

Re: Security log full, why?

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2007-09/msg00260.html

- *From:* "Jim" <j.n@xxxxxxxxxxx>
 - *Date:* Sun, 30 Sep 2007 16:11:06 GMT
-

"Bo Berglund" <boberglund@xxxxxxx> wrote in message <news:prhuf3p69tc05irc8mbnmkp11lem6ggg7@xxxxxxxxxxx>

I am getting warnings on my DELL Dimension desktop running XP SP2 when I log on using RDP. The warning is about the security log being full and that an administrator should fix it...

After I use Event Viewer to clear all log entries it only takes a short time until it fills up with new entries again. Almost all of them are titled "Failure Audit". The text in the listbox when I open one of these is:

The Windows Firewall has detected an application listening for incoming traffic.

Name: –
Path: C:\WINDOWS\system32\svchost.exe
Process identifier: 1416
User account: SYSTEM
User domain: NT AUTHORITY
Service: Yes
RPC server: No
IP version: IPv4
IP protocol: UDP
Port number: 1219
Allowed: No
User notified: No

If I use Taskmanager to find svchost.exe I find no less than 7 of them. One of these stands out among the others because it has used lots of CPU time (right now 0:05:52, whereas all others are below a minute) and I/O Read Bytes is over 2.2 Gbytes and counting. This one also has the PID mentioned in the event log.

When I use ProcessExplorer from SysInternals I get more info:
"Generic Host Process for Win32 Services"
Command line of process: C:\WINDOWS\System32\svchost.exe -k netsvcs

Re: Security log full, why?

If I look in the Services tab I find no less than 30 entries...

How can I find out what is causing this audit failure and why?
And how can I stop it from doing whatever it is doing?

BTW: "Tasklist /SVC" gives the following output related to svchost:
Image Name PID Services

```
-----  
svchost.exe 1124 DcomLaunch, TermService  
svchost.exe 1284 RpcSs  
svchost.exe 1416 AppMgmt, AudioSrv, BITS, Browser, CryptSvc,  
Dhcp, dmserver, ERSvc, EventSystem, helpsvc,  
HidServ, lanmanserver, lanmanworkstation,  
Messenger, Netman, Nla, RasMan, Schedule,  
seclogon, SENS, SharedAccess,  
ShellHWDetection, srservice, TapiSrv,  
Themes, TrkWks, w32time, winmgmt, wuau serv,  
WZCSVC  
svchost.exe 1528 Dnscache  
svchost.exe 1700 LmHosts, RemoteRegistry, SSDPSRV, WebClient  
svchost.exe 3048 stisvc  
svchost.exe 5268 HTTPFilter
```

Bo Berglund
bo.berglund(at)nospam.telia.com

Svchost.exe is a general purpose program which can be used for quite a few different processes. It is not unusual to find 7 different processes executing this program.

If I had your problem, the first thing I would do is to perform a thorough malware test. It does seem likely that you have a bad case of infestation.

The second thing I would do is dependent on what the results of the first test are.

Jim

.