



**JAIN**  
DEEMED-TO-BE UNIVERSITY

SCHOOL OF  
COMPUTER  
SCIENCE AND IT

Department of  
**Bachelor of Computer Applications**

**Information security & Mobile Applications – Section <A>**

## **Ethical Hacking Fundamentals**

**Activity #01**

**LinkedIn Learning Certification Course**  
*[Part-1: Introduction to Ethical Hacking]*

**Subject Code: 19BCA4C02L**  
**Class: II<sup>nd</sup> Year II<sup>nd</sup> Semester**

**Submitted On:**

**23-12-2022**

**By:**

**Suman Garai**  
**20BCAR0246**

---

Signature

**Faculty In-Charge:**

**Dr. Ajay Shriram**

**Khushwaha**

---

Signature

## 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.

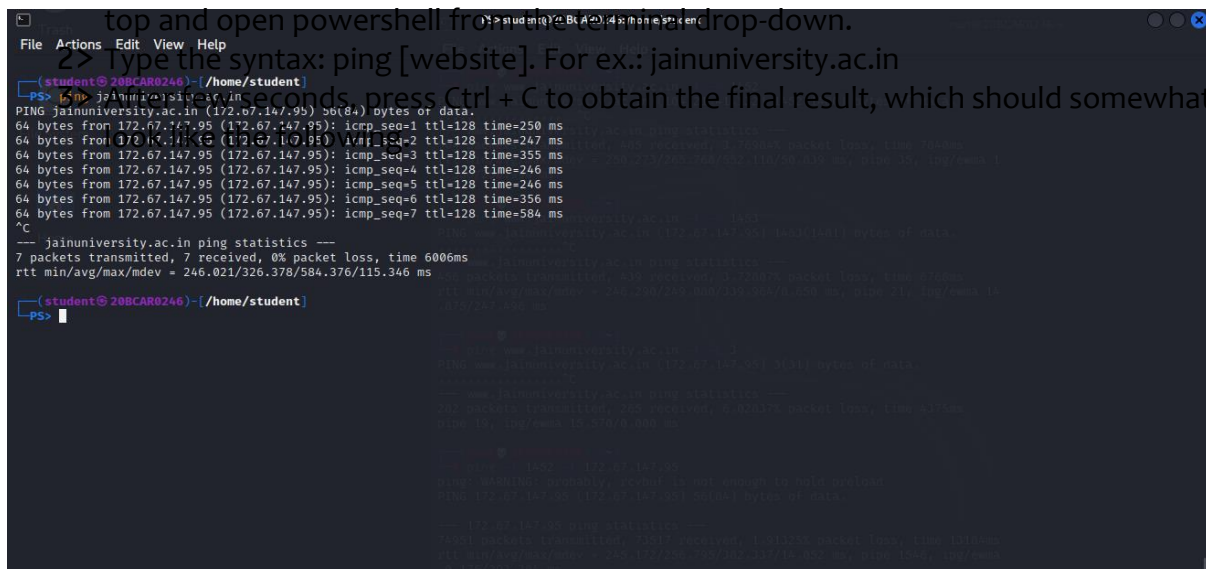
## Procedure :

### Finding IP Using Ping

1> After logging into kali linux virtual machine, head over to taskbar present on the top and open powershell from taskbar and click on drop-down.

2> Type the syntax: ping [website]. For ex.: jainuniversity.ac.in

After 30 seconds, press Ctrl + C to obtain the final result, which should somewhat



```
(student@20BCAR0246) [/home/student]
PS> ping jainuniversity.ac.in
PING jainuniversity.ac.in (172.67.147.95) 64(84) bytes of data:
64 bytes from 172.67.147.95: icmp_seq=1 ttl=128 time=250 ms
64 bytes from 172.67.147.95: icmp_seq=2 ttl=128 time=247 ms
64 bytes from 172.67.147.95: icmp_seq=3 ttl=128 time=355 ms
64 bytes from 172.67.147.95: icmp_seq=4 ttl=128 time=246 ms
64 bytes from 172.67.147.95: icmp_seq=5 ttl=128 time=246 ms
64 bytes from 172.67.147.95: icmp_seq=6 ttl=128 time=356 ms
64 bytes from 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.
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)  0.185 ms  0.266 ms  0.219 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
```

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.



# JAIN

DEEMED-TO-BE UNIVERSITY

SCHOOL OF  
COMPUTER  
SCIENCE AND IT

```
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, 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(1480) 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)~  
#
```

## Discovering Maximum Frame Size of the Domain

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.



```
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=256 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 = 0.448/0.811/2.616/0.561 ms  
  
root@20BCAR0246:~#
```

Finding TTL of the Domain

1> In the root terminal emulator, use the following syntax: ping -t [value] [website],  
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.

