

B | EHC

Ethical Hacking Class

2: Footprinting or Information Gathering

i

by Lokesh Singh

www.hackingloops.com

CONTENTS

Overview of Last BEH Issue: Introduction to Ethical Hacking	3
What we will learn in this issue?	3
Introduction of Footprinting	4
IP Address: Unique number to identify host	5
How to check our own IP address?	6
How to find IP address of any website?	6
How to Find IP address of other's computer?	6
Using PHP Scripts	7
Using Read Notify Script	8
Using Blogs or websites	8
Sniffing Chat Sessions and Online Gaming session	9
Ping Sweep: Victim is alive or dead	9
How to use the Ping sweep command in windows?	10
What are the other uses of Ping Sweep?	10
Trace routes: know the network structure or connectivity	11
How trace route is done practically?	12
Understanding Trace Route:	13
Benefits of Trace Route	15
WHO IS: WHO is the Owner of Website and his contact Information	15
Steps to gather who is information	16
DNS QUERIES.....	21
Basic terms related to DNS (Domain Name System).....	22
How to Run DNS queries?	24

OVERVIEW OF LAST BEH ISSUE: INTRODUCTION TO ETHICAL HACKING

In our last issue we have learnt about basics of terms related to Ethical Hacking or simply Hacking and about how a hacker prepares or launches a hacking attempt or simply say hack attack. We have also discussed brief about different phases that involves in launching a hacking attempt like information gathering, scanning, gaining access, maintaining access and covering tracks respectively. This is what we have discussed in our last issue.

WHAT WE WILL LEARN IN THIS ISSUE?

It's really a curious question and its answer is itself in the overview. Ok no more puzzles, in this issue we will learn more about Information Gathering or Footprinting techniques. Because of lot of techniques involved in Foot Printing we have decided to publish the issue into two parts.

Below is the list of Footprinting techniques we are going to learn in first part.

1. Finding IP address
2. Ping Sweeps
3. Tracing routes
4. Who is data
5. DNS queries

What we will learn in Footprinting Part 2 Issue:

1. Search Engine discovery or Reconnaissance
2. Spiders, Crawlers or Robots discovery
3. Web data Extraction
4. Reviewing Metadata and JavaScript's
5. Web application fingerprint
6. Web server fingerprint
7. People Search

So let's begin with introduction and basics of Information gathering or Footprinting.

INTRODUCTION OF FOOTPRINTING

Footprinting is also referred as information gathering phase of any hacking attempt. It is one of the preparatory phases or simply say one of the initial phases of any hacking attempt. The data we capture in this phase will be useful for below reasons.

1. We can use extracted data for Social Engineering or password guessing.
2. Can be used to prepare blue print or prototype of any website or network structure.
3. Can be used to prepare the passwords file for brute force and other type of attacks.
4. If none of above then we will use the information for next phases :P

According to Wikipedia, **Footprinting** is the technique of gathering information about computer systems and the entities they belong to.

But you will not get further information about it. Let's learn the same in detail.

Footprinting is one the best or most convenient way that hackers use to gather information about computer systems and the companies they belong to. The main purpose of Footprinting is to learn as much as you can about a system or website, its remote access capabilities, its ports and services or server information, and the aspects of its security.

In order to perform a successful hack attack against somebody, it is always beneficial to know everything about the victim. If everything is not possible then try as much as you can gather.

We are discussing about negative impacts of Information gathering or Footprinting from very start but friends. Information gathering is as good as for security professionals like it's for Hackers. How it's possible? Answer is quite simple. Information security analysts perform information gathering technique to protect their own systems or companies systems. Don't get confused with term security analysts and Ethical Hackers, both are same.

Let's try to understand this by considering a simple example. Say I have finished my 12th standard exams and now I am searching for some good college to get admission into. What are the steps we will follow? Let's consider basic ones:

1. Find the list of all good colleges
2. Querying about their Placement records
3. Fee Structure
4. Gather related information from your seniors or relatives and so on.

Why we are gathering all these information? Off course for making our future secured, is it really helpful? Ask yourself. We can also join the college without following any of the above steps but do you really call yourself intelligent? Similarly, in hacking domain we have to know our victim quite well. Against whom we actually are? What consequences it may cause in future? And most important can it be helpful.

Considering all above facts you all know the answer.

Let's move to the techniques that we use for Footprinting or Information Gathering.

IP ADDRESS: UNIQUE NUMBER TO IDENTIFY HOST

What is IP address? What's its importance? How hackers use IP address to attack victim. What are the different ways of stealing or getting IP address? I know these are the questions that might be rushing to all of your brains. Relax buddies; it's not HI FI stuff. Frankly IP address is the very first staircase of Hacker's journey. If you get clear idea about IP address then all things will go smoothly. So keep ask your brain cells to remain active until this session ends.

IP address stands for Internet Protocol address. What is Protocol? Protocol is a set of rules that will define how your network device will behave with internet connection and one without internet connection. For time being just keep in mind that Protocol is a set of rules like every other thing has rules say cricket i.e. 11 players both sides, two batsman on crease, one bowler bowling, Limited over's etc.

IP address is basically a numerical value which is assigned to every network device, so that we can uniquely identify that device during communication with other network devices. I am not going into much deep like IPV4 or IPV6. Because there will be a separate Issue on IP address in later classes because concepts of Subnet, broadcast address, multicasting, gateway cannot be shared now else you all will be confused.

IP address serves for two basic purposes:

1. Host or network interface identification
2. Location Addressing

HOW TO CHECK OUR OWN IP ADDRESS?

For windows XP users, go to start up → Run → type cmd and press enter to open command prompt → type command **IPCONFIG/all** in command prompt to get the IP address, default gateway adapter wise i.e. for all network adapters.

For windows 7 users, go to start up → in search box type cmd and press enter to open command prompt → type command **IPCONFIG/all** in command prompt to get the IP address, default gateway adapter wise i.e. for all network adapters.

For Linux users, go to terminal → type IPCONF and press enter to get you own IP address.

For knowing more information or optional command related to IP address type **IPCONFIG/?** in the command prompt.

HOW TO FIND IP ADDRESS OF ANY WEBSITE?

Follow the steps explained above to open command prompt i.e. cmd. There type any of below command to get the IP address of website.

Ping www.websiteaddress.com

Tracert www.websiteaddress.com

Now in the very first line you will get the Website IP address along with its web address.

For Example: when you type Ping www.google.com and press enter, you will see something like this Pinging www.google.com [173.194.36.20] with 32 bytes where [173.194.36.20] is the IP address of the website.

HOW TO FIND IP ADDRESS OF OTHER'S COMPUTER?

There are several ways of finding IP address of other's computer. And we are going to discuss them one by one.

1. Using PHP Scripts
2. Using Read Notify service
3. Using Blogs or websites
4. Sniffing Chat sessions (audio or video)
5. Sniffing Online Game sessions

There are several other methods too that you will come across in later issues of Hacking Classes.

