



Department of
Bachelor of Computer Applications

Ethical Hacking Fundamentals
Lab File – CA 01

Subject Code: 19BCA4C02L
Class: IInd Year IInd Semester

Prepared By:
Suman Garai
20BCAR0246

Aim :

The objective of this practical is to learn the basics of Footprinting methodologies, used for ethical hackers and pen testers.

Requirements :

- Virtualisation Software
- Kali Linux 2021.4a
- Basics of networking

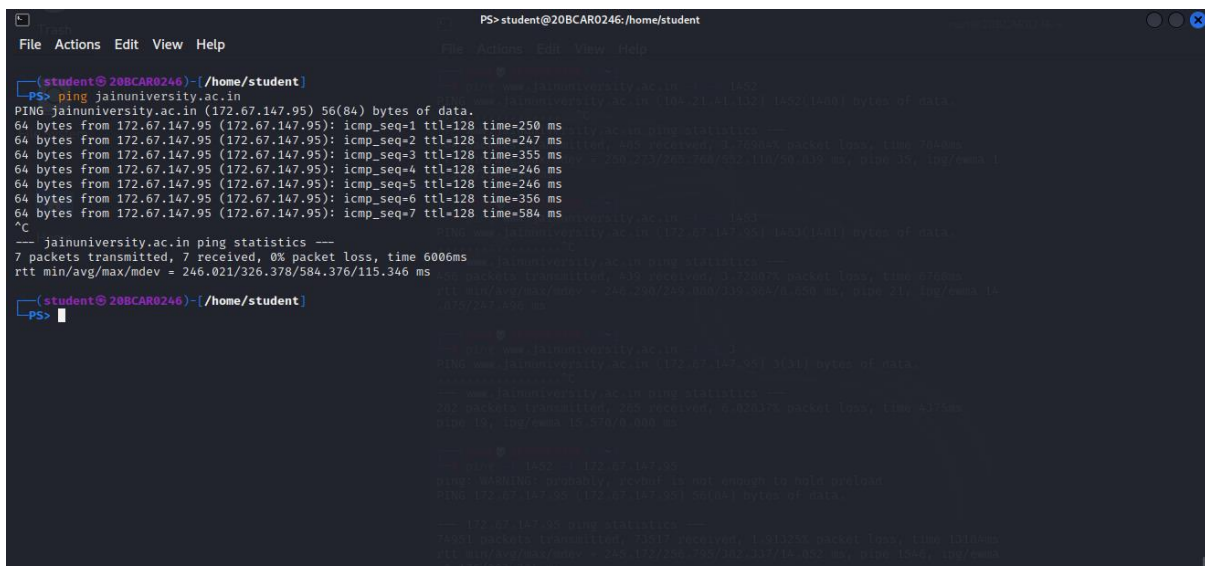
Objectives :

- ✓ Find IP address of target domain using ping command.
- ✓ Emulate traceroute of the domain.
- ✓ Discover Maximum frame size (MTU) for the domain.
- ✓ Find Time To Live (TTL) of the domain.
- ✓ Non-Authoritative Name Server of the domain.
- ✓ Use Google Hacking Keywords and Netcraft.

Procedure :

Finding IP Using Ping

- 1> After logging into kali linux virtual machine, head over to taskbar present on the top and open powershell from the terminal drop-down.
- 2> Type the syntax: ping [website]. For ex.: jainuniversity.ac.in
- 3> After few seconds, press Ctrl + C to obtain the final result, which should somewhat look like the following.

