Ethical Hacking Experiment 1

Ojas Patil

2019130048

TE COMPS

Batch: C

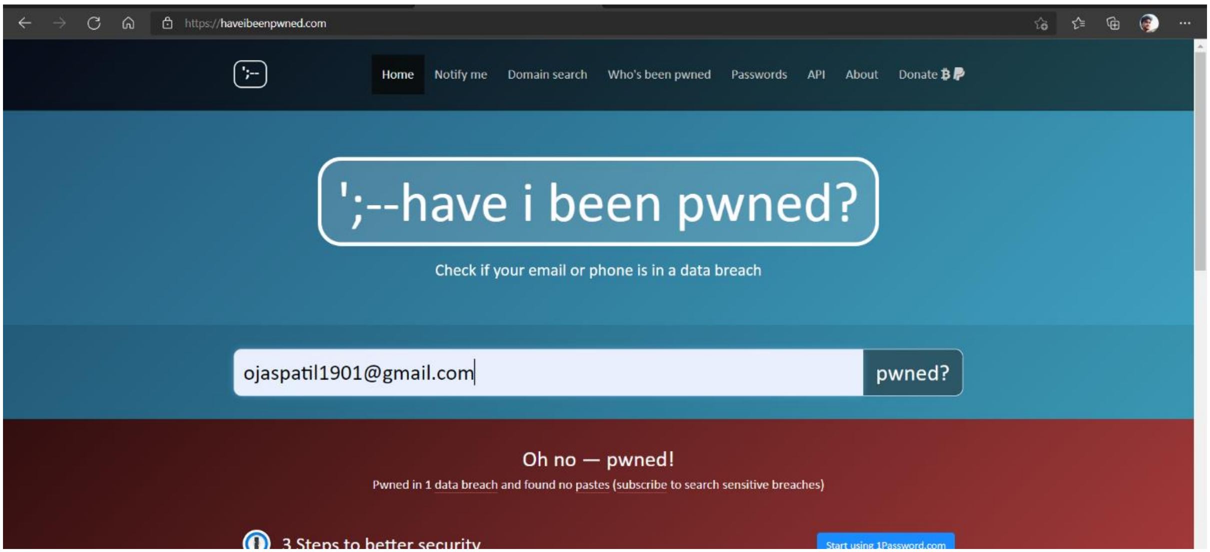
Aim: To try foot printing with the help of various tools and utilities available.

1) What is foot printing?

Foot printing means gathering information about a target system which can be used to execute a successful cyber-attack. To get this information, a hacker might use various methods with variant tools. This information is the first road for the hacker to crack a system.

Information gathered from foot printing:

Operating system of the target machine, firewall, IP address, security configuration of target machine, email id, passwords, server configuration, URLs, etc.



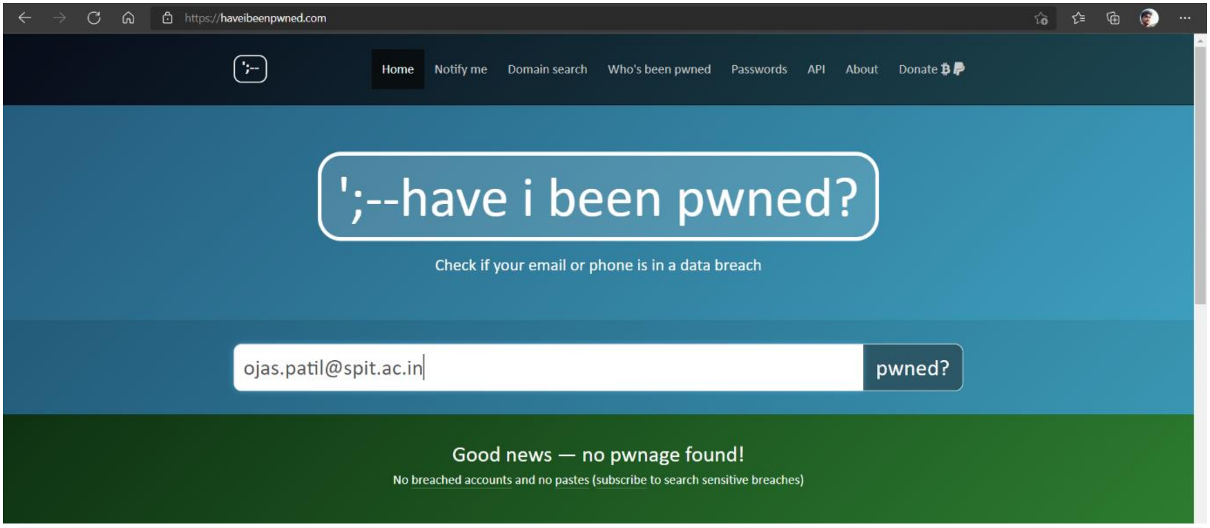
Check if your email or phone is in a data breach

ojaspatil1901@gmail.com

Oh no — pwned!

Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches)

3 Steps to better security

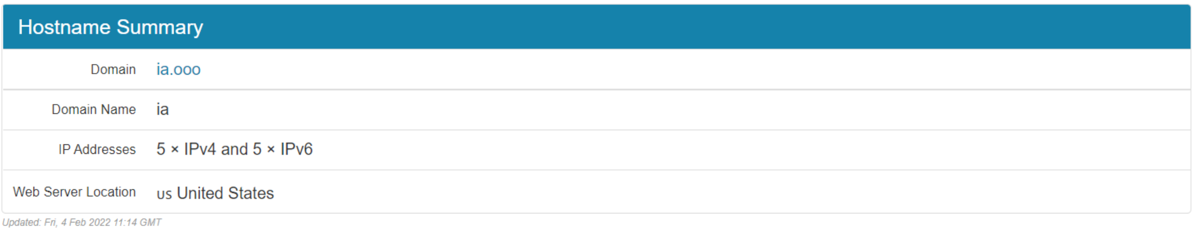


Check if your email or phone is in a data breach

ojas.patil@spit.ac.in

Good news — no pwnage found!

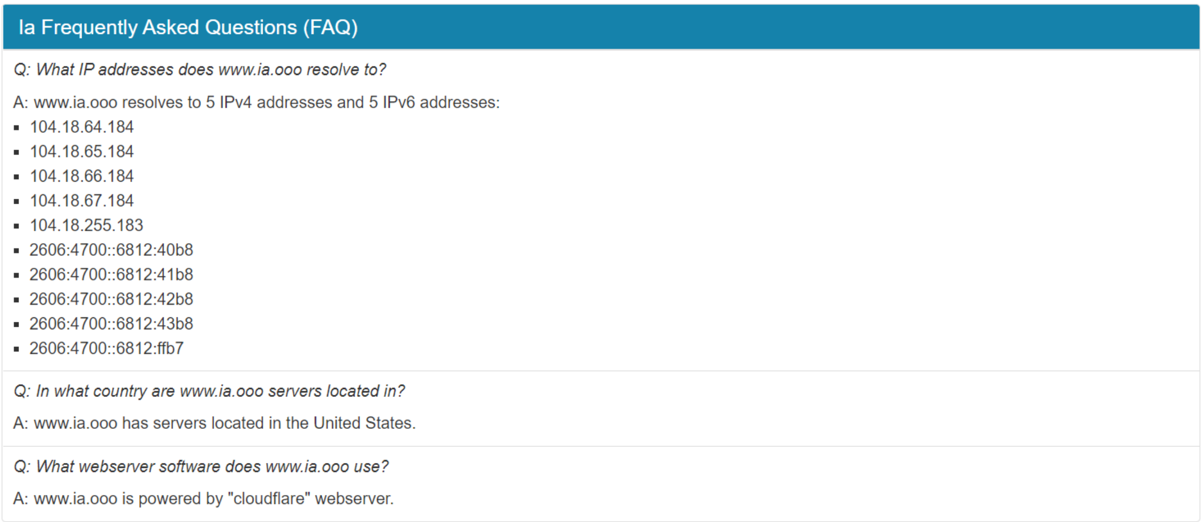
No breached accounts and no pastes (subscribe to search sensitive breaches)



Hostname Summary

Domain	ia.ooo
Domain Name	ia
IP Addresses	5 × IPv4 and 5 × IPv6
Web Server Location	US United States

Updated: Fri, 4 Feb 2022 11:14 GMT



Ia Frequently Asked Questions (FAQ)

Q: What IP addresses does www.ia.ooo resolve to?

