

RE: Event ID 529

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2006-08/msg04955.html>

- *From:* v-chacez@xxxxxxxxxxxxxx (chace zhang)
 - *Date:* Fri, 25 Aug 2006 11:53:13 GMT
-

Hi,

Thank you for posting here.

To keep this thread clean, I recommend you to open a new thread for further discussion. A support engineer will be assigned (maybe it will be me again).

Thank you for your understanding and we look forward to hearing from you soon.

Back on your issue, currently can't get a clear picture on this issue, since I can see a real Event error description on this issue.

According to your description, the source is not from your domain. I suppose this is a network attack on week password.

You can check to see which process handles the session. For example, in this event, the process ID is 1744. Write down the process ID, Ctrl+Alt+Del and click "Task Manager". In the task manager window, click "Processes" tab. Click "View"--->"Select Columns". Check "PID (Process Identifier)" and click "OK". In the process list, find the process with 1744 PID. What's the process?

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 following action plan to improve the network security:

1. Scan virus on the workstations. Please use the anti-virus software to perform full scan on the internal workstations. There is a online virus scan link below:

<http://housecall.trendmicro.com>

2. Implement Strong password policies. Open "Server Management console", navigate to Users snap-in. In the right panel, click 'Configure Password Policies'. Enable the password policies.

For more information:

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/bpactlck.mspx>

3. Monitor the internal users to see if anyone is testing the admin accounts.

NOTE: This response contains a reference to a Third party World Wide Web site. You should know that Third party sites are not under the control of Microsoft. Accordingly, Microsoft can make no representation concerning the content of these sites. Microsoft is providing this information only as a convenience to you. This is to inform you that Microsoft has not tested any software or information found on these sites and therefore cannot make any representations regarding the quality, safety, or suitability of any software or information found there. There are inherent dangers in the use of any software found on the Internet, and Microsoft cautions you to make sure that you completely understand the risk before retrieving any software on the Internet.

Please do not hesitate to let me know if you have any further concerns.

Sincerely,

Best Regards,

Chace Zhang (MSFT)

Microsoft CSS Online Newsgroup Support

Get Secure! – www.microsoft.com/security

=====
This newsgroup only focuses on SBS technical issues. If you have issues regarding other Microsoft products, you'd better post in the corresponding newsgroups so that they can be resolved in an efficient and timely manner.

You can locate the newsgroup here:

<http://www.microsoft.com/communities/newsgroups/en-us/default.aspx>

When opening a new thread via the web interface, we recommend you check the "Notify me of replies" box to receive e-mail notifications when there are any updates in your thread. When responding to posts via your newsreader, please "Reply to Group" so that others may learn and benefit from your issue.

Microsoft engineers can only focus on one issue per thread. Although we provide other information for your reference, we recommend you post different incidents in different threads to keep the thread clean. In doing so, it will ensure your issues are resolved in a timely manner.

For urgent issues, you may want to contact Microsoft CSS directly. Please

check <http://support.microsoft.com> for regional support phone numbers.

Any input or comments in this thread are highly appreciated.

=====
This posting is provided "AS IS" with no warranties, and confers no rights.

| Thread-Topic: Event ID 529
| thread-index: AcbID3l3oCJt8ck5QbaJCtOVE4xq1A==
| X-WBNR-Posting-Host: 67.49.169.231
| From: =?Utf-8?B?Sm9obmF0aG9uIEpvbmVz?= <Johnathon
Jones@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
| References: <6AA4593D-7DB4-4984-901F-2FA2389C8F9D@xxxxxxxxxxxx>
<00Tar7cwGHA.1992@xxxxxxxxxxxxxxxxxxxxxxxx>
| Subject: RE: Event ID 529
| Date: Thu, 24 Aug 2006 23:27:01 -0700
| Lines: 233
| Message-ID: <B3814BAD-087C-4797-9870-C9884103D694@xxxxxxxxxxxx>
| MIME-Version: 1.0
| Content-Type: text/plain;
| charset="Utf-8"
| Content-Transfer-Encoding: 7bit
| X-Newsreader: Microsoft CDO for Windows 2000
| Content-Class: urn:content-classes:message
| Importance: normal
| Priority: normal
| X-MimeOLE: Produced By Microsoft MimeOLE V6.00.3790.1830
| Newsgroups: microsoft.public.windows.server.sbs
| Path: TK2MSFTNGXA01.phx.gbl
| Xref: TK2MSFTNGXA01.phx.gbl microsoft.public.windows.server.sbs:292837
| NNTP-Posting-Host: TK2MSFTNGXA01.phx.gbl 10.40.2.250
| X-Tomcat-NG: microsoft.public.windows.server.sbs
|

