

Re: Help with possible hacker...

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2002-12/14251.html>

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

Date: 12/31/02

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

Date: Tue, 31 Dec 2002 16:26:18 -0500

"Tom Rossi" <TomRossi7@yahoo.com> wrote in message

news:cb00dd30.0212310622.4a922227@posting.google.com...

> *I continue to get a group of login failures every few days. The login
> attempts spread all of the local accounts on one of my servers. I
> cannot tell from the security log the IP address of the hacker. Is
> there somewhere else I can look? Please help...*

>

> *Here is an example from the event log:*

>

> *12/23/2002 12:18:25 PM Security Failure Audit Account Logon 681 NT*

> *AUTHORITYSYSTEM SERVERNAME The logon to account: MemProxyUser1*

> *by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0*

> *from workstation: SPSEVER*

> *failed. The error code was: 3221226036*

> *1*

If you think you've been hacked, here's how to determine whether you have and how it happened:

<http://securityadmin.info/faq.htm#hacked>

...then, how to re-secure and harden your computer:

<http://securityadmin.info/faq.htm#re-secure> [only necessary if you have been hacked]

<http://securityadmin.info/faq.htm#harden>