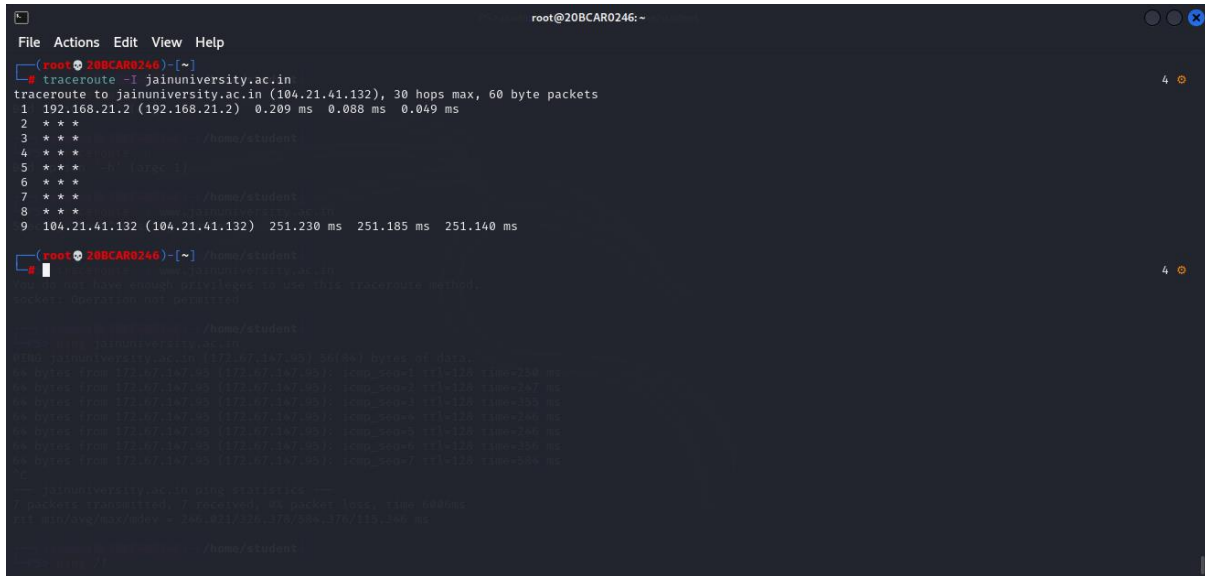


```
PS> student@20BCAR0246:/home/student
File Actions Edit View Help
(student@20BCAR0246)-[/home/student]
PS> ping jainuniversity.ac.in
PING jainuniversity.ac.in (172.67.147.95) 56(84) bytes of data:
64 bytes from 172.67.147.95 (172.67.147.95): icmp_seq=1 ttl=128 time=250 ms
64 bytes from 172.67.147.95 (172.67.147.95): icmp_seq=2 ttl=128 time=247 ms
64 bytes from 172.67.147.95 (172.67.147.95): icmp_seq=3 ttl=128 time=355 ms
64 bytes from 172.67.147.95 (172.67.147.95): icmp_seq=4 ttl=128 time=246 ms
64 bytes from 172.67.147.95 (172.67.147.95): icmp_seq=5 ttl=128 time=246 ms
64 bytes from 172.67.147.95 (172.67.147.95): icmp_seq=6 ttl=128 time=356 ms
64 bytes from 172.67.147.95 (172.67.147.95): icmp_seq=7 ttl=128 time=584 ms
^C
-- jainuniversity.ac.in ping statistics --
7 packets transmitted, 7 received, 0% packet loss, time 6006ms
rtt min/avg/max/mdev = 246.021/326.378/584.376/115.346 ms
(student@20BCAR0246)-[/home/student]
PS>
```

As we can see, 172.67.147.95 is the required IPv4. Other than that, a lot of other information provided too like packet size, round time of responding the request etc.

Using traceroute command

- 1> Head over to taskbar present on the top and open root terminal emulator from the terminal drop-down.
- 2> Type the syntax: `traceroute -I [website]`. For ex.: `jainuniversity.ac.in`
The '-I' is essential, since it uses ICMP and UDP can't obtain final result.
- 3> It will automatically run for few loops and stop. The final result should look something like this.



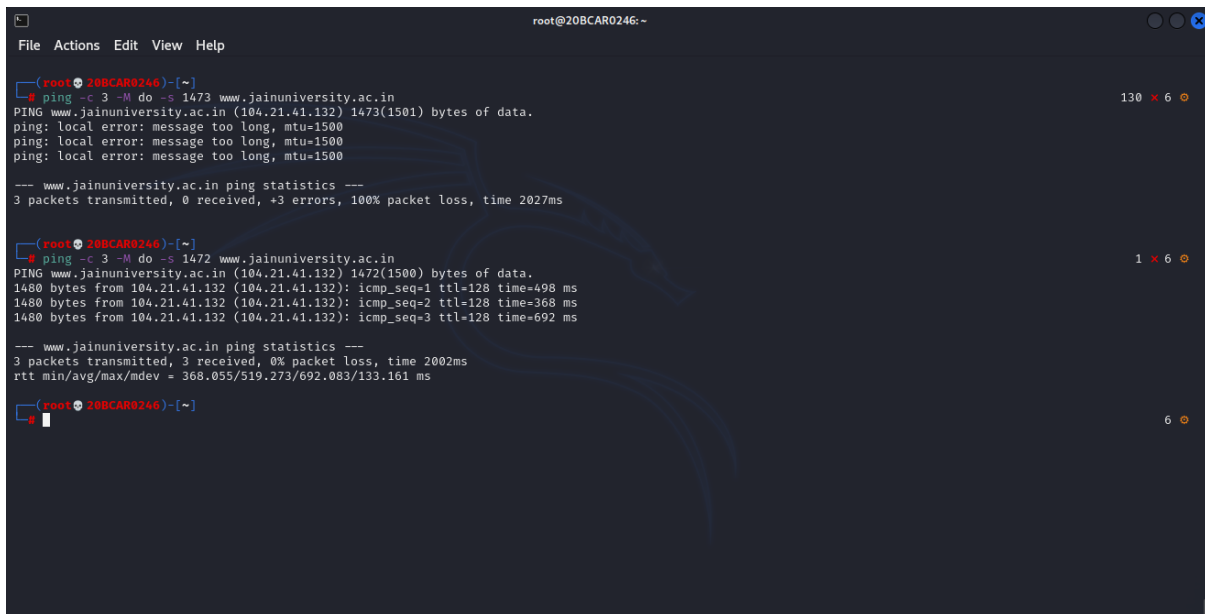
```
root@20BCAR0246: ~  
File Actions Edit View Help  
root@20BCAR0246: ~  
# traceroute -I jainuniversity.ac.in  
traceroute to jainuniversity.ac.in (104.21.41.132), 30 hops max, 60 byte packets  
1 192.168.21.2 (192.168.21.2) 0.209 ms 0.088 ms 0.049 ms  
2 * * *  
3 * * *  
4 * * *  
5 * * *  
6 * * *  
7 * * *  
8 * * *  
9 104.21.41.132 (104.21.41.132) 251.230 ms 251.185 ms 251.140 ms  
root@20BCAR0246: ~  
#
```