A: www.ia.ooo resolves to 5 IPv4 addresses and 5 IPv6 addresses:

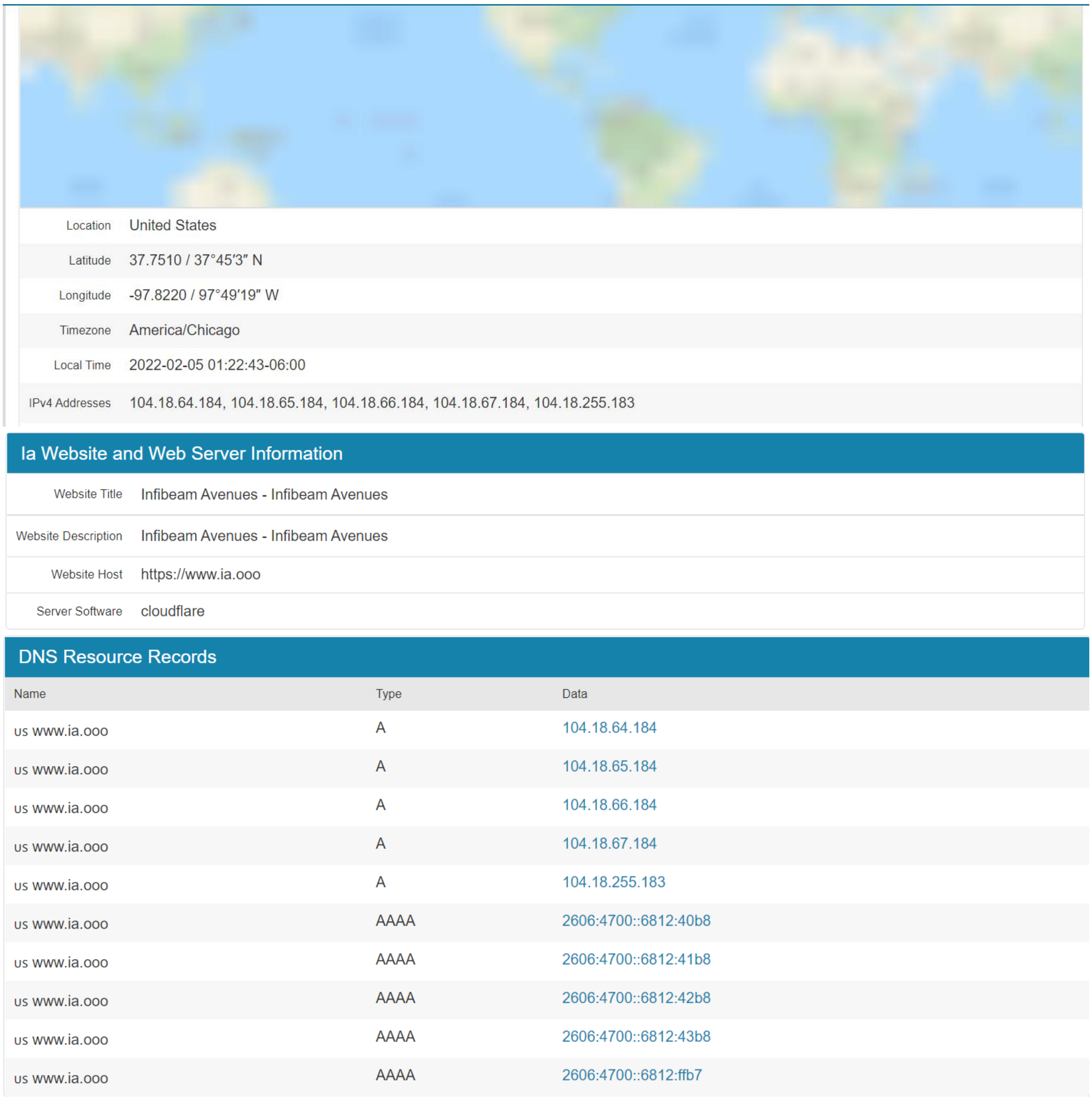
- 104.18.64.184
- 104.18.65.184
- 104.18.66.184
- 104.18.67.184
- 104.18.255.183
- 2606:4700::6812:40b8
- 2606:4700::6812:41b8
- 2606:4700::6812:42b8
- 2606:4700::6812:43b8
- 2606:4700::6812:ffb7

Q: In what country are www.ia.ooo servers located in?

A: www.ia.ooo has servers located in the United States.

Q: What webserver software does www.ia.ooo use?

A: www.ia.ooo is powered by "cloudflare" webserver.



Location	United States
Latitude	37.7510 / 37°45′3″ N
Longitude	-97.8220 / 97°49′19″ W
Timezone	America/Chicago
Local Time	2022-02-05 01:22:43-06:00
IPv4 Addresses	104.18.64.184, 104.18.65.184, 104.18.66.184, 104.18.67.184, 104.18.255.183

Ia Website and Web Server Information

Website Title	Infibeam Avenues - Infibeam Avenues
Website Description	Infibeam Avenues - Infibeam Avenues
Website Host	https://www.ia.ooo
Server Software	cloudflare

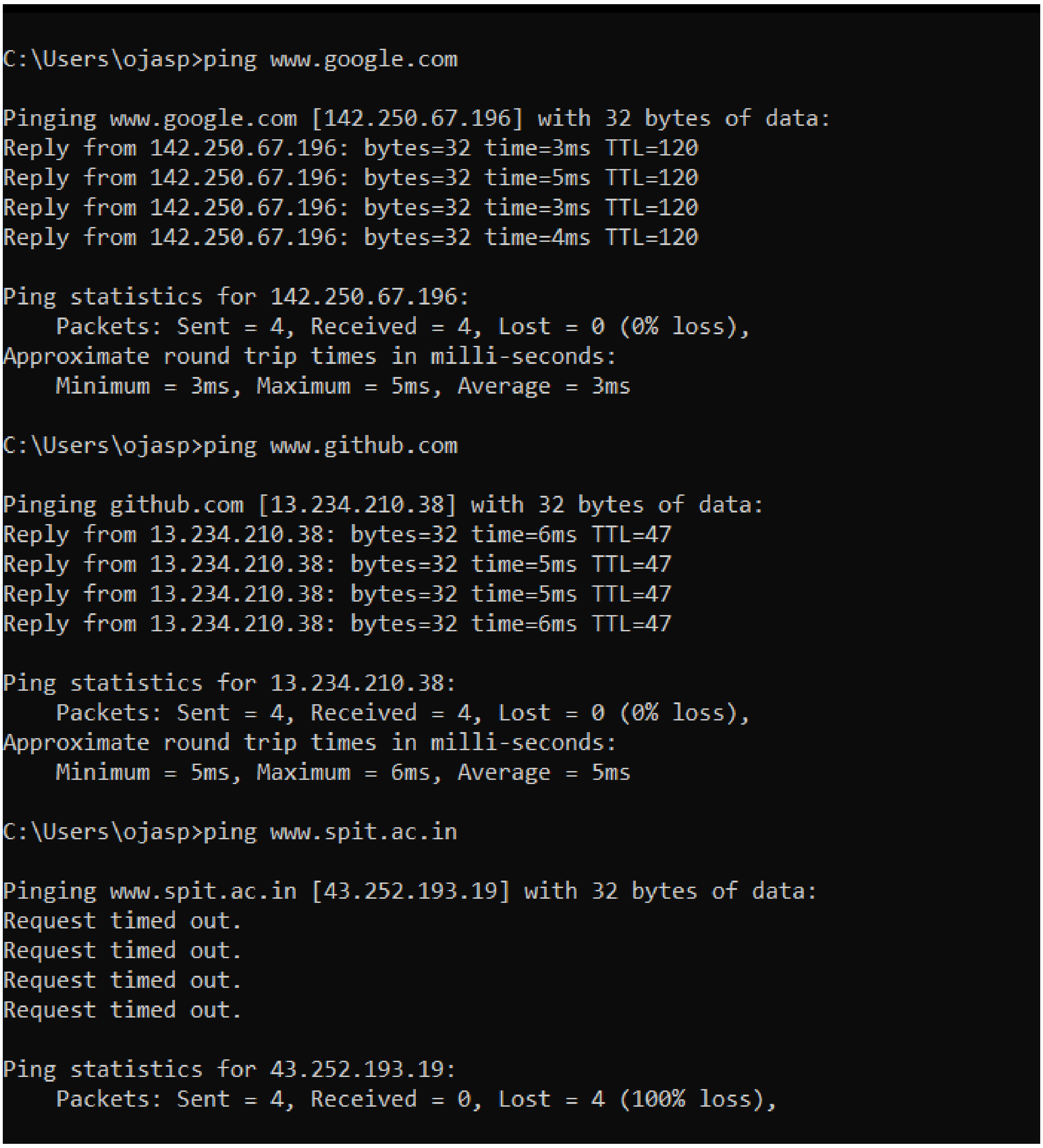
DNS Resource Records

Name	Type	Data
US www.ia.ooo	A	104.18.64.184
US www.ia.ooo	A	104.18.65.184
US www.ia.ooo	A	104.18.66.184
US www.ia.ooo	A	104.18.67.184
US www.ia.ooo	A	104.18.255.183
US www.ia.ooo	AAAA	2606:4700::6812:40b8
US www.ia.ooo	AAAA	2606:4700::6812:41b8
US www.ia.ooo	AAAA	2606:4700::6812:42b8
US www.ia.ooo	AAAA	2606:4700::6812:43b8
US www.ia.ooo	AAAA	2606:4700::6812:ffb7

