JGi JAIN DEEMED-TO-BE UNIVERSITY | SCHOOL OF COMPUTER SCIENCE AND IT

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

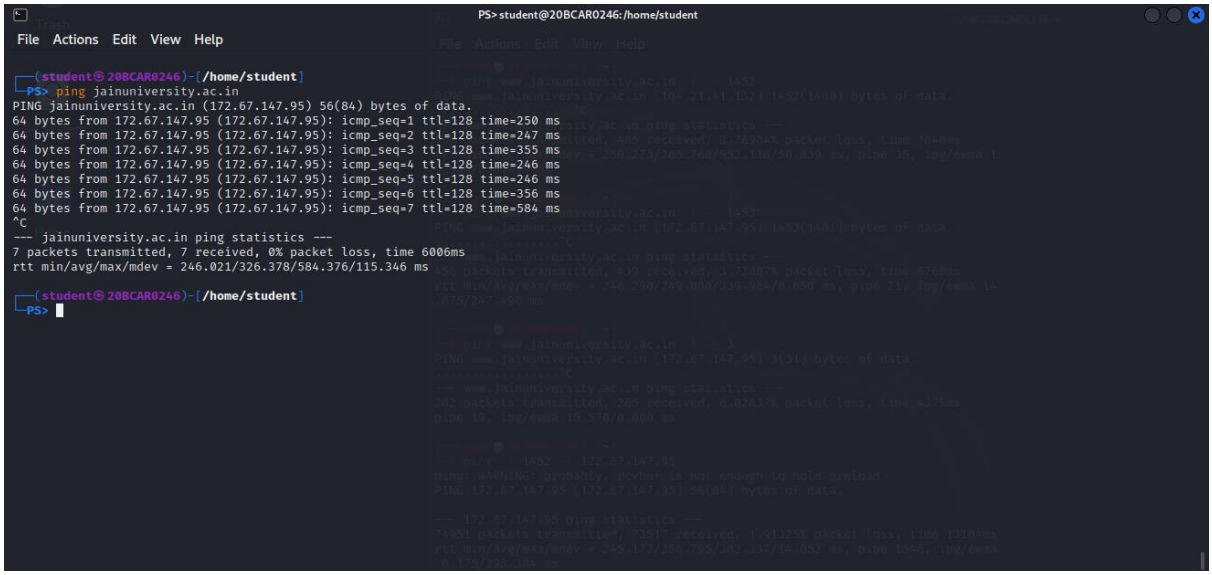
Objectives :

- ✓ 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-Authoriatitve 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.



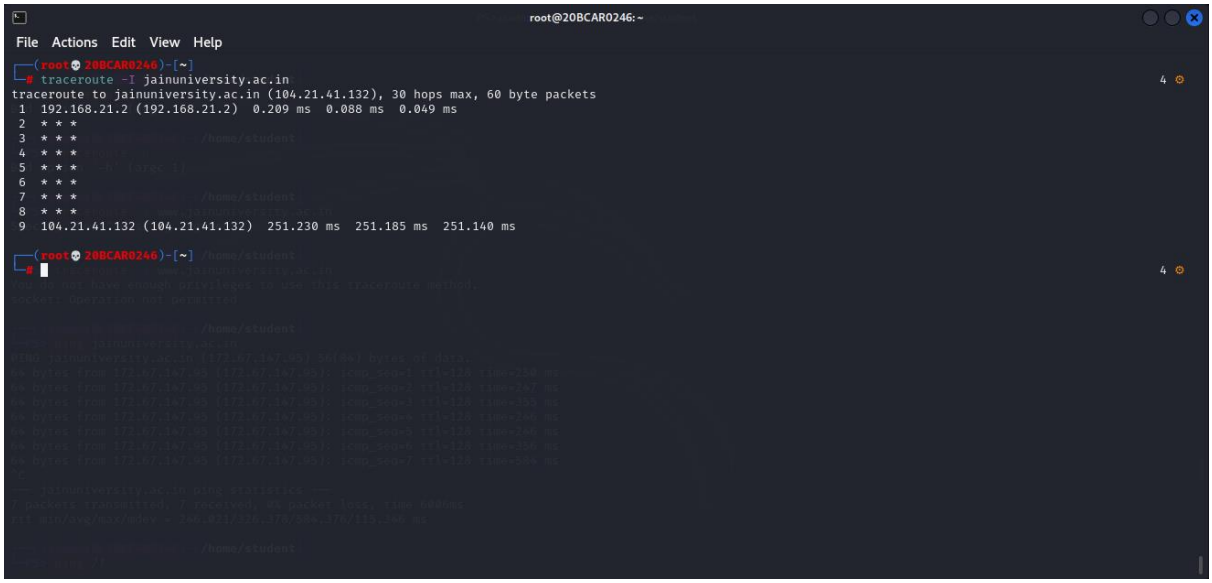
As we can see, 172.67.147.95 is the required IPv4. Other than that, a lot of other information provided too like packet size, round time of responding the request etc.