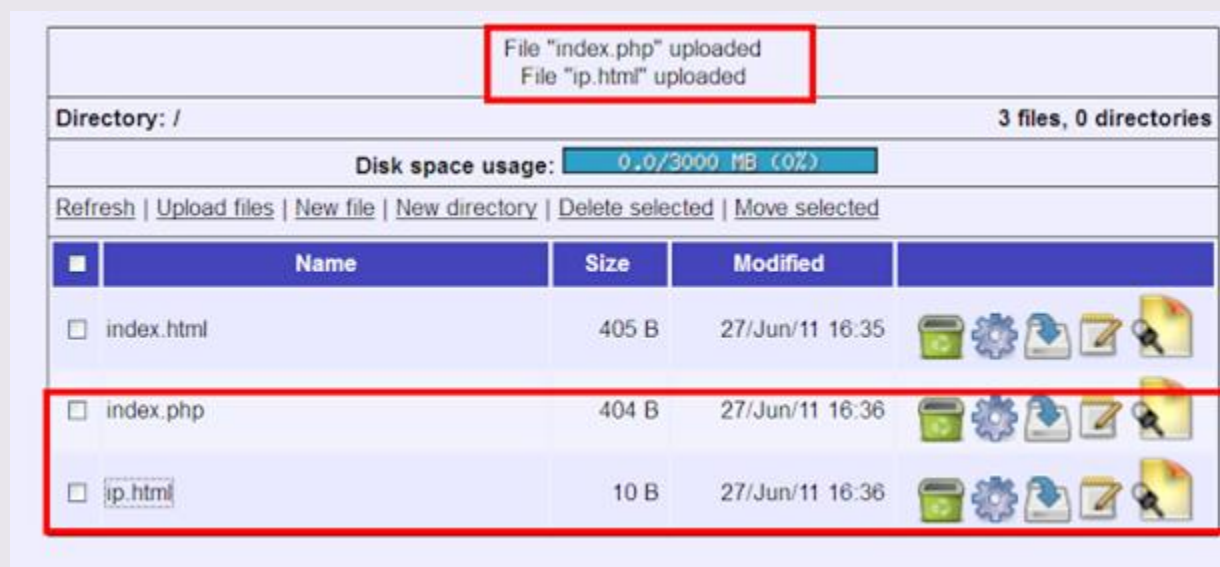
USING PHP SCRIPTS

Using this Notification script you can get the IP address in just seconds. Steps of using this PHP script:

1. Download the PHP notify script and extract files.

[Download here](#)

2. Now you will get two files IP.html and index.php. You need to upload these two files to any free web hosting server.
3. Example: say www.my3gb.com to upload these two files. Create an account there and upload these two files there as shown below.



4. Now you will need to send the link of index.php to the victim whose password you want to get. To get the link click on index.php shown in above snapshot. Now a new window will open copy the link in the address bar and send to the victim whose IP address you want.
5. Now when the victim opens the above link nothing will open but his IP address is written into the ip.html file. So open the ip.html file to get his IP address.
6. That all. We have victim's IP address.

USING READ NOTIFY SCRIPT

This is an email based service. Steps to use Read Notify service:

- a. First open the Read Notify website: [RCPT](#)
- b. Now register on this website and then it will send you confirmation mail. Verify your account.
- c. Once your account is activated.

Do the following steps use this service?

1. Compose your email just like you usually would in your own email or web email program
2. Type: [readnotify.com](#) on the end of your recipients email address (don't worry, that gets removed before your recipients receive the email). Like this: [shiviskingg@gmail.com.readnotify.com](#)
3. Send your email

Some things to remember:

- Don't send to and from the same computer
- If your email program 'auto-completes' email addresses from your address book, you'll need to keep typing over the top of the auto-completed one to add the [readnotify.com](#)
- if you are cc-ing your email to other readers, you must add tracking to all of them.

USING BLOGS OR WEBSITES

This is one of the most legitimate way to steal the IP address of the victim and victim will never going to know that his IP address has been stolen. The process of capturing IP address based on the fact of using third party Web Statistic scripts on the website or blog. So this method is for those who have their blogs or websites. Normal users can also do this as blog is free to make. Make a new blog and use any stats service like **HISTATS** or any other stats widget. Just add a new widget and put HISTATS code there and save template. And send the link of your blog to your friend and get his IP. Once the victim opens your blog or website, you will get his/her IP address, Operating System information, Web browser information and other critical information. This is the easiest method to get the IP address.

SNIFFING CHAT SESSIONS AND ONLINE GAMING SESSION

In this way we are going to exploit the direct connectivity bug of Chat and online gaming sessions. Whenever we start audio or video chat with anybody, our system creates a TCP, 3 way handshake connections between our system and victim's system. Same is exploited in case of online gaming sessions. During these i.e. chat and online gaming sessions if we capture our network adapter traffic, it becomes quite easy to catch the victims IP address. We can use any of these tools to capture our Network traffic like Wireshark, Eternal Cap, Ettercap etc. In windows 7, there is even no need of any external tool, just open the task manager and then go to Performance tab, at below you will see Resource monitor button. Click on that and select network to see all applications that are using network bandwidth.

So from next time, don't get surprised if someone steals your IP address while chatting or playing with you and shuts down your PC.

Note: We can do lot of things if victim is on same subnet like we can mount his data drives on our machine and see or delete whatever we want.

We can even shut down his PC if we are on same subnet.

PING SWEEP: VICTIM IS ALIVE OR DEAD

Ping is a network based utility which is use to identify that host is up or down i.e. online or offline and the technique that is used to achieve it is called Ping sweep.

Ping sweep can only be useful if you know the IP address or web address of the host i.e. victim.

Note: Host can be anything like computer system, website, network or any other network device.

Let's understand it more technically; Ping Sweep is also called **Ping scan** or **ICMP sweep** (Internet Control message protocol) or **2 way handshake protocol**. It is two way handshake protocol because one host sends data(packets) and other host validates the data and return the acknowledgement (basically packets) that ping is successful or not. Normally windows operating system sends 32byte packets.

Normal ping sweep command:

Ping "IP address or web-address" "Optional command"

For example: If you wish to ping to Google, then ping sweep command will be:

Ping www.google.com or Ping 173.194.36.51

Note: Optional commands can be easily extracted by typing **ping/?** in command prompt.

HOW TO USE THE PING SWEEP COMMAND IN WINDOWS?

1. Open the command prompt i.e. cmd. For windows XP users, go to start up→Run and then type cmd and then press enter. For windows 7 users, go to start up, there in search box type cmd and press enter. For Linux users, open the terminal.
2. In command prompt or terminal i.e. cmd. Type any of the below command:
Ping www.google.com
Ping 173.194.36.51
3. Now there you will encounter two things sent packets and received packets. If receive packets count is greater than 0 then it means host is up i.e. online. If all the requested packets are timed out, then there can be two situations; First host is down i.e. offline or secondly, connection is blocked by Firewall. This we will learn in our Scanning Issue i.e. Next issue.