As we can see, 104.21.41.132 in the final destination we entered. In between, the details of the route are asterisked, due to security reasons, which can be viewed in Windows devices.

NOTE: Syntax: `traceroute --help`, can be used to discover additional functionalities of the command.

Discovering Maximum Frame Size of the Domain

- 1> In the root terminal emulator, use the following syntax: `ping -c [value] -M do -s [value] [website]`, where `-c` stands for times, response is needed and `-s` stands for size of data bytes to be sent.
- 2> Try this command with multiple `-s` values until the objective is fulfilled.



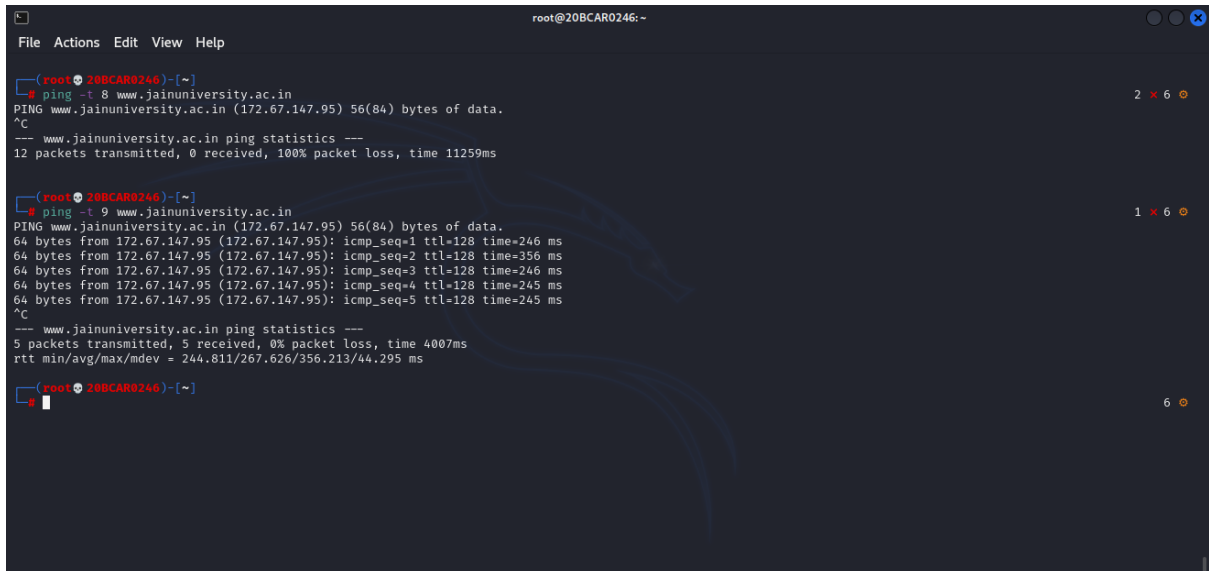
```
root@20BCAR0246: ~  
File Actions Edit View Help  
root@20BCAR0246:~  
# ping -c 3 -M do -s 1473 www.jainuniversity.ac.in  
PING www.jainuniversity.ac.in (104.21.41.132) 1473(1501) bytes of data.  
ping: local error: message too long, mtu=1500  
ping: local error: message too long, mtu=1500  
ping: local error: message too long, mtu=1500  
--- www.jainuniversity.ac.in ping statistics ---  
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2027ms  
  
root@20BCAR0246:~  
# ping -c 3 -M do -s 1472 www.jainuniversity.ac.in  
PING www.jainuniversity.ac.in (104.21.41.132) 1472(1500) bytes of data.  
1480 bytes from 104.21.41.132 (104.21.41.132): icmp_seq=1 ttl=128 time=498 ms  
1480 bytes from 104.21.41.132 (104.21.41.132): icmp_seq=2 ttl=128 time=368 ms  
1480 bytes from 104.21.41.132 (104.21.41.132): icmp_seq=3 ttl=128 time=692 ms  
--- www.jainuniversity.ac.in ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2002ms  
rtt min/avg/max/mdev = 368.055/519.273/692.083/133.161 ms  
root@20BCAR0246:~
```

As we can see, 1473 gives error message, therefore we can conclude, 1472 bytes as the maximum frame size.