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 IMCP 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.

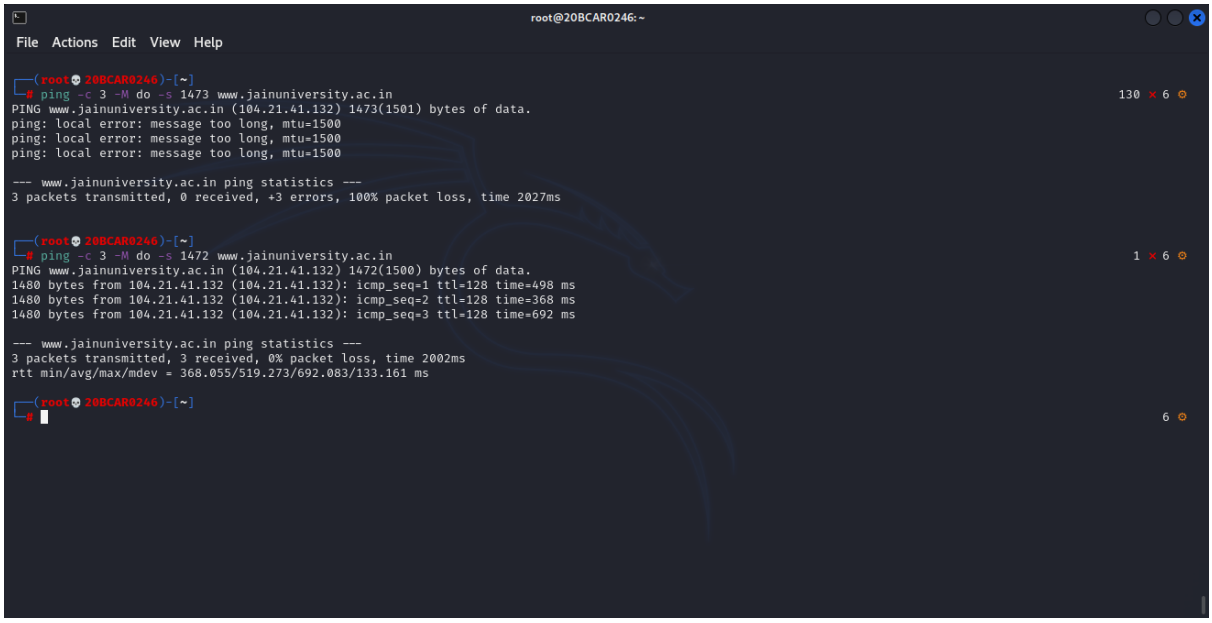


As we can see, 104.21.41.132 in the final destination we entered. In between, the details of the route are asterisked, due to security reasons, which can be viewed in Windows devices.

<u>NOTE</u>: 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.



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

<u>NOTE</u>: 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.