WHAT ARE THE OTHER USES OF PING SWEEP?

From above discussion, you might have under-estimated the power of ping. Let's discuss its real power.

Most of times in news, you all might have heard that Anonymous group has launched DOS attack on some GOVT websites, because of this they are responding quite slow or not at all. This is all the magic of Ping. Ping sweep technique is usually (in negative aspect) used to launch a DDOS attack i.e. Distributed denial of service attack. What is DDOS? DDOS is a hack attack which is used to consume all the bandwidth of the web server and made the resources unavailable for its legitimate users. The DDOS attack which is launched using the Ping sweep technique is known as **Flood Pinging**.

Here is the command for Launching Flood Pinging, say I want to flood Hackingloops website then command will be:

Ping www.hackingloops.com -t -l 65535

What this command will do? It will flood Hackingloops.com for infinite requests with a buffer size of 64k. :P don't try against my website as it will be vain because my website have unlimited bandwidth.

Best use: If you play counter strike or any other online game; you can use this technique to turn down any counter strike or online game server. If not

able to turn it down, you will create a huge lag on server that will result into crash.

Flood Pinging is a kind of **denial of service** attack, it occurs when you flood a lot of pings to a website or simply a host. These results in that normal or legitimate user will not be able to access that website because every host (website or victim network) has certain maximum capacity limit when flooding of pings cross that limit; it jams the network and host stops responding. This is done by making automated scripts or you can directly do this using **flood pinging** software's like server attack etc. **Flood pinging** is sometimes also called ping of death as it make the host behaves like a dead host which does not respond to anything.

Note: This will work only if attacker's bandwidth is more than host. But launching this from multiple machines can do the trick.

Normally what happens, only few website owners go for unlimited bandwidth plans as they are too costly. So they opt for plans like 10 GB bandwidth etc. Now if you do this from your 2 or 4 Mbps connections it's vain. But when you do this in group means now suppose you and your group has 20 members. Now if you launch the same attack from 20 computers having 2 Mbps connection means 40 mbps at a time. But now you are thinking bandwidth is 10 GB and we only reached 40mbps, here the trick, hackers creates multiple connections around 1000 from one PC and 20 means 20000 connections at a time. What this will result, it will slowdown websites database and other functionality and website will stop responding.

For doing this on victim (means an IP address of PC), what you need is just a connection faster than him, if you don't have do this in group.

Flood Pinging is highly helpful in Session Hijacking, that i will explain later so keep reading and keep learning, as learning is the only key to become a elite.

TRACE ROUTES: KNOW THE NETWORK STRUCTURE OR CONNECTIVITY

Trace route is a network based utility which shows the path over the network between two systems and lists all the intermediate routers to get to the final destination. For what purpose trace route is used? Main purpose of trace route is to fix network problems. This helps you in identifying, while connecting to some network where the connection is actually slowing down, which intermediate router is responsible for that.

Technically trace route is also an ICMP echo based protocol similar to ping.

But it's only a primary use, for what else we can use this. As I have already explained above how to get an IP address. Now when you do trace route with that IP address

what it will show is that which service provider the victim is using means ISP(Internet service provider), this will help you in determining his few basic things like Country, state and sometime more deeper information too. Now how this is going to be helpful for Network forensic experts. Suppose you have made a hacking attempt on some bank or some government or some security concerned website, what they do is that they store an IP address and timestamps of each visitor in their database. Now what network forensic expert will do is that it will trace route your IP address and confirm your ISP and your country (country from which ISP belongs). Now Forensic expert will contact your ISP and provide your IP address and time to ISP and ask him to provide details that at that time this IP was assigned to which person and that how they will get complete address of the hacker and catch him red handed. I hope you got my point why trace route is that much important.

HOW TRACE ROUTE IS DONE PRACTICALLY?

In windows, trace route is done by using the command `tracert` in command prompt. You can do it two different ways:

1. To trace route an IP address: This can be of any website or any computer system or of any network.

SYNTAX:

`tracert IP(like tracert 127.0.0.1)`

2. To trace route websites: When you don't know website's IP address let trace route to translate that address for you.

SYNTAX:

`tracert websiteaddress(like tracert www.google.com)`

More options:

- d Do not resolve address to host-names
- h (maximum hops) Maximum number of hops to search the target system
- j (host-list) Loose source route along with host-list
- w timeout Wait timeout milliseconds for each reply

Linux trace route has more options available.

Note: You will always get fewer results when you try to trace route computer system of any victim. More precisely you will only get around 3 to 10 entries. Three to Four when firewall of the victim doesn't alter your trace routing and more when firewall blocks ICMP echo's.

Note: If you get asterisks(*) after the first entry then it confirms that firewall is playing its part and it doesn't allowing us to trace route the system but still we will be able to get his ISP address and with that we can get his location overview.

UNDERSTANDING TRACE ROUTE:

Below is snapshot of normal trace route output of victim (normal computer):

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\IC4-HACKER>tracert 14.97.26.146
Tracing route to Static-146.26.97.14.tataidc.co.in [14.97.26.146]
over a maximum of 30 hops:
  1  61 ms  46 ms  45 ms  172.29.145.65
  2  *      *      *      Request timed out.
  3  *      *      *      Request timed out.
  4  *      *      *      Request timed out.
  5  *      *      *      Request timed out.
  6  *      *      *      Request timed out.
  7  *      *      *      Request timed out.
  8  *      *      *      Request timed out.
  9  *      *      *      Request timed out.
 10  *      *      *      Request timed out.
 11  *      *      *      Request timed out.
 12  *      *      *      Request timed out.
 13  *      *      *      Request timed out.
 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  *      *      *      Request timed out.
 21  *      *      *      Request timed out.
 22  *      *      *      Request timed out.
 23  *      *      *      Request timed out.
 24  *      *      *      Request timed out.
 25  *      *      *      Request timed out.
 26  *      *      *      Request timed out.
 27  *      *      *      Request timed out.
 28  *      *      *      Request timed out.
 29  *      *      *      Request timed out.
 30  *      *      *      Request timed out.

Trace complete.

C:\Documents and Settings\IC4-HACKER>tracert 14.97.26.147
Tracing route to Static-147.26.97.14.tataidc.co.in [14.97.26.147]
over a maximum of 30 hops:
  1  67 ms  55 ms  47 ms  172.29.145.65
  2  380 ms 379 ms 377 ms Static-147.26.97.14.tataidc.co.in [14.97.26.147]

Trace complete.

