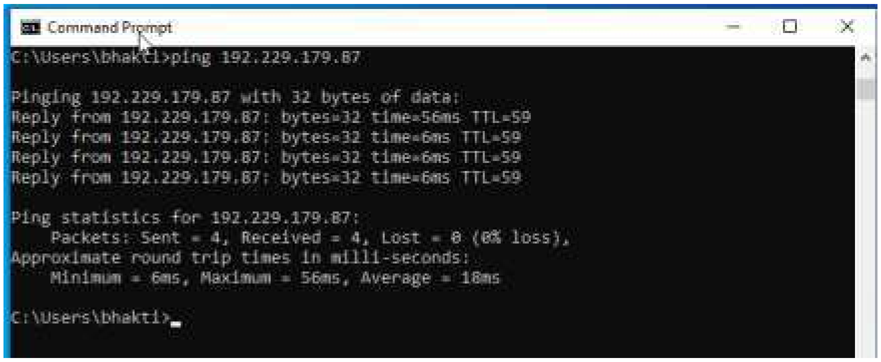
B. Windows Command Line Utilities

1. **Ping :** Ping is a command-line utility, available on virtually any operating system with network connectivity, that acts as a test to see if a networked device is reachable. The ping command sends a request over the network to a specific device.

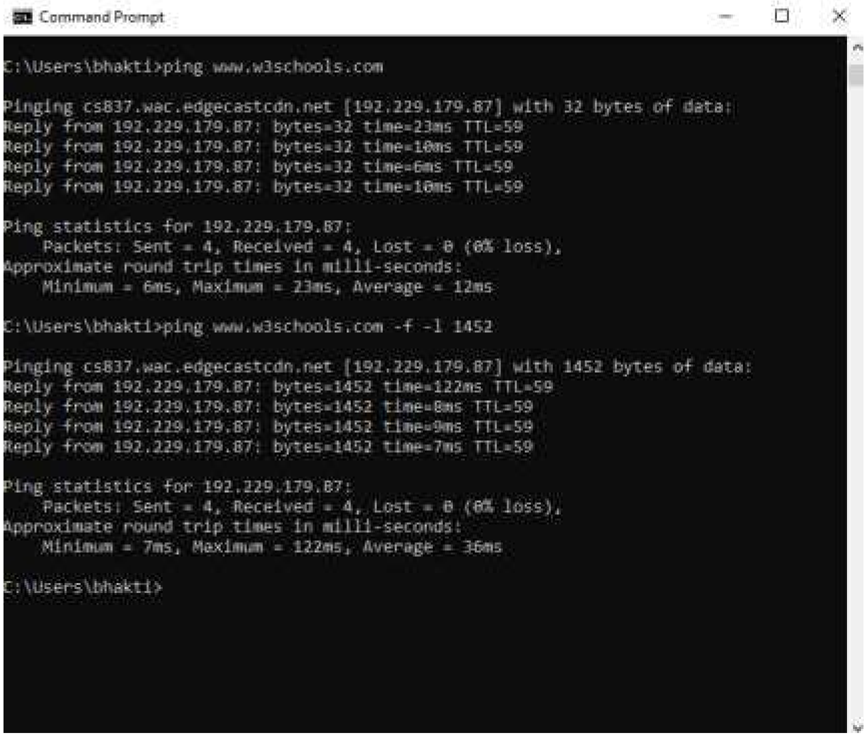


```
Microsoft Windows [Version 10.0.18362.30]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\bhakti>ping -h
Bad option -h.

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP
                   Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
                   Per RFC 5095 the use of this routing header has been
                   deprecated. Some systems may drop echo requests if
                   this header is used.
    -S srcaddr     Source address to use.
    -c compartment Routing compartment identifier.
    -p             Ping a Hyper-V Network Virtualization provider address.
    -4             Force using IPv4.
    -6             Force using IPv6.


C:\Users\bhakti>
```

Get the Public IP of the given domain. Check the size of the packet which can be receive by the destination.

