

Re: Unexplained Failed Logins

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2007-01/msg00075.html>

- *From:* "Roger Abell [MVP]" <mvpNoSpam@xxxxxxx>
 - *Date:* Fri, 19 Jan 2007 22:49:30 -0700
-

"James B" <JamesB@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:47C55EAD-3A8E-4E3A-A344-9B1888E288AC@xxxxxxxxxxxxxxxxxxxx

Roger,

We do audit successful logins. There were no successful user logins for hours before or after these failures. The things that bookended these failures were a backup job at 11:58 pm and a NAV scan at 5:00 am.

We do have a VPN. I checked the log file and didn't see anything near that time, though that file only shows successful connections.

Do you have any other recommendations regarding what files/logs I should check?

No, I do not. Again, you seem to have looked most places that may leave trace, so I would recommend that you ask in the SBS newsgroup in order to key in on peculiarities of that bundle.

Roger

"Roger Abell [MVP]" wrote:

It is going to be pretty hard to get much further with the available info (i.e. evt log examples). Since it apparently negotiated Kerberos authentication we could assume that the originator was recognized as part of the domain (except I am a bit thrown off by the stated client IP – it is almost as if the DC is attempting a login via a delegation, plus I have been noticing increase "probes" which seem to skirt negotiation and directly attempt Kerberos authN on network exposed machines/interfaces).

Re: Unexplained Failed Logins

As I said, the evt msgs you showed do not fit a FrontPage authentication which would show IIS and use NTLM.

Are you auditing login success so that you could see if there is a subsequent successful login?

There are ways to make Kerberos logging more verbose, but that is not something one would want to leave enabled.

Is there any type of VPN capability enabled?

Also, you may want to post to the windows.server.sbs newsgroup as people there are more deeply familiar with the exposures SBS has to the external network.

Roger