NOTE: Syntax: `ping -help`, can be used to discover additional functionalities of the command.

Finding TTL of the Domain

- 1> In the root terminal emulator, use the following syntax: `ping -t [value] [website]`, where `-t` stands for TTL definition.
- 2> Try this command with multiple `-t` values until the objective is fulfilled.



```
root@20BCAR0246: ~  
File Actions Edit View Help  
  
(root@20BCAR0246)~  
# ping -t 8 www.jainuniversity.ac.in  
PING www.jainuniversity.ac.in (172.67.147.95) 56(84) bytes of data.  
^C  
--- www.jainuniversity.ac.in ping statistics ---  
12 packets transmitted, 0 received, 100% packet loss, time 11259ms  
  
(root@20BCAR0246)~  
# ping -t 9 www.jainuniversity.ac.in  
PING www.jainuniversity.ac.in (172.67.147.95) 56(84) bytes of data.  
64 bytes from 172.67.147.95 (172.67.147.95): icmp_seq=1 ttl=128 time=246 ms  
64 bytes from 172.67.147.95 (172.67.147.95): icmp_seq=2 ttl=128 time=356 ms  
64 bytes from 172.67.147.95 (172.67.147.95): icmp_seq=3 ttl=128 time=246 ms  
64 bytes from 172.67.147.95 (172.67.147.95): icmp_seq=4 ttl=128 time=245 ms  
64 bytes from 172.67.147.95 (172.67.147.95): icmp_seq=5 ttl=128 time=245 ms  
^C  
--- www.jainuniversity.ac.in ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4007ms  
rtt min/avg/max/mdev = 244.811/267.626/356.213/44.295 ms  
  
(root@20BCAR0246)~  
#
```

As we can see, 8 doesn't have responses, therefore we can conclude, 9 as the TTL.