[illegible]

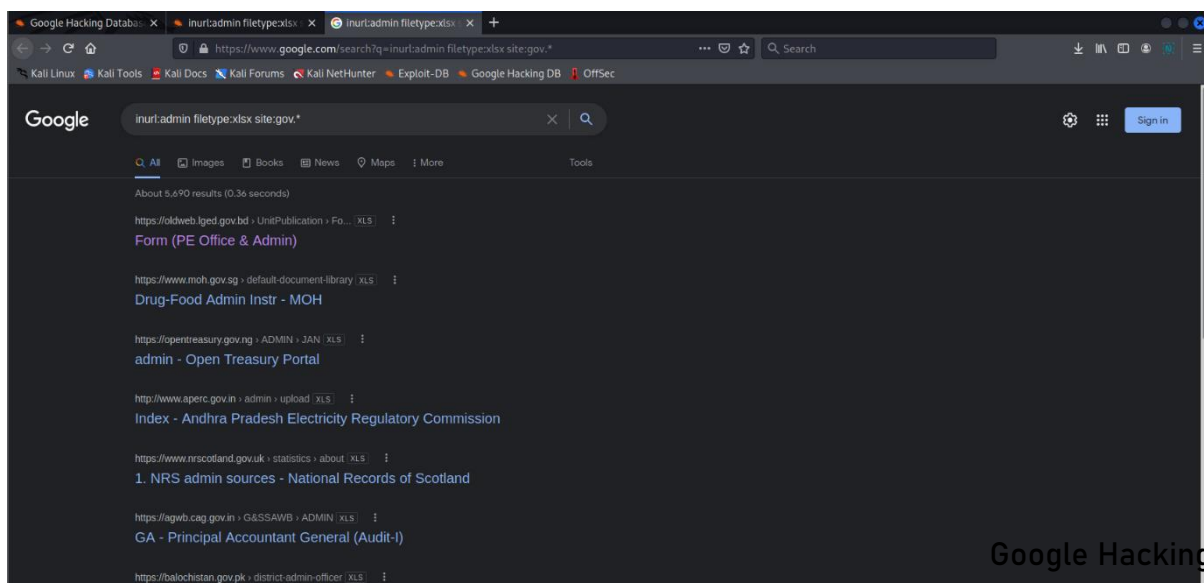
As we can see, mia and paul.ns.cloudflare.com denoted as the name server on the second half of the screen, we can conclude getting the required result.



# JAIN

DEEMED-TO-BE UNIVERSITY

SCHOOL OF  
COMPUTER  
SCIENCE AND IT



- 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.





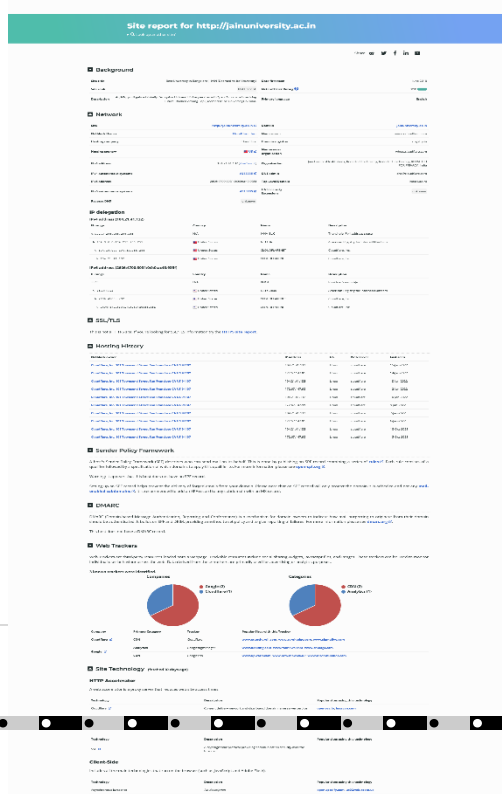
# JAIN

DEEMED-TO-BE UNIVERSITY

SCHOOL OF  
COMPUTER  
SCIENCE AND IT

## Netcraft

- 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.





# JAIN

DEEMED-TO-BE UNIVERSITY

SCHOOL OF  
COMPUTER  
SCIENCE AND IT

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 a search icon. Below this, a teal banner reads 'Hostnames matching jainuniversity' with a sub-link 'Search with another pattern?'. The main content area displays '5 results' in a table format. The table has columns for Rank, Site, First seen, Netblock, OS, and Site Report. The results list various hostnames like www.jainuniversity.ac.in, online.jainuniversity.ac.in, etc., along with their first seen dates and netblocks. Below the table, a dark grey box contains the text 'Can't find what you're looking for?' followed by a message about the site's data coverage and a 'Request Trial' button. At the bottom, there's a footer with links for Commercial Services, Resources, and Company, along with contact information and social media icons.