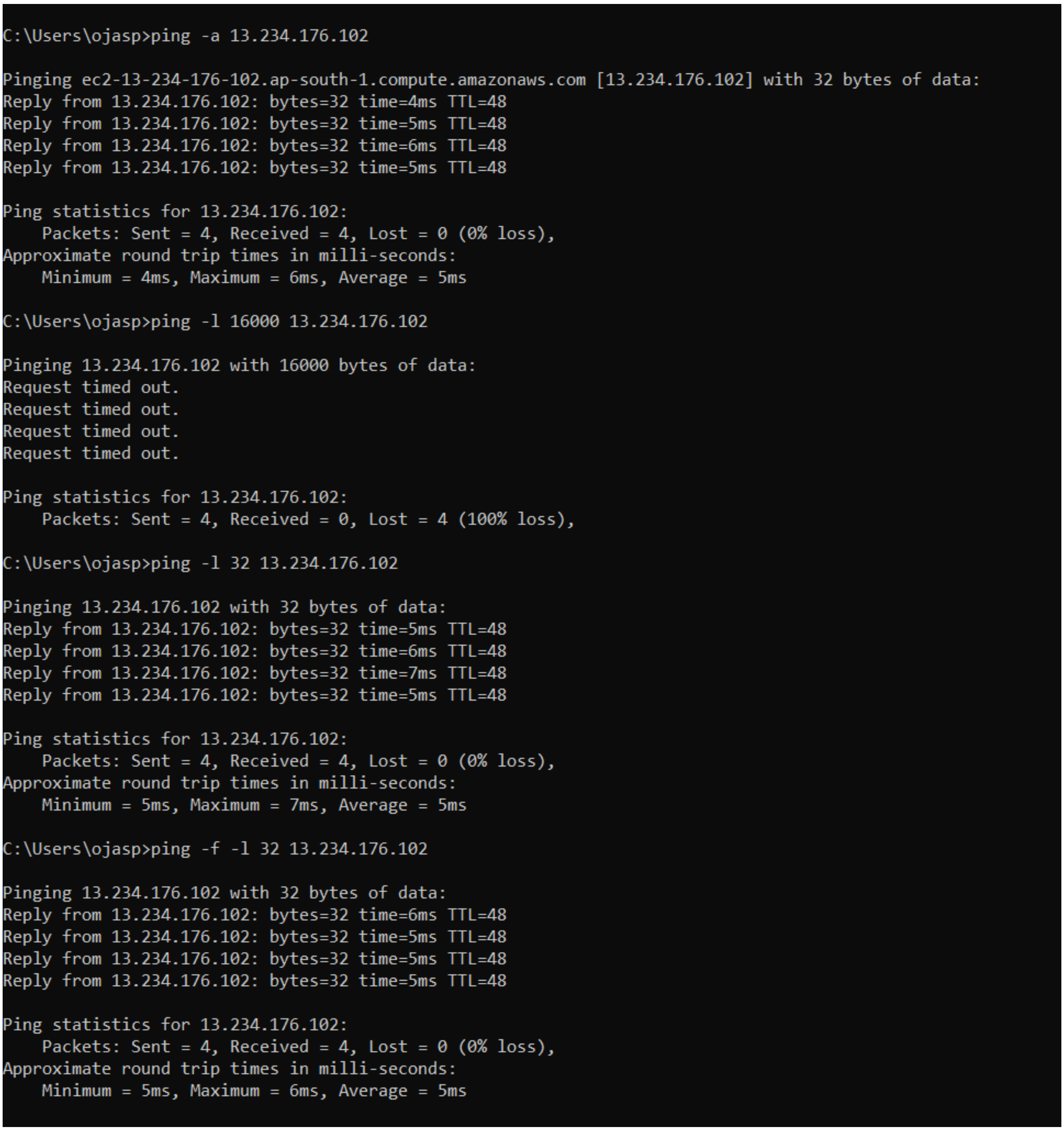
2) Explain the process using command line utility i.e. Ping , tracert, nslookup, DNS footprinting.

Ping:

ping command in command prompt along with mentioned URL or IP address, sends specific number of ICMP packages to mentioned address. The size of ICMP packages can be varied. Ping commands helps to get IP address of target URL. Also ping command is simplest tool to launch a denial-of-service attack.



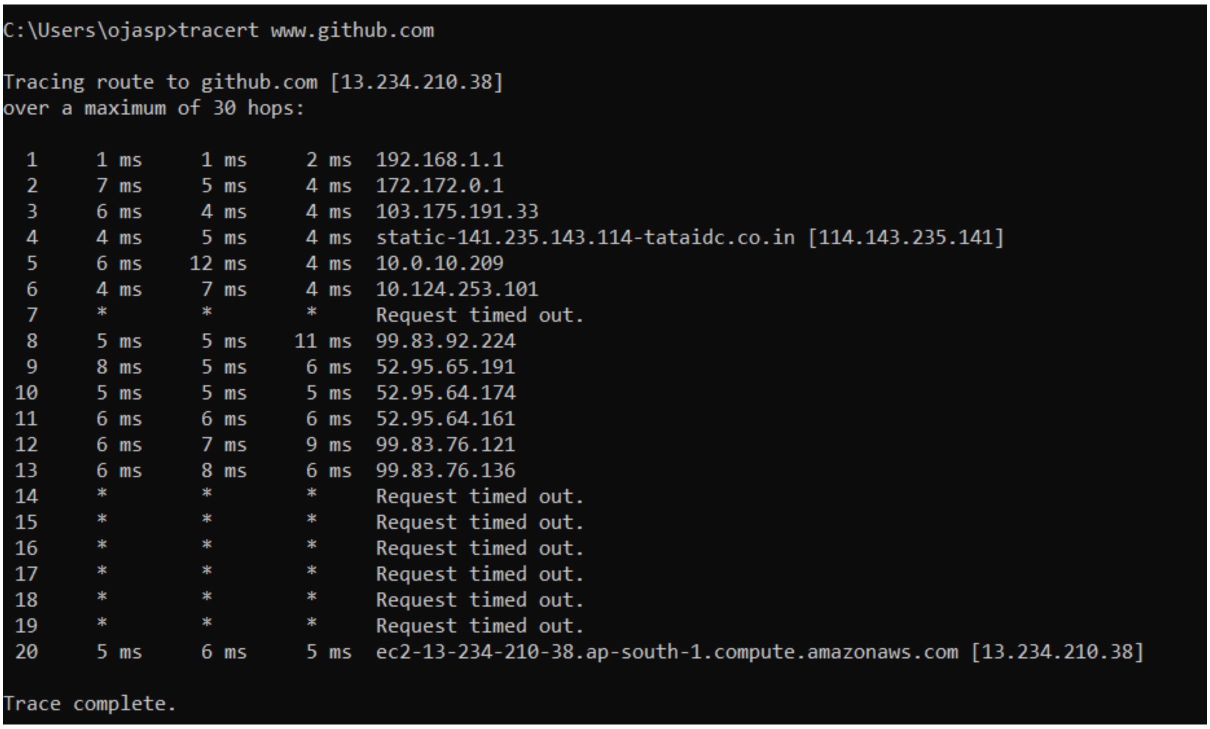
```
C:\Users\ojasp>ping www.google.com

Pinging www.google.com [142.250.67.196] with 32 bytes of data:
Reply from 142.250.67.196: bytes=32 time=3ms TTL=120
Reply from 142.250.67.196: bytes=32 time=5ms TTL=120
Reply from 142.250.67.196: bytes=32 time=3ms TTL=120
Reply from 142.250.67.196: bytes=32 time=4ms TTL=120

Ping statistics for 142.250.67.196:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 5ms, Average = 3ms

C:\Users\ojasp>ping www.github.com

Pinging github.com [13.234.210.38] with 32 bytes of data:
Reply from 13.234.210.38: bytes=32 time=6ms TTL=47
Reply from 13.234.210.38: bytes=32 time=5ms TTL=47
Reply from 13.234.210.38: bytes=32 time=5ms TTL=47
Reply from 13.234.210.38: bytes=32 time=6ms TTL=47

Ping statistics for 13.234.210.38:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 6ms, Average = 5ms

C:\Users\ojasp>ping www.spit.ac.in

Pinging www.spit.ac.in [43.252.193.19] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 43.252.193.19:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```



```
C:\Users\ojasp>ping -a 13.234.176.102

Pinging ec2-13-234-176-102.ap-south-1.compute.amazonaws.com [13.234.176.102] with 32 bytes of data:
Reply from 13.234.176.102: bytes=32 time=4ms TTL=48
Reply from 13.234.176.102: bytes=32 time=5ms TTL=48
Reply from 13.234.176.102: bytes=32 time=6ms TTL=48
Reply from 13.234.176.102: bytes=32 time=5ms TTL=48

Ping statistics for 13.234.176.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 6ms, Average = 5ms

C:\Users\ojasp>ping -l 16000 13.234.176.102

Pinging 13.234.176.102 with 16000 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 13.234.176.102:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\ojasp>ping -l 32 13.234.176.102