Non-Authoritative Name Server of the domain

1> In the root terminal emulator, use the following syntax: nslookup ↵ set type=ns ↵ [website], where ns stands for name server.

```
File Actions Edit View Help
root@20BCAR0246:~# nslookup
> set type=ns
> jainuniversity.ac.in
addlookup()
name_empty_lookup()
name_empty_lookup() = 0x7f9a5d000000-references = 1
looking up jainuniversity.ac.in
start_lookup()
setup_lookup(0x7f9a5d000000)
resetting lookup counter.
cloning server list
clone_server_list()
name_server(192.168.21.2)
idn_textname: jainuniversity.ac.in
using root 0x0
recursive query
add_question()
starting to render the message
done rendering
create query 0x7f9a5d03e000 linked to lookup 0x7f9a5d000000
digest.c:2083:lookup_attach(0x7f9a5d03e000) = 2
digest.c:2587:new_query(0x7f9a5d03e000) = 1
do_lookup()
start_wup(0x7f9a5d03e000)
digest.c:2923:query_attach(0x7f9a5d03e000) = 2
working on lookup 0x7f9a5d03e000, query 0x7f9a5d03e000
digest.c:2981:query_attach(0x7f9a5d03e000) = 3
digest.c:2099:query_attach(0x7f9a5d03e000) = 4
receiving with lookup 0x7f9a5d000000, query 0x7f9a5d03e000, handle=(nil)
received()
have local timeout of 5000
digest.c:2264:query_attach(0x7f9a5d03e000) = 5
sending a request
sendcount()
digest.c:1576:query_detach(0x7f9a5d03e000) = 4
digest.c:2519:query_detach(0x7f9a5d03e000) = 3
recv_done(0x7f9a5d03e000, timed out, 0x7f9a5d0f0340, 0x7f9a5d03e000)
lock_lookup digest.c:3579
Success
received()
digest.c:3591:lookup_attach(0x7f9a5d000000) = 3
resolving IP request to first server, 2 tries left
create query 0x7f9a5d03e1c0 linked to lookup 0x7f9a5d000000
digest.c:2083:lookup_attach(0x7f9a5d03e1c0) = 4
digest.c:2640:new_query(0x7f9a5d03e1c0) = 1
start_wup(0x7f9a5d03e1c0)
digest.c:2923:query_attach(0x7f9a5d03e1c0) = 2
working on lookup 0x7f9a5d03e1c0, query 0x7f9a5d03e1c0
digest.c:2981:query_attach(0x7f9a5d03e1c0) = 3
digest.c:4081:lookup_detach(0x7f9a5d03e000) = 2
digest.c:4089:lookup_detach(0x7f9a5d03e000) = 3
unlock_lookup digest.c:4092
send_done(0x7f9a5d03e000, success, 0x7f9a5d03e000)

148 digest.c:2616:query_detach(0x7f9a5d03e1c0) = 4
digest.c:2519:query_detach(0x7f9a5d03e1c0) = 3
send_done(0x7f9a5d03e1c0, success, 0x7f9a5d03e1c0)
sendcount()
lock_lookup digest.c:2615
Success
digest.c:2629:lookup_attach(0x7f9a5d03e000) = 4
digest.c:2648:query_detach(0x7f9a5d03e1c0) = 2
digest.c:2649:lookup_detach(0x7f9a5d03e1c0) = 3
check_if_done()
list_empty
unlock_lookup digest.c:2652
recv_done(0x7f9a5d03e1c0, success, 0x7f9a5d07a020, 0x7f9a5d03e1c0)
lock_lookup digest.c:3579
Success
received()
digest.c:3591:lookup_attach(0x7f9a5d03e000) = 4
Before parse starts
after parse
printmessage()
Server: 192.168.21.2
Address: 192.168.21.2853

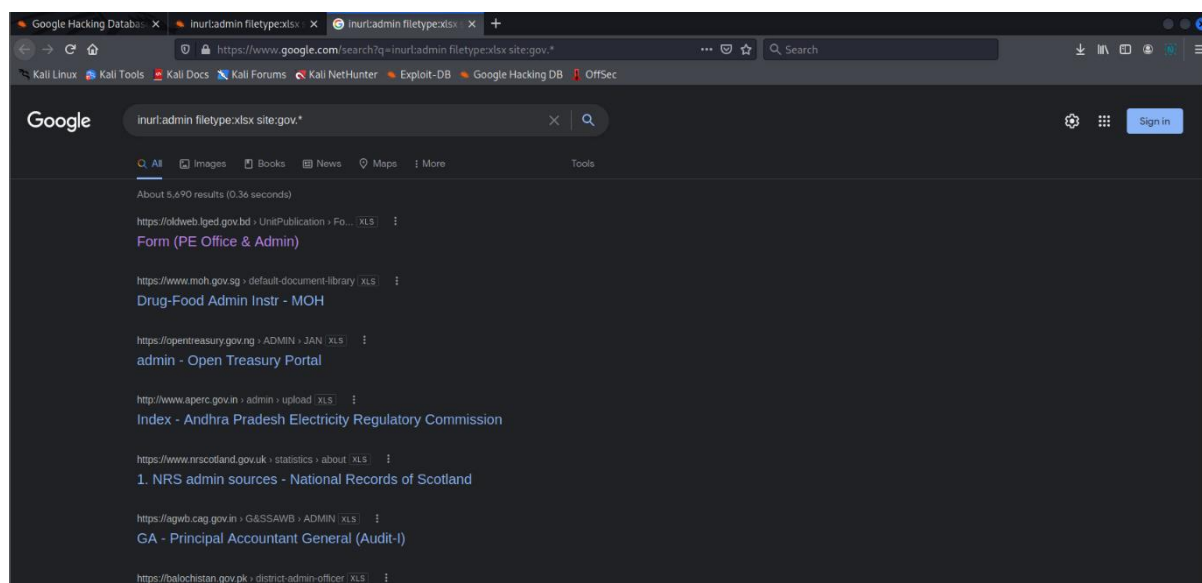
Non-authoritative answer:
printsection()
jainuniversity.ac.in nameserver = mia.ns.cloudflare.com.
jainuniversity.ac.in nameserver = paul.ns.cloudflare.com.

Authoritative answers can be found from:
printsection()
printsection()
Still pending.
digest.c:4083:cancel_lookup()
digest.c:2660:query_detach(0x7f9a5d03e1c0) = 0
digest.c:2659:destroy_query(0x7f9a5d03e1c0) = 0
digest.c:1831:lookup_detach(0x7f9a5d03e000) = 3
digest.c:2669:query_detach(0x7f9a5d03e000) = 0
digest.c:2669:destroy_query(0x7f9a5d03e000) = 0
digest.c:1831:lookup_detach(0x7f9a5d03e000) = 2
check_if_done()
list_empty
digest.c:4089:lookup_detach(0x7f9a5d03e000) = 1
clear_current_lookup()
digest.c:1970:lookup_detach(0x7f9a5d03e000) = 0
destroy_lookup
Freeing server 0x7f9a5d03e000 belonging to 0x7f9a5d03e000
start_lookup()
check_if_done()
list_empty
shutting down
digest_shutdown()
unlock_lookup digest.c:4092
```

As we can see, mia and paul.ns.cloudflare.com denoted as the name server on the second half of the screen, we can conclude getting the required result.

