Practical No. 1

Aim: Use of open-source intelligence and passive reconnaissance

Objectives:

- **OSINT**

Open-Source Intelligence (OSINT) reconnaissance involves using publicly available resources to passively gather information on a target (a person or organization). To best protect your organization, take the mindset of a threat actor.

- **Passive OSINT**

Passive Reconnaissance is one of the most important phases for successful hacking. Passive Reconnaissance uses Open-Source Intelligence (OSINT) techniques to gather information about the target. To explain, we attempt to gather information about the target without interacting with it.

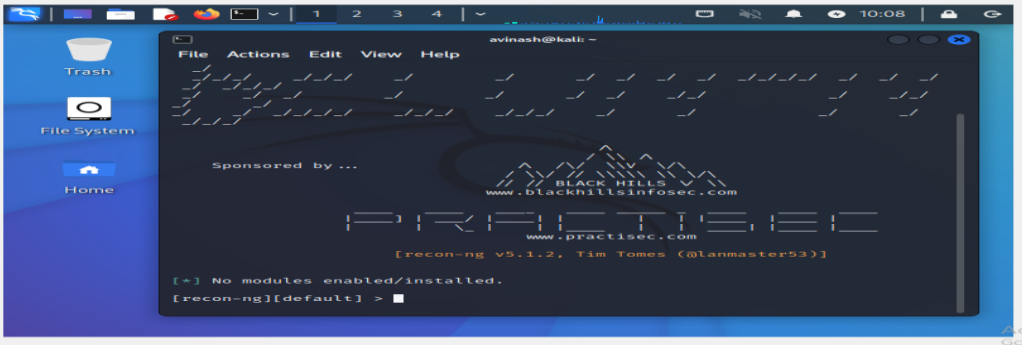
- **Recon-ng**

Recon-ng is a Web Reconnaissance tool written in Python. It has so many 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, and we can gather all information

Implementation:

A. Using Recon-ng tool

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

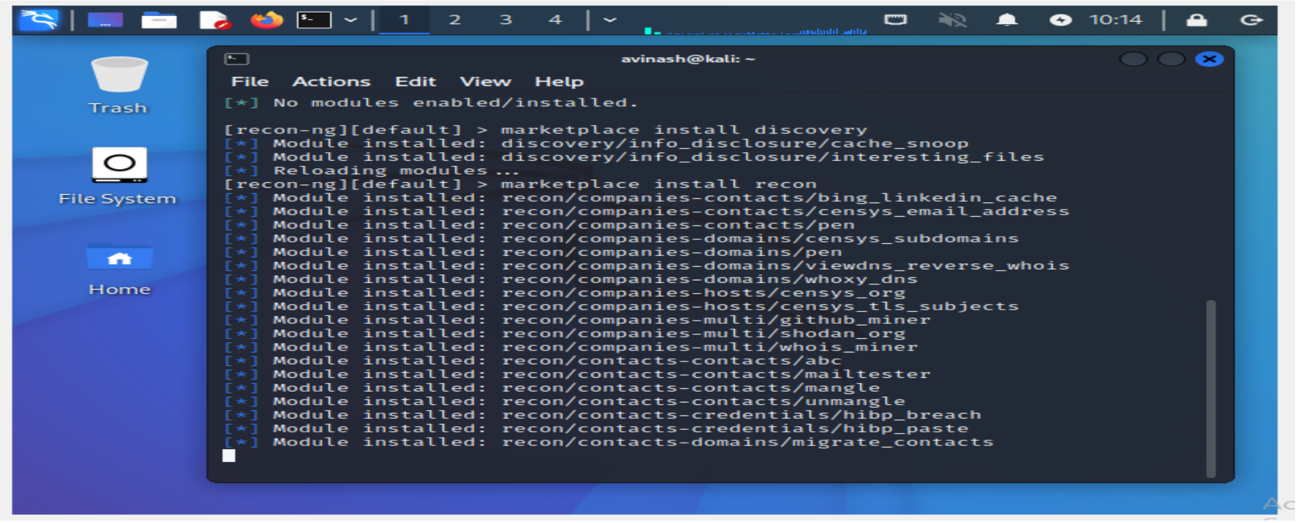


```
Sponsored by ...
                    BLACK HILLS
              www.blackhillsinfosec.com

                  www.practisec.com

          [recon-ng v5.1.2, Tim Tomes (@lanmaster53)]

[*] No modules enabled/installed.
[recon-ng][default] > 
```