Pinging 13.234.176.102 with 32 bytes of data:
Reply from 13.234.176.102: bytes=32 time=5ms TTL=48
Reply from 13.234.176.102: bytes=32 time=6ms TTL=48
Reply from 13.234.176.102: bytes=32 time=7ms TTL=48
Reply from 13.234.176.102: bytes=32 time=5ms TTL=48

Ping statistics for 13.234.176.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 7ms, Average = 5ms

C:\Users\ojasp>ping -f -l 32 13.234.176.102

Pinging 13.234.176.102 with 32 bytes of data:
Reply from 13.234.176.102: bytes=32 time=6ms TTL=48
Reply from 13.234.176.102: bytes=32 time=5ms TTL=48
Reply from 13.234.176.102: bytes=32 time=5ms TTL=48
Reply from 13.234.176.102: bytes=32 time=5ms TTL=48

Ping statistics for 13.234.176.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 6ms, Average = 5ms
```

Tracert:

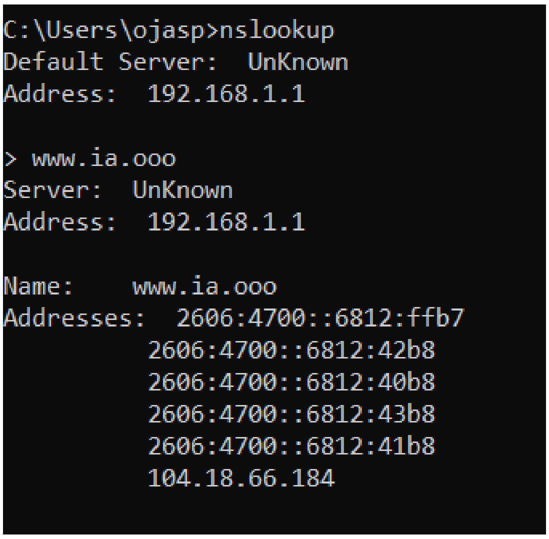
Tracert command sends 3 ICMP packet to each node in between the source and destination. It records RTT of each packet. It also returns IP address and domain name of each node it has passed through. It is helpful for attacker to identify the path followed by packets so that it can exploit it in between.



```
C:\Users\ojasp>tracert www.github.com

Tracing route to github.com [13.234.210.38]
over a maximum of 30 hops:

  1     1 ms     1 ms     2 ms  192.168.1.1
  2     7 ms     5 ms     4 ms  172.172.0.1
  3     6 ms     4 ms     4 ms  103.175.191.33
  4     4 ms     5 ms     4 ms  static-141.235.143.114-tataidc.co.in [114.143.235.141]
  5     6 ms    12 ms     4 ms  10.0.10.209
  6     4 ms     7 ms     4 ms  10.124.253.101
  7     *        *        *     Request timed out.
  8     5 ms     5 ms    11 ms  99.83.92.224
  9     8 ms     5 ms     6 ms  52.95.65.191
 10     5 ms     5 ms     5 ms  52.95.64.174
 11     6 ms     6 ms     6 ms  52.95.64.161
 12     6 ms     7 ms     9 ms  99.83.76.121
 13     6 ms     8 ms     6 ms  99.83.76.136
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     5 ms     6 ms     5 ms  ec2-13-234-210-38.ap-south-1.compute.amazonaws.com [13.234.210.38]

Trace complete.
```

<u>NS lookup</u>:

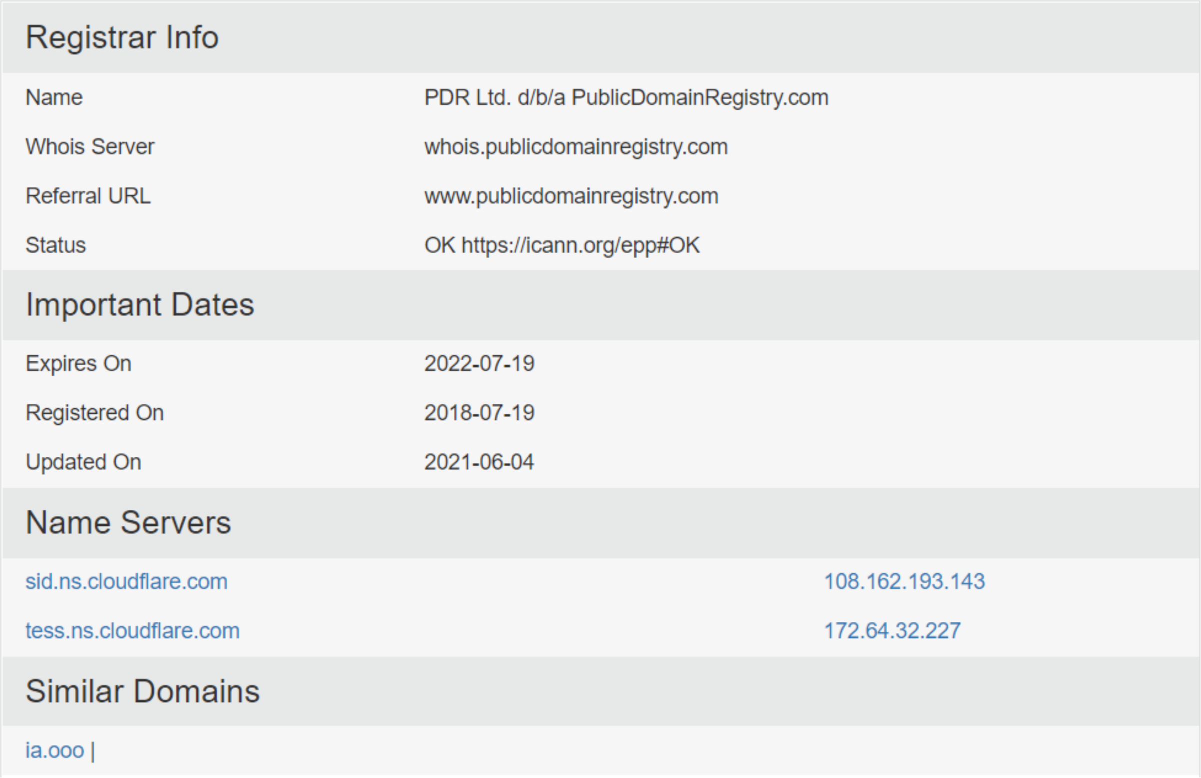
Nslookup is a domain name resolver command. With the help of nslookup command, we can find out the IP address of any domain name. Also, given an IP address, its domain name can also be identified with this command.