Google Hacking

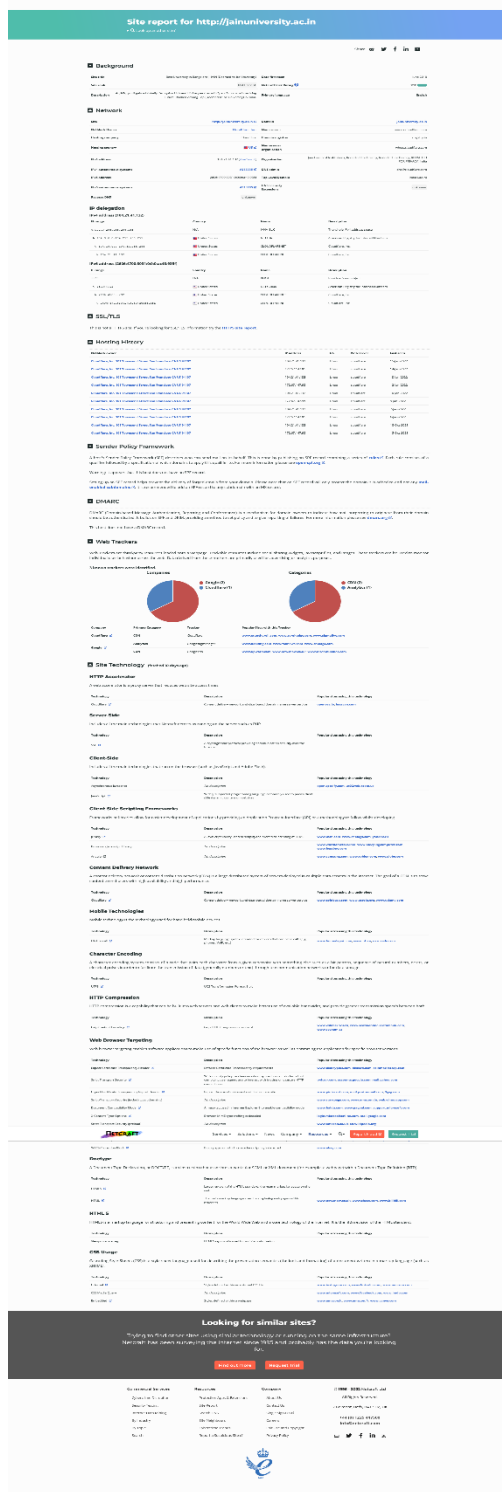
- 1> Head over to <https://www.google.com> and use keywords like inurl, intitle, filetype, site, etc. to find information that generally doesn't show up while searching.



As we can see, according to the keywords, a lot of excel sheets have appeared which normally doesn't show up while searching.

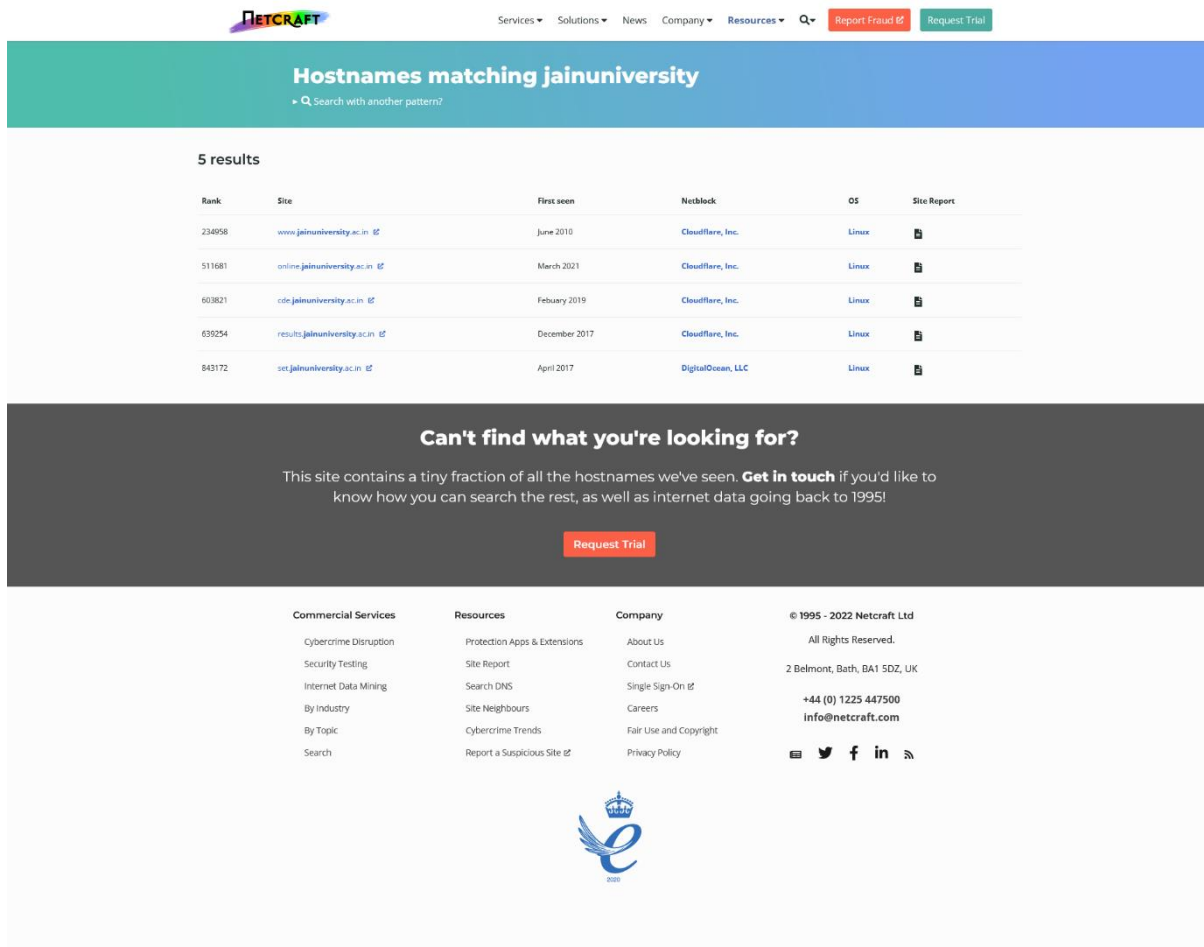
NOTE: Sites like <https://www.exploit-db.com/google-hacking-database> can be used to search for active exploits from databases.