3. Initially there are no modules installed. To install the modules,

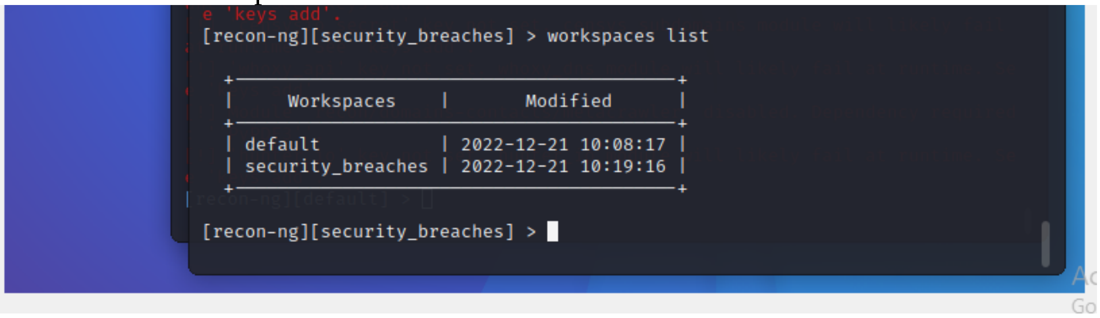
    a. Discovery module
    b. Recon module
    c. Importing module
    d. Exploitation module
    e. Reporting module

Now, the required modules are installed



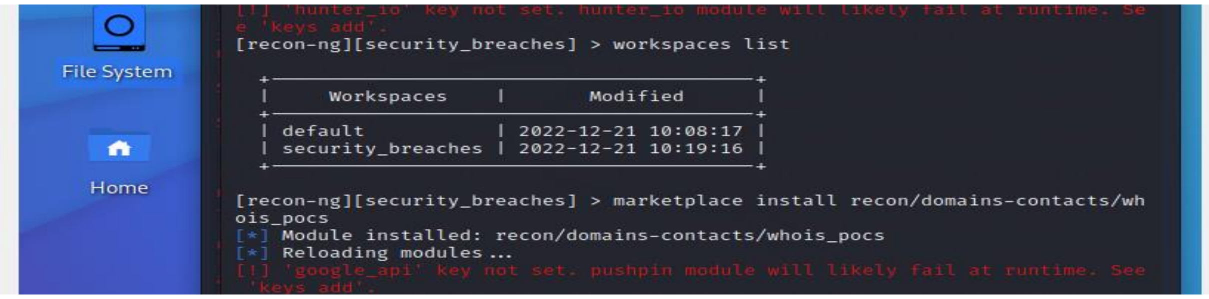
```
[*] No modules enabled/installed.

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

4. To create a new workspace



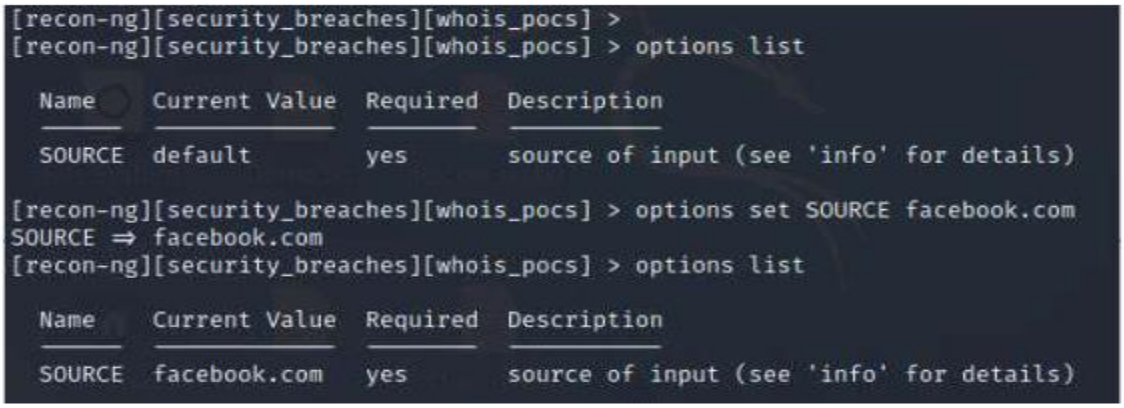
```
e 'keys add'.
[recon-ng][security_breaches] > workspaces list