| Perhaps someone can help me in this thread. I experience 30-50 of these
| every day. The source is clear - workstations that are not part of my
| SBS2003 domain share the same local network (it's a shared local network
in
| an office suite). There are approximately five machines on the network
that
| are not part of my domain, and the users of those machines never
| intentionally attempt to contact the server, but it appears that their
| machines to this automatically. These users obviously don't have
accounts in
| my domain either. Is there any way I can get SBS2003 to ignore
communication
| attempts from these machines (perhaps they are network browser
| communications?) so that these errors go away?
| Thanks!

| John

| "chace zhang" wrote:

|> Hi,

|> Thank you for posting here.

|> From your post, I understand this issue is: there are lots of Kerberos
529

|> events in event log. If I have misunderstood your concerns, please feel
|> free to let me know.

|> First I want to know to confirm the Source Network Address:
192.168.1.102

|> is the IP address of Windows client in your domain.

|> 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.

|> 2. Based on my experience, this issue can occur if you enabled the
"Audit

|> logon event" policy enabled on the SBS server and a failure logon
attempt

|> is performed from the remote client. Security Event ID 529 is a failure
|> audit for logon/logoff. It may be related to Exchange/IIS, client
computer

|> or inconsistent computer account password of the SBS 2003.

|> 3. As the Logon Type: 3, it is Network logon, Intended for high
|> performance servers to authenticate clear text passwords. LogonUser
does

|> not cache credentials for this logon type.

|> 4. You can check to see which process handles the session. For
example,

|> in this event, the Caller Process ID is 2788. Write down the process
ID, go

|> to client computer where user account Joe is logon from, press
Ctrl+Alt+Del

|> and click "Task Manager". In the task manager window, click
"Processes"

|> tab. Click "View"-->"Select Columns". Check "PID (Process
|> Identifier)" and click "OK". In the process list, find the process

with

|> 2788 PID. What's the process?

|> We can perform a clean boot troubleshooting for workstation:

|>

|> 310353 How to perform a clean boot in Windows XP

|> <http://support.microsoft.com/?id=310353>

|>

|> 281770 How to perform clean-boot troubleshooting for Windows 2000

|> <http://support.microsoft.com/?id=281770>

|>

|> 5. 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 following action plan to improve the network security:

|>

|> 1. Scan virus on the workstations. Please use the anti-virus software to

|> perform full scan on the internal workstations. There is an online virus

|> scan link below:

|>

|> <<http://housecall.trendmicro.com/>>

|>

|> 2. Implement Strong password policies. Open "Server Management console",

|> navigate to Users snap-in. In the right panel, click "Configure Password

|> Policies". Enable the password policies.

|>

|> For more information:

|>

|> <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/>

|> security/bpactlck.mspx

|>

|>

|>

|> Also the 529 error may be related to the NTLM Authentication level that SBS

|> 2003 server sets. By default, the SBS 2003 Server is set to "Send NTLM

|> response only", you get the event log because the authentication level does

|> not match or it meets error during the authentication procedure. In some

|> cases, when the partner stopped the Exchange routing engine service (only

|> for test purpose because this is an Exchange core service), the events were

|> terminated.

|>
|> You can change the specific setting in registry to downgrade the
|> authentication level (I do not recommend you do that since you just get
the
|> event log and all things are working correctly, it's up to you)
|>
|> Please open regedt32 on SBS 2003 and go to
|> HKLM\System\CurrentControlSet\Control\LSA\nolmhash=1
|>
|> Setting nolmhash to 0 and reboot the Server
|>
|> For more information about the NTLM authentication level, please refer
to
|> this KB article:
|> 147706 How to Disable LM Authentication on Windows NT
|> <http://support.microsoft.com/?id=147706>
|>
|> Note this article also apply to Windows 2003
|>
|>
|> 6. If the issue persists, please kindly check the following
information
|> if it is the case:
|>
|> There are several running processes on the SBS server that will attempt
to
|> connect using the machine account.
|> One of the most active is the Microsoft Exchange Routing Engine.
|>
|> This behavior can happen when the machine password is not properly sync.
|>
|> In order to reset the machine account password of a domain controller
use:
|>
|> NETDOM RESETPWD /Server:ServerName /UsedD:Administrator /PasswordD:*
|>
|> The syntax of this command is:
|> NETDOM RESETPWD /Server:domain-controller /UserD:user
/PasswordD:[password
|> |*]
|>
|> NETDOM RESETPWD Resets the machine account password for the domain
|> controller
|> on which this command is run. Currently there is no support for
resetting
|> the machine password of a remote machine or a member server. All
parameters
|> must be specified.
|>
|> /Server Name of a specific domain controller that should have
its

