DonkBoy Internet
Home of the famous
Information Archives.
Terms of use

Traceroute is definitely a very exciting tool or utility. It should indeed be a part of every hacker's toolkit as it can be used to gain some very important information regarding the target system's configuration and its network configuration. In this white paper, we will not only understand the workings and intricacies of this kewl utility, but we will also explore all its possible uses and resourcefulness.

Traceroute was originally developed with the intention of providing a debugging tool, which could be used to pinpoint the exact system or computer on a network (Internet or a Local Network), which was causing the problem experienced. Whenever there was a problem in the data transit or whenever there was a network problem, then the traceroute tool provided the network administrator with an option, which could be used to pinpoint the exact system in the network that was the root of the problem. In other words, the traceroute tool could be used to trace the path of the entire network or a part of the entire network and in this process pinpoint the exact system that was causing the problem experienced.

However, the bottom line remained that the traceroute tool could indeed be used to trace the path taken by a packet from the source system to the destination system, over the Internet.

Whenever a particular chunk of data is to sent from the source system to the destination system, then the data packets sent are first routed through a number of routers (on way to the destination system and if there are any routers in between.) and only then do the data packets arrive at the destination system. The typical path taken by data packets sent by the source to the destination has been depicted by the below figure:

Source System---------à Router of the Source Network----------à Router of the Source Network's ISP-------à Router of the Destination 's ISP-------à Router of the Destination Network-----à Destination System.

Whenever data travels over the Internet, then it is not necessary that the data packets in question, would automatically take the shortest path possible from the source to the destination system. More often than not, data packets sent across a network end up taking a much longer route than what the shortest route is. This means that most of the times data packets sent across a network end up taking more time for the data transit to be completed, than what it should actually be taking. This brings us to a widely known feature of the Internet:

"It is not necessary for all data packets sent from the same source system to the same destination system across a network, to take the same exact route every single time."

Thus the traceroute tool can be used in order to trace the route taken by data packets from the source system to the destination system. Traceroute displays all the routers through which data packets pass on way to the destination system from the source system. Thus, in effect, we come to know the exact path taken by the data packets in the data transit.

"Traceroute can be used to depict the exact path taken by data packets from the source system to the destination system. However, the path displayed by Traceroute for two data packets sent from the same source system to the same destination system in two different sessions may or may not vary."

For Example,

The below example exhibits a simple traceroute to a remote host, displaying all the routers on way to the destination system:

```
C:\WINDOWS>tracert 202.*.2.241
```

```
Tracing route to 202.*.2.241over a maximum of 30 hops:

1 146 ms 138 ms 126 ms 203.94.246.35
2 146 ms 137 ms 127 ms 203.94.246.1
3 126 ms 133 ms 129 ms 203.94.255.33
4 130 ms 122 ms 128 ms 206.103.10.113
5 134 ms 139 ms 132 ms 203.200.87.75
6 140 ms 125 ms 128 ms 203.200.87.15
7 220 ms 146 ms 137 ms delhi-stm1.Bbone.vsnl.net.in [202.*.2.241]
```

Traceroute: A Look Under The Hood

The Internet Control Message Protocol or the ICMP protocol is that protocol of the TCP/IP suite, which handles or is used for diagnosing networking problems and reporting error messages. Whenever an error occurs during the data transit then the ICMP protocol jumps in and does the job of reporting and displaying the error that occurred. Thus, the main function of the ICMP protocol is to communicate the error messages to the host and the client systems.

"The ICMP Protocol reports and displays all errors that took place in the data transfer."

The Traceroute tool can be considered to be a part of the ICMP protocol as it makes use of mainly this protocol. The reason why traceroute is able to display the path between the source and destination system is by making use of the ICMP protocol and the error messages that it displays.

The format of a typical ICMP error message, is as follows:

```
______________________________________________________________________
| | | |
| 8-Bit Type | 8-bit Code | Checksum Value |
| | | |
|_____________ |_____________________|_________________________________|
| |
| |
| |
| (Contents depending upon Error that occurred.) |
| |
| |
| |
|_____________________________________________________________________ |
```

The 'Type' and 'Code' fields are the fields, which stand for the type of error message that has occurred. These fields contain a particular value, which tells the client and the host systems as to what error has occurred.

