

Re: How to know if someone accessed using RDP

Source:

http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active_directory/2006-08/msg00163.html

- *From:* "Ken Aldrich" <supportw@xxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 19 Jul 2006 13:42:07 -0500
-

Was he logging in with a domain account?

If so, check the security logs on your domain controllers. Look for authentication from his user account.

Was he logging in with a local computer account?

If so, check the security logs on the server he was logging into.

To do so, right-click on My Computer and select "Manage". Open "Event Viewer". Go to "Security". You can look through the logs to find authentication for his account. You can use the filter tools to make your search more efficient.

How does one access your network remotely? Do they have to VPN in first?

If so, check the VPN access logs.

This will most likely not apply if you have your remote desktop available to the public without authenticating to VPN first.

Ken Aldrich
DSRAZOR for Windows
Visual Click Software, Inc.
www.visualclick.com

"JM" <jm@xxxxxxxx> wrote in message
[news:o6evg.30122\\$vl5.7062@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:o6evg.30122$vl5.7062@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

We have Windows 2000 server (SP4), and our IT guy just left under questionable circumstances. In the couple of days after he left but before we changed the server password, we think that IT person used remote desktop to get in a mess with some things.

Is there a log file that would document his activity, at least show us a connection date and time?

thank you,

Re: How to know if someone accessed using RDP

jm