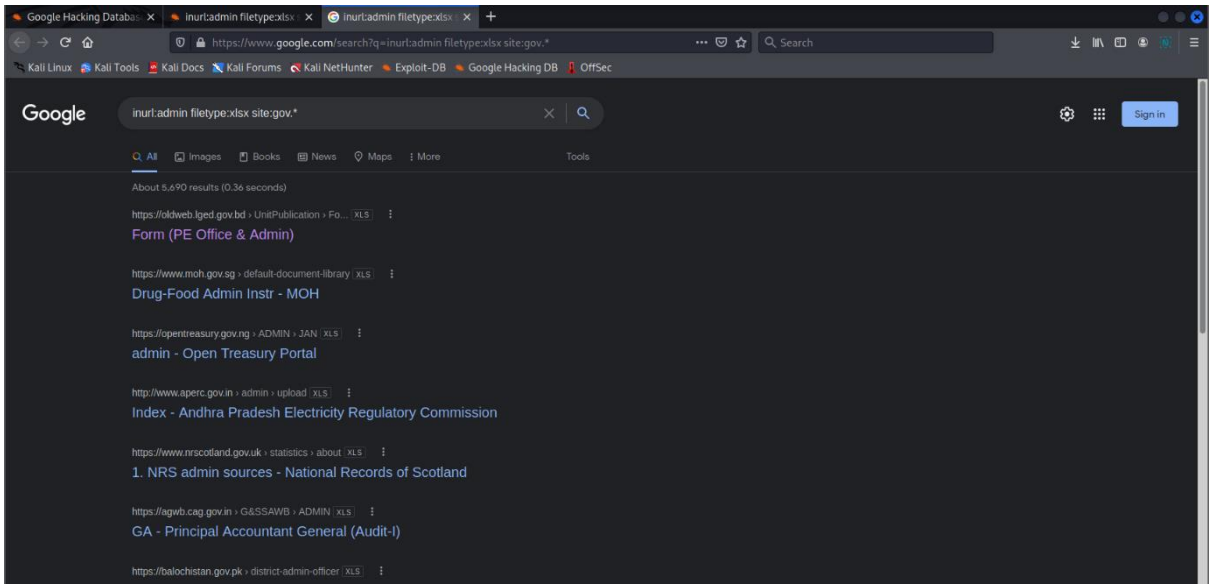
As we can see, 8 doesn't have responses, therefore we can conclude, 9 as the TTL.

Non-Authoriatitve 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.

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.

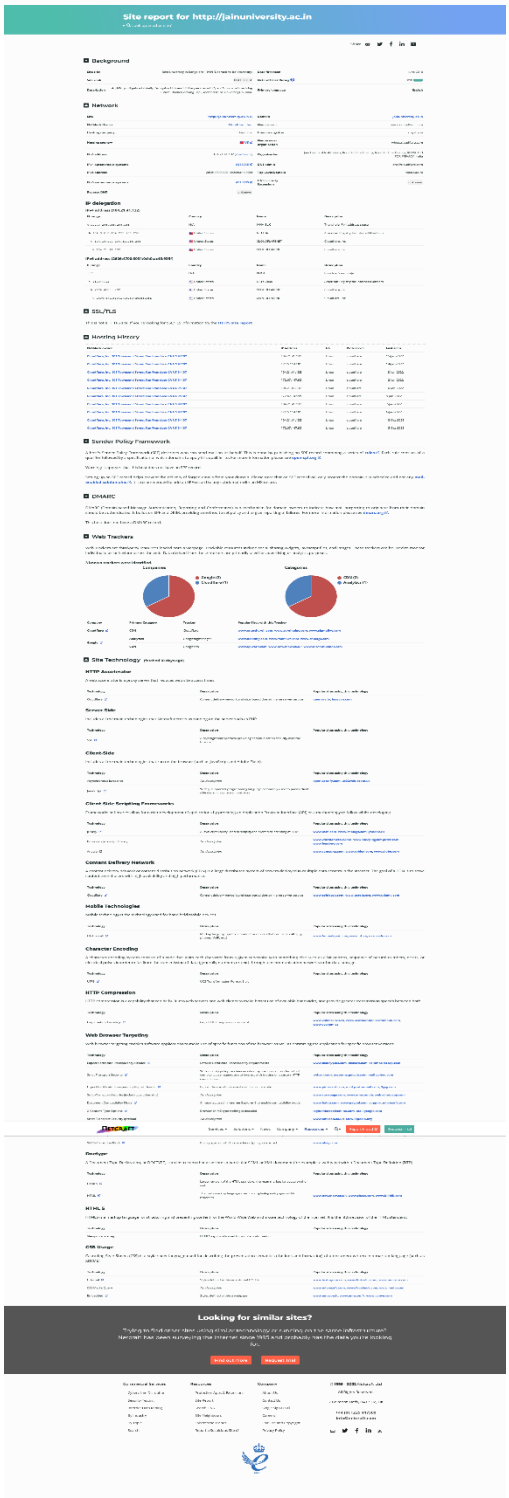
1> Head over to https://www.google.com and use keywords like inurl, intitle, filetype, site, etc. to find information that generally doesn't show up while searching.