The two error messages that Traceroute mainly makes use of are as follows:

1. The Time Exceeded error message: It has a 'type' value of 11 and a 'code' value of 0. The Time Exceeded error occurs when a particular system receives a data packet with a TTL or Time to Live value of 0 or 1. The below will further explain as to when the this error message is displayed:

"If a system receives a data packet whose TTL field has a value of 0 or 1, then it sends the Time Exceeded error message to the client, who sent the data packet to it."

2. The Port Unreachable error message: It has a 'type' value of 3 and a 'code' value of 3. This error message is displayed when the client system is trying to establish a connection with the host system on a closed port. In other words, such an error occurs when the client system is trying to establish a connection with a port where there is no service or daemon running.

"If a client tries to establish a connection with the host on a closed port, then the host replies with a Port Unreachable error message, sent to the client."

It is with the use of these two ICMP error messages that the Traceroute tool is able to display or trace the exact path from the source system to the destination system. Before we move onto the exact explanation of the working of the traceroute tool, let us learn as to what TTL or Time to Live is?

The Time To Live or the TTL value of a data packet is an 8-bit field, which determines the maximum number of routers through which that particular data packet can pass through. In other words, the TTL value decides the maximum number of routers through which the data packet can pass, before it must be discarded. The TTL value is to a data packet, what the value of maximum age is to a human.
The TTL value depicts the maximum number of routers through which it can pass, before it is declared 'dead' and is dropped.

The TTL value of a packet is set by the source system each time a new data packet is sent by it. The value of the TTL field set by the source system varies from system to system depending upon the operating system running on it. Each router receiving a data packet is expected to decrement the TTL value of that particular packet by 1. This means that if the initial TTL value set by the source system is 64 and if this particular packet passes through 2 routers, then its final TTL value will become 62.

Each time a router receives a data packet, it checks to see what the TTL value of that particular packet is. According to the TTL value of the received packet, the following two cases can take place:

1. If the TTL value of the received packet is greater than 1, then the router decrements this TTL value by 1 and forwards the data packet to the next router.

2. If the TTL value of the received packet is either 0 or 1, then the router discards the data packets and sends back a "Time Exceeded" ICMP error message to the source system, which originally had sent the data packet.

"If the TTL value of the received data packet is greater than 1, then the router decrements the TTL value by 1 and forwards the data packet to the next router. However, if the TTL value of the received data packet is either 0 or 1, then the router discards the packet and sends back a Time Exceeded ICMP error message to the source system."

The original reason behind the introduction of the TTL value was to ensure that the data packets sent across networks, do not end up in infinite loops, which may occur due to unfinished transactions or when the client or server shuts disconnects from the network without following the proper steps required to close all the open connections. However, today the same concept of TTL values is being widely used in the form of the Traceroute command in order to trace paths between source and destination systems on the Internet.

The first step in the traceroute command is that it creates a packet with a TTL value of 1 and sends it to the destination system (to which the path is to be traced). The first router on way to the destination system from the source system (on which the command was executed) will discard the data packet, as the TTL value of this received data packer is 1. In addition, this first router will also send back a "Time Exceeded" error message to the source system. Since this Time Exceeded error message received by the source system, has its source IP Address as that of the first router, as a result the traceroute tool (running on the source system) will come to know this IP Address of the first router. In this way, the traceroute command comes to know the Address of the first router on the path to the destination system and displays it on the screen.

Similarly, in the next step, traceroute sends a data packet with a TTL value of 2 to the destination system. The first router receiving this data packet will decrement the TTL value of the packet by 1 to 1 and then it would forward the packet to the second router on path to the destination system. This second router would in turn, discard this packet and send back a "Time Exceeded" error message to the source system. Hence, revealing its IP Address. Please note that the second router discards this packet, as the TTL value of this packet is 1.

This process of sending packets with increasing TTL values is carried out, until the data packet has a TTL value high enough to make sure that it reaches the destination system.

Following the above method, Traceroute is able to trace the entire path from the source system to the destination system and also in the process gather the hostnames and IP Addresses of all routers on the path. Until now traceroute has made use of only the first (Time Exceeded) of the two ICMP error messages that we discussed earlier.