  +--------------------------------------------+
  |      Workspaces     |       Modified       |
  +--------------------------------------------+
  | default             | 2022-12-21 10:08:17 |
  | security_breaches   | 2022-12-21 10:19:16 |
  +--------------------------------------------+

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

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



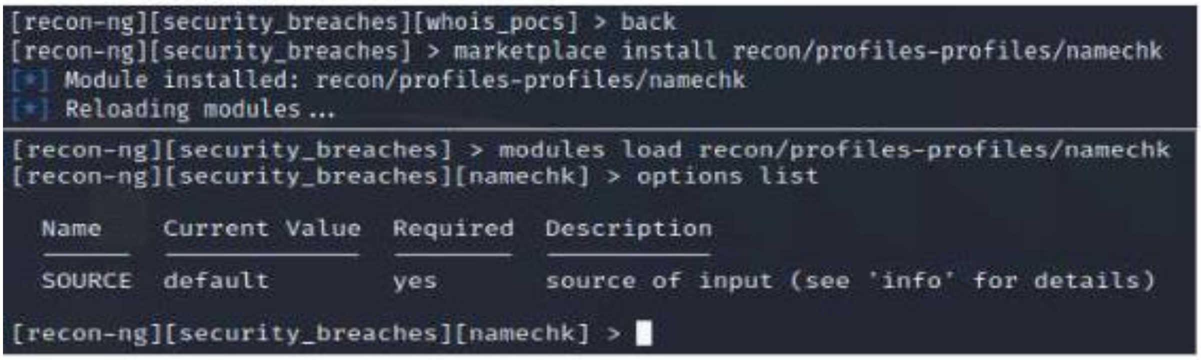
```
[!] 'hunter_io' key not set. hunter_io module will likely fail at runtime. Se
e 'keys add'.
[recon-ng][security_breaches] > workspaces list

  +--------------------------------------------+
  |      Workspaces     |       Modified       |
  +--------------------------------------------+
  | default             | 2022-12-21 10:08:17 |
  | security_breaches   | 2022-12-21 10:19:16 |
  +--------------------------------------------+

[recon-ng][security_breaches] > marketplace install recon/domains-contacts/wh
ois_pocs
[*] Module installed: recon/domains-contacts/whois_pocs
[*] Reloading modules ...
[!] 'google_api' key not set. pushpin module will likely fail at runtime. See
 'keys add'.
```

6. Set the option and run the module.



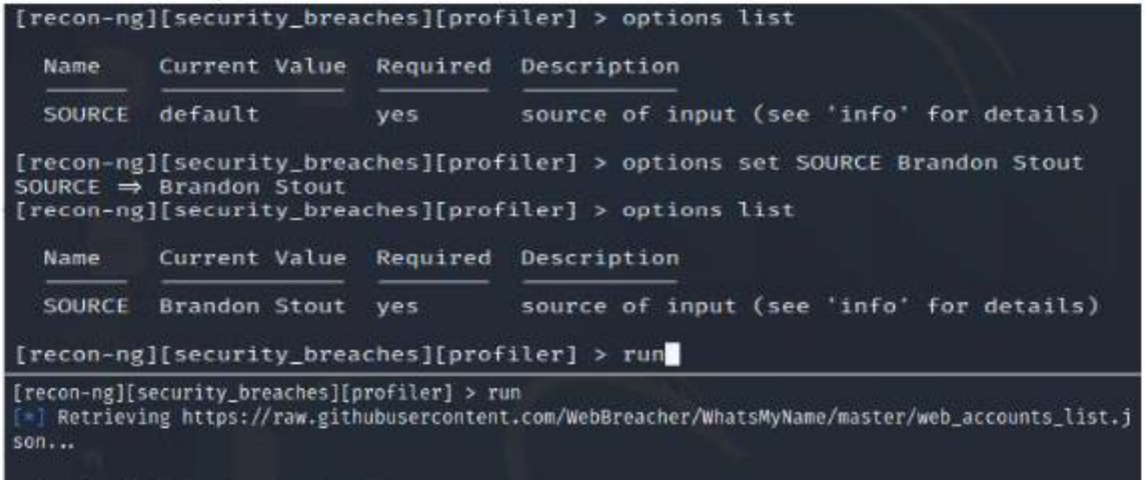
```
[recon-ng][security_breaches][whois_pocs] >
[recon-ng][security_breaches][whois_pocs] > options list

  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)
```

