
//////////*1000+ HACKING TRICKS & TUTORIALS - ebook By Mukesh Bhardwaj Blogger - Paid Version - only @ TekGyd | itechhacks | Mukeshtricks4u*///////

When you first turn on you computer (BEFORE DIALING INTO YOUR ISP),
open a MS-DOS Prompt window (start/programs MS-DOS Prompt).
Then type netstat -arn and press the Enter key.
Your screen should display the following (without the dotted lines
which I added for clarification).

Active Routes:

Network Address	Netmask	Gateway Address	Interface	Metric
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
255.255.255.255	255.255.255.255	255.255.255.255	0.0.0.0	1

Route Table

Active Connections

Proto	Local Address	Foreign Address	State

If you see anything else, there might be a problem (more on that later).
Now dial into your ISP, once you are connected;
go back to the MS-DOS Prompt and run the same command as before
netstat -arn, this time it will look similar to the following (without
dotted lines).

Active Routes:

Network Address	Netmask	Gateway Address	Interface	Metric
0.0.0.0	0.0.0.0	216.1.104.70	216.1.104.70	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
216.1.104.0	255.255.255.0	216.1.104.70	216.1.104.70	1
216.1.104.70	255.255.255.255	127.0.0.1	127.0.0.1	1
216.1.104.255	255.255.255.255	216.1.104.70	216.1.104.70	1
224.0.0.0	224.0.0.0	216.1.104.70	216.1.104.70	1
255.255.255.255	255.255.255.255	216.1.104.70	216.1.104.70	1

Route Table

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:0	0.0.0.0:0	LISTENING
TCP	216.1.104.70:137	0.0.0.0:0	LISTENING
TCP	216.1.104.70:138	0.0.0.0:0	LISTENING

```
  TCP    216.1.104.70:139      0.0.0.0:0            LISTENING
  UDP    216.1.104.70:137      *:*
```

What you are seeing in the first section (Active Routes) under the heading of Network Address are some additional lines. The only ones that should be there are ones belonging to your ISP (more on that later). In the second section (Route Table) under Local Address you are seeing the IP address that your ISP assigned you (in this example 216.1.104.70).

The numbers are divided into four dot notations, the first three should be the same for both sets, while in this case the .70 is the unique number assigned for THIS session. Next time you dial in that number will more than likely be different.

To make sure that the first three notation are as they should be, we will run one more command from the MS-DOS window.
From the MS-DOS Prompt type tracert /www.yourispwebsite.com or .net or whatever it ends in. Following is an example of the output you should see.

Tracing route to /www.motion.net [207.239.117.112]over a maximum of 30 hops:
1 128 ms 2084 ms 102 ms chat-port.motion.net [216.1.104.4]
2 115 ms 188 ms 117 ms chat-core.motion.net [216.1.104.1]
3 108 ms 116 ms 119 ms www.motion.net [207.239.117.112]
Trace complete.

You will see that on lines with the 1 and 2 the first three notations of the address match with what we saw above, which is a good thing. If it does not, then some further investigation is needed.

If everything matches like above, you can almost breath easier. Another thing which should you should check is programs launched during startup. To find these, Click start/programs/startup, look at what shows up. You should be able to recognize everything there, if not, once again more investigation is needed.

Now just because everything reported out like we expected (and demonstrated above) we still are not out of the woods. How is this so, you ask? Do you use Netmeeting? Do you get on IRC (Internet Relay Chat)? Or any other program that makes use of the Internet. Have you every recieved an email with an attachment that ended in .exe? The list goes on and on, basically anything that you run could have become infected with a trojan. What this means, is the program appears to do what you expect, but also does just a little more. This little more could be blasting ebay.com or one of the other sites that CNNlive was talking about.

What can you do? Well some anti-virus software will detect some trojans.

Another (tedious) thing is to start each of these "extra" Internet programs one at a time and go through the last two steps above, looking at the routes and connection the program uses. However, the tricky part will be figuring out where to tracert to in order to find out if the addresses you see in step 2 are "safe" or not. I should forewarn you, that running tracert after tracert, after tracert might be considered "improper" by your ISP. The steps outlined above may not work exactly as I have stated depending upon your ISP, but with a true ISP it should work. Finally, this advise comes with NO warranty and by following my "hints' you implicitly release me from ANY and ALL liability which you may incur.

Other options

Display protocol statistics and current TCP/IP network connections.
Netstat [-a] [-e] [-n] [-s] [-p proto] [-r] [intervals]

-a.. Display all connections and listening ports.
-e.. Display Ethernet statistics. This may be combined with the -s option.
-n.. Diplays address and port numbers in the numerical form.
-p proto..Shows connections for the protocol specified by proto; proto may be TCP or UDP. If used with the -s option to display per-protocol statistics, proto may be TCP, UDP, of IP.
-r.. Display the routing table.
-s.. Display per-protocol statistics. By default, statistics are shown for TCP UDP and IP; the -p option may be used to specify a subset of the default interval..Redisplay selected statistics, pausing intervals seconds between each display. If omitted. netstat will print the current configuration information once