```
C:\Users\ojasp>nslookup
Default Server:  UnKnown
Address:  192.168.1.1

> www.ia.ooo
Server:  UnKnown
Address:  192.168.1.1

Name:    www.ia.ooo
Addresses:  2606:4700::6812:ffb7
          2606:4700::6812:42b8
          2606:4700::6812:40b8
          2606:4700::6812:43b8
          2606:4700::6812:41b8
          104.18.66.184
```

3) Explain Who is database

This is a website which serves a good purpose for Hackers. Through this website information about the domain name, email-id, domain owner, etc; a website can be traced. Basically, this serves a way for Website Footprinting.



Registrar Info

Name	PDR Ltd. d/b/a PublicDomainRegistry.com
Whois Server	whois.publicdomainregistry.com
Referral URL	www.publicdomainregistry.com
Status	OK https://icann.org/epp#OK

Important Dates

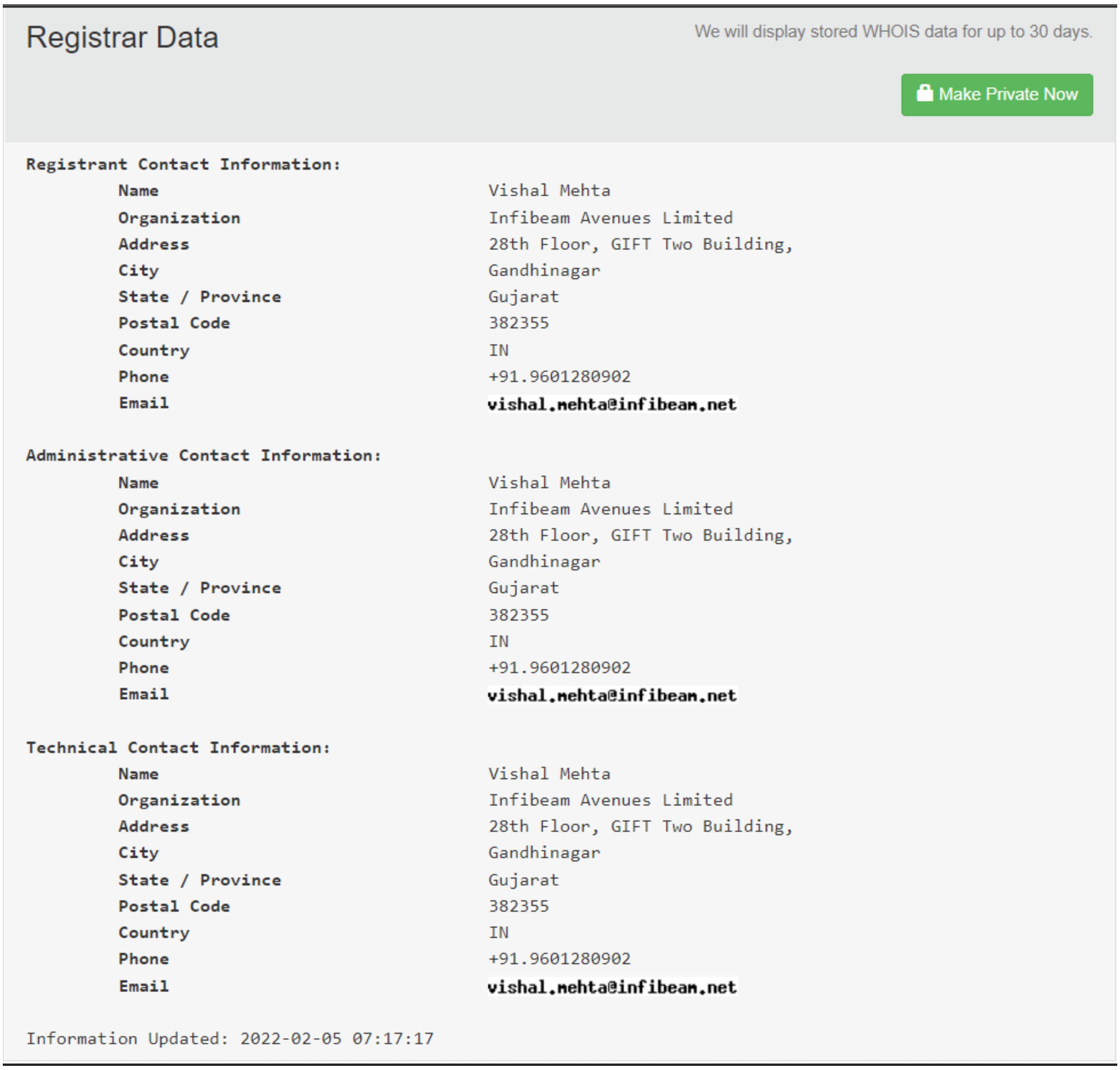
Expires On	2022-07-19
Registered On	2018-07-19
Updated On	2021-06-04

Name Servers

sid.ns.cloudflare.com	108.162.193.143
tess.ns.cloudflare.com	172.64.32.227

Similar Domains

ia.ooo |



Registrar Data

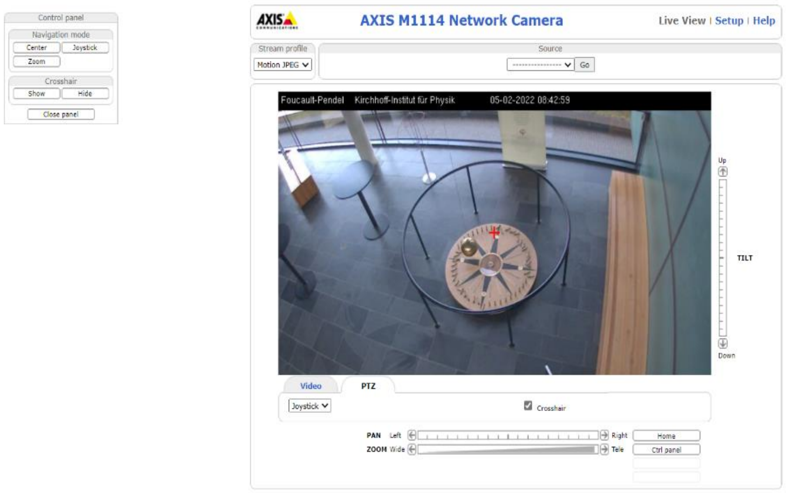
We will display stored WHOIS data for up to 30 days.

```
Registrant Contact Information:
        Name                            Vishal Mehta
        Organization                    Infibeam Avenues Limited
        Address                         28th Floor, GIFT Two Building,
        City                            Gandhinagar
        State / Province                Gujarat
        Postal Code                     382355
        Country                         IN
        Phone                           +91.9601280902
        Email                           vishal.mehta@infibeam.net

Administrative Contact Information:
        Name                            Vishal Mehta
        Organization                    Infibeam Avenues Limited
        Address                         28th Floor, GIFT Two Building,
        City                            Gandhinagar
        State / Province                Gujarat
        Postal Code                     382355
        Country                         IN
        Phone                           +91.9601280902
        Email                           vishal.mehta@infibeam.net

Technical Contact Information:
        Name                            Vishal Mehta
        Organization                    Infibeam Avenues Limited
        Address                         28th Floor, GIFT Two Building,
        City                            Gandhinagar
        State / Province                Gujarat
        Postal Code                     382355
        Country                         IN
        Phone                           +91.9601280902
        Email                           vishal.mehta@infibeam.net

