

Re: Event id 529

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2007-07/msg00143.html

- *From:* THI_IB <myself@xxxxxxxxxxx>
 - *Date:* Wed, 11 Jul 2007 13:40:04 -0700
-

Hi Jose :)

Are your machines accessible through the internet? Don't ask me – you should know better.

No I won't ask you !!!

The machines are not accessible from the Internet. There is this little thing called ACL that only allows connections that are "established" from the inside source. Everthing else gets "dropped". Yea, I took a look at the Pfirewall.log before posting and nothing. I don't have access to my Network Observer software at the moment, but that will be my next step.

Thanks for asking though.

--

Harv-man
Network Support

"Jose" wrote:

10 years of experience huh? :)

Saw such a thing once when my XP box was connected directly to the internet without an intermediate router/firewall+nat device. I guess these are infected win boxes on the internet doing scans for other vulnerable boxes and trying to login with some standard/random usernames/passwords.

Are your machines accessible through the internet? Don't ask me – you should know better. What comes to my mind for troubleshooting this is to enable windows firewall, enable logging and, after 529 event appears, take a look in the firewall log to see where it is coming from. Of course, you could do that with any sniffer/packet capturing tool like Ethereal or Network Monitor, but I think as a first step windows firewall would be easier to use.

After you see the source of this request, maybe this situation will clear out or maybe you will be able to decide on additional troubleshooting steps.

Re: Event id 529

"THI_IB" <myself@xxxxxxxxxx> wrote in message
news:C5C6E172-9B18-4B1D-8985-257B1BD40BB3@xxxxxxxxxxxxxxxxxxx

Hello to All:

Problem:

No domain controllers, just windows xp machines in a workgroup connected to the Internet behind a secure DMZ, firewall, and proxy server. I have listed just a couple of the machines in the workgroup, but there are about half a dozen more in the workgroup that show up in the event log with event id 529 as the shown below.

I setup a brand new pc right out the box and as you can guess a day later it shows up in my security logs (event id 529). All pc's including mine are xp boxes.

This occurs on a daily basis, at least 7 or 8 times a day with different pc's in the workgroup. It is not causing a problem, but from a technical view I would like to know why this is happening.

Virus def's are set to update 3 times a day. Virus scans are done once in the morning and once in the evening. Windows updates are applied on a regular basis.

I have been over my system with a fine tooth comb and found nothing. I have read several threads from a google search that are experiencing the same problem, but no solid solution. Of course every network is different. Only common denominator is Microsoft OS (xp, w2k, etc etc)

As one of the network admins here with the company and 10 years in the network support field (MCSE, A+ certified, CCNA) I'm pretty sure I do not have an application installed that says hey come and logon to my pc why don't ya.

My fellow techies of the world, am I missing something here? Thanks

1.) Event Type: Failure Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 529
Date: 7/10/2007

Re: Event id 529

Time: 1:40:25 PM
User: NT AUTHORITY\SYSTEM
Computer: HMORRISPC
Description:
Logon Failure:
Reason: Unknown user name or bad password
User Name: jbauch
Domain: JBAUCHPCC
Logon Type: 3
Logon Process: NtLmSsp
Authentication Package:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Workstation Name: JBAUCHPCC

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

2.)
Event Type: Failure Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 529
Date: 7/9/2007
Time: 4:48:48 PM
User: NT AUTHORITY\SYSTEM
Computer: HMORRISPC
Description:
Logon Failure:
Reason: Unknown user name or bad password
User Name: Emily
Domain: EMISRACHPC
Logon Type: 3
Logon Process: NtLmSsp
Authentication Package:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Workstation Name: EMISRACHPC

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

--
Harv-man
Network Support

Re: Event id 529