C:\Documents and Settings\IC4-HACKER>tracert 14.97.26.148
Tracing route to Static-148.26.97.14.tataidc.co.in [14.97.26.148]
over a maximum of 30 hops:
  1  59 ms  42 ms  39 ms  172.29.145.65
  2  128 ms 105 ms 110 ms Static-148.26.97.14.tataidc.co.in [14.97.26.148]

Trace complete.
```

Let's start from very first Line:

1. Very first line after the tracert shows Host Name and IP address which it got using the reverse DNS (domain name system) look up.
2. Over maximum 30 hops: 30 hops mean that traceroute will only route first 30 routes between your system and victim's system. 30 is too much it usually ends in 3 to 15 hops but sometimes it goes deeper based on security and no response(as in our first case when we tries to route 14.97.26.147).

Note: Timings are basically round trip times. There are three round trip times in ping. The round trip times (or RTTs) tell us how long it took a packet to get from me to that system and back again, called the latency between the two systems. By default, three packets are sent to each system along the route, so we get three RTTs.

3. This is the address translation private IP by any one of the services from these (RIPE, ARIN, APNIC, LACNIC, AfriNIC).

These are the IP address ranges for these private IP's:

10.0.0.0 – 10.255.255.255,

172.16.0.0 – 172.31.255.255,

192.168.0.0 – 192.168.255.255

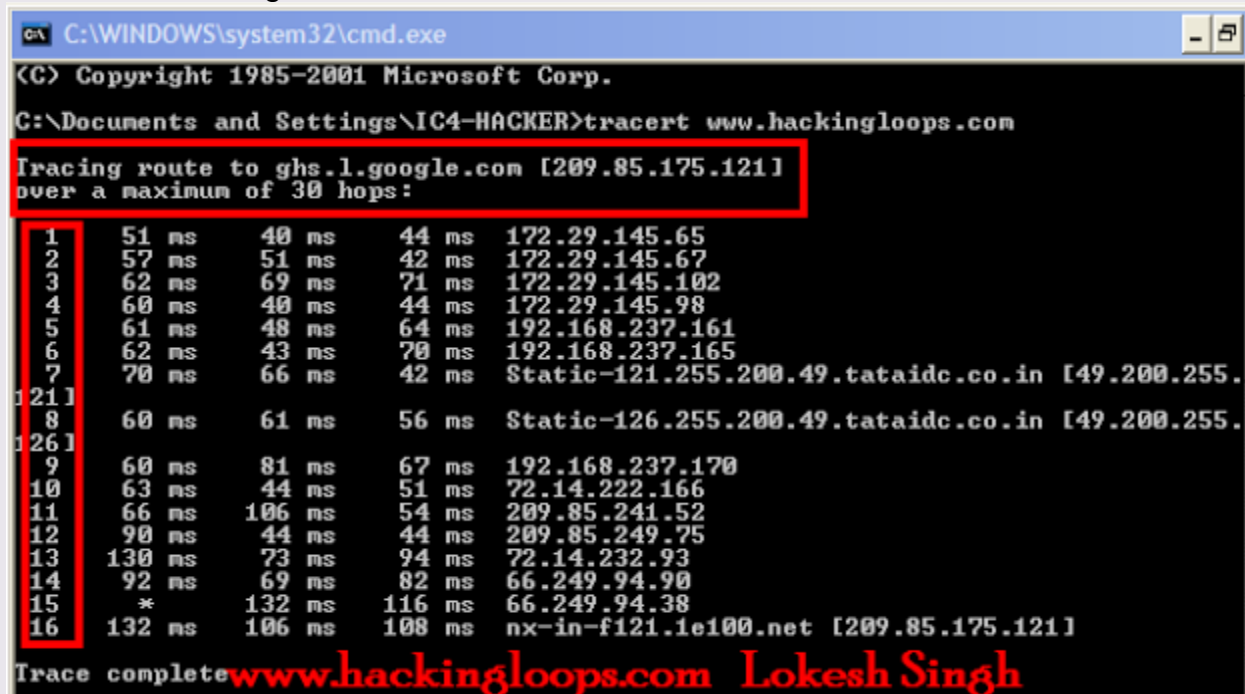
and 224.0.0.0 - 239.255.255.255 are reserved IP Addresses for private internet use for network address translations of above mentioned services.

4. This means that the target system could not be reached. More accurately, it means that the packets could not make it there and back; they may actually be reaching the target system but encountering problems on the return trip (more on this later). This is possibly due to some kind of problem, but it may also be an intentional block due to a firewall or other security measures, and the block may affect trace route but not actual server connections.

5. If firewall doesn't block remote connections then the result will be like this.

Note: This step provides the ISP (Internet service provider).

Now Understanding trace route for websites:



```
C:\WINDOWS\system32\cmd.exe
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\IC4-HACKER>tracert www.hackingloops.com

Tracing route to ghs.l.google.com [209.85.175.121]
over a maximum of 30 hops:
 0  51 ms  40 ms  44 ms  172.29.145.65
 1  57 ms  51 ms  42 ms  172.29.145.67
 2  62 ms  69 ms  71 ms  172.29.145.102
 3  60 ms  40 ms  44 ms  172.29.145.98
 4  61 ms  48 ms  64 ms  192.168.237.161
 5  62 ms  43 ms  70 ms  192.168.237.165
 6  70 ms  66 ms  42 ms  Static-121.255.200.49.tataidc.co.in [49.200.255.121]
 7  60 ms  61 ms  56 ms  Static-126.255.200.49.tataidc.co.in [49.200.255.126]
 8  60 ms  81 ms  67 ms  192.168.237.170
 9  63 ms  44 ms  51 ms  72.14.222.166
10  66 ms  106 ms  54 ms  209.85.241.52
11  90 ms  44 ms  44 ms  209.85.249.75
12  130 ms  73 ms  94 ms  72.14.232.93
13  92 ms  69 ms  82 ms  66.249.94.90
14  *      132 ms  116 ms  66.249.94.38
15  132 ms  106 ms  108 ms  nx-in-f121.1e100.net [209.85.175.121]

