TRACING an IP

Introduction

In here I have figure out some very easy but cool ways to trace out the geographical location and various other infos like ISP details etc of a remote computer using its IP.

Well I guess its one of the most important must learn manul for boys out there if you want to impress your friends particularly gals whom you'll meet online in a chat room and tell them their geographical locations and ISP details and make them surprised and impressed J.

In the practical execution of this manual you don't have to work much as it is very simple only you have to use your brain to understand some symbols and some format of expressions and use your IQ to execute things the right way.

What is IP and how to get the IP of a remote system

Getting the IP or Internet Protocol of a remote system is the most important and the first step of hacking into it. Probably it is the first thing a hacker do to get info for researching on a system. Well IP is a unique number assigned to each computer on a network. It is this unique address which represents the system on the network. Generally the IP of a particular system changes each time you log on to the network by dialing to your ISP and it is assigned to you by your ISP. IP of a system which is always on the network remains generally the same. Generally those kind of systems are most likely to suffer a hacking attack because of its stable IP. Using IP you can even execute system commands on the victim's computer.

Lets take the example of the following IP address: 202.144.49.110 Now the first part, the numbers before the first decimal i.e. 209 is the Network number or the Network Prefix.. This means that it identifies the number of the network in which the host is. The second part i.e. 144 is the Host Number that is it identifies the number of the host within the Network. This means that in the same Network, the network number is same. In order to provide flexibility in the size of the Network, here are different classes of IP addresses:

Code:

```
Address Class               Dotted Decimal Notation Ranges

Class A ( /8 Prefixes)         1.xxx.xxx.xxx through 126.xxx.xxx.xxx

Class B ( /16 Prefixes)        128.0.xxx.xxx through 191.255.xxx.xxx

Class C ( /24 Prefixes)        192.0.0.xxx through 223.255.255.xxx
```

The various classes will be clearer after reading the next few lines.

Each Class A Network Address contains a 8 bit Network Prefix followed by a 24-bit host number. They are considered to be primitive. They are referred to as "/8"s" or just "8's" as they have an 8-bit Network prefix.

In a Class B Network Address there is a 16 bit Network Prefix followed by a 16-bit Host number. It is referred to as "16's".

A class C Network address contains a 24-bit Network Prefix and a 8 bit Host number. It is referred to as

"24's" and is commonly used by most ISP's.

Due to the growing size of the Internet the Network Administrators faced many problems. The Internet routing tables were beginning to grow and now the administrators had to request another network number from the Internet before a new network could be installed at their site. This is where sub-netting came in.

Now if your ISP is a big one and if it provides you with dynamic IP addresses then you will most probably see that whenever you log on to the net, your IP address will have the same first 24 bits and only the last 8 bits will keep changing. This is due to the fact that when sub-netting comes in then the IP Addresses structure becomes:

xxx.xxx.zzz.yyy

where the first 2 parts are Network Prefix numbers and the zzz is the Subnet number and the yyy is the host number. So you are always connected to the same Subnet within the same Network. As a result the first 3 parts will remain the same and only the last part i.e. yyy is variable.

****

For Example, if say an ISP xyz is given the IP: 203.98.12.xx Network address then you can be awarded any IP, whose first three fields are 203.98.12. Get it?

So, basically this means that each ISP has a particular range in which to allocate all its subscribers. Or in other words, all subscribers or all people connected to the internet using the same ISP, will have to be in this range. This in effect would mean that all people using the same ISP are likely to have the same first three fields of their IP Addresses.

This means that if you have done a lot of (By this I really mean a lot) of research, then you could figure out which ISP a person is using by simply looking at his IP. The ISP name could then be used to figure out the city and the country of the person. Right? Let me take an example to stress as to how cumbersome but easy (once the research is done) the above method can be.

In my country, say there are three main ISP's:

Code:

```
ISP Name                Network Address Allotted

ISP I                      203.94.47.xx

ISP II                     202.92.12.xx

ISP III                    203.91.35.xx
```

Now, if I get to know the IP of an e-pal of mine, and it reads: 203.91.35.12, then I can pretty easily figure out that he uses ISP III to connect to the internet. Right? You might say that any idiot would be able to do this. Well, yes and no. You see, the above method of finding out the ISP of a person was successful only because we already had the ISP and Network Address Allotted list with us. So, what my point is, that the above method can be successful only after a lot of research and experimentation. And, I do think such research can be helpful sometimes.

