

RE: Tracing source of remote logons

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2006-09/msg02589.html>

- *From:* v-crinal@xxxxxxxxxxxxxxxxxxxxxx ("Crina Li")
 - *Date:* Mon, 18 Sep 2006 08:44:45 GMT
-

Hi Tom,

Thank you for posting in SBS newsgroup.

I am sorry for the delayed response due to weekend. Please understand that the newsgroups are staffed weekdays by Microsoft Support professionals to answer your systems and applications questions. Your understanding is greatly appreciated!

Based on your description, I understand this issue to be: you receive security event 529 on your SBS 2k3 server and logon type is 10. If I have misunderstood your concerns, please do not hesitate to let me know.

As I know, Logon type 10 is interpreted to RemoteInteractive. When you access a computer through Terminal Services, Remote Desktop or Remote Assistance windows logs the logon attempt with logon type 10 which makes it easy to distinguish true console logons from a remote desktop session. Note however that prior to XP, Windows 2000 doesn't use logon type 10 and terminal services logons are reported as logon type 2.

Do you mean the Source Network Address of the event is internal IP of SBS?

As I know, the Failure event may be caused by dictionary attack to crack the administrator password. So, the result could be someone was trying to logon your SBS server through Remote Desktop via 3389 with different username and password combinations, but failed.

Regarding this situation, I would like to give the following suggestions:

1. Please enforce the strong password policy and make sure passwords are well managed throughout your network. Implement Strong password policies. Open 'Server Management console', navigate to Users snap-in. In the right panel, click 'Configure Password Policies'. Enable the password policies.

For more information:

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/bpactlck.mspx>

RE: Tracing source of remote logons

2. Close the 3389 port on your hardware router or on your SBS 2k3 ISA/Basic Firewall configuration. 3389 port is necessary for the Remote Desktop connection. By disabling this port, bad guys could no longer initiate the remote desktop session and try the dictionary attack. For administrating the SBS server, I would suggest you access the server through the RWW portal. With logging to the RWW first and then logon to the SBS server remotely, traffics are actually going through 443 and 4125 proxy port. This could successfully prevent Robot Dictionary Attack on 3389 port.

3. More information:

Securing Your Windows Small Business Server 2003 Network

<http://download.microsoft.com/download/1/f/1/1f15a874-f696-4992-b5ad-b1e7b258de1c/SecuringSBSnetwork.doc>

Also if you would like to check the real-time TS sessions, we can use Terminal Server Manager. To do that:

1. Click Start | Programs | Administrative Tools | Terminal Service Manager.
2. Click <Server Name> in the left pane, and then you can see detailed information in the right pane.

If you want the real time logging for the Terminal service, I suggest that you use WinStation Monitor to get the real-time status of the user name, domain, IP address, session ID, and connection status of currently logged-on users. For more detailed information, please refer to the KB article:

320190 HOW TO: Use WinStation Monitor to Monitor Terminal Services Client
<http://support.microsoft.com/?id=320190>

If you want to check who and when log on the TS server, you can use the "Audit logon events" to audit the "logon locally" events since users should have the "logon locally" permission to log on the TS server. If the TS server is a member server, you can configure the local security policy. You can refer to the following KB article:

174073 Auditing User Authentication
<http://support.microsoft.com/?id=174073>

If you have any questions or concerns related to this issue, please let me know.

I appreciate your time and look forward to hearing from you.

Best regards,

Crina Li (MSFT)

Microsoft CSS Online Newsgroup Support

RE: Tracing source of remote logons

RE: Tracing source of remote logons

| Reply in group, but if emailing add another
| zero, and remove the last word.

|
|
|

.