Trace complete
```

Since Hackingloops is a blog hosted on Google that's why at start it reverse DNS name as ghs.l.google.com and translated IP address of Hackingloops is 209.85.175.121. So our destination is 209.85.175.121

Now steps 1 to step 4 shows private internet use addresses as explained above which is used for address translation. Step 5,6 and 9 are also static private IP addresses with which but these are local IP addresses for your localhost with the DNS communicates.

Step 7 and 8 determines the response from your ISP address. Above clearly predicts i am using tata teleservices ISP.

Step 10 and 13, 14 and 15 are also Google IP address responses as this is Google blog.

Steps 11 and Step 12 retrieves the different DNS servers of Hackingloops.

Step 16 shows our destination..

The above was meaning now let's explain whole process in a go....

First of all my system reverse DNS the IP address of Hackingloops which is found to be 209.85.175.121, Now since I haven't mentioned any specific hop count so by default it considers maximum value as 30 hops. Now my computer system (WLAN adapter) contacts to IANA service (RIPE, ARIN, APNIC, LACNIC, AfriNIC) requesting the response from IANA to get the translated address. After a successful query to IANA service it returns the response back to my local system (192.168.***.***). In between my system also get response from my ISP which is tata teleservices. Now after a successful acknowledgement our system contacts to Google server (72.14.222.166 and 72.14.232.93) which in return returns the DNS server names (for Hackingloops and then Google confirms the response and returns back the actual web page.

BENEFITS OF TRACE ROUTE

There are several benefits of doing trace route, some of them are mentioned below and rest you will know during later issues.

- Using trace route we can track any website and predict its network structure.
- As we have seen above, trace route reveals all intermediate IP addresses involved. This will help us to do IP poisoning. We will find the weakest node and flood it with requests which might result into DDOS.
- For creating prototype of network architecture.
- For tracing any user globally. Note: trace route will only help you to reach the ISP i.e. Internet Service Provider. Now for tracking anyone, we shall have to send a request to ISP that following "IP Address" is assigned to which user at particular time. That's all because ISP stores one configuration file of user's data which stores list of IP addresses assigned to users with their timestamp. And for all Hackers security, always remember that IP address is unique to network at particular instance.

WHO IS: WHO IS THE OWNER OF WEBSITE AND HIS CONTACT INFORMATION

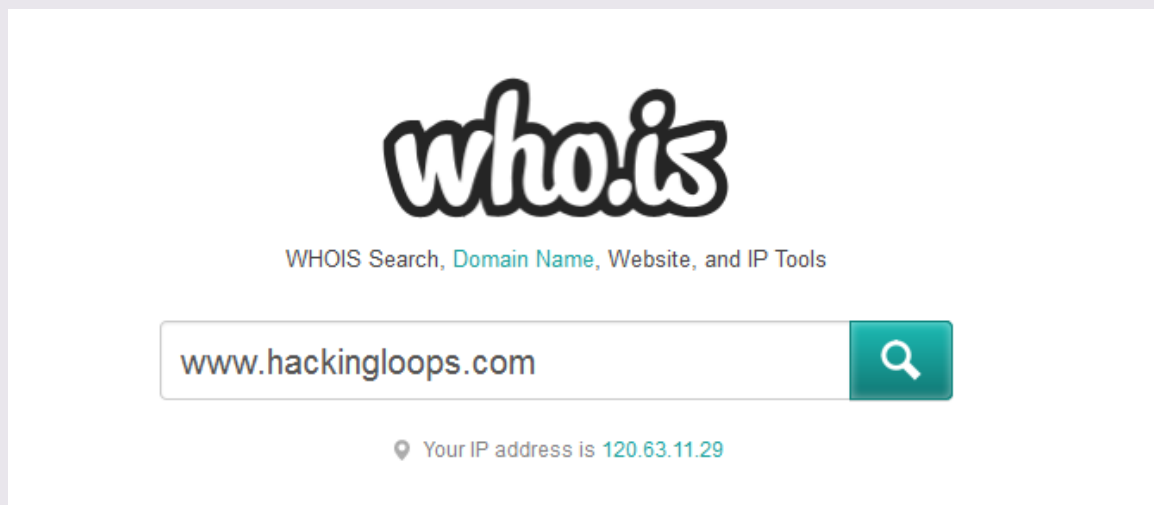
WHOIS or WHO IS Information is basically a query and response protocol, which is used to query the databases which stores details of domain(basically website name) and IP address registrar's. Using **WHOIS** technique we can get personal and contact information of the person who has registered the domain.

For example: If we want to know that who is the owner or registrar of the website www.hackingloops.com and what is his contact information.

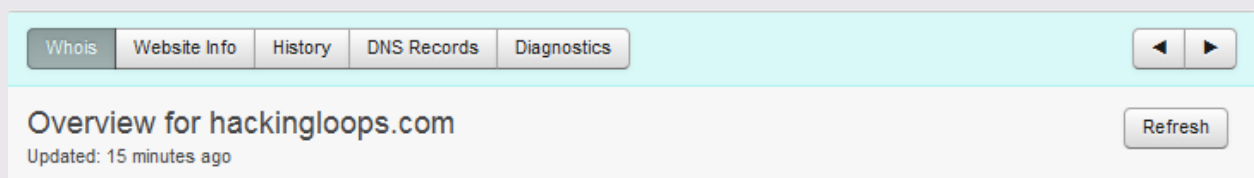
There are several ways of doing it but I will share the easiest and smartest way.

STEPS TO GATHER WHO IS INFORMATION

1. Open the website who.is (Note: No .com or anything, just open who.is).
2. Now Enter the website URL in the text box named "Search Domain Name or IP address" and press enter.



3. Now you will see something like this:



4. Now whois tab is selected as shown above. Now you need to scroll down to see the who is details and contact information.

Registrar Info

Name	BIGROCK SOLUTIONS LIMITED
Whois Server	Whois.bigrock.com
Referral URL	http://www.bigrock.com
Status	clientTransferProhibited

Important Dates

More Info

Expires On	June 30, 2014
Registered On	June 30, 2011
Updated On	July 01, 2011

Name Servers

More Info

dns1.bigrock.in	50.23.136.230
dns2.bigrock.in	50.23.75.44
dns3.bigrock.in	67.15.47.188
dns4.bigrock.in	184.173.150.58

Site Status

IP Address	74.125.139.121
Status	active
Server Type	GSE

Traffic Info

More Info

97,599	▲ 73,629
Alexa Trend/Rank One Month ⓘ	
131,342	▲ 95,514
Alexa Trend/Rank Three Month ⓘ	
2.9	▲ 100%
Page Views Per Visit One Month	
2.1	▲ 26%
Page Views Per Visit Three Month	

This is the general high level information means which seller has registered the domain. But this is not what we want. So scroll down more to get the Raw Registrar's data as shown below:

● Raw Registrar Data

Domain Name: HACKINGLOOPS.COM

1. Domain name(whose details we are searching)

Registrant:

Isoftdl
Lokesh Singh (shiviskingg@gmail.com)
A-304,Shramdeep Apartment,Sector 62
Line 2: (Optional)
Noida
Uttar Pradesh,201307
IN
Tel.  +91.9820251734

Creation Date: 01-Jul-2011
Expiration Date: 01-Jul-2014

2. Actual Contact Information of the Registrant and domain registration date and expiry date.

Domain servers in listed order:

dns1.bigrock.in
dns2.bigrock.in
dns3.bigrock.in
dns4.bigrock.in

3. Domain Name servers used by hackingloops to get IP address details for websites.

Administrative Contact:

Isoftdl
Lokesh Singh (shiviskingg@gmail.com)
A-304,Shramdeep Apartment,Sector 62
Line 2: (Optional)
Noida
Uttar Pradesh,201307
IN
Tel.  +91.9820251734

4. Administrative Contact (Most of time same as Registrant contact

Technical Contact:

Isoftdl
Lokesh Singh (shiviskingg@gmail.com)
A-304,Shramdeep Apartment,Sector 62
Line 2: (Optional)

5. Technical Contact (same as above two).

5. Now we have website registrant's contact information, we can use this to gather more information about the owner of the website. Just Google his contact details to get more info. We can also use email address to find the Social Networking profile, so that we can gather as much information we can.
6. There are more other tabs as shown in step 2 like Website Info tab , History tab, DNS records tab and Diagnostics tab. Website info tab contains the contact information of the owner of website and Meta data like description and keywords of the website as shown below:

● Contact Information

Owner Name	Lokesh Singh
Phone	09820251734
Email	Lokesh @hackingloops.com