|> machine account password reset.
|>
|> /UserD User account used to make the connection with the domain
|> controller specified by the /Server argument.
|>
|> /PasswordD Password of the user account specified with /UserD. A
*
|> means
|> to prompt for the password
|>
|> ** After completing the command, reboot the server.
|>
|>
|> Hope this helps, if you have any other concerns on this issue, please
feel
|> free to let me know.
|>
|> Have a nice day!
|>
|> Best Regards,
|>
|> Chace Zhang (MSFT)
|>
|> Microsoft CSS Online Newsgroup Support
|>
|> Get Secure! – www.microsoft.com/security
|>
|> =====
|> This newsgroup only focuses on SBS technical issues. If you have issues
|> regarding other Microsoft products, you'd better post in the
corresponding
|> newsgroups so that they can be resolved in an efficient and timely
manner.
|> You can locate the newsgroup here:
|> <http://www.microsoft.com/communities/newsgroups/en-us/default.aspx>
|>
|> When opening a new thread via the web interface, we recommend you check
the
|> "Notify me of replies" box to receive e-mail notifications when there
are
|> any updates in your thread. When responding to posts via your
newsreader,
|> please "Reply to Group" so that others may learn and benefit from your
|> issue.
|>
|> Microsoft engineers can only focus on one issue per thread. Although we
|> provide other information for your reference, we recommend you post
|> different incidents in different threads to keep the thread clean. In
doing
|> so, it will ensure your issues are resolved in a timely manner.
|>

|> For urgent issues, you may want to contact Microsoft CSS directly.

Please

|> check <http://support.microsoft.com> for regional support phone numbers.

|>

|> Any input or comments in this thread are highly appreciated.

|>

|> =====

|>

|> This posting is provided "AS IS" with no warranties, and confers no rights.

|>

|>

|> -----

|> | Thread-Topic: Event ID 529

|> | thread-index: AcbBRBdxDIOJpZa/SnaigvI/xl54Hg==

|> | X-WBNR-Posting-Host: 67.154.6.66

|> | From: =?Utf-8?B?U2NvdHQ=? <Scott@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

|> | Subject: Event ID 529

|> | Date: Wed, 16 Aug 2006 07:56:02 -0700

|> | Lines: 22

|> | Message-ID: <6AA4593D-7DB4-4984-901F-2FA2389C8F9D@xxxxxxxxxxxxxx>

|> | MIME-Version: 1.0

|> | Content-Type: text/plain;

|> | charset="Utf-8"

|> | Content-Transfer-Encoding: 7bit

|> | X-Newsreader: Microsoft CDO for Windows 2000

|> | Content-Class: urn:content-classes:message

|> | Importance: normal

|> | Priority: normal

|> | X-MimeOLE: Produced By Microsoft MimeOLE V6.00.3790.1830

|> | Newsgroups: microsoft.public.windows.server.sbs

|> | Path: TK2MSFTNGXA01.phx.gbl

|> | Xref: TK2MSFTNGXA01.phx.gbl microsoft.public.windows.server.sbs:290375

|> | NNTP-Posting-Host: TK2MSFTNGXA01.phx.gbl 10.40.2.250

|> | X-Tomcat-NG: microsoft.public.windows.server.sbs

|>

|> | Yesterday I had 71 occurrences of the following error. The user is on

|> | vacation and has confirmed no remote logon attempts. I have attempted

to

|> | grasp similar posts here which describe a sync issue but it seems

that

|> | would

|> | assume a connection to the server. Is this a hack attempt at the

|> | workstation?

|> | Thanks.

|>

|> | Logon Failure:

|> | Reason: Unknown user name or bad password

|> | User Name: (valid user name removed for this post)

|> | Domain: SERV

|> | Logon Type: 3

|> | Logon Process: NtLmSsp
|> | Authentication Package: NTLM
|> | Workstation Name: DELL2400
|> | Caller User Name: –
|> | Caller Domain: –
|> | Caller Logon ID: –
|> | Caller Process ID: –
|> | Transited Services: –
|> | Source Network Address: 192.168.1.102
|> | Source Port: 0
|> |
|> |
|>
|>
|

.