

Re: Failure Audits 529 & 680: How to track the IP address?

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2005-07/0743.html

From: Wesley Vogel (123WVogel955_at_comcast.net)

Date: 07/13/05

Date: Wed, 13 Jul 2005 14:00:03 -0600

Nothing to worry about. I get Event ID 529 & 680 all the time.

[[The event occurred on Windows XP if the machine environment meets the following criteria:

- The machine is a member of a domain.
- The machine is using a machine local account.
- Logon failure auditing is enabled.

When the user logs off, Windows will write event ID 529 to the log file because the OS incorrectly tries to contact the domain controller (DC), despite the fact that the machine is using a local account. Microsoft currently doesn't provide a fix for this problem, but you can safely ignore this event ID.]]

Event Type: Failure Audit

Event Source: Security

Event Category: Logon/Logoff

Event ID: 529

Date: 12/27/2003

Time: 7:49:48 AM

User: NT AUTHORITY\SYSTEM

Computer: MYPENTIUM450

Description:

Logon Failure:

Reason: Unknown user name or bad password

Security Event 529 Is Logged for Local User Accounts

<http://support.microsoft.com/?kbid=811082>

Failure Events Are Logged When the Welcome Screen Is Enabled

<http://support.microsoft.com/?kbid=305822>

Event Type: Failure Audit

Event Source: Security

Event Category: Account Logon

Event ID: 680

microsoft.public.windowsxp.security_admin: Re: Failure Audits 529 & 680: How to track the IP address?

Date: 12/27/2003

Time: 7:49:48 AM

User: NT AUTHORITY\SYSTEM

Computer: MYPENTIUM450

Description:

Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0

Explanation

A program or service attempted to start with the logon credentials specified in the message, which do not match the credentials of the current user. This message is logged for informational purposes only.

User Action

No user action is required.

Failure Events Are Logged When the Welcome Screen Is Enabled

<http://support.microsoft.com/?kbid=305822>

--

Hope this helps. Let us know.

Wes

MS-MVP Windows Shell/User

In news:OQxPtP%23hFHA.328@tk2msftngpl3.phx.gbl,

Juerg Reimann <jr@jworld.ch> hunted and pecked:

> *** I'm not quite sure in what NS this post fits best, so I set a
> followup-to: microsoft.public.security ***

>

> I get quite a lot of 529 and 680 Failure Audits in the Security Log of the
> Event Viewer. Some folks try (probably mistakenly, hopefully) to get into
> my computer (yes, it's not behind a fw at the moment). So I want to track
> down those Failure Audits with IP addresses of the hosts that cause them.

>

> Does anybody know a (maybe freeware) solution to achieve something like
> that? (Note: I'm talking about future events, it's clear that past ones
> cannot be resolved to IPs anymore.)

>

> As always, any help would be much appreciated!

>

> Cheers, Juerg

>

> --

> It's time to tune in: <http://iradio.ch/>