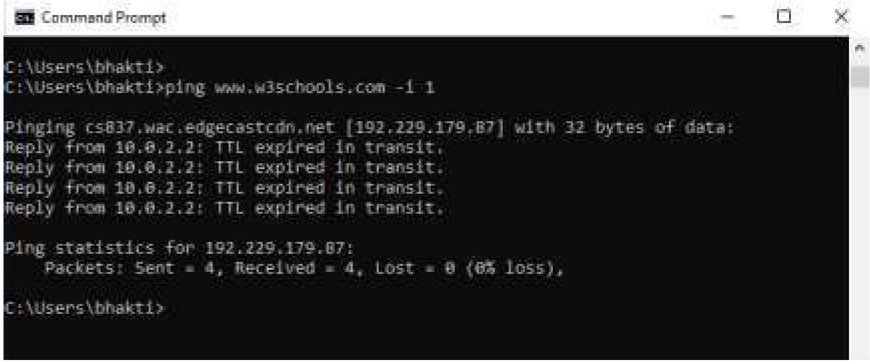


```
C:\Users\bhakti>ping 192.229.179.87

Pinging 192.229.179.87 with 32 bytes of data:
Reply from 192.229.179.87: bytes=32 time=56ms TTL=59
Reply from 192.229.179.87: bytes=32 time=6ms TTL=59
Reply from 192.229.179.87: bytes=32 time=6ms TTL=59
Reply from 192.229.179.87: bytes=32 time=6ms TTL=59

Ping statistics for 192.229.179.87:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 56ms, Average = 18ms

C:\Users\bhakti>
```



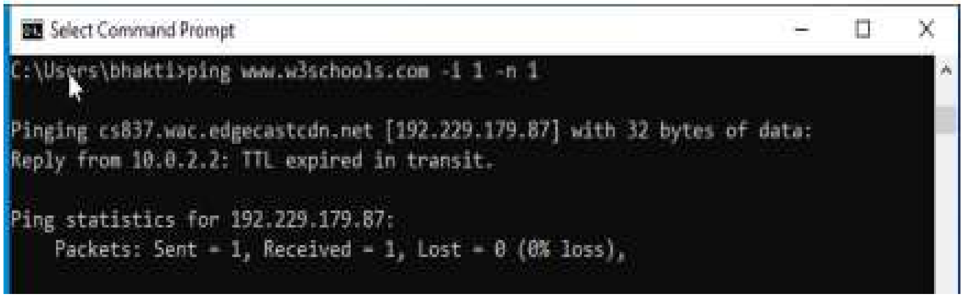
```
C:\Users\bhakti>ping www.w3schools.com

Pinging cs837.wac.edgecastcdn.net [192.229.179.87] with 32 bytes of data:
Reply from 192.229.179.87: bytes=32 time=23ms TTL=59
Reply from 192.229.179.87: bytes=32 time=10ms TTL=59
Reply from 192.229.179.87: bytes=32 time=6ms TTL=59
Reply from 192.229.179.87: bytes=32 time=10ms TTL=59

Ping statistics for 192.229.179.87:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 23ms, Average = 12ms

C:\Users\bhakti>ping www.w3schools.com -f -l 1452

Pinging cs837.wac.edgecastcdn.net [192.229.179.87] with 1452 bytes of data:
Reply from 192.229.179.87: bytes=1452 time=122ms TTL=59
Reply from 192.229.179.87: bytes=1452 time=8ms TTL=59
Reply from 192.229.179.87: bytes=1452 time=9ms TTL=59
Reply from 192.229.179.87: bytes=1452 time=7ms TTL=59

Ping statistics for 192.229.179.87:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 122ms, Average = 36ms

C:\Users\bhakti>
```

Check how much TTL router would take to discard the packet.

