

Re: Services & Firewall port settings

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2005-04/0569.html>

From: Karl Levinson, mvp (levinson_k_at_despammed.com)

Date: 04/13/05

Date: Wed, 13 Apr 2005 09:54:08 -0400

"Will" <Will@discussions.microsoft.com> wrote in message
news:89D3DED4-2324-44B5-A86E-B860189BB23C@microsoft.com...
> *Services & Firewall port settings*
> *In my HpM370n Mce2005 system32\drivers\etc\Services (dated 7/30/2003)*
> *I've 2 entries for systat*
> *systat 11/tcp users #Active users*
> *systat 11/tcp users #Active users*
> *In IANA wesite, services defined shows the second systat being udp.*
>
> *Because this definition of port numbers allowed I/O is a basic security*
> *issue, where is there a smaller list for home users?*
>
> *For example, what do*
> *I need Doom, Radius, or SQL(shudder quiver,?) etc. for? Or telnet for that*
> *matter, if I never use it? Does removing an entry from here result in a*
lack
> *of resolution by my computer, and more dropped packets than there now*
> *are or should I copy this into "Permit only" in Advanced Tcp/Ip filtering?*
> *Would appreciate an answer to this reasonable question.*

I recommend you don't change anything. This services file is really not a basic security issue. In Windows, this list does nothing to permit those ports or weaken the security on your system. Pretty much all of the Windows security checklists I've seen don't mention editing that file.

On the other hand, it is pretty safe to edit that file, as long as you comment out a line with a # at the start of the line. Avoid deleting any lines. If you reboot and something breaks, you'll know it was caused by one of your changes. Some of those lines your computer does need, and you may not be aware that your computer needs them. If you disable a needed service, Windows may not know what default port to use when initiating a new outbound connection using that protocol [http, smtp, dns, etc.] and you may lose use of that protocol.

Having "SQL" on your system sounds bad, but it is not likely that your system would be hacked because of it. On a Windows workstation, that file primarily affects outbound connections. The only line I can think of in

that file that causes some insecurity is the line about tftp. The last time I remember people recommending editing this file was in 2001, with the Code Red and Nimda worms. Commenting out the line regarding tftp could help prevent some automated worms and malware that have already infected your computer from going out and downloading additional malware tools. Note however that in this case, your computer is not being infected by tftp, and disabling tftp does not prevent your system from being infected. If the worm or hacker used ftp or http or smtp to upload or download files instead of tftp, then editing the services file won't help you there.

The copy of the services file on your computer is the only one I'm aware of for home users. The copy on my Windows 2000 system is already relatively small, so it seems to me someone at Microsoft has already gone through and thought about whether that entry would be somewhat useful.

I believe the "advanced TCP/IP filtering" only blocks inbound connections, not outbound, so adding these settings there wouldn't be the same as removing them from your services file and wouldn't have the effect you are looking for. I would use a third party firewall instead, it's much easier and more secure. www.kerio.com, www.sygate.com and www.zonealarm.com are all free firewall software.