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

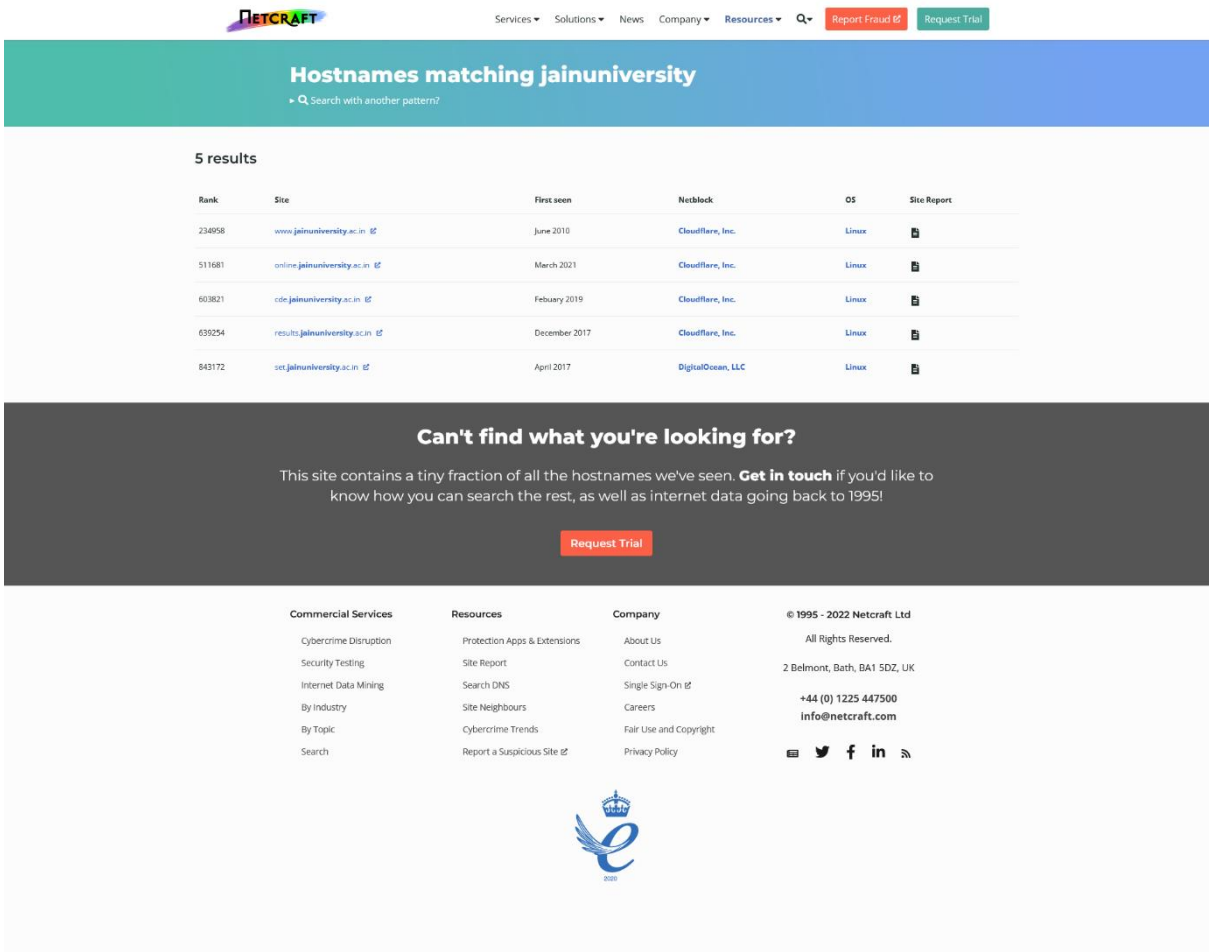
NOTE: Sites like https://www.exploit-db.com/google-hacking-database can be used to search for active exploits from databases.