Address	A-304, Shramdeep Apartment Noida, Uttar Pradesh 201307 India

● Content Data

Title	Learn How to hack Security Online with Hackingloops
Description	Learn how to hack ethically and get latest security tips, tricks and hacks that will add flavor to your computing life.
Speed: Median Load Time	12990
Links In Count	97

History tab contains the comparison of WHO IS data i.e. How website WHO is looks when it was registered and how it looks today.

● Old Registrar Info August 04, 2011

Name	BIGROCK SOLUTIONS PRIVATE LIMITED
Whois Server	Whois.bigrock.com
Referral URL	http://www.bigrock.com
Status	clientTransferProhibited

● Important Dates

[More Info](#)

Expires On	June 30, 2014
Registered On	June 30, 2011
Updated On	July 01, 2011

● Name Servers

[More Info](#)

dns1.bigrock.in	50.23.136.230
dns2.bigrock.in	50.23.75.44
dns3.bigrock.in	67.15.47.188
dns4.bigrock.in	184.173.150.58

● Registrar Info January 17, 2013

Name	BIGROCK SOLUTIONS LIMITED
Whois Server	Whois.bigrock.com
Referral URL	http://www.bigrock.com
Status	clientTransferProhibited

● Important Dates

[More Info](#)

Expires On	June 30, 2014
Registered On	June 30, 2011
Updated On	July 01, 2011

● Name Servers

[More Info](#)

dns1.bigrock.in	50.23.136.230
dns2.bigrock.in	50.23.75.44
dns3.bigrock.in	67.15.47.188
dns4.bigrock.in	184.173.150.58

● Old Raw Registrar Data August 04, 2011

Registration Service Provided By:
BIGROCK

Contact: [S +91.2230797900](tel:+91.2230797900)

Domain Name: HACKINGLOOPS.COM

Registrant:

Isoftdl
Lokesh Singh (shiviskingg@gmail.com)
A-304, Shramdeep Apartment, Sector 62
Line 2: (Optional)
Noida
Uttar Pradesh, 201307
IN
Tel. [S +91.9820251734](tel:+91.9820251734)

Creation Date: 01-Jul-2011

Expiration Date: 01-Jul-2014

Domain servers in listed order:

dns1.bigrock.in
dns2.bigrock.in
dns3.bigrock.in
dns4.bigrock.in

Administrative Contact:

Isoftdl
Lokesh Singh (shiviskingg@gmail.com)
A-304, Shramdeep Apartment, Sector 62
Line 2: (Optional)
Noida
Uttar Pradesh, 201307
IN
Tel. [S +91.9820251734](tel:+91.9820251734)

● Raw Registrar Data January 17, 2013

Domain Name: HACKINGLOOPS.COM

Registrant:

Isoftdl
Lokesh Singh (shiviskingg@gmail.com)
A-304, Shramdeep Apartment, Sector 62
Line 2: (Optional)
Noida
Uttar Pradesh, 201307
IN
Tel. [S +91.9820251734](tel:+91.9820251734)

Creation Date: 01-Jul-2011

Expiration Date: 01-Jul-2014

Domain servers in listed order:

dns1.bigrock.in
dns2.bigrock.in
dns3.bigrock.in
dns4.bigrock.in

Administrative Contact:

Isoftdl
Lokesh Singh (shiviskingg@gmail.com)
A-304, Shramdeep Apartment, Sector 62
Line 2: (Optional)
Noida
Uttar Pradesh, 201307
IN
Tel. [S +91.9820251734](tel:+91.9820251734)

Technical Contact:

Isoftdl
Lokesh Singh (shiviskingg@gmail.com)

Now the Most important data: DNS Records and website name server records. Next tab contains the DNS records information which is most critical for any website any misconfiguration can result into domain Hijacking attack or domain poisoning.

DNS (Domain name system) is used to translate the website address into IP address. There are several record type associated with DNS like MX for mail servers, NS for name servers, CNAME for translating web address. Details about DNS is below. This is how DNS records will look like:

DNS Records – HACKINGLOOPS.COM

Record	Type	TTL	Priority	Content
hackingloops.com	A	8 hours		216.239.32.21 (Mountain View, CA, US)
hackingloops.com	MX	10 hours 40 minutes	100	mx3.mailhostbox.com
hackingloops.com	MX	10 hours 40 minutes	100	mx1.mailhostbox.com
hackingloops.com	MX	10 hours 40 minutes	100	mx2.mailhostbox.com
hackingloops.com	NS	10 hours 40 minutes		dns4.bigrock.in
hackingloops.com	NS	10 hours 40 minutes		dns2.bigrock.in
hackingloops.com	NS	10 hours 40 minutes		dns1.bigrock.in
hackingloops.com	NS	10 hours 40 minutes		dns3.bigrock.in
hackingloops.com	SOA	10 hours 40 minutes		dns4.bigrock.in. shiviskingg.gmail.com. 2011080501 7200 7200 172800 7200
hackingloops.com	TXT	10 hours 40 minutes		v=spf1 redirect=_spf.mailhostbox.com
www.hackingloops.com	CNAME	8 hours		ghs.google.com

Last but not the least is Diagnostics, this tab contains the two tools PING and Trace Route which we have discussed above. If you are looking for GUI based tools for ping and trace route then this is one of the best tool.

DNS QUERIES

DNS (Domain name system) is basically a hierarchical system of naming any website or resource on the internet or private network. Its main use is to translate the domain name into some meaningful numerical IP address. Like a telephone book, which contains names and their phone number, on similar terms we have Domain name system which has hostnames and their corresponding Unique IP address and DNS queries is that which helps in doing so. Host names can be aliases. Now you all will be wondering that what host name is. Host name is basically the name given to any internet resource like Hackingloops is name of my website. Now to locate any Host name we need an address which we generally call as IP address.

What is DNS Query?

Each domain name (Example: hackingloops.com) is structured in hosts (ex: www.hackingloops.com) and the DNS (Domain Name System) allow everybody to translate the domain name or the hostname in an IP Address to contact via the TCP/IP protocol. There are several types of queries, corresponding to all the implementable types of DNS records such as A record, MX, AAAA, CNAME and SOA.

So DNS query is a query which is used to retrieve the DNS record types of any domain name.

BASIC TERMS RELATED TO DNS (DOMAIN NAME SYSTEM)

1. Host name: It is the logical name assigned to any internet resource.
2. IP address: It is the physical address of the resource i.e. of hostname.
3. Name server: A **name server** is a computer server that hosts a network service for providing responses to queries against a directory service. It maps a *human-recognizable* identifier to a system-internal, often numeric, identification or addressing component. This service is performed by the server according to a network service protocol.