Rank	Site	First seen	Netblock	OS	Site Report
234958	<a href="http://www.jainuniversity.ac.in">www.jainuniversity.ac.in</a>	June 2010	Cloudflare, Inc.	Linux	<a href="#">Site Report</a>
511681	<a href="http://online.jainuniversity.ac.in">online.jainuniversity.ac.in</a>	March 2021	Cloudflare, Inc.	Linux	<a href="#">Site Report</a>
603821	<a href="http://cde.jainuniversity.ac.in">cde.jainuniversity.ac.in</a>	February 2019	Cloudflare, Inc.	Linux	<a href="#">Site Report</a>
639254	<a href="http://results.jainuniversity.ac.in">results.jainuniversity.ac.in</a>	December 2017	Cloudflare, Inc.	Linux	<a href="#">Site Report</a>
843172	<a href="http://set.jainuniversity.ac.in">set.jainuniversity.ac.in</a>	April 2017	DigitalOcean, LLC	Linux	<a href="#">Site Report</a>

**Can't find what you're looking for?**

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!

[Request Trial](#)

**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](mailto:info@netcraft.com)

[Facebook](#) [Twitter](#) [LinkedIn](#) [YouTube](#)

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

inurl:admin filetype:pdf

netcraft at DuckDuckGo

Tools | Netcraft

Site report for https://www...

Hostnames matching ja...

Site report for http://ww...

Who are that site's nei...

https://www.netcraft.com/tools/

Kali Linux

Kali Tools

Kali Docs


Kali Forums

Kali NetHunter

Exploit-DB

Google Hacking DB

OffSec



Services

Solutions

News

Company

Resources

Report Fraud


Request Trial

### Tools

Use our tools to find out what infrastructure and technologies any site is using, which sites are the most popular, how reliable common hosting / OSCP providers are, and to stay safe on the internet

Internet Research

Protect Yourself



### Internet Research Tools

#### What's that site running?

Using results from our **internet data mining**, find out the technologies and infrastructure of any site.

#### Search Web by DNS

Explore hostnames visited by users of the **Netcraft extensions**. Search by domain or keyword.

#### Who neighbours that site?

Find out which sites share a netblock using results from our **internet data mining**.

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

Look up neighbours of another site?

#### 421 results (showing 1 to 20)

Rank	Site	First Seen	Webserver	OS	Site Report / Search DNS
-	<a href="#">www.bigtimebrewery.com</a>	November 1996	GitHub.com	Unknown	 / 
-	<a href="#">brends.com</a>	November 2021	GitHub.com	Unknown	 / 
-	<a href="#">healthblacks.com</a>	November 2014	GitHub.com	Unknown	 / 
-	<a href="#">microsearch.net</a>	September 2014	GitHub.com	Unknown	 / 
43355	<a href="#">stellarium.org</a>	June 2006	GitHub.com	Unknown	 / 
523559	<a href="#">lathain.com</a>	February 2017	GitHub.com	Unknown	 / 
30762	<a href="#">www.android-x86.org</a>	October 2009	GitHub.com	Unknown	 / 
-	<a href="#">taya.ru</a>	May 2020	GitHub.com	Unknown	 / 
358057	<a href="#">help.github.com</a>	July 2012	Cowboy	Unknown	 / 
48841	<a href="#">jekyllrb.com</a>	October 2015	GitHub.com	Unknown	 / 
14902	<a href="#">angryip.org</a>	January 2010	GitHub.com	Unknown	 / 
-	<a href="#">eastfi.net</a>	March 2008	GitHub.com	Unknown	 / 
-	<a href="#">emaahaymphonicchorus.org</a>	September 2018	GitHub.com	Unknown	 / 
-	<a href="#">hackmanhattan.com</a>	March 2012	GitHub.com	Unknown	 / 
105440	<a href="#">tigerenc.org</a>	January 2018	GitHub.com	Unknown	 / 
275337	<a href="#">newnc.com</a>	March 2017	GitHub.com	Unknown	 / 
143143	<a href="#">www.allenframework.com</a>	January 2011	GitHub.com	Unknown	 / 
-	<a href="#">ccf.nullcon.net</a>	December 2016	GitHub.com	Unknown	 / 
1256499	<a href="#">github.io</a>	July 2013	Variash	Unknown	 / 
43947	<a href="#">pymetax.com</a>	October 2015	GitHub.com	Unknown	 / 

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



**JAIN**  
DEEMED-TO-BE UNIVERSITY

SCHOOL OF  
COMPUTER  
SCIENCE AND IT

### 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.