Information Updated: 2022-02-05 07:17:17
```

4) Explain Google hacking database

"Google hacking" involves using advanced operators in the Google search engine to locate specific errors of text within search results.

The Google Hacking Database (GHDB) is a categorized index of Internet search engine queries designed to uncover interesting, and usually sensitive, information made publicly available on the Internet. this information was never meant to be made public but due to any number of factors this information was linked in a web document that was crawled by a search engine which subsequently followed that link and indexed the sensitive information. It is Googling with specific search strings that can force Google to return a specific result.



5) **Specify the ways by which we can maximize the attacker's efforts to do footprinting.**
   1. Delete or De-activate old accounts
   2. Use footprinting techniques to identify vulnerabilities ind leaks in your application and fix them
   3. Use VPN
   4. Do not post sensitive information on social media.
   5. Keep passwords strong and change them regularly.

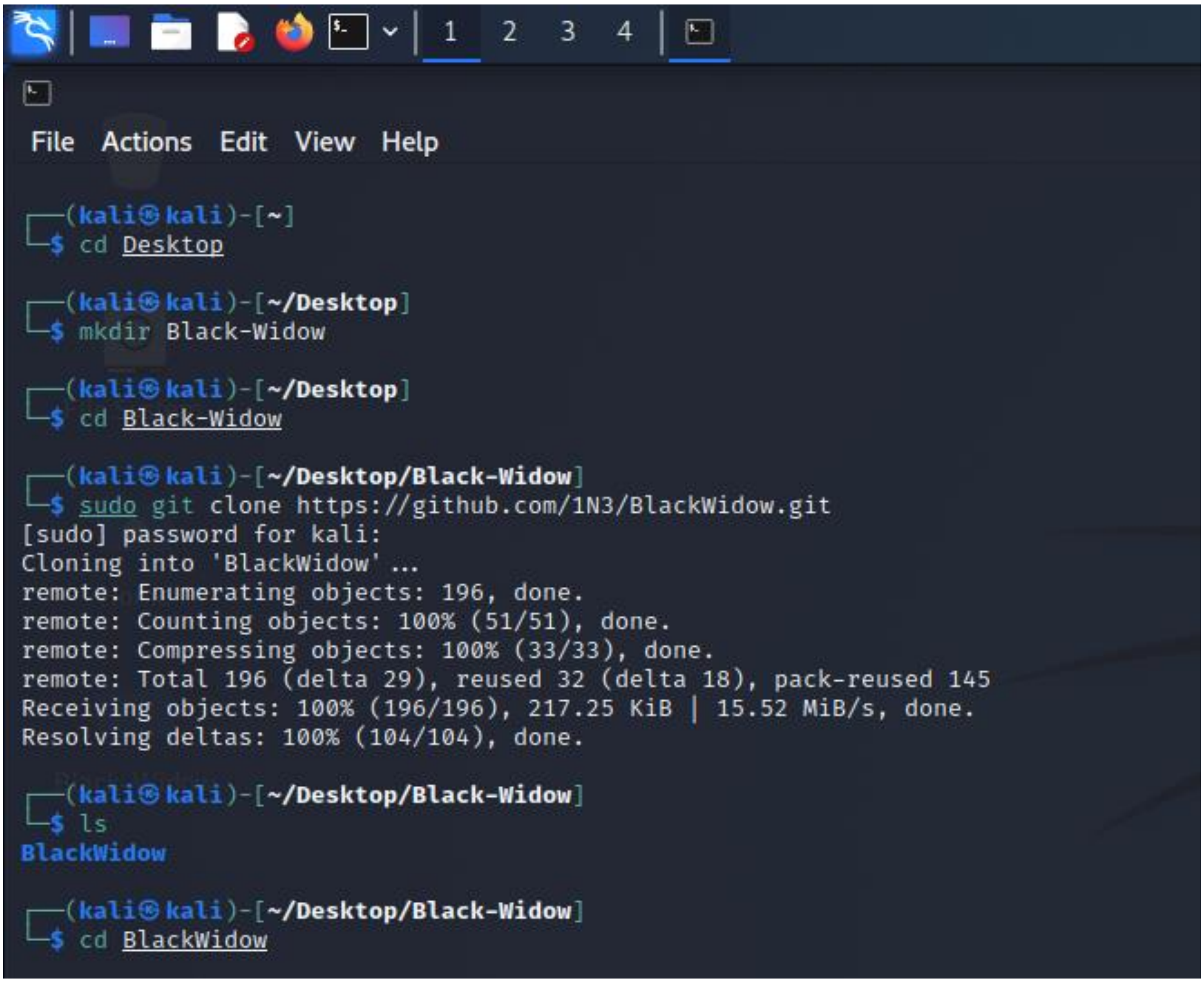
6) **Specify ways to avoid archive to snapshot the website.**

   To avoid snapshot capture by archieve.org, we just need to add a robot.txt file into our application. Add following two lines into robot.txt file

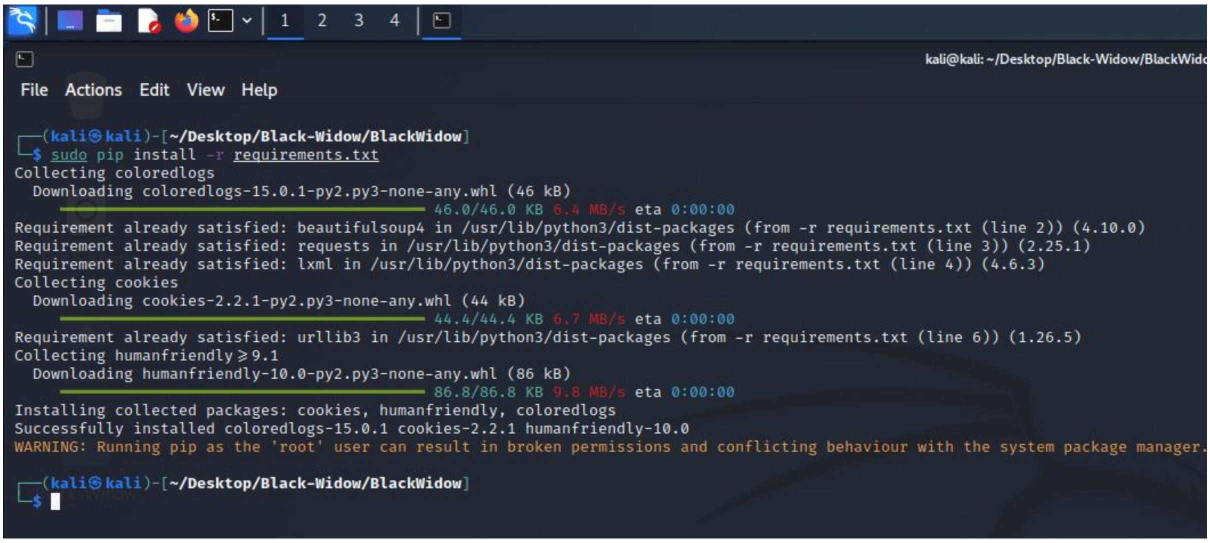
   ```
   User-agent: ia_archiver
   Disallow: /
   ```

   This file stops snapshot capturers and crawlers from archiving the site.

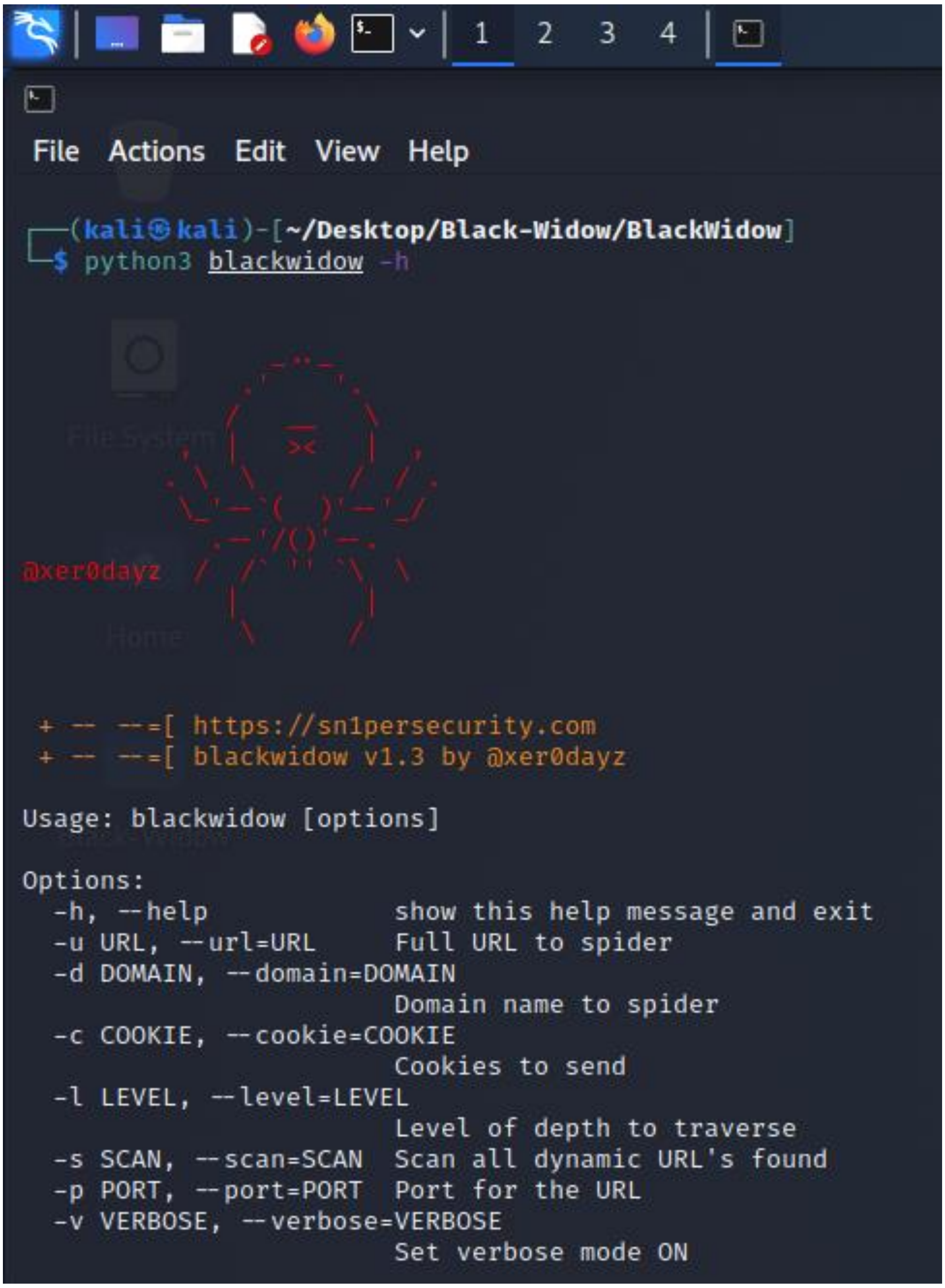
7) **Tried website footprinting tool black-widow.**



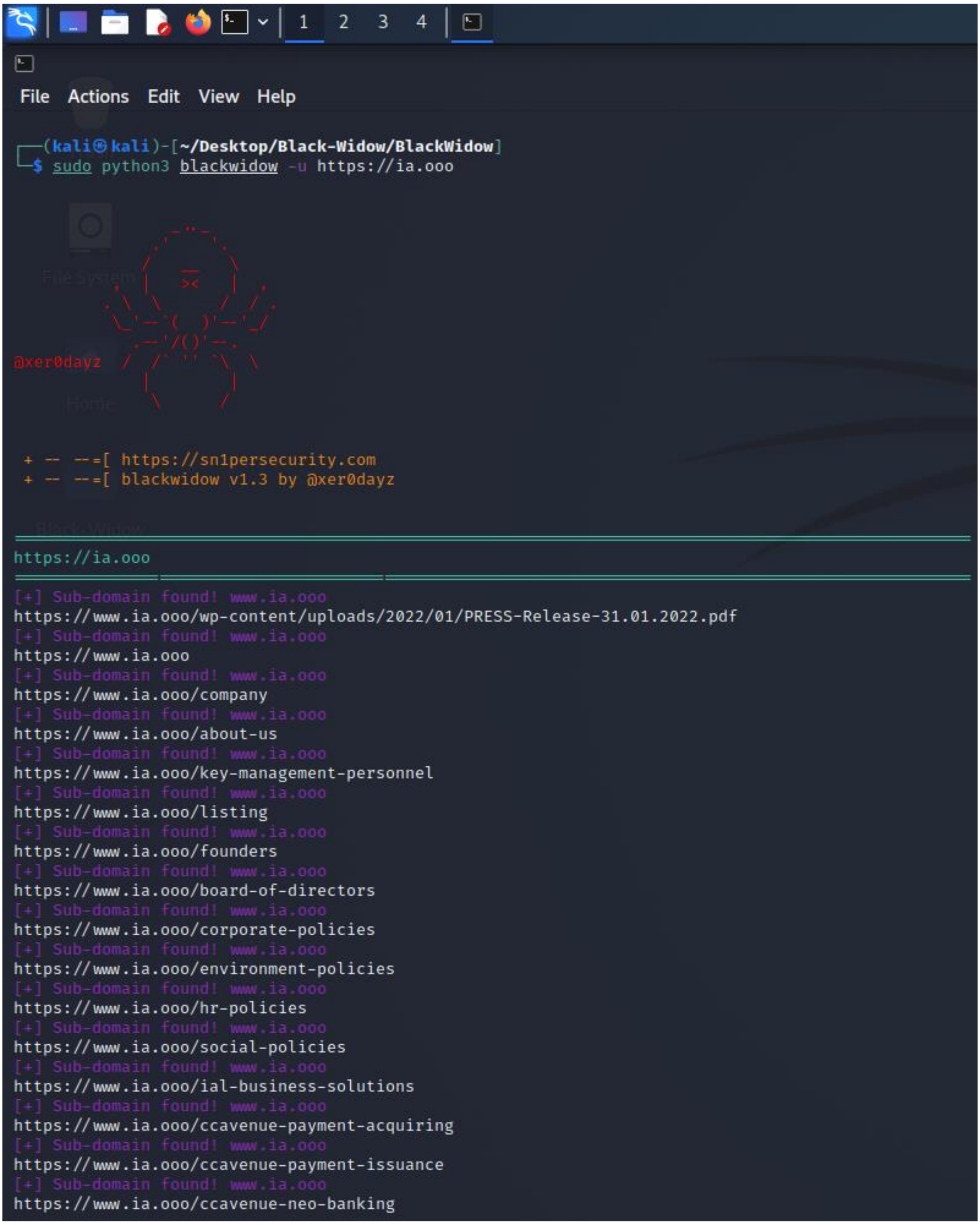
```
┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ mkdir Black-Widow