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.

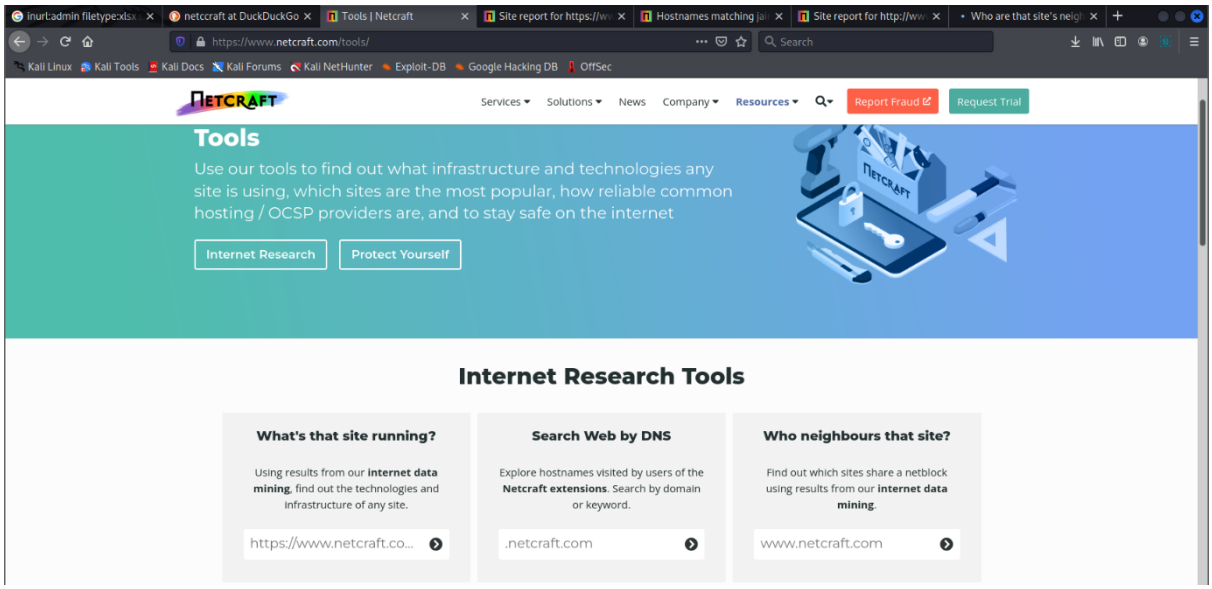


As we can see, 'What's that site running' gives us details about IP Addresses, domains, hosting, site security & technology etc.