- 1> Google search 'Netcraft' or head over to <https://www.netcraft.com>.
- 2> From the top ribbon hover mouse cursor over 'Resources' Tab and then from the drop down menu click on 'Tools' option.
- 3> Three prominent tools present under Internet Research Tools, Site report, Site DNS, Site neighbours, can be used to obtain different results, as follows.



As we can see, 'What's that site running' gives us details about IP Addresses, domains, hosting, site security & technology etc.

As we can see, 'Search Web by DNS' gives us details about URL's containing the keywords provided during the search.



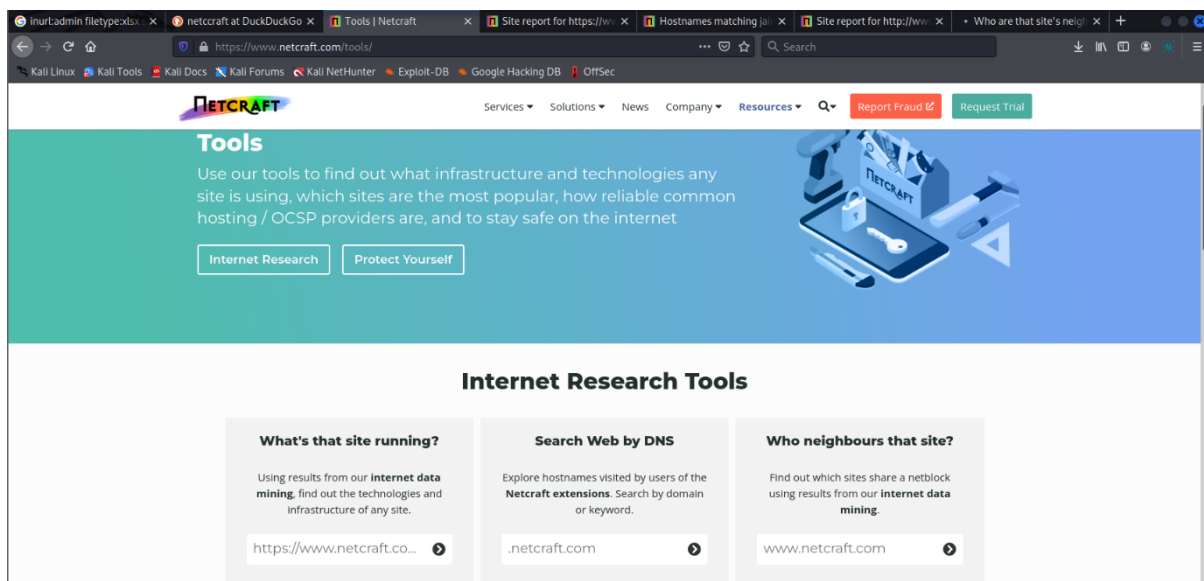
The screenshot shows the Netcraft website interface. At the top, there's a navigation bar with links for Services, Solutions, News, Company, Resources, and buttons for 'Report Fraud' and 'Request Trial'. The main heading is 'Hostnames matching jainuniversity' with a sub-link 'Search with another pattern?'. Below this, it says '5 results' and displays a table of search results.

Rank	Site	First seen	Netblock	OS	Site Report
234958	www.jainuniversity.ac.in	June 2010	Cloudflare, Inc.	Linux	Report
511681	online.jainuniversity.ac.in	March 2021	Cloudflare, Inc.	Linux	Report
603821	cde.jainuniversity.ac.in	February 2019	Cloudflare, Inc.	Linux	Report
635254	results.jainuniversity.ac.in	December 2017	Cloudflare, Inc.	Linux	Report
843172	net.jainuniversity.ac.in	April 2017	DigitalOcean, LLC	Linux	Report

Below the table, there's a section titled 'Can't find what you're looking for?' with a message: 'This site contains a tiny fraction of all the hostnames we've seen. **Get in touch** if you'd like to know how you can search the rest, as well as internet data going back to 1995!' and a 'Request Trial' button.