Also, this would not work, if you take it all on in larger scale. What if the IP that you have belongs to someone living in a remote igloo in the North Pole? You could not possibly get the Network Addresses of all the ISP’s in the world, could you? If yes please send it to me J.

Well now I guess you have pretty good knowledge about what an IP is and what you can do by knowing the IP of a remote system. Now lets come to the point of finding out the IP of remote system.

Well you can easily figure out the IP of a remote system using the netstat utility available in the microsoft’s version of DOS. The netstat command shows the connections in which your system is engaged to and the ports they are using. Suppose you are checking your mail in hotmail and you want to find out the IP of msn. All you need to do is to open a dos window (command.com) and type netstat. You will see all the open connections of your system. There you will see something :

Code:

```
Proto  Local Address          Foreign Address            State

  TCP    abhisek:1031           64.4.xx.xx:80           ESTABLISHED
```

Now you got the IP address of hotmail *** 64.4.xx.xx .

Similarly you can figure out the IP address of most http or ftp connections.

To know your own IP type the following command in a dos windows

C:\netstat –n

[this commands converts the IP name into IP addresses]

this is what you will probably see on typing the above command :

Code:

```
Proto    Local Address          Foreign Address        State

  TCP    203.xx.251.161:1031    194.1.129.227:21       ESTABLISHED

  TCP    203.xx.251.161:1043    207.138.41.181:80      FIN_WAIT_2

  TCP    203.xx.251.161:1053    203.94.243.71:110      TIME_WAIT

  TCP    203.xx.251.161:1058    194.1.129.227:20       TIME_WAIT

  TCP    203.xx.251.161:1069    203.94.243.71:110      TIME_WAIT

  TCP    203.xx.251.161:1071    194.98.93.244:80       ESTABLISHED

  TCP    203.xx.251.161:1078    203.94.243.71:110      TIME_WAIT
```

Here 203.xx.251.161 is your IP address.

Now lets clarify the format used by netstat :

Proto : It shows the type of protocol the connection with the remote system is using.

Here TCP (transmission control protocol) is the protocol used by my system to connect to other systems.

Local Address : It shows the local address ie the local IP. When the netstat command is executed without –n switch then the name of the local system is displayed and when the netstat is executed with –n switch then the IP of the local system is displayed. Here you can also find out the port used by the connection.

xxx.yyy.zzz.aaa:1024

in this format you will see the local address. Here 1024 is the port to which the remote system is connected in your system

Foreign Address :: It shows the IP address of the remote system to which your system is connected. In this case also if the netstat command is excuted with –n switch then you directly get the IP of the victim but if the netstat is executed without –n switch then you will get the address of the remote system. Something like

```
C:\netstat

Proto Local Address Foreign Address State

TCP abhisek:1031 msgr.lw4.gs681.hotmail.com:80 ESTABLISHED
```

Here msgr.lw4.gs681.hotmail.com is the address of the foreign system . putting this address in any IP lookup program and doing a whois lookup will reveal the IP of the remote system.

Note: The port to which your system is connected can be found from this in the same way as I have shown in the case of local address. The difference is that, this is the port of the remote system to which your computer is connected to.

Below I have produced a list of ports and popular services generally found to be running.

21 :: FTP port

80 :: http port

23 :: Telnet port

Note: If your execute the netstat command and find ports like 12345,27374 are open and are in use then make it sure that your sweat heart computer is infected with her boyfriend.. J J J J I mean your computer is infected with some sort of Trojan.

Below I have produced a list of commonly known Trojans and the ports they use by default. So if you find these ports open then get a good virus buster and get these stupid servers of the Trojans kicked out. Well if you want to play with these Trojan by keeping them in your computer but not letting them ruin your system performance then just disble it from the system registry run and they wont be loaded to memory each time when windows starts up[This trick doesn’t work for all Trojans].

Code:

```
Netbus            ::          12345(TCP)

Subseven          ::          27374(TCP)

Girl Friend       ::          21554(TCP)
```

```
Back Oriface      ::          31337 (UDP)
```

Well guys and gals I hope you are now well familiar with the term IP and what is the utility of IP in cyber world and how to get the IP of a remote system to which you are connected. I hope you find my writings very easy to undertstand. I know I lack the capacity of explaining myself but I try my level best to make things very easy and clear for you'll.

How to get the IP of a remote system while chatting through msn messenger ::

This is a tutorial on how to get IP address from MSN messenger. This is actually a really easy thing to do. It is not like going through the hard time and reversing MSN messenger like many people think.