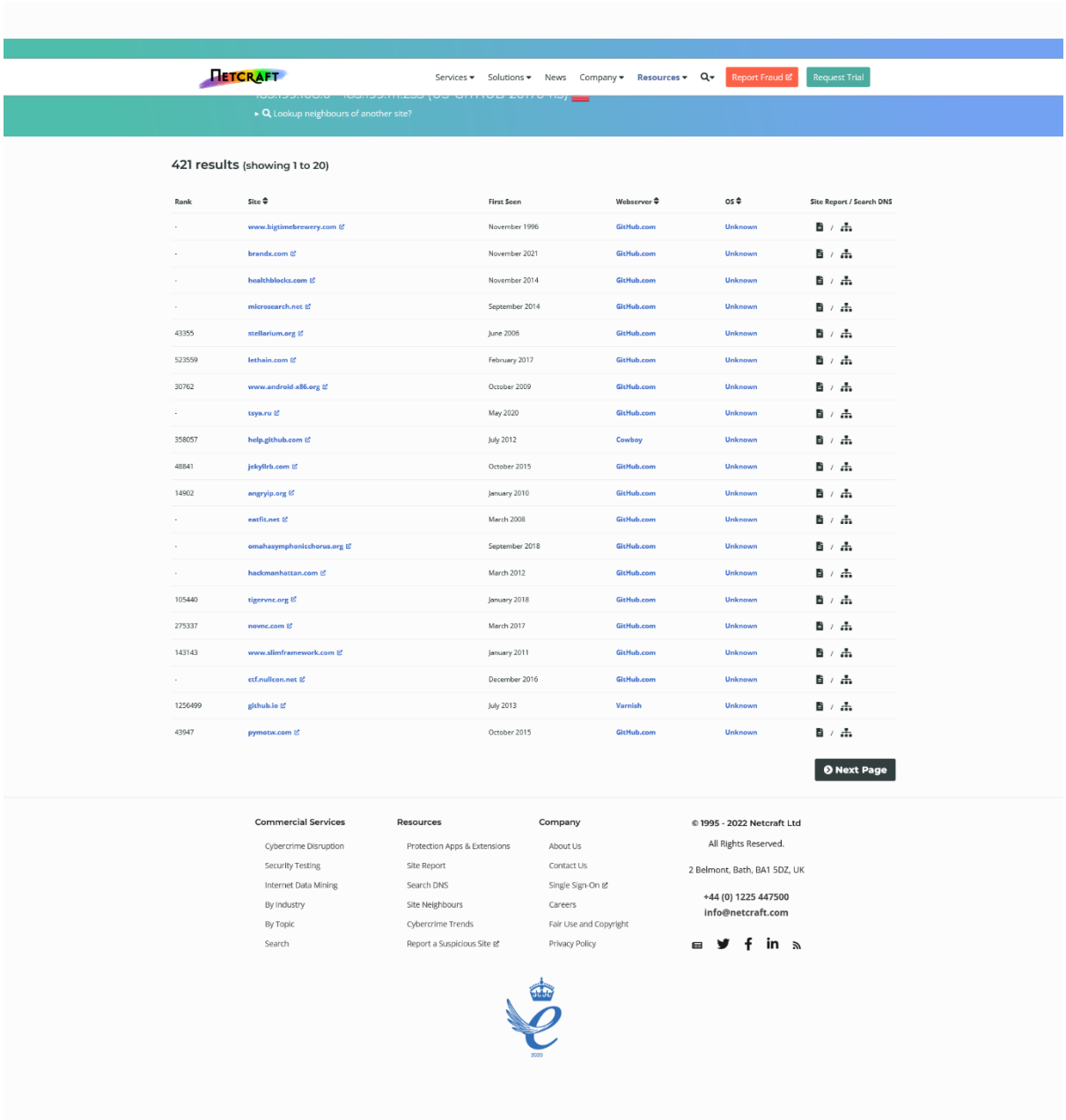
As we can see, 'Search Web by DNS' gives us details about URL's containing the keywords provided during the search.



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



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



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.