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



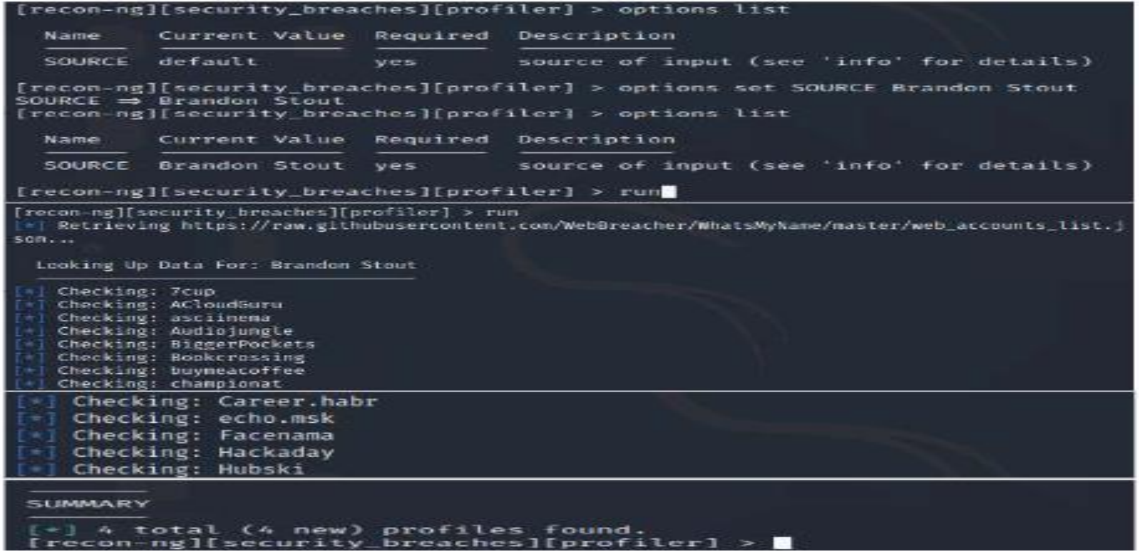
```
[recon-ng][security_breaches][whois_pocs] > back
[recon-ng][security_breaches] > marketplace install recon/profiles-profiles/namechk
[*] Module installed: recon/profiles-profiles/namechk
[*] Reloading modules ...
[recon-ng][security_breaches] > modules load recon/profiles-profiles/namechk
[recon-ng][security_breaches][namechk]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



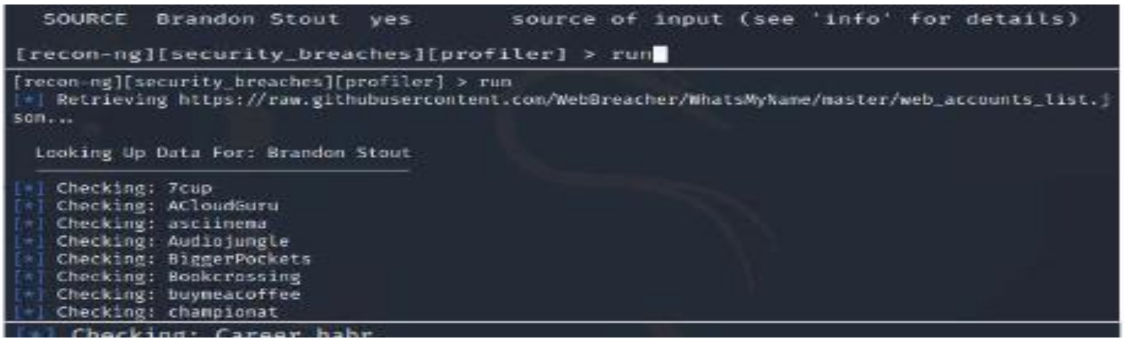
```
[recon-ng][security_breaches][profiler] > options list