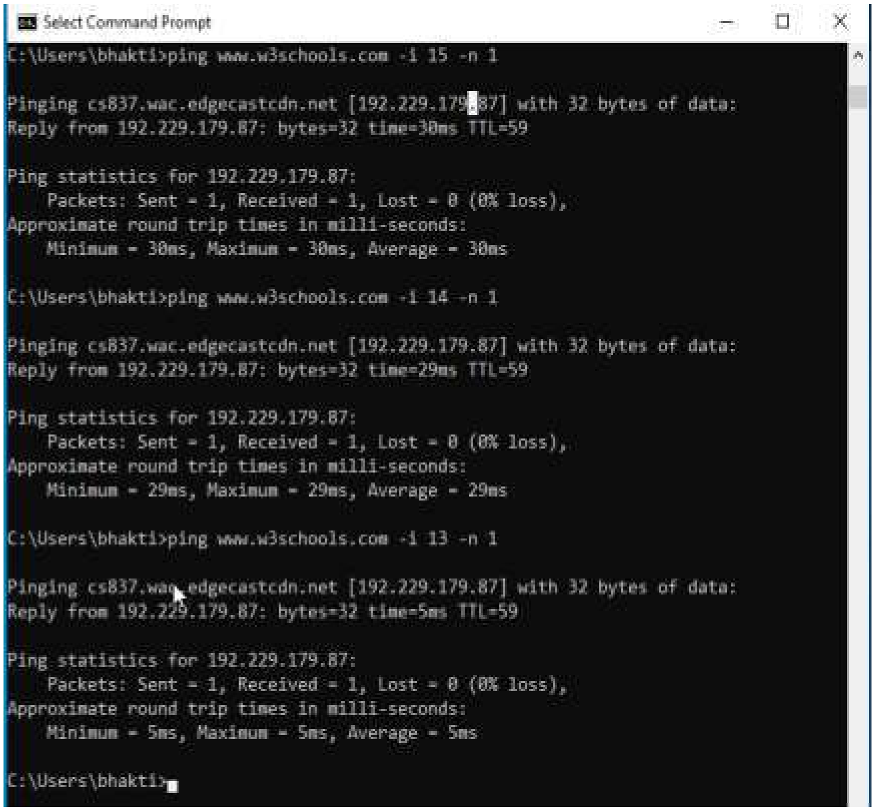


```
C:\Users\bhakti>
C:\Users\bhakti>ping www.w3schools.com -i 1

Pinging cs837.wac.edgecastcdn.net [192.229.179.87] with 32 bytes of data:
Reply from 10.0.2.2: TTL expired in transit.
Reply from 10.0.2.2: TTL expired in transit.
Reply from 10.0.2.2: TTL expired in transit.
Reply from 10.0.2.2: TTL expired in transit.

Ping statistics for 192.229.179.87:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\bhakti>
```

2. Tracert using Ping

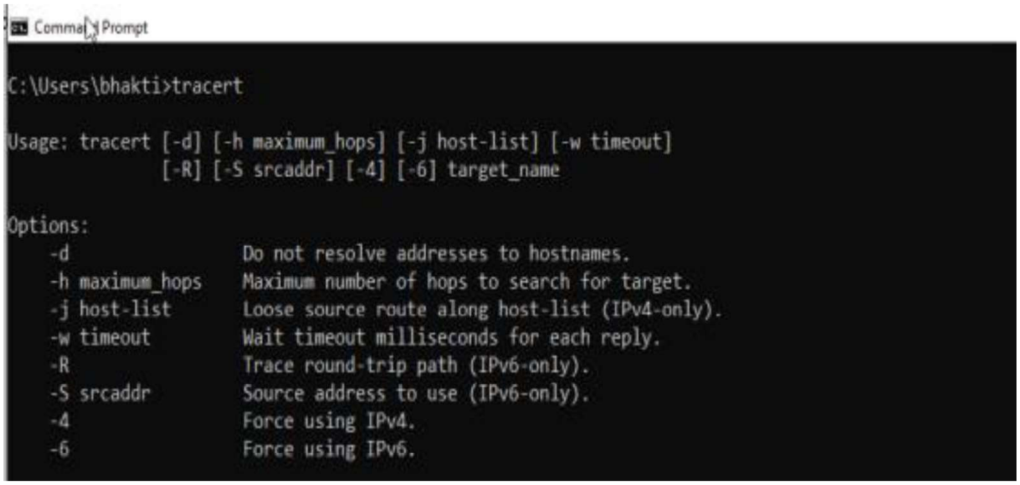


```
C:\Users\bhakti>ping www.w3schools.com -i 1 -n 1

Pinging cs837.wac.edgecastcdn.net [192.229.179.87] with 32 bytes of data:
Reply from 10.0.2.2: TTL expired in transit.

Ping statistics for 192.229.179.87:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
```