4. TLD (Top Level Domain): A **top-level domain (TLD)** is one of the domains at the highest level in the hierarchical Domain Name System of the Internet. The top-level domain names are installed in the root zone of the name space. For all domains in lower levels, it is the last part of the domain name, that is, the last label of a fully qualified domain name. For example, in the domain name `www.example.com`, the top-level domain is `.com` (or `.COM`, as domain names are not case-sensitive). Management of most top-level domains is delegated to responsible organizations by the Internet Corporation for Assigned Names and Numbers (ICANN), which operates the Internet Assigned Numbers Authority (IANA) and is in charge of maintaining the DNS root zone.
5. DNS Record types: The DNS implements a distributed, hierarchical, and redundant database for information associated with Internet domain names and addresses. In these domain servers, different record types are used for different purposes.
Read More about DNS record types: [Wikipedia](#)
6. DNS Resolver: The client-side of the DNS is called a DNS resolver. It is responsible for initiating and sequencing the queries that ultimately lead to a full resolution (translation) of the resource sought, e.g., translation of a domain name into an IP address.
7. Record Caching: The DNS Resolution Process reduces the load on individual servers by *caching* DNS request records for a period of time after a response.

This entails the local recording and subsequent consultation of the copy instead of initiating a new request upstream. The time for which a resolver caches a DNS response is determined by a value called the time to live (TTL) associated with every record. The TTL is set by the administrator of the DNS server handing out the authoritative response. The period of validity may vary from just seconds to days or even weeks.

8. **Reverse Lookup:** A reverse lookup is a query of the DNS for domain names when the IP address is known. Multiple domain names may be associated with an IP address. The DNS stores IP addresses in the form of domain names as specially formatted names in pointer (PTR) records within the infrastructure top-level domain arpa. For IPv4, the domain is `in-addr.arpa`. For IPv6, the reverse lookup domain is `ip6.arpa`. The IP address is represented as a name in reverse-ordered octet representation for IPv4, and reverse-ordered nibble representation for IPv6.
9. **Resource Records:** A Resource Record (RR) is the basic data element in the domain name system. Each record has a type (A, MX, etc.), an expiration time limit, a class, and some type-specific data. Resource records of the same type define a resource record set (RRset). The order of resource records in a set, returned by a resolver to an application, is undefined, but often servers implement round-robin ordering to achieve Global Server Load Balancing. DNSSEC, however, works on complete resource record sets in a canonical order.

RR (Resource record) fields		
Field	Description	Length (octets)
NAME	Name of the node to which this record pertains	(variable)
TYPE	Type of RR in numeric form (e.g. 15 for MX RRs)	2
CLASS	Class code	2
TTL	Count of seconds that the RR stays valid (The maximum is $2^{31}-1$, which is about 68 years.)	4
RDLENGTH	Length of RDATA field	2
RDATA	Additional RR-specific data	(variable)

Now we are aware of most of the terminologies used in DNS records we can write our own DNS queries.

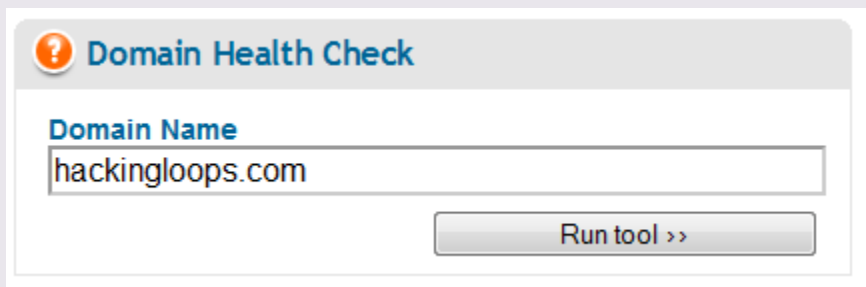
I think we have already discussed above in WHO IS technique that how DNS records will look like. But that was just a brief, for detailed information about the DNS records we need to run the health check for DNS. It can be good as well as bad. Good for developer that he knows where are issues in domain, bad for developer when some hacker knows them as it increases the risk of Domain Hijacking and Domain Poisoning attacks.

HOW TO RUN DNS QUERIES?

There are several methods of executing DNS queries like running DNS health checks or just simply running queries on DNS record types. Which is best? From Hackers point of view DNS health check is best, because more we know, easier to exploit the victim and as Ethical Hacker, again more we know, better we protect.

Steps to run DNS Health Check:

1. Go to website <http://www.dnsqueries.com>
2. Now there you will see several tools related to DNS and IP. Type the domain name in domain health check one as shown below and press run tool.



Domain Health Check

Domain Name
hackingloops.com

Run tool >>

3. Now it will execute all the possible DNS queries on the domain name and display all the record types with details and issues with them if any as shown below.




Results for checks on hackingloops.com		
Category	Test name	Informations
Parent	Parent Zone	The calculated parent zone for your domain is com .
	Parent NS records	The parent zone DNS server a.gtld-servers.net says that your DNS are: dns1.bigrock.in. (No Glue) [TTL: 172800] dns2.bigrock.in. (No Glue) [TTL: 172800] dns3.bigrock.in. (No Glue) [TTL: 172800] dns4.bigrock.in. (No Glue) [TTL: 172800]
	TLD Parent Check	Good. a.gtld-servers.net , the parent server I asked for, has information for your TLD. This is a good thing as there are some other domain extensions like " co.us " for example that are missing a direct check.
	Your nameservers are listed	Good. The parent server a.gtld-servers.net has your nameservers listed. This is a must if you want to be found as anyone that does not know your DNS servers will first ask the parent nameservers.
	Parent sent glue	Since not all the NS records have the same domain's TLD, it is not expected that the parent server sends out glue records!
	DNS servers have A records	Since the domain and the NS are on different TLDs, it's ok if the A records at zone parent server are missing.
NS	Your NS records	Your DNS servers return the following NS records: dns1.bigrock.in.: dns4.bigrock.in. [TTL: 38400] dns2.bigrock.in. [TTL: 38400] dns1.bigrock.in. [TTL: 38400] dns3.bigrock.in. [TTL: 38400] dns2.bigrock.in.: dns3.bigrock.in. [TTL: 38400] dns2.bigrock.in. [TTL: 38400]

		<p>dns3.bigrock.in. ⓘ:</p> <div> <p>dns1.bigrock.in. ⓘ [TTL: 38400]</p> <p>dns4.bigrock.in. ⓘ [TTL: 38400]</p> <p>dns3.bigrock.in. ⓘ [TTL: 38400]</p> <p>dns2.bigrock.in. ⓘ [TTL: 38400]</p> </div> <p>dns4.bigrock.in. ⓘ:</p> <div> <p>dns3.bigrock.in. ⓘ [TTL: 38400]</p> <p>dns1.bigrock.in. ⓘ [TTL: 38400]</p> <p>dns4.bigrock.in. ⓘ [TTL: 38400]</p> <p>dns2.bigrock.in. ⓘ [TTL: 38400]</p> </div>