When the TTL value is high enough for the data packet to reach the destination system, then by the time the destination system receives the data packet, its TTL value would have been decremented to 1. However, even though the destination system will receive a data packet having a TTL value of 1, it will not discard the packet. This is because the destination (i.e. the system to which the path was to be traced) has been reached. Since the destination system does not discard the data packet that it receives, it means that the destination system does not generate a Time Exceeded error message. As a result, since no "Time Exceeded" error message is generated, the source system does not have any way by which it can ensure that the destination system has been reached.

Thus, in order to deduce that the destination system has indeed been reached, the traceroute command makes use of the "Port Unreachable" error message.

We have already seen in the previous sections that the host generates the "Port Unreachable" error message, when a client is trying to establish a connection with it on a closed port. Traceroute sends UDP (User Datagram Protocol) packets to the destination system on extremely high ports. These high port numbers are chosen in such a manner, that the traceroute tool is sure that there is no service running on these high ports. In effect, the traceroute tool is actually trying to establish a connection on a closed port. Since the destination system receives UDP packets addressed to high "closed" ports, it thus replies with the "Port Unreachable" ICMP error message.

The source system thus can identify that the destination system has been reached, as it would receive a "Port Unreachable" error message from it.

"In the Traceroute tool, if the source system receives a Time Exceeded error message, then a router must have generated it. However, if the source system receives a Port Unreachable error message, then the destination system must have generated it"

The actual working of the traceroute command can be summarized in the following steps:

1. The Traceroute tool sends UDP packets to the destination system on a high port number chosen such that there is no service running on it. Since the chosen port to which the UDP packet have been sent is closed, as a result the destination system replies with a "Port Unreachable" ICMP error message. In this manner, the source system gets to know the Destination system's identity.

2. Traceroute then performs the process of sending data packets with increasing TTL values to the destination system, starting with the initial TTL value of 0. This process reveals the identity of all the routers on the path from the source to the destination system.

3. Traceroute just has to differentiate between the two ICMP error messages that it engineered and received and it will be able to trace the path from the source system to the destination system. The fact that the routers generate a different error message as compared to the destination system is used to differentiate

between the two.

"Each router that handles an IP datagram is required to decrement the datagram's TTL value by one or by the number of seconds it holds it. As almost all routers do not hold a datagram longer that 1 second, the TTL value has thus essentially become a hop counter, giving the number of routers through which the datagram has passed."

The following is an example of the typical results displayed by a traceroute command executed on a Windows system:

```
C:\WINDOWS>tracert yahoo.com

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

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.
```

Uses of the Traceroute command

Besides being used to identify the system causing the problem in the data transit, traceroute is also used for several different purposes:

1. To trace the geographical location of a particular system.

If one observes the above example closely, then one would find that Traceroute also displays the hostnames of all routers on way to the destination system and also the hostname of the destination system. Hostnames are nothing but the human understandable representations of IP Addresses. They besides containing the address of a system also may or may not store within themselves, some important information on the geographical location of that particular system.

For Example,

In our example we see that the ninth hostname displayed by traceroute is:

if-3-0.core2.NewYork.teleglobe.net

This hostname clearly indicates that that particular router is situated in New York, USA.

Similarly, one should also watch out for hostnames ending in country codes.

For Example,

xyz.jp would mean that that particular system is situated in Japan.

For a complete Country Code Reference List, kindly visit: http://hackingtruths.box.sk/cc.txt

Thus, we can say that Traceroute in some cases can actually be used to pinpoint the exact location of a system on the globe. In most cases, Traceroute is indeed able to locate the city and country in which a particular system is located. Visual Traceroute is specifically widely used for tracing the geographical location of a system on the Internet.

2. To Get Information on Network Topography

Using the traceroute command, one can find out the manner in which a particular network is structured, the class to which it belongs and in general, to get related information on topography of a remote network. Getting more information on the network topography of the target network can be used to determine a list of possible weak points, which could be exploited.

