

Re: Event Viewer: Security: Failure Audit: Username/Password question

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2005-01/6120.html>

From: Jerry zhao (v-jerryz_at_online.microsoft.com)

Date: 01/21/05

Date: Fri, 21 Jan 2005 08:57:42 GMT

Hi Bryce,

Thanks for your posting. Also thanks for Marina's update.

Actually, you can not see the password that has been attempted just like Marina mentioned. Generally, password is sensitive personal information. Even the domain administrator who can view the account information of every user in the domain can not view the Password of the users. That's a by design feature to protect user privacy.

You may have interest in details of Event 529:

Product: Windows Operating System

ID: 529

Source: Security

Version: 5.0

Component: Security Event Log

Symbolic Name: SE_AUDITID_UNKNOWN_USER_OR_PWD

Message: Logon Failure:

Reason: Unknown user name or bad password

User Name: %1

Domain: %2

Logon Type: %3

Logon Process: %4

Authentication Package: %5

Workstation Name: %6

Explanation

This event record indicates an attempt to log on using an unknown user account or a valid user account but with an incorrect password. An unexpected increase in the number of these audits could represent an attempt by someone to find user accounts and passwords (such as a "dictionary" attack, in which a list of words is used by a program to attempt entry).

User Action

The person with administrative rights for the computer should establish a threshold limit for attempted log ons. Attempts in excess of the limit should be investigated as a possible attempt to break into the computer.

Meanwhile, you may want to disable a user account if an incorrect password is entered a specified number of times over a specified period. These policy settings help you to prevent attackers from guessing users' passwords, and they decrease the likelihood of successful attacks on your network. For more information about this, please refer:

To apply or modify account lockout policy

http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/password_lockout.asp

FOR YOUR INFORMATION:

You can check any Events from the Microsoft web site:

<http://www.microsoft.com/technet/support/ee/search.aspx?DisplayName=Windows%20Server%202003&ProdName=Windows%20Operating%20System&MajorMinor=5.2&LCID=1033>

I hope the above information helps.

Please feel free to let me know if you have any questions or if you need further assistance.

Have a nice day!

Best regards,

Jerry Zhao (MSFT)

Microsoft Online Partner Support

Get Secure! – www.microsoft.com/security

=====
When responding to posts, please "Reply to Group" via your newsreader so that others may learn and benefit from your issue.
=====

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