The IP address is only given when you accept or are sending a file through MSN messenger. When you send IM's, the message is sent through the server thus hiding your victims IP and your. But when you send a file or recieve a file, it is direct connection between the two computers.

To obtain the IP accept a file transfer or send a file to the victim, when the file sending is under way from the dos prompt type "netstat" without the quotation marks. You should get a table like this:

```
Proto Local Address Foreign Address State
TCP kick:1033 msgr-ns29.msgr.hotmail.com:1863 ESTABLISHED
TCP kick:1040 msgr-sb36.msgr.hotmail.com:1863 ESTABLISHED
TCP kick: <REMOTE HOST> ESTABLISHED
```

The top name in the list is the server's address for IMing. There could be many of the second name in the list, as a new connection is made to the server for every room you are IMing to. You are looking for the address of the remote host in this table it may be something similar to "host63-7-102-226.ppp.cal.vsnl.com" or “203..64.90.6”. without the quotation marks.

All you need to do now is to put this address in you IP lookup programe and get the IP of the remote system.

Well 50%of the work is done now. Now you know how to get the IP of a remote system, so its time to trace it down and find some details about the IP.

Tracing an IP is quite simple. You can do it the easy way by using some sweet softwares like Visual Trace 6.0b

ftp://ftp.visualware.com/pub/vr/vr.exe

Neotrace

http://www.neoworx.com/download/NTX325.exe

or by our way ie. Using MS DOS or any other version of DOS.

Well I suggest you to use DOS and its tracert tool for tracing the IP cause using it will give you a clear conception about the art of tracing an IP and I guarantee that you will feel much satisfied on success than using a silly software. Furthur you will know how things work and how the IP is traced down and the different networks associated in this tracing process.

Let us take a look at tracert tool provided for DOS by Microsoft.

It is a very handy tool for peoples need to trace down an IP.

Just open any DOS windows and type tracert.

C:\windows>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name

Code:

```
Options:

    -d                 Do not resolve addresses to hostnames.

    -h maximum_hops    Maximum number of hops to search for target.

    -j host-list       Loose source route along host-list.

    -w timeout         Wait timeout milliseconds for each reply.
```

You will now see a description of the tracert command and the switches associated with it.

Well these switches doesn’t makes much difference. All you can do is to increase the timeout in milliseconds by using –w switch if you are using a slow connection and the –d switch if you wish not resolve address to hostnames by default.

By default tracert performs a maximum of 30 hops trace. Using the –h switch you can specify the number of hops to perform.

Now its time for execution.

Let us trace down the IP yahoo.com [216.115.108.243]

TIP: If you have done a long research (I mean a lot) then simply looking at the IP you can figure out some info from it. For example the IP 203.90.68.8 indicates that the system is in India. In India IPs generally begin with 203 and 202

C:\WINDOWS>tracert yahoo.com

Tracing route to yahoo.com [216.115.108.243] over a maximum of 30 hops:

Code:

```
  1   308 ms   142 ms   127 ms  203.94.246.35

  2   140 ms   135 ms     *     203.94.246.1

  3   213 ms   134 ms   132 ms  203.94.255.33

  4   134 ms   130 ms   129 ms  203.200.64.29

  5   122 ms   135 ms   131 ms  203.200.87.75

  6   141 ms   137 ms   121 ms  203.200.87.15
  7   143 ms   170 ms   154 ms  vsb-delhi-stm1.Bbone.vsnl.net.in
[202.54.2.241]

  8   565 ms   589 ms   568 ms  if-7-0.bb8.NewYork.Teleglobe.net
[207.45.198.65]

  9   596 ms   584 ms   600 ms  if-3-0.core2.NewYork.teleglobe.net
[207.45.221.66]

 10     *        *        *     Request timed out.

 11   703 ms   701 ms   719 ms  if-3-0.core2.PaloAlto.Teleglobe.net
[64.86.83.205]

 12   694 ms   683 ms   681 ms  if-6-1.core1.PaloAlto.Teleglobe.net
[207.45.202.33]

 13   656 ms   677 ms   700 ms  ix-5-0.core1.PaloAlto.Teleglobe.net
[207.45.196.90]

 14   667 ms   673 ms   673 ms  ge-1-3-0.msr1.pao.yahoo.com [216.115.100.150]

 15   653 ms   673 ms   673 ms  vl20.bas1.snv.yahoo.com [216.115.100.225]

 16   666 ms   676 ms   674 ms  yahoo.com [216.115.108.243]

Trace complete.
```

Note: Here I have traced yahoo.com. In place of yahoo.com you can give the IP of yahoo or any other IP you want to trace, the result will be the same.