3. Firewall Detection Purposes

Using the traceroute tool, one can also detect the presence of a firewall installed on the target system's network. If you execute traceroute and find the '*' (asterix) sign as an entry in the output, then it means that the traceroute attempt has timed out. However, if you repeat the same traceroute procedure to the target system several times at different times of the day and still receive the same output with the '*', then it probably means that a firewall has been installed on the target system. The asterix signs are being displayed as the firewall installed on the target system's network is filtering out your traceroute attempts and as a result, the target system does not reply to your requests and thus a time out is "artificially created" by the firewall.

The above concept can be summarized in the following steps:

1. Your traceroute program sends packets to the target system, however the firewall installed on the target system's network intercepts these packets, making sure that the target system does not receive them.

2. Since the target system does not receive the Traceroute data packets, as a result it does not reply with the ICMP error message, as it is normally supposed to. Thus, your system does not receive any response.

3. After the passage of some amount of time, if still no response is received, then the connection gets timed out, due to "artificial" conditions created due to the filtering done by the firewall. As a result, asterix are displayed in the output.

A typical output, which shows the presence of a firewall installed on the target system, is as below-:

```
C:\windows>tracert target.com
Tracing route to target.com [207.x.197.100] over a maximum of 30 hops:

1 140 ms 126 ms 128 ms 203.94.246.35
2 137 ms 125 ms 138 ms 203.94.246.1
3 125 ms 136 ms 169 ms 203.94.255.33
4 137 ms 139 ms 130 ms 203.200.64.149
5 138 ms 119 ms 130 ms 203.200.87.15
6 168 ms 157 ms 161 ms vsb-delhi-stm1.Bbone.vsnl.net.in [202.54.2.241]
7 345 ms 377 ms 359 ms if-4-0.bb7.NewYork.Teleglobe.net [209.58.17.5]
```

```
8 351 ms * 407 ms if-3-2.core2.NewYork.Teleglobe.net [207.45.220.09]
9 445 ms 450 ms 425 ms if-8-0.core1.Seattle.Teleglobe.net [64.86.83.1]
10 432 ms 436 ms 437 ms if-8-0-0.bb1.Seattle.Teleglobe.net [207.45.223.8]
11 766 ms 740 ms 668 ms iuscmdistc1206-p-7-0.msft.net [207.46.190.117]
12 * * * Request timed out.
13 * * * Request timed out.
14 * * * Request timed out.
15 * * * Request timed out.
Ctrl+C
```

In the above output, we see that after hop number 11, no results are shown. The same procedure of traceroute is repeated several times, however, still we receive the same result. This probably means that a firewall is installed after router number 11 and it is filtering out all traceroute attempts.

4. Remote OS Detection using Traceroute

Traceroute used along with a packet sniffer can be used to detect the name and version of the operating system running on the target system.

We have already learnt that the TTL value of a data packet is an 8-bit value, set by the system, which originally created and sent that particular data packet. Every operating system has a certain default TTL value associated with it. Every operating system assigns this default TTL value to all outgoing data packets. This in effect means that the initial TTL values of all data packets originating at the same operating system will be same.

This means that if there are two different systems, each running Windows 95, then all packets sent by either of these two systems (running the same operating system) will actually have the same initial TTL value. Hence, different operating systems assign different TTL values to all outgoing packets, while all systems running the same operating system will attach the same TTL value to all outgoing data packets.

"Initial TTL values of all data packets originating at the same OS but different systems will be same. However, TTL values of all data packets originating at the same system (where two OS's are running) but sent using different Operating systems will have different initial TTL values."

The below is a complete reference list of operating systems and their respective initial, default TTL values:

Note: The following table is courtesy Lance Spitzner and the Honeypot Project.

OS	VERSION	PLATFORM	TTL
Windows	9x/NT	Intel	32
Windows	9x/NT	Intel	128
Windows	2000	Intel	128
DigitalUnix	4.0	Alpha	60
Unisys	x	Mainframe	64
Linux	2.2.x	Intel	64
FTX(UNIX)	3.3	STRATUS	64
SCO	R5	Compaq	64
Netware	4.11	Intel	128
AIX	4.3.x	IBM/RS6000	60
AIX	4.2.x	IBM/RS6000	60
Cisco	11.2	7507	60
Cisco	12.0	2514	255
IRIX	6.x	SGI	60
FreeBSD	3.x	Intel	64

OpenBSD 2.x	Intel	64
Solaris 8	Intel/Sparc	64
Solaris 2.x	Intel/Sparc	255

Before we move onto the step-by-step guide to OS Detection with the help of TTL values and traceroute, there are certain rules, which one must remember:

a.) All packets sent by a particular operating system will have the same initial TTL value, which will decrement, each time that particular packet passes through a router.

b.) TTL values are stored in the TTL field, which is a part of the IP Header of a data packet. ICMP error messages are nothing but error messages encapsulated within an IP Datagram. These IP datagrams have the TTL field as one of its fields. This means that an ICMP error message too will have an IP Header with it and in effect all ICMP error message too will have a TTL value associated with them.