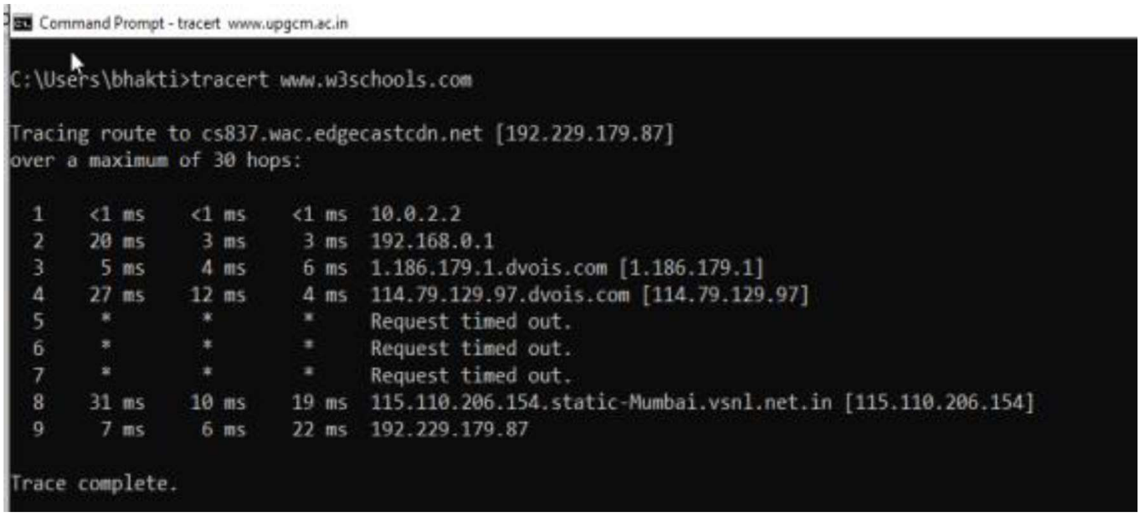


```
C:\Users\bhakti>ping www.w3schools.com -i 15 -n 1

Pinging cs837.wac.edgecastcdn.net [192.229.179.87] with 32 bytes of data:
Reply from 192.229.179.87: bytes=32 time=30ms TTL=59

Ping statistics for 192.229.179.87:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 30ms, Maximum = 30ms, Average = 30ms

C:\Users\bhakti>ping www.w3schools.com -i 14 -n 1

Pinging cs837.wac.edgecastcdn.net [192.229.179.87] with 32 bytes of data:
Reply from 192.229.179.87: bytes=32 time=29ms TTL=59

Ping statistics for 192.229.179.87:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 29ms, Maximum = 29ms, Average = 29ms

C:\Users\bhakti>ping www.w3schools.com -i 13 -n 1

Pinging cs837.wac.edgecastcdn.net [192.229.179.87] with 32 bytes of data:
Reply from 192.229.179.87: bytes=32 time=5ms TTL=59

Ping statistics for 192.229.179.87:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 5ms, Average = 5ms

C:\Users\bhakti>
```

3. **Tracert :** Traceroute is a network diagnostic tool used to track in real-time the pathway taken by a packet on an IP network from source to destination, reporting the IP addresses of all the routers it pinged in between. Traceroute also records the time taken for each hop the packet makes during its route to the destination.