┌──(kali㉿kali)-[~/Desktop]
└─$ cd Black-Widow

┌──(kali㉿kali)-[~/Desktop/Black-Widow]
└─$ sudo git clone https://github.com/1N3/BlackWidow.git
[sudo] password for kali:
Cloning into 'BlackWidow' ...
remote: Enumerating objects: 196, done.
remote: Counting objects: 100% (51/51), done.
remote: Compressing objects: 100% (33/33), done.
remote: Total 196 (delta 29), reused 32 (delta 18), pack-reused 145
Receiving objects: 100% (196/196), 217.25 KiB | 15.52 MiB/s, done.
Resolving deltas: 100% (104/104), done.

┌──(kali㉿kali)-[~/Desktop/Black-Widow]
└─$ ls
BlackWidow

┌──(kali㉿kali)-[~/Desktop/Black-Widow]
└─$ cd BlackWidow
```


1 2 3 4
kali@kali: ~/Desktop/Black-Widow/BlackWid
File Actions Edit View Help

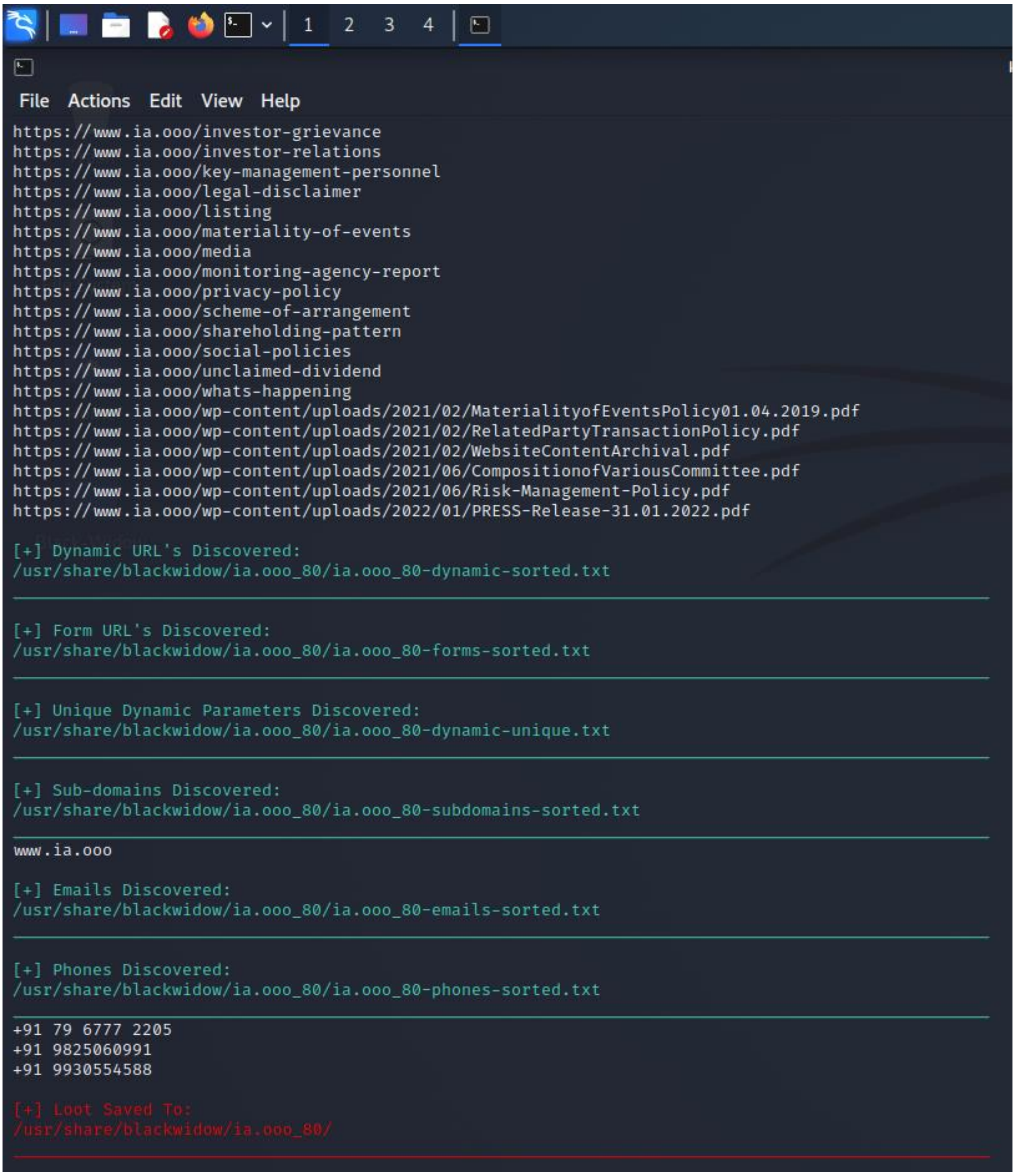
```
┌──(kali㉿kali)-[~/Desktop/Black-Widow/BlackWidow]
└─$ sudo pip install -r requirements.txt
Collecting coloredlogs
  Downloading coloredlogs-15.0.1-py2.py3-none-any.whl (46 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 46.0/46.0 KB 6.4 MB/s eta 0:00:00
Requirement already satisfied: beautifulsoup4 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 2)) (4.10.0)
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r requirements.txt (line 3)) (2.25.1)
Requirement already satisfied: lxml in /usr/lib/python3/dist-packages (from -r requirements.txt (line 4)) (4.6.3)
Collecting cookies
  Downloading cookies-2.2.1-py2.py3-none-any.whl (44 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 44.4/44.4 KB 6.7 MB/s eta 0:00:00
Requirement already satisfied: urllib3 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 6)) (1.26.5)
Collecting humanfriendly≥9.1
  Downloading humanfriendly-10.0-py2.py3-none-any.whl (86 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 86.8/86.8 KB 9.8 MB/s eta 0:00:00
Installing collected packages: cookies, humanfriendly, coloredlogs
Successfully installed coloredlogs-15.0.1 cookies-2.2.1 humanfriendly-10.0
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system package manager.