Thus, one can easily determine the OS running on the remote system by following the below steps-:

a.) Determine the number of hops (routers) between your system and the target system

The first step to perform is to determine the number of hops between your system and the target system. In other words, one must determine the number of routers on path to the target system from your system i.e. number of routers between your system and the target system. This can easily be done, by using the traceroute command.

```
C:\windows>tracert target.com

Tracing route to target.com [203.x.y.224] over a maximum of 30 hops:

1 308 ms 142 ms 127 ms 216.34.46.11
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.x.y.224
Trace Complete.
```

In the above example, we see that the target system was reached in 6 steps. This means that there are 5 routers separating your system and the target system. In other words, if data is sent from your system to the target system or if data is sent from the target system to your system, then as there are 5 routers through which the data must pass, as a result the TTL value of the data packets will be decremented by 5 in the data transit.

In other words, if the initial TTL value of the data packet were set to 128 by the target system, then when your system receives that particular data packet, then its TTL value would already have been reduced to 123. (As it passes through 5 routers in the data transit.)

"The number of routers in between your system and the target system, tells you as to by how much the initial TTL value set by either system will be reduced in the data transit between the two systems."

In our example, we have already seen that since there are 5 routers in between our system and the target system, thus the TTL value is reduced by 5 in the data transit, between the two systems.

b.) Determine the final TTL value of a data packet sent by the target system to your system

When the target system sends a data packet to your system, then it sets the initial TTL value of the data packet to a default value (according to the earlier chart.). Each router on the path from the target system to your system reduces this initial TTL value by 1 and forwards the data packet to the next router. Finally, when your system receives that particular data packet, then the TTL value of the data packet at that time is less than the initial TTL value that it was given by the target system, as the routers had already reduced the TTL value.

Hence, the TTL value of a data packet when your system receives it (final TTL value) is much lesser than the initial TTL value that the same data packet was given by the target system. This difference in the TTL values of the data packet is due to the fact that each router in the path, reduce the TTL value of the data packet by one.

"The initial TTL value is the TTL value set by the target system, while the final TTL value is the TTL value which the same data packet has, when it reaches your system. The initial TTL value is always greater than the final TTL value."

The final TTL value of a data packet sent by the target system can easily be determined by sending any arbitrary data to the target system. The response generated by the target system, due to this arbitrary packet can then be found out, by logging all incoming data packets, on your system, using a packet sniffing software.

In our example, we run the packet-sniffing tool in the background, while we simply do a traceroute on the target system. This packet-sniffing tool must be configured to monitor and log all incoming data packets.

When we traceroute the target system (or send any other arbitrary data to the target system) then we generate a response from the target system. Since we use traceroute in our example, the target system generates an ICMP error message, which is nothing but an error message encapsulated within an IP Datagram. Hence, since the packet sniffing software is monitoring and logging all incoming data packets, it is thus also able to log the incoming ICMP error message.

Once we have logged the response generated by the target system we can easily determine the reduced or final TTL value of the packet containing this response.

For our example, let us assume the final TTL value to be 27. We already know that the number of routers between our system and the target system is 5.Thus in other words the TTL value of a data packet sent by the target system to our system, is reduced by 5.

Initial TTL value of a data packet= Final TTL value of the packet + Number of routers in the path

As a result, in our example, hence the initial TTL value becomes 27+5=32.

c.) Comparing the Deduced Initial TTL value to the default TTL values chart

In the previous step, we have deduced the initial TTL value set by the target system, to be 32. If we compare this initial TTL value, to the chart, then we know that the target system is probably running either Windows NT or Windows 9x.