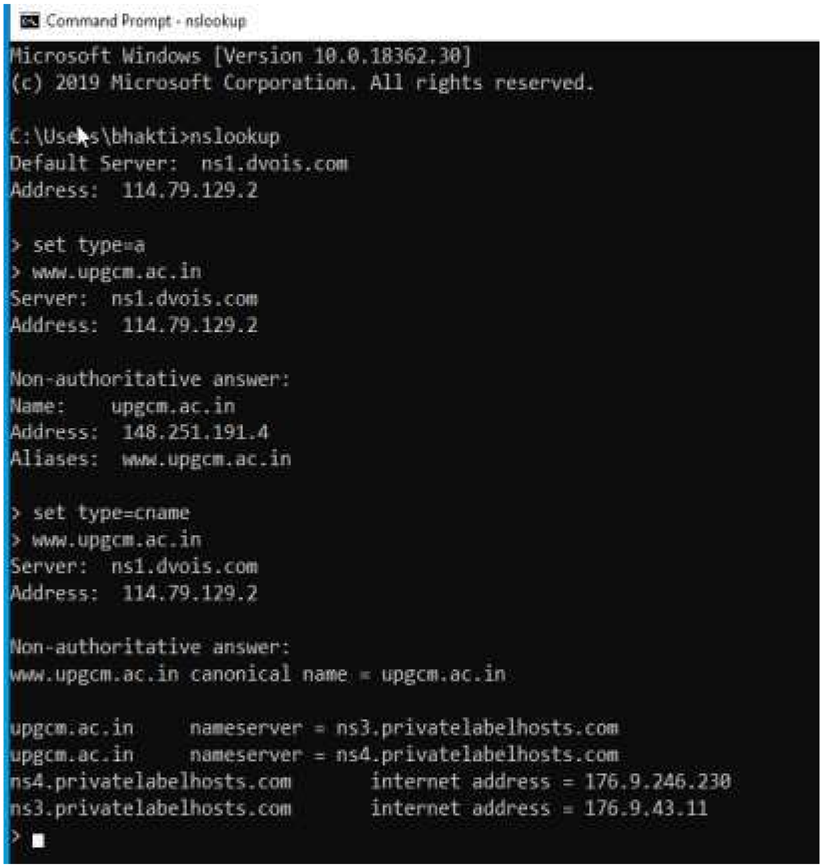


```
C:\Users\bhakti>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.
```



```
C:\Users\bhakti>tracert www.w3schools.com

Tracing route to cs837.wac.edgecastcdn.net [192.229.179.87]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  10.0.2.2
  2    20 ms     3 ms     3 ms  192.168.0.1
  3     5 ms     4 ms     6 ms  1.186.179.1.dvois.com [1.186.179.1]
  4    27 ms    12 ms     4 ms  114.79.129.97.dvois.com [114.79.129.97]
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8    31 ms    10 ms    19 ms  115.110.206.154.static-Mumbai.vsnl.net.in [115.110.206.154]
  9     7 ms     6 ms    22 ms  192.229.179.87

Trace complete.
```

4. **NSLookup :** NSLookup (from name server lookup) is a network administration command-line tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping, or other DNS records.



```
Microsoft Windows [Version 10.0.18362.30]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\bhakti>nslookup
Default Server:  ns1.dvois.com
Address:  114.79.129.2

> set type=a
> www.upgcm.ac.in
Server:  ns1.dvois.com
Address:  114.79.129.2

Non-authoritative answer:
Name:    upgcm.ac.in
Address:  148.251.191.4
Aliases:  www.upgcm.ac.in

> set type=cname
> www.upgcm.ac.in
Server:  ns1.dvois.com
Address:  114.79.129.2

Non-authoritative answer:
www.upgcm.ac.in canonical name = upgcm.ac.in

upgcm.ac.in     nameserver = ns3.privatelabelhosts.com
upgcm.ac.in     nameserver = ns4.privatelabelhosts.com
ns4.privatelabelhosts.com       internet address = 176.9.246.230
ns3.privatelabelhosts.com       internet address = 176.9.43.11
> 
```