  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...
```

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

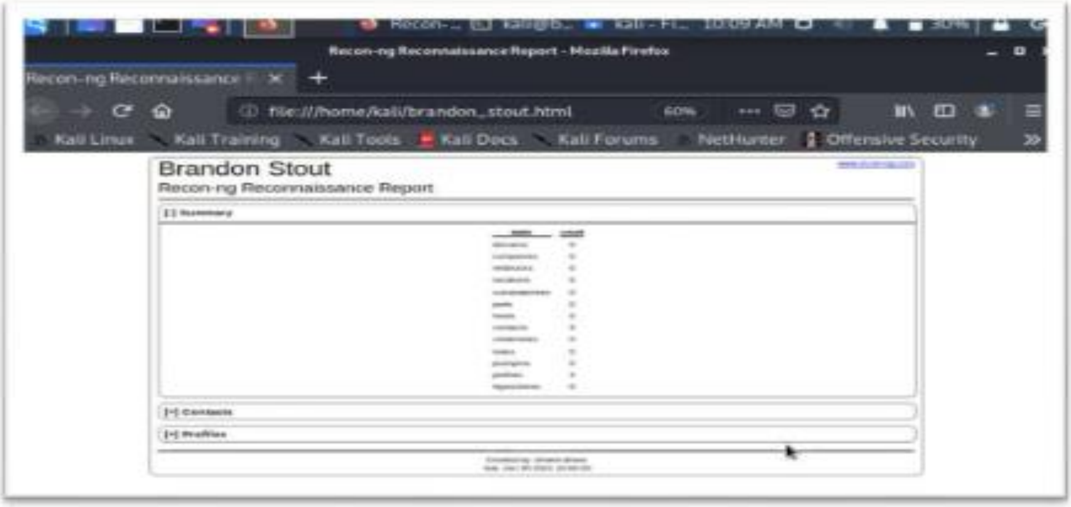
11. Generate a Report. We will install another module reporting/html and load the module to generate a report in html file. Set the all options and Run the module



```
  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
```

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



Brandon Stout
Recon-ng Reconnaissance Report

[-] Summary

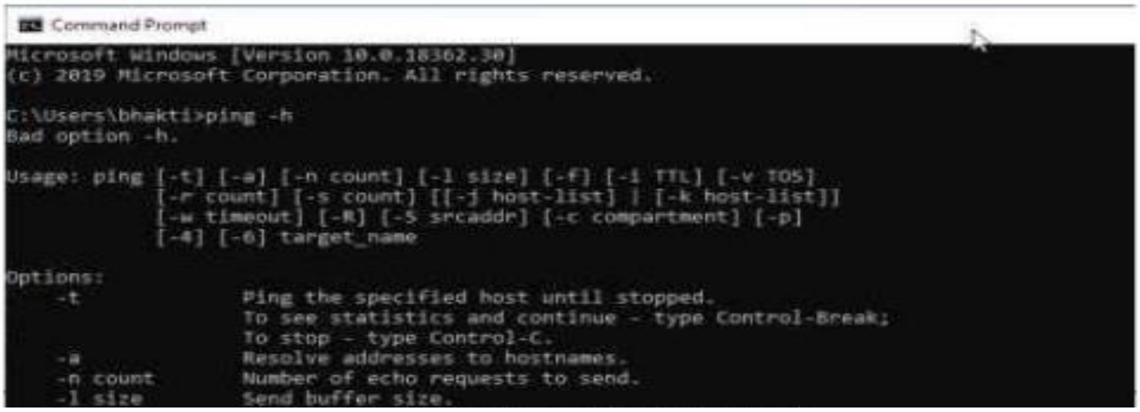
[+] Contacts

[+] Profiles

B. Windows Command Line Utilities

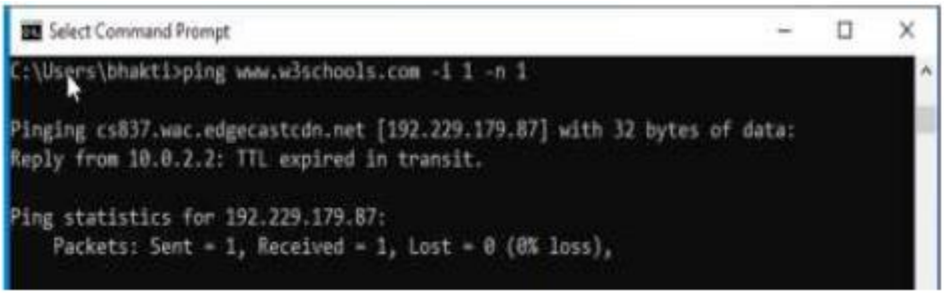
1. Ping

(**Packet Internet or Inter-Network Groper**) is a basic Internet program that allows a user to test and verify if a particular destination IP address exists and can accept requests in computer network administration. The acronym was contrived to match the submariners' term for the sound of a returned sonar pulse.