Hence, by following the above 3 steps in which we make use of traceroute, TTL values and packet sniffers, we can thus, get a very good idea regarding the type of Operating system running on the target system. The process of OS Detection discussed above, can be summarized in the following steps:

1. Determine the number of hops away, the target system lies. This can be done using the traceroute tool.

2. Send any arbitrary data to the target system, in order to generate a response. This response is logged using a packet-sniffing tool running on your system. Using the sniffed data, determine the final TTL value of the target system.

3. Use the relation: Initial TTL value= Final TTL value + Number of hops away it is located, to determine the target system's initial TTL value.

4. Finally, compare the initial TTL value determine in Step 3 with the chart and get the OS running on the target system.

Example for Remote OS Detection using this method

Following the above 4 steps method, let us take an example, to determine the operating system running on the target system.

1. In the first step, we traceroute the target system to determine the number of hops away the target system lies. This is done in the using the simple traceroute tool:

```
C:\WINDOWS>tracert 202.x.2.241

Tracing route to target.net.in [202.x.2.241] over a maximum of 30 hops:

1 130 ms 121 ms 133 ms 203.94.246.35
2 132 ms 128 ms 120 ms 203.94.246.1
3 123 ms 126 ms 125 ms 203.94.255.33
4 193 ms 137 ms 128 ms 203.200.64.153
5 128 ms 133 ms 127 ms 203.200.87.15
6 204 ms 141 ms 154 ms target..net.in [202.x.2.241]
```

Here we see that the target system (i.e. target.net.in) is 5 hops away from our system. In other words, there are 5 routers between our system and the target system.

2. In the second step, using a packet sniffing software, we find that each time we send a Data packet to the target system, it replies with a response whose TTL value is always 250.

3. Using the relation discussed earlier, we find that the initial TTL value of all data Packets sent by the target system, to our system is 250+5=255.

4. Comparing this initial TTL value to the chart, we find that the operating system Running on the target system is probably Solaris. (We remove Cisco from the list of probabilities by other remote OS detection methods, like banner grabbing, command manipulation, passive and active fingerprinting, ICMP scanning etc.)

Shortcomings and Countermeasures to OS Detection

This type of remote OS Detection method may not be accurate every single time. This method, however, most of the times does remain fairly accurate.

One simple countermeasure that one could apply to prevent OS detection through prediction of initial TTL value of your system is by changing the default TTL value that your operating system assigns to all outgoing packets.

"Traceroute can be used to detect firewalls, remote OS detection, getting information on network topography, tracing a system geographically and to detect infinite loops routing errors in networks etc."

Breeds of the Traceroute Command

There are several variations or breeds of the very popular Traceroute tool. The most common and popular forms of the traceroute utility are as follows:

1. Text Based Traceroute Tools

Almost every operating system ships with its own text based traceroute tool. Such text based traceroute tools display the path from the source system to the destination system, in the form of a normal text based result page. Such traceroute tools are probably the most commonly available and most commonly used. They are quite effective too.

Pros and Cons

+Ships with almost all operating systems
+Free to use
+Classic example of the traceroute tool
-Not as visually appealing as other breeds

2. Visual Traceroute:

This breed of the traceroute tool is in my opinion probably the easiest to use, best and most effective breed. It maps the path from the location of the source system to that of the destination system on a world map and is very accurate in this respect. It not only displays the exact geographical location of the systems, but also mentions the IP Addresses of all systems and their organization names. Visual Traceroute's latest version also has a new feature, which claims to trace the location of email spammers and analyze and detect network problems.

Pros and Cons

+Maps the path on a world map
+Very Accurate
+Visually Attractive and Easy to use
+Displays names of organization owning the servers
-Not Free to Use

3. 3D traceroute Programs: The final breed of Traceroute tools is also a quite good and effective one. The 3D Traceroute program displays the path from the source system to the destination system, in the form of a 3D graph. It also displays tons of other information, including the minimum, maximum, average and standard deviation. On top of everything, this program also displays the exact latitude, longitude and altitude at which the routers and the destination system are located. I would definitely recommend this program to be checked out at least once by every one even remotely related to computer security.