┌──(kali㉿kali)-[~/Desktop/Black-Widow/BlackWidow]
└─$ █
```



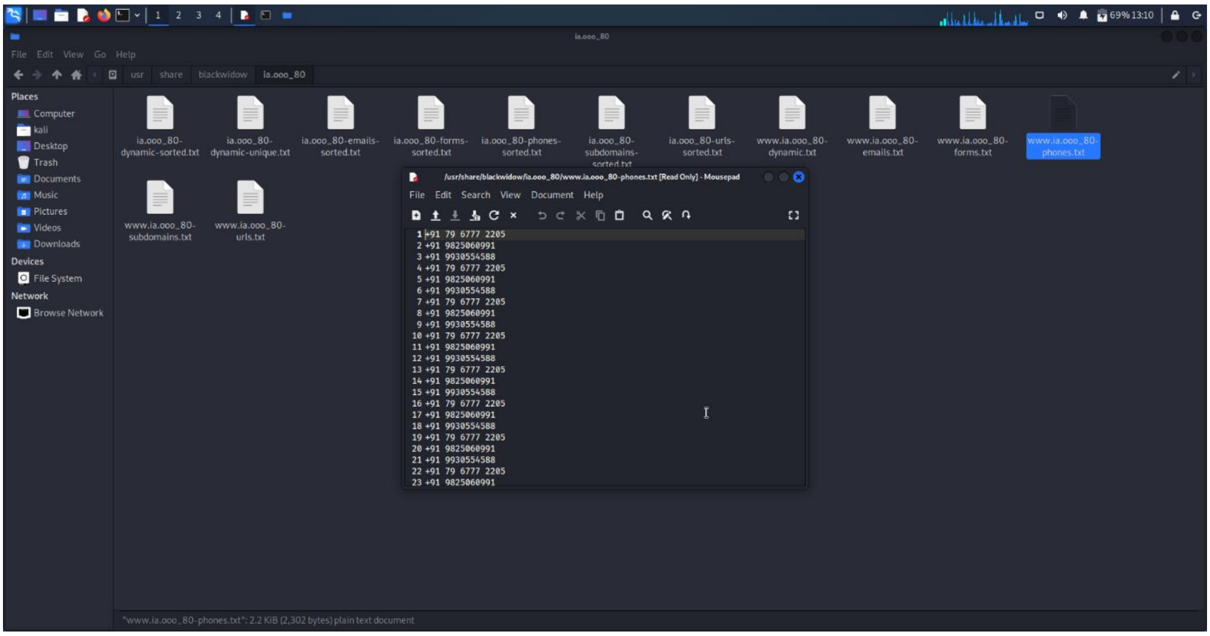
```
┌──(kali㉿kali)-[~/Desktop/Black-Widow/BlackWidow]
└─$ python3 blackwidow -h

@xer0dayz

 + -- --=[ https://sn1persecurity.com
 + -- --=[ blackwidow v1.3 by @xer0dayz

Usage: blackwidow [options]

Options:
  -h, --help            show this help message and exit
  -u URL, --url=URL     Full URL to spider
  -d DOMAIN, --domain=DOMAIN
                        Domain name to spider
  -c COOKIE, --cookie=COOKIE
                        Cookies to send
  -l LEVEL, --level=LEVEL
                        Level of depth to traverse
  -s SCAN, --scan=SCAN  Scan all dynamic URL's found
  -p PORT, --port=PORT  Port for the URL
  -v VERBOSE, --verbose=VERBOSE
                        Set verbose mode ON
```



```
┌──(kali㉿kali)-[~/Desktop/Black-Widow/BlackWidow]
└─$ sudo python3 blackwidow -u https://ia.ooo


                 _.''._
               .'      '.
              /          \
             |    _      |
         ,   |    ><     |   ,
       .  \   \         /   /  .
          \_'--`(     )'--'_/
            .--'/()'--.
@xer0dayz  /   /`  ''  `\   \
              |          |
               \        /


 + -- --=[ https://sn1persecurity.com
 + -- --=[ blackwidow v1.3 by @xer0dayz


════════════════════════════════════════════════════════════════════════════════
https://ia.ooo
════════════════════════════════════════════════════════════════════════════════
[+] Sub-domain found! www.ia.ooo
https://www.ia.ooo/wp-content/uploads/2022/01/PRESS-Release-31.01.2022.pdf
[+] Sub-domain found! www.ia.ooo
https://www.ia.ooo
[+] Sub-domain found! www.ia.ooo
https://www.ia.ooo/company
[+] Sub-domain found! www.ia.ooo
https://www.ia.ooo/about-us
[+] Sub-domain found! www.ia.ooo
https://www.ia.ooo/key-management-personnel
[+] Sub-domain found! www.ia.ooo
https://www.ia.ooo/listing
[+] Sub-domain found! www.ia.ooo
https://www.ia.ooo/founders
[+] Sub-domain found! www.ia.ooo
https://www.ia.ooo/board-of-directors
[+] Sub-domain found! www.ia.ooo
https://www.ia.ooo/corporate-policies
[+] Sub-domain found! www.ia.ooo
https://www.ia.ooo/environment-policies
[+] Sub-domain found! www.ia.ooo
https://www.ia.ooo/hr-policies
[+] Sub-domain found! www.ia.ooo
https://www.ia.ooo/social-policies
[+] Sub-domain found! www.ia.ooo
https://www.ia.ooo/ial-business-solutions
[+] Sub-domain found! www.ia.ooo
https://www.ia.ooo/ccavenue-payment-acquiring
[+] Sub-domain found! www.ia.ooo
https://www.ia.ooo/ccavenue-payment-issuance
[+] Sub-domain found! www.ia.ooo
https://www.ia.ooo/ccavenue-neo-banking
```



```
https://www.ia.ooo/investor-grievance
https://www.ia.ooo/investor-relations
https://www.ia.ooo/key-management-personnel
https://www.ia.ooo/legal-disclaimer
https://www.ia.ooo/listing
https://www.ia.ooo/materiality-of-events
https://www.ia.ooo/media
https://www.ia.ooo/monitoring-agency-report
https://www.ia.ooo/privacy-policy
https://www.ia.ooo/scheme-of-arrangement
https://www.ia.ooo/shareholding-pattern
https://www.ia.ooo/social-policies
https://www.ia.ooo/unclaimed-dividend
https://www.ia.ooo/whats-happening
https://www.ia.ooo/wp-content/uploads/2021/02/MaterialityofEventsPolicy01.04.2019.pdf
https://www.ia.ooo/wp-content/uploads/2021/02/RelatedPartyTransactionPolicy.pdf
https://www.ia.ooo/wp-content/uploads/2021/02/WebsiteContentArchival.pdf
https://www.ia.ooo/wp-content/uploads/2021/06/CompositionofVariousCommittee.pdf
https://www.ia.ooo/wp-content/uploads/2021/06/Risk-Management-Policy.pdf
https://www.ia.ooo/wp-content/uploads/2022/01/PRESS-Release-31.01.2022.pdf

[+] Dynamic URL's Discovered:
/usr/share/blackwidow/ia.ooo_80/ia.ooo_80-dynamic-sorted.txt
_______________________________________________________________________________

[+] Form URL's Discovered:
/usr/share/blackwidow/ia.ooo_80/ia.ooo_80-forms-sorted.txt
_______________________________________________________________________________

[+] Unique Dynamic Parameters Discovered:
/usr/share/blackwidow/ia.ooo_80/ia.ooo_80-dynamic-unique.txt
_______________________________________________________________________________

[+] Sub-domains Discovered:
/usr/share/blackwidow/ia.ooo_80/ia.ooo_80-subdomains-sorted.txt
_______________________________________________________________________________
www.ia.ooo

[+] Emails Discovered:
/usr/share/blackwidow/ia.ooo_80/ia.ooo_80-emails-sorted.txt
_______________________________________________________________________________

[+] Phones Discovered:
/usr/share/blackwidow/ia.ooo_80/ia.ooo_80-phones-sorted.txt
_______________________________________________________________________________
+91 79 6777 2205
+91 9825060991
+91 9930554588

[+] Loot Saved To:
/usr/share/blackwidow/ia.ooo_80/
_______________________________________________________________________________
```


ia.ooo_80
File Edit View Go Help
usr share blackwidow ia.ooo_80
Places
Computer
kali
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
ia.ooo_80-dynamic-sorted.txt
ia.ooo_80-dynamic-unique.txt
ia.ooo_80-emails-sorted.txt
ia.ooo_80-forms-sorted.txt
ia.ooo_80-phones-sorted.txt
ia.ooo_80-subdomains-sorted.txt
ia.ooo_80-urls-sorted.txt
www.ia.ooo_80-dynamic.txt
www.ia.ooo_80-emails.txt
www.ia.ooo_80-forms.txt
www.ia.ooo_80-phones.txt
www.ia.ooo_80-subdomains.txt
www.ia.ooo_80-urls.txt
/usr/share/blackwidow/ia.ooo_80/www.ia.ooo_80-phones.txt [Read Only] - Mousepad
File Edit Search View Document Help
69% 13:10

```
+91 79 6777 2205
+91 9825060991
+91 9930554588
+91 79 6777 2205
+91 9825060991
+91 9930554588
+91 79 6777 2205
+91 9825060991
+91 9930554588
+91 79 6777 2205
+91 9825060991
+91 9930554588
+91 79 6777 2205
+91 9825060991
+91 9930554588
+91 79 6777 2205
+91 9825060991
+91 9930554588
+91 79 6777 2205
+91 9825060991
+91 9930554588
+91 79 6777 2205
+91 9825060991
```

"www.ia.ooo_80-phones.txt": 2.2 KiB (2,302 bytes) plain text document

Conclusion:

Foot printing helps to get sensitive information of target through different means. Foot printing is first and most important step of any attack. Nearly 90% of time is invested in footprinting.

I tried black widow website foot printing tool. The tool parsed through all the URLs of the site and collected information that might be sensitive for the owner. It collected all the phone numbers, documents, dynamic URLs, subdomains, etc. and stored it into respective files.