

# Re: Win2k Netstat sockets interpretation

---

*Source:* <http://www.derkeiler.com/Newsgroups/alt.computer.security/2007-01/msg00110.html>

---

- *From:* warf <[dan@xxxxxxxxxxxxx](mailto:dan@xxxxxxxxxxxxx)>
  - *Date:* Tue, 30 Jan 2007 21:15:39 GMT
- 

Sebastian Gottschalk wrote:

warf wrote:

I have been trying to learn as much as I can about internet 'security'

snip diatribe and gratuitous snarling...

to get a better feeling for what data is leaving my home,

Eh... is that any serious problem at all?

Yes, if you have, or ever did have, any media on your system, or if you realize the RIAA and ilk will someday get the legal club to go after 'other' citizens for \$750USD/title, or even if you are just fed up with surreptitious datamining for unstated purposes. or if subversion of your

connection for nepharious purposes is 'problematic: then, YES.

>> BUT, netstat /a indicates netbios ports 137,138,139,445 listening

See, you didn't learn anything. You didn't even disable the SMB binding and the NetBIOS bindings. And this even when some clever guys already collected an easily understandable overview on websites like <[http://ntsvcfg.de/ntsvcfg\\_eng.html](http://ntsvcfg.de/ntsvcfg_eng.html)>.

I said I was "trying"....never claimed to 'know'. better is should be like the rest of the cattle and pretend it is not really going to affect me?  
By making an effort to learn I take responsibility...you have been helpful..even if grumpy.

when I allow ZA to allow T-bird to act as a server

## Re: Win2k Netstat sockets interpretation

snip.....

Restated "When I run T-bird ZA tells me T-bird wants to access the internet and act as a server. I have deleted "file and print sharing" under "internet connections and disabled most recognizable "remote access" services under 'services.msc' but ZA detects a few remote access modules running and gives them permission if select "OK" to the suggested query.

AND

For eg; If I allow scvhost to access 0.0.0.0 when firefox2.0 opens i notice randomly ports assigned to urls or ip addresses.

and firefox always has 4 connections local and 4 remote open in addition to the url i am browsing????

\*repeating the thousandth time\*

'netstat' on Win2K provides a view on the state of the \*TDI interface\*, not the actual TCP/IP sockets. The TDI interface has different semantics, and something appearing as 0.0.0.0 listening means "an outstanding request to open a TCP/IP connection", thus no actual TCP/IP socket in LISTENING state.

If you had just take the simplest measures to actually verify such bogus open ports with a port scan, you'd have found them closed.

I am using Ethereal and there is traffic...I am 'learning' but it is a very complex topic ...for non-pro's like me...but that is why i ask.

but Akamai tech~ is frequently there

Wow... Windows Automatic Updates... the mysterious of technology aren't to be believed !!!!

no, WINUPDATE is manual...I reassembled the TCP/IP stream and saw in one instance it was a ZA update. This concurs with the stated utility of those servers. I read conflicting ideas as to the scope of the AKAMAI servers and wondered why I would be 'uploading' to them as well...with optout selected for all products 'satisfaction' reports.

I have checked many netstat resources to no avail...help?

MSDN... Ah, might just be better to get a replacement which works like the real netstat command, f.e. TcpView from Sysinternals^W Microsoft.

## Re: Win2k Netstat sockets interpretation

Now I have to spracken ze duetch. That is exactly what i needed but the launage for the links is all german!!! Damn.

Breifly: How does one interpret the 'listening', 'waiting', 'established' and all the other port information netstat lists? The only one I get is one with a 'foreign' ip and 'established'...those are actual internet connections right? Eastlink is very coy and stingy with 'what services and ports I require' info...so I am trying to learn thru you and int-resources.

Thanks for that helpful link...wish I spoke enough german to decipher it!  
Warf.