

Re: ATTN : Microsoft – Security Event 529....Second Request for help....

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2006-04/msg01650.html>

- *From:* Art Vandalay <noone@xxxxxxxxxxxx>
 - *Date:* Mon, 10 Apr 2006 19:12:23 -0400
-

Thanks for the reply Jenny... According to the events, the logon failure is from the local machine account (SERVER1\$). It is always the local machine account that exhibits the failures. Events are logged every couple of minutes. I'm sure it is not a hacking attempt or virus, since the events occur even if the server is physically disconnected from the network. This is also a brand new server SBS2003 installation... If the server is rebooted, the process PIDs that produce the logon failure change, but always point back to the same three processes : store.exe, wmiprvse.exe, and inetinfo.exe.

It really seems like something is out of sync with the local machine account password....

On Mon, 10 Apr 2006 06:55:12 GMT, v-yanniw@xxxxxxxxxxxxxxxxxxxxxxxx ("Jenny wu [MSFT]") wrote:

Hi Art,

Thank you for posting here!

I am sorry for the delayed response due to weekend. Please understand that the newsgroups are staffed weekdays by Microsoft Support professionals to answer your systems and applications questions. Your understanding is greatly appreciated!

From your description, I understand the issue to be: you received security event 529 and 552 in the Security log.

Security Event ID 529 is a failure audit for logon/logoff. The security events are controlled by the audit policies. The policies of "logon events" generate the events on domain controllers for domain account activity. The log type 3 is a Network event means "A user or computer logged on to this computer from the network".

Re: ATTN : Microsoft – Security Event 529....Second Request for help....

This kind of issue may be caused by Application logon such as while Outlook is connecting to Exchange Server, or this is an automated dictionary attack on weak passwords. The hacker is trying variable username/password (here it is webmaster) combinations to access the network. The attack can be initiated from internal network or external network.

Technically speaking, this is a normal behavior as you cannot prevent a hacker from attacking your server. You can ignore the events as the attack was unsuccessful. However, since it indicated the hacker attacking, I would like to give the fol