Pros and Cons

+Free to Use
+Displays tons of information about routers and destination system
+Effective and displays even advanced information
-Lacks a bit on the Usability side

Download URL: http://www.hlembke.de/prod/3dtraceroute/

Fadia's Hot Pick for Traceroute Breeds

1. Utility Name: Visual Traceroute

Features: Maps the path to a remote system on a world map and displays the hostname, name and other important information about all routers and even the destination system.

Download URL: http://www.visualware.com/visualroute/index.html

Anonymous 'Tracerouting'

No matter what tool one might use to Trace the path to the target system, one is always exposing ones identity to the target system. Each time you traceroute a remote system, you are actually putting your IP Address or putting your identity at risk and are putting behind your traces (read: IP Address) on the target system's log files.

This means that the system administrator of the target system does actually come to know your identity and he might also be able to trace you. Thus, arises the need of a technique of Anonymous Tracerouting.

When you normally traceroute a remote system, using any normal technique, then since a direct connection has been established between your system and the remote system, thus your identity gets revealed to the remote system. However, on the other hand, if there were a way by which one could perform a traceroute on a target system via an indirect connection, then one's identity would be protected.

There are several websites, which provide free online traceroute tools. It is such free online traceroute tools, which provide a method of anonymous Tracerouting. All that one has to do to perform anonymous Tracerouting, is following the below steps:

a.) Go to the online traceroute tool and use it to perform a traceroute to the target system. Since only the online tool establishes a direct connection with the target system, thus your identity is protected and only the identity of the online tool's server is revealed. This step just traces the path from the online tool's server to the target system.

b.) In the second step, one has to use a normal traceroute tool to trace the path from our system to the online tool's server.

c.) Finally, if we combine the results obtained by both the above steps, then we would get a complete traceroute result from our system to the target system.

Since in the above steps, we established a direct connection only with the online tool's server, thus our identity is revealed only to this server and not to the target system.

Another method, by which one can perform anonymous Tracerouting, is to register at a shell account provider and then use this shell account to traceroute the target system. However, most shell account service providers are very particular about maintaining logs, which again might reveal your activity on their server.

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 observe 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.

Traceroute Countermeasures

1. Traceroute can easily be used to find how exactly a particular network is organized and to determine the potential entry points. This means that using the traceroute command is one of the first things that a hacker would do on his quest to getting root on a system. It is also widely being used to determine the geographical position of a particular system and to detect the presence of a firewall. Besides this there are several other purposes for which the traceroute command has started being used. This has created increased need to detect and filter out Traceroute requests at either the router level or the system level.

If you wish to log all Traceroute requests, then using any of the commercial Firewalls will do. Certain advanced firewalls not only detect traceroute requests and log them but also send fake responses. Alternatively you could use any of the various third party freeware utilities for this purpose.

Tdetect is one such utility, which detects and logs all ICMP and UDP traceroute packets with a TTL value equal to 1. There is yet another, more interesting, utility named RotoRouter which not only detects and logs all such request but also sends fake responses.

You can easily get any of these utilities at any of the below sites:

http://www.anticode.com/
http://www.packetstormsecurify.com/
http://www.hackersclub.com/

2. It is also advisable that one filters out traceroute requests at as many routers and systems as possible. All that one needs to keep in mind is the fact that we need to look out for ICMP and UDP packets with a TTL value of 1 and filter them out.

The recommended method to prevent your network from responding to traceroute requests is to configure your routers to not respond to any packet having a TTL value of 1. (or 0). This can easily be done by adding the below access list:

```
access-list 101 deny ip any any 11 0 ! ttl-exceeded
```

What this basically does is that it configures the router to not respond with a TTL Exceeded message to a traceroute request packet. One could also use the following ACL as a traceroute countermeasure:

```
access-list 101 deny icmp any any 11 0
```

On this note, we come to the end of the white paper on traceroute.

Ankit Fadia
ankit@bol.net.in

http://hackingtruths.box.sk/

To receive tutorials written by Ankit Fadia join his mailing list by sending a blank email to: programmingforhackers-subscribe@yahoogroups.com

Tracing the Traceroute: A White Paper by Ankit Fadia
@ Articles -> Networking   Apr 18 2002 - 07:31 EST
ankit_fadia writes: a white paper by Ankit Fadia - ankit@bol.net.in

Home