KAK - Windows account keeps getting locked out!

http://social.technet.microsoft.com/Forums/windowsserver/en-US/4f72c4b1-343c-459a-b431-de24ea2d5136/windows-account-keeps-getting-locked-out?forum=winserverManagement

I have a Windows network with 3 domain controllers and 5 member servers, all running Windows 2003 server. All workstations are XP professional. Since Monday, I have noticed that my user account keeps getting locked out every 6 or 7 minutes. The AD accounts are set to lock out after 4 tries with a wrong password. How do I setup an audit process to find out which computer, user, process or perhaps hacker is trying to access what part of the network on which server that is causing this?

thank you for your help

Vahid

Wednesday, September 26, 2007 4:37 PM

|

All replies

You can use LockoutStatus.exe which is part of Account Lockout and Management tools to identify domain controller that are involved in lock-out user account.

http://www.microsoft.com/downloads/details.aspx?FamilyID=7AF2E69C-91F3-4E63-8629-B999ADDE0B9E&displaylang=en

If you have audit account logon security policy enabled, then you can proceed to filter through the security log of domain controller identify earlier for event related to lockout of this account.

The event log will provide you the error code which can help you identify reason for account lockout and source IP addresss/computer to help you identify which computer that generate the invalid logon attempt.

You can refer to following article for information related to troubleshooting account lockout issue:

http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/bpactlck.mspx#EEEAG

- Proposed as answer by Shaun Gorman Monday, November 12, 2012 10:45 PM

Wednesday, September 26, 2007 5:18 PM

Thank you for your help.

I have enabled auditing for account log in events. But, from what I understand, events related to login attempts are logged on computers that are sending the credentials not on the servers receiving requests for logging. If I understand this correctly, I will have to go on a fishing expedition on all workstations and servers trying to find out which computer is sending bad credentials. The exercise will be futile especially in the case of an attack. The computer sending bad credentials may be sitting thousands of miles away beyond my reach.

Is there any source on any of the Domain controllers that keeps track of such activities?

Thank you again

- Proposed as answer by IMTech Wednesday, May 12, 2010 7:27 PM

Wednesday, September 26, 2007 6:13 PM

Sorry wrong click on the proposed part..

I notice that some of my user's account keep getting locked out, even after I unlock them as well. By the way, their machines are not joined to the domain.

What I did was I went onto their machine and delete all the saved credentials or change all the saved credentials on the machine to the current password. With that, I was able to stop the account from getting locked out. If this is too much, you can configure the group policy to not lock out users. You need to right click on domain in AD, properties, Group Policy tab, edit the "main" Group Policy for the domain, expand Computer Configuration, expand Windows Settings, Expand security settings, Expand account policies, select Account Lockout, then right click on Account lockout threshold and set that to 0 and leave the other two undefined or set it to 0. This is fix for whole domain...You might not want to do this for security reasons but it will fix your error..if it's the same as mine.

IMTech

Wednesday, May 12, 2010 7:36 PM

alternatively, on the domain controller, you can log in as admin, and set the event logging under security in the mmc(event logs) to audit security access failures only. This will pinpoint the problem machine or user trying to access the account, with the time and originating location of the failed login.

"http://support.microsoft.com/fixit/default.aspx ". This is MICROSOFT'S new, FREE, fully automated, anonymous support portal, which can help users resolve windows and other product issues with a few mouse clicks.
BOOKMARK THIS SITE, EVERYBODY !!!

- Proposed as answer by NTauthority T.Welch Monday, November 29, 2010 11:16 PM

Monday, November 29, 2010 11:16 PM

The most common cause of phantom lockouts is a hung remote session somewhere. The user remains logged in after their password has expired and the password gets reset; however in the original session the original password is still cached and once the Kerberos session ticket expires it tries to renew it causing the lockout.

Other causes of lockouts include hard coded credentials in:

- logon scripts & command files (BAT, CMD, VBS, KIX, etc)
- scheduled tasks

Microsoft provides a free set of tools called Account Lockout and Management Tools which you can download as the self-extracting file ALTools.exe from the Microsoft Download Center. The remainder of this article examines several of these tools.
For details please go through below post :

http://social.technet.microsoft.com/Forums/en-US/winserverDS/thread/415d165e-a004-479c-9644-b7f9263fc6d8/
http://social.technet.microsoft.com/Forums/en-US/identitylifecyclemanager/thread/ac570c8a-5df4-4e16-af8b-abda6b54c7f9
http://www.windowsecurity.com/articles/Implementing-Troubleshooting-Account-Lockout.html

---

Dinesh S.

- Proposed as answer by Dinesh111 Wednesday, December 15, 2010 1:04 PM

Wednesday, December 15, 2010 1:01 PM

Hi Vahid

If is just one or few accounts has been locked out, try to change username. In certain cases this could be helpfull.

I have similar case where (for some reason) Croatian caracters in Display name causes problem.

Otherwise you can track what is going on using ProcesExplorer on suspected workstation (if it is reachable by you)

Best regards
Dubravko Marak
MCP
Blog: **Windows Server Administration**
Please remember to click **"Mark as Answer"** on the post that helps you, and to click **"Unmark as Answer"** if a marked post does not actually answer your question. This can be beneficial to other community members reading the thread.

- Proposed as answer by Koyo1974 Tuesday, July 10, 2012 5:44 AM
- Unproposed as answer by Koyo1974 Tuesday, July 10, 2012 5:44 AM

Saturday, May 19, 2012 6:08 PM

Depending on which version of Server you are using; in the **Security** *Event Log* look for Event ID 644 (Windows Server 2003) or Event ID 4740 (Windows Server 2008). You should see something like this:

---------- Cut from Event Log ----------

A user account was locked out.

Subject:
Security ID: SYSTEM
Account Name: SERVER$
Account Domain:

YOURDOMAIN
Logon ID: 0x3e7

Account That Was Locked Out:
Security ID: DOMAIN\User
Account Name: User

Additional Information:
Caller Computer Name:

ComputerName

---------- End of Cut ----------

This last bit is the important bit, the ***ComputerName*** is the PC/laptop or device that the logon attempt was made from; this is your starting point in solving the problem.

I hope this helps.

Wednesday, July 10, 2013 11:07 AM