The footer contains four columns of links: Commercial Services (Cybercrime Disruption, Security Testing, Internet Data Mining, By Industry, By Topic, Search), Resources (Protection Apps & Extensions, Site Report, Search DNS, Site Neighbours, Cybercrime Trends, Report a Suspicious Site), Company (About Us, Contact Us, Single Sign-On, Careers, Fair Use and Copyright, Privacy Policy), and contact information (© 1995 - 2022 Netcraft Ltd, All Rights Reserved, 2 Belmont, Bath, BA1 5DZ, UK, +44 (0) 1225 447500, info@netcraft.com, and social media icons).

The screen below is of the site's tools to be used for fulfilling this objective.



The screenshot shows the 'Tools' section of the Netcraft website. The header says 'Tools' and describes the purpose: 'Use our tools to find out what infrastructure and technologies any site is using, which sites are the most popular, how reliable common hosting / OCSP providers are, and to stay safe on the internet'. There are two buttons: 'Internet Research' and 'Protect Yourself'.

Below this, there's a section titled 'Internet Research Tools' with three sub-sections:

- What's that site running?**: Using results from our **Internet data mining**, find out the technologies and infrastructure of any site. Input: `https://www.netcraft.com...`
- Search Web by DNS**: Explore hostnames visited by users of the **Netcraft extensions**. Search by domain or keyword. Input: `.netcraft.com`
- Who neighbours that site?**: Find out which sites share a netblock using results from our **Internet data mining**. Input: `www.netcraft.com`

As we can see, 'Who neighbours the site?' gives us details about the site connected with the provided URL during search.

Netcraft Services Solutions News Company Resources Report Fraud Request Trial

Lookup neighbours of another site?

421 results (showing 1 to 20)

Rank	Site	First Seen	Webserver	OS	Site Report / Search DNS
-	www.bigtimebrewery.com	November 1996	GitHub.com	Unknown	Site Report / Search DNS
-	brandx.com	November 2021	GitHub.com	Unknown	Site Report / Search DNS
-	healthblocks.com	November 2014	GitHub.com	Unknown	Site Report / Search DNS
-	microsearch.net	September 2014	GitHub.com	Unknown	Site Report / Search DNS
43355	stellarium.org	June 2006	GitHub.com	Unknown	Site Report / Search DNS
523559	lsthain.com	February 2017	GitHub.com	Unknown	Site Report / Search DNS
30762	www.android.x86.org	October 2009	GitHub.com	Unknown	Site Report / Search DNS
-	taya.ru	May 2020	GitHub.com	Unknown	Site Report / Search DNS
358057	help.github.com	July 2012	Cowboy	Unknown	Site Report / Search DNS
48841	jekyllrb.com	October 2015	GitHub.com	Unknown	Site Report / Search DNS
14902	angryip.org	January 2010	GitHub.com	Unknown	Site Report / Search DNS
-	wafic.net	March 2008	GitHub.com	Unknown	Site Report / Search DNS
-	emahasympsonichorus.org	September 2018	GitHub.com	Unknown	Site Report / Search DNS
-	hackmanhattan.com	March 2012	GitHub.com	Unknown	Site Report / Search DNS
105440	tigerenc.org	January 2018	GitHub.com	Unknown	Site Report / Search DNS
275337	nvmc.com	March 2017	GitHub.com	Unknown	Site Report / Search DNS
143143	www.slimframework.com	January 2011	GitHub.com	Unknown	Site Report / Search DNS
-	ctf.milcon.net	December 2016	GitHub.com	Unknown	Site Report / Search DNS
1256499	github.io	July 2013	Varnish	Unknown	Site Report / Search DNS
43947	pymatu.com	October 2015	GitHub.com	Unknown	Site Report / Search DNS

Next Page

Commercial Services
 Cybercrime Disruption
 Security Testing
 Internet Data Mining
 By Industry
 By Topic
 Search

Resources
 Protection Apps & Extensions
 Site Report
 Search DNS
 Site Neighbours
 Cybercrime Trends
 Report a Suspicious Site

Company
 About Us
 Contact Us
 Single Sign-On
 Careers
 Fair Use and Copyright
 Privacy Policy

© 1995 - 2022 Netcraft Ltd
 All Rights Reserved.
 2 Belmont, Bath, BA1 5DZ, UK
 +44 (0) 1225 447500
 info@netcraft.com

Twitter Facebook LinkedIn

Conclusion :

We can conclude, ping, traceroute, nslookup are pretty useful and powerful tools in kali linux, used to obtain basically any information related to the domains, like ip, packet size, route to reach the site etc. Along with those, comes netcraft, a web-tool, which can obtain basically any information related to the site's technology, behind-the-scene security and mechanisms. We also saw how, Google is also helpful to obtain behind the curtain information, if the right keywords are used.