

Re: Log file full of security problems!

Re: Log file full of security problems!

Source:

http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.network_web/2006-11/msg00304.html

- *From:* Mark Grantom <mgrantom@xxxxxxxxxx[no spam]>
 - *Date:* Thu, 9 Nov 2006 12:59:02 -0800
-

Here is the latest. I'm still hoping someone can help. My specific problem seems to be "Event ID 577 appears repeatedly in the security event log of your Windows XP-based computer" found here <http://support.microsoft.com/kb/831905#top>

I requested a hotfix and it was emailed to me, however when I try to run it, I get an error message stating that I already have this security fix and I don't need the patch. Since my Win XP has 366 patches on it since I first installed in 2003, it seems like it might be A LITTLE DIFFICULT to say the least, to try and uninstall / reinstall. Is there anyway to fix this problem without going through computer hell? Thanks (hopefully, in advance)

--

Mark G

"Mark Grantom" wrote:

I really appreciate the reply. I do own and have used a wide array of AV programs and antispyware tools including Spybot. I do not believe I have a virus since for the most part I do not experience any problems. I have also looked at all of the processes that are running (all 76 of them) and I can't see anything that is outright suspicious. I do have several instances of svchost.exe running as follows:

svchost.exe 1408 6to4, AudioSrv, BITS, Browser, CryptSvc,
Dhcp, dmserver, ERSvc, EventSystem,
FastUserSwitchingCompatibility, helpsvc,
HidServ, lanmanserver, lanmanworkstation,
Netman, Nla, RasMan, Schedule, seclogon,
SENS, SharedAccess, ShellHWDetection,
srsservice, TapiSrv, Themes, TrkWks, W32Time,
winmgmt, wscsvc, wuauerv, WZCSVC

Most of these I have tracked down to something I expect, but I'm not sure about all of them. I thought the audit logs might indicate which process is

Re: Log file full of security problems!

causing the problem, but it is beyond my level of understanding.

--
Mark G

"Pop`" wrote:

Mark Grantom wrote:

I am hoping that someone can help me with the problem that I am having with my small peer-to-peer network. The network consists of three computers, all running windows XP Pro edition. The "main" computer hosts a SQL server (the free version). I enabled the logging of events on this computer. Recently, I inadvertently ran the system for approximately 1 month with out a firewall, and with the antivirus program disabled. I currently use the computer Associates version of an antivirus program that comes with my DSL phone line and I also have run from the beginning MS Defender. I remotely access my system using Microsoft's remote desktop. Recently, whenever I log onto the system I get a message indicating that "the security log for this computer is full". I have cleared the log file, and it immediately fills back up. Under the security tab, I have hundreds if not thousands of entries that look as follows:

Event Type: Failure Audit
Event Source: Security
Event Category: Privilege Use
Event ID: 577
Date: 11/2/2006
Time: 10:19:25 AM
User: INTEL\Mark
Computer: INTEL
Description:
Privileged Service Called:
Server: Security
Service: -
Primary User Name: Mark
Primary Domain: INTEL

Re: Log file full of security problems!

Primary Logon ID: (0x0,0x1451D)
Client User Name: –
Client Domain: –
Client Logon ID: –
Privileges: SeTcbPrivilege

For more information, see Help and Support Center at
<http://go.microsoft.com/fwlink/events.asp>.

I also have hundreds of entries as follows:

Event Type: Failure Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 529
Date: 11/2/2006
Time: 11:44:56 AM
User: NT AUTHORITY\SYSTEM
Computer: INTEL
Description:
Logon Failure:
Reason: Unknown user name or bad password
User Name: Mark
Domain: INTEL
Logon Type: 2
Logon Process: Advapi
Authentication Package: Negotiate
Workstation Name: INTEL

For more information, see Help and Support Center at
<http://go.microsoft.com/fwlink/events.asp>.

Obviously, I am concerned that I may have some sort of Trojan program on my system. Although, I have scanned with both Microsoft defender, and the antivirus program, and nothing is found. I would greatly appreciate any assistance in determining what may be causing this problem with my System. Thanks in advance.

I'm unlikely to have your needed answer, but here's a couple thoughts.

Disconnect from the network and single out the exposed pc.

Disable the logging for the time being; Clear the logs or copy them to another media for study later if you think you'll need them. For the moment you obviously don't need those logs; that volume is useless in an ongoing basis right now.

Re: Log file full of security problems!

Check the Event Viewer logs; copy/Clear those, too.

MS Defender is OK, but not the end—all. You should add Adaware and Sybot

S&D at least to this arsenal. I also have WinPatrol which I like, and SpyWare Blaster. With spyware, no single app as yet can do everything all the rest of them can do. You need as many reputable ones as you can find. Adaware and Spybot found the most problems in my case; lately I've been lucky and haven't had a problem in many months.

CA's antivirus is OK, I forget whose it is, but it's a reputable one. That said however, I'd additionally download Avast or AVG scanners and run those too, just for grins. If they find nothing, then you can go back to the CA av.

Be certain to UPDATE EVERYTHING before you use it to scan.

Get the firewall, av, anti-spyware, etc., all completely updated and run all scans ASAP.

If you're using a NAT router, there may be logs there too, BTW.

Once the machine "feels" clean, exercise it well to be certain everything you want/need is in good shape and no problems.

Then you can reconnect it to the network and think about turning the logging audits etc. back on.

Hopefully, any actual problems will show up during the above process.

Pop`