```
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.
```

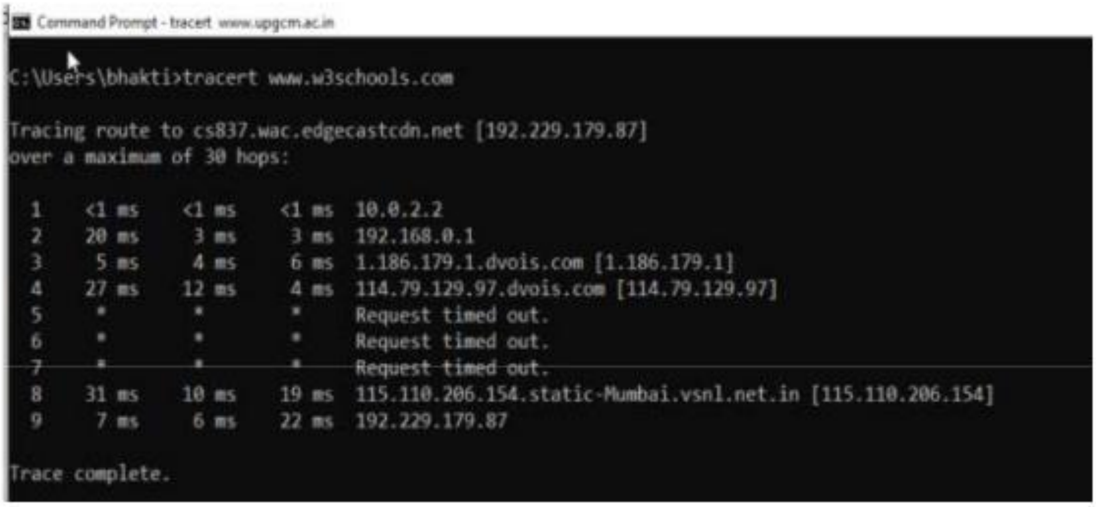
Get the public ip of the given domain. Check the size of the packet which can be receive by destination.



```
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),
```

Check how much TTL router would take to discard the packet

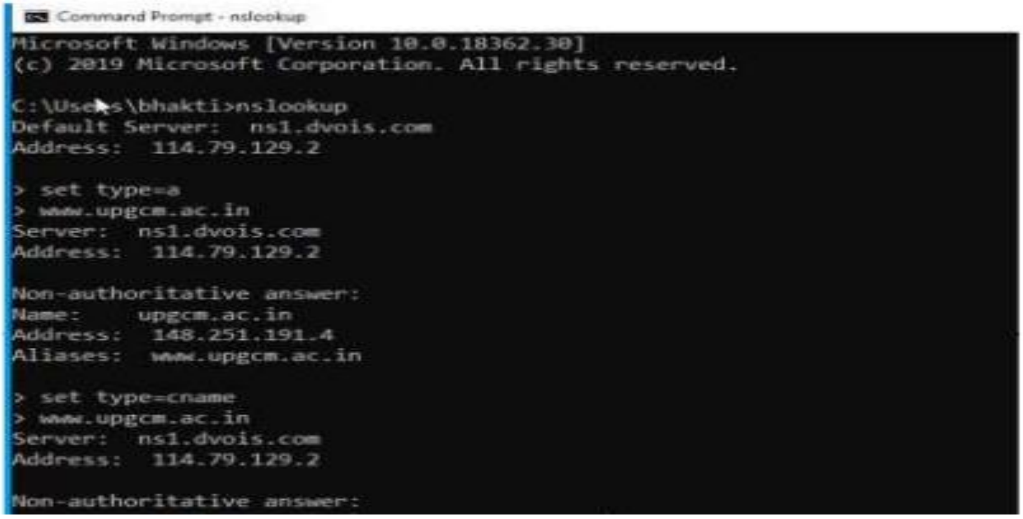
2. **Tracert using ping**



```
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.
```

3. **TRACERT** is useful for troubleshooting large networks where several paths can lead to the same point or where many intermediate components (routers or bridges) are involved.

4. **nslookup** is the name of a program that lets an Internet server administrator or any computer user enter a host name (for example, "whatis.com") and find out the corresponding IP address or domain name system (DNS) record.



```
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:
```