

Re: random lockouts

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2002-11/10861.html>

From: Karl Levinson [x y] mvp (levinson_k@excite.com)

Date: 11/04/02

From: "Karl Levinson [x y] mvp" <levinson_k@excite.com>

Date: Mon, 4 Nov 2002 13:14:16 -0500

"KevinB" <kevinb@centralchurch.com> wrote in message
news:bd2d01c2842a\$02a84430\$3bef2ecf@TKMSFTNGXA10...

> I've got a network with several Windows 2000 Servers and
> about 150 Windows 98 clients. At random times, currently
> logged on users will lose authentication. They can log in
> just fine, and work in network shares just fine, but then
> suddenly they are told they do not have permission to
> access the network drive. They lose access to everything
> on the network. When they try to log back in they are
> locked out. My security log shows the attempts to access
> the file they were working in just minutes before, lists
> it with invalid logon name or password. There are no
> previous logon failures for that account, and there are no
> login attempts from computers other than the one the user
> was working on. Has anyone had a similar situation of
> users being booted and then locked out. Kerberos does not
> log any errors. When I unlock their account, they can log
> in just fine. This usually happens to 3 or 4 users a
> day. My network is behind a firewall, with current virus
> sigs, and current patching. Anyone seen similar, or have
> any ideas?

I assume that you're sure that the caps lock is not on, a key on your keyboard is not broken, the password has not been changed by someone else, the user has not changed his password at one computer while being logged into another computer, that there are no network drives mapped on a computer using the login ID with an old password, and no network services on Windows NT / 2000 / XP are trying to load as the login ID with an old password.

There are a number of issues causing people with Windows 98 computers to have this problem. Searching www.microsoft.com/support for the error message you're receiving should bring some of them up. For example, here are some of the possible causes and solutions as described in the knowledgebase. Unfortunately it sounds like Microsoft is still working on the patch and probably won't give it to you unless you call them and convince them to.

<http://support.microsoft.com/default.aspx?scid=kb:en-us:Q272594>

"CAUSE

This problem occurs because the Windows 2000-based server rejects your logon password when the client computer does not correctly de-allocate an internal structure that is used to track the logon session. The client attempts to reuse the expired encryption key that is passed to it by the server during the original logon.

This problem does not occur in conjunction with Microsoft Windows NT-based clients because the client does not attempt to use Distributed File System (DFS) because the session that is reused is against a DFS referral from the Windows 95-based or Windows 98-based client.

[possibly also related:]

The client computer sends invalid encrypted password information to the server if the session that has been established between them is reset more than once. A session on the server can automatically time out, as noted in the Microsoft Knowledge Base article that is listed in the "Workaround" section of this article. Additionally, a session on a Microsoft Windows 2000-based computer can be disconnected in the user interface by right-clicking My Computer, clicking Manage, clicking Computer Management, clicking Shared Folders, and then clicking Sessions.

You can see a session reset that is initiated by the server in network traces as a TCP Reset packet on port 139 (NetBios Server service). During reconnection, the client computer sends a C Session Setup And X server message block (SMB) for the share. The server returns ACCESS_DENIED in an R Session Setup SMB.

WORKAROUND

To work around this issue, use any of the following methods:

- Reboot?
- Click Start, click Run, type winipcfg, and then release and renew the DHCP lease. This essentially resets the entire network stack.
- Open Network Neighborhood, and then double-click the affected server and share.
- Type net use \\servername\sharename at a command prompt.
- Click Start, click Run, and then type \\servername.

You might also try making sure you have all the latest patches on the workstations and also try the fix in the following article:

<http://support.microsoft.com/default.aspx?scid=kb:en-us:Q293793>

For additional information about control of the LAN Autodisconnect feature in Windows 2000, click the article number below to view the article in the Microsoft Knowledge Base:

Q138365 How the Autodisconnect Works in Windows NT

microsoft.public.win2000.security: Re: random lockouts

<http://support.microsoft.com/default.aspx?scid=kb:en-us:Q138365>