Open DNS servers	✓	All of your nameservers don't accept recursive queries. This is very good, since can cause problems (anyone could use them) and can cause Denial of Service attacks.
Mismatched glue	ⓘ	<p>Since not all the NS records have the same domain's TLD, i don't have the glues for the NS records</p> <div> <p>dns1.bigrock.in. ⓘ</p> <p>dns2.bigrock.in. ⓘ</p> <p>dns3.bigrock.in. ⓘ</p> <p>dns4.bigrock.in. ⓘ</p> </div> <p>Additionally it can happen that some records with the same domain's TLD mismatch the glues sent by parent name servers</p>
NS A records at nameservers	✗	Your nameserver do not include A records when asked for your NS records.
All nameservers report identical NS records	✓	The NS records at all your nameservers are identical.
All nameservers respond	✓	All of your nameservers listed at the parent nameservers responded.
Nameserver name validity	✓	All of the NS records that your nameservers report seem valid hostnames.
Number of nameservers	✓	You have 4 nameservers. You must have at least 2 nameservers and no more than 7.
Lame nameservers	✓	All the nameservers listed at the parent servers answer authoritatively for your domain.
Mission (stealth) nameservers	✓	All of your nameservers are listed at the parent zone servers.

SOA	Your SOA records	<p>ⓘ Your DNS servers return the following SOA records:</p> <p>dns1.bigrock.in. ⓘ:</p> <div> <p>dns4.bigrock.in. ⓘ shiviskingg.gmail.com. ⓘ 2011080501 7200 7200 172800 7200. [TTL: 38400]</p> </div> <p>dns2.bigrock.in. ⓘ:</p> <div> <p>dns4.bigrock.in. ⓘ shiviskingg.gmail.com. ⓘ 2011080501 7200 7200 172800 7200. [TTL: 38400]</p> </div> <p>dns3.bigrock.in. ⓘ:</p> <div> <p>dns4.bigrock.in. ⓘ shiviskingg.gmail.com. ⓘ 2011080501 7200 7200 172800 7200. [TTL: 38400]</p> </div> <p>dns4.bigrock.in. ⓘ:</p> <div> <p>dns4.bigrock.in. ⓘ shiviskingg.gmail.com. ⓘ 2011080501 7200 7200 172800 7200. [TTL: 38400]</p> </div>
-----	------------------	---


MX	Your MX records	<p> Your DNS servers return the following MX records: dns1.bigrock.in. </p> <div> 100 mx1.mailhostbox.com. [TTL: 38400] 100 mx3.mailhostbox.com. [TTL: 38400] 100 mx2.mailhostbox.com. [TTL: 38400] </div> <p>dns2.bigrock.in. </p> <div> 100 mx2.mailhostbox.com. [TTL: 38400] 100 mx1.mailhostbox.com. [TTL: 38400] 100 mx3.mailhostbox.com. [TTL: 38400] </div> <p>dns3.bigrock.in. </p> <div> 100 mx1.mailhostbox.com. [TTL: 38400] 100 mx3.mailhostbox.com. [TTL: 38400] 100 mx2.mailhostbox.com. [TTL: 38400] </div> <p>dns4.bigrock.in. </p> <div> 100 mx1.mailhostbox.com. [TTL: 38400] 100 mx2.mailhostbox.com. [TTL: 38400] 100 mx3.mailhostbox.com. [TTL: 38400] </div>
	Multiple MX records	You have multiple MX records and this is a very good thing! When one MX server is down the others can continue to accept mail.
	Invalid characters	It seems that all of your MX records use valid hostnames, without any invalid characters.
	All MX IPs public	Your NS don't return their IPs when looking explicitly for MX records.
	MX records are not CNAMEs	None of the lookups of your MX records did return CNAMEs.
	MX A lookups have no CNAMEs	Looking up for the A records of your MX servers i did not detect problems.
	MX is host name, not IP	All the MX records retrieved are host names. Using IP addresses in MX records is not allowed.
	Differing MX-A records	I have searched for differing IPs for your MX records between what are declaring your NS and the authoritative NS for the MX records. All was fine.

MAIL	Connect to mail servers	I have connected successfully to all of your mailservers. <div> mx1.mailhostbox.com. : Connected with greeting: mx1.mailhostbox.com mx3.mailhostbox.com. : Connected with greeting: mx1.mailhostbox.com mx2.mailhostbox.com. : Connected with greeting: mx1.mailhostbox.com </div>
	Mail server host name in greeting	The configuration of your mail servers and your DNS are not ok! The report of the test is: <div> mx1.mailhostbox.com. -> mx1.mailhostbox.com -> 70.87.29.2 -> mx1.mail.pw mx3.mailhostbox.com. -> mx1.mailhostbox.com -> 70.87.29.2 -> mx1.mail.pw mx2.mailhostbox.com. -> mx1.mailhostbox.com -> 70.87.29.2 -> mx1.mail.pw </div> <p>Spam recognition software and RFC821 4.3 (also RFC2821 4.3.1) state that the hostname given in the SMTP greeting MUST have an A record pointing back to the same server.</p>
	Acceptance of NULL <> sender	All of your mailservers accept mail from "<>". RFC1123 5.2.9 requires all mailservers to receive mail from this kind of address, which is used in reject/bounce messages and return receipts. The report of the test is: <div> mx1.mailhostbox.com. : Accepts null sender mx3.mailhostbox.com. : Accepts null sender mx2.mailhostbox.com. : Accepts null sender </div>
	Acceptance of postmaster address	Not all of your mailservers accept mail to postmaster@hackingloops.com.. RFC822 6.3, RFC1123 5.2.7, and RFC2821 4.5.1 require all mailservers to accept mail to this kind of address. The report of the test is: <div> mx1.mailhostbox.com. : Does not accept mail to postmaster@hackingloops.com. mx3.mailhostbox.com. : Does not accept mail to postmaster@hackingloops.com. mx2.mailhostbox.com. : Does not accept mail to postmaster@hackingloops.com. </div>

WWW	WWW Record	 I have asked your DNS server for www.hackingloops.com. but i did not receive an IP address (maybe i received a CNAME...), however these are the records i received: <div style="border: 1px solid #add8e6; padding: 5px; margin: 5px 0;"> www.hackingloops.com. = CNAME ghs.google.com. </div>
	All WWW IPs public	 I have no ip addresses to check
	CNAME Lookup	 There is one or more CNAMEs record pointing to www.hackingloops.com. . This can cause extra bandwidth usage since the resolution of www.hackingloops.com. is done in multiple steps. However this is only a warning!

I think there is now no need to explain these terms more because report explains more than enough.

You can try individual records too by just scrolling down on dnsqueries.com website as shown below:

 **Perform DNS query**

HostName:

Type:

MX ▼

Just select put the domain name and select the record type and run the tool. But after checking health check it's really of no use.

That's all I this issue, will continue our Foot-printing and Information Gathering techniques in the next issue.

ⁱ If a Hacker wants to get into your system then he will, what all you can do is that make his entry harder.