Re: Failure Audits in the secruity log Event Viewer

Source:
http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2005−04/0650.html

---

From: Wesley Vogel (*123WVogel955_at_comcast.net*)
Date: 04/12/05

```
Date: Tue, 12 Apr 2005 15:40:49 −0600
```

I don't know anything about Event ID: 615 and

Windows XP Home/Professional Events and Errors
http://www.microsoft.com/technet/support/ee/search.aspx?DisplayName=Windows%20XP%20Professional&ProdNam

brings up nothing.
−−−−−

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
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:9B988DE8-E661-4F44-B1C6-7C638C914989@microsoft.com,
Techno Phobe <Techno Phobe@discussions.microsoft.com> hunted and pecked:
> Hello fellow Newsgroup members.  :-)
>
> I have a computer running Windows XP Home Editon.  This is a stand alone
> computer, it is not connected to a network.
>
> Since I have had my computer there are always 3 different Failure Audits
> shown in the secruity log in the Event Viewer.  The Event Viewer is under
> Aministrative Tools in the Start Menu.
>
> When I click on the Failure Audit event messages in the Event Viewer this
> is the information given for each of the 3 different Failure Audits:
>
> 1ST FAILURE AUDIT:
>
> Source:     Secruity
> Category:  Policy Change
> Type:        Failure Audit
> Event ID:   615
> User:        NT AUTHORITY\NETWORK SERVICE
>
> Description:
> IPSec Services:  IPSec Services failed to get the complete list of network
> interfaces on the machine.  This can be a potential security hazard to the
> machine since some of the network interfaces may not get the protection as
> desired by the applied IPSec filters.  Please run IPSec monitor snap-in to
> further diagnose the problem.
```

```
> ---------------------------------------------------------------------------
------
> I have tried to run the IPSec monitor snap-in but I could not figure out
> how to use it.  I clicked on the help link in the error message but the
> information in the help web site is too technical for me to understand.
>
> This event, 615 Policy Change, has a Failure Audit when the computer
> starts and sometimes has a Success Audit straight after.
>
>
> 2ND FAILURE AUDIT:
>
> Source:     Secruity
> Category:  Account Logon
> Type:        Failure Audit
> Event ID:   680
> User:        NT AUTHORITY\SYSTEM
>
> Description:
>     Logon attempt by:  MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
>     Logon account:  "User Name"
>     Source Workstation:  "Computer Name"
>     Error Code:  0xC000006A
> ---------------------------------------------------------------------------
--------
> This event, 680 Account Logon, always has a Failure Audit when the
> computer starts and always has a Success Audit straight after.
>
> 3RD FAILURE AUDIT:
>
> Source:     Secruity
> Category:  Logon/Logoff
> Type:        Failure Audit
> Event ID:   529
> User:        NT AUTHORITY\SYSTEM
>
> Description:
>      Logon Failure:
>   Reason: Unknown user name or bad password
>   User Name: "User Name"
>   Domain: "Computer Name"
>   Logon Type: 2
>   Logon Process: Advapi
>   Authentication Package:  Negotiate
>   Workstation Name: "Computer Name"
> ---------------------------------------------------------------------------
-------
> I do have a password created for my Windows XP Account, which is an
> administrators account.  I enter the password on the welcome screen and I
> can log on with no problem.  So why do I have this error which says that
> there is an "unknown user name or bad password" when I am able to log on
> perfectly??
>
> This event, 529 Logon/Logoff, always has a Failure Audit.  It has never
> had a Success Audit!!!  But like I said, I am always able to log on to my
> Windows XP account using my user name and password at the welcome screen
> everytime.
>
> QUESTIONS ABOUT THESE FAILURE AUDITS:
>
> What are the causes of each of these 3 Failure Audits?
>
```

```
> How can I fix these Failure Audits and prevent them from happening again?
>
> Are these 3 Failure Audits a serious threat to my computer?
>
> Can someone please help me correct these errors.  I am NOT a computer
> expert so  for me to understand your generous help and advice, please do
> not use technical computer language and acronymes.
>
> I am very grateful for any help and advice you generous people out there
> are willing to give me!!!  :-)  :-)
>
> THANK YOU,
>
> Techno Phobe.
```