Now carefully looking at the results you can figure out many information about yahoo's server [216.115.108.243]

First packets of data leave my ISP which is at 203.94.246.35 .Similarly you can find out the different routers through which the packets of data are send and received to and from the target system. Now take a look at the 13th line you'll see that the router is in PaloAlto.Teleglobe.net from this you can easily figure out that the router is in Palo Alto. Now finally look at the target system ie. Yahoo's server vl20.bas1.snv.yahoo.com . Now you got the address of yahoo's server. Now put this address in any IP lookup programe and perform and reverse DNS lookup and you will get most of the info about this address,like the place where it is in.

Well another thing you can find out using the tracert tool is that the number of hops (routers) the target system is away from you. In case of tracerouting yahoo.com we find that the target system ie yahoo's server is 16 hops away from my system. This indicates that there are 16 routers between my system and yahoo's server.

Apart from tracing an IP you can find out many usefull details about the target system using the tracert tool.

Firewall Detection

While tracerouting a target system, if you get * as an output then it indicates timeout error. Now if you peform another tracerout to the same taeget system at some other time with a good connection and in this way few times more and if you always get * as the output then take it for sure that the target system is running a firewall which prevents sending of data packets from the target system.

Example

Some days ago I tried to tracert hotmail’s server in plain and simple way using tracert without any trick.This is what I found out :

c:\windows>tracert 64.4.53.7

Tracing route to lc2.law5.hotmail.com [64.4.53.7]

over a maximum of 30 hops:

Code:

```
  1     *        *        *     Request timed out.

  2   161 ms   147 ms    85 ms  203.90.69.81

  3   126 ms   261 ms   219 ms  203.90.66.9

  4   121 ms   115 ms   228 ms  delswp2.hclinfinet.com [203.90.66.133]

  5   727 ms   725 ms   711 ms  203-195-147-250.now-india.net.in
[203.195.147.250]

  6  1006 ms   794 ms   952 ms  core-fae-0-0.now-india.net.in [203.195.147.3]

  7   826 ms   731 ms   819 ms  213.232.106.9

  8   885 ms   744 ms   930 ms  213.166.3.209

  9   851 ms  1020 ms  1080 ms  213.232.64.54

 10  1448 ms   765 ms  1114 ms  pos8-0.core2.London1.Level3.net
[212.113.0.118]

 11   748 ms   789 ms   750 ms  ge-4-2-1.mp2.London1.Level3.net
[212.187.131.146]

 12   719 ms   733 ms   846 ms  so-3-0-0.mp1.London2.Level3.net
[212.187.128.46]
```

```
 13   775 ms   890 ms   829 ms  so-1-0-0.mp2.Weehawken1.Level3.net
[212.187.128.138]

 14   853 ms   852 ms   823 ms  so-3-0-0.mp1.SanJose1.Level3.net
[64.159.1.129]

 15   889 ms   816 ms   803 ms  so-7-0-0.gar1.SanJose1.Level3.net
[64.159.1.74]

 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.
```

I performed the same tracert many times a day but concluded with the same result. This indicates that the systems after the router SanJose1.Level3.net has firewalls installed which prevents the outgoing of data packets.

Detecting Traceroute Attempts on your System

You can detect that an attacker is performing a traceroute on your system, if you see the following symptoms:
1. If you observe port scans on very high UDP ports. This symptom means that the attacker has performed a traceroute on your system. However, it could also mean a simply port scan. Either way, it signifies the fact that your system is being scanned.
2. If the packet-monitoring tool installed in your network, picks up several outgoing TTL-exceeding messages, then it is yet another sign that someone is doing a traceroute on your system.
3. If in these log files, you also observer an outgoing ICMP port unreachable error message, then it means that since a traceroute was done on your system and as the target system i.e. your system, was reached, it responded with this error message.

You can also find our more information on the attacker (if he performs a traceroute on your system) by simply studying the sniffer log files. If you observer the TTL values, then we can easily figure out the following information on the attacker by making use of OS detection techniques discussed earlier in this white paper:

1. The Operating System running on the attacker's target system.
2. Number of hops away, the attacker is from you.

OKI DOKI that's all for this article. Hope you will find this article very easy to understand and implement.

Source: http://www.go4expert.com/articles/tracing-an-ip-t11846/