

Re: Event 627 Failure of Change Password Attempt

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2007-10/msg00415.html

- *From:* kn0tu <kn0tu@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 29 Oct 2007 18:51:00 -0700
-

Steve,

I would agree with you about the Guest account. However there were password change attempts on the AspNet account also.

BTW, I downloaded and installed Spyware Doctor and it found some tracking cookies. No viruses though.

I have been getting some error messages about not being able to write to my hard disk, but when I look at Event Viewer there are no errors recorded. I think I am being spoofed.

I think I may be the victim of some Remote Access Trojan that has yet to be named and handled by the major software companies.

—

kn0tu

"Steven L Umbach" wrote:

Though that is odd behavior I really tend to doubt your computer was hacked in that a hacker does not target the guest account as they wan administrator access but since your computer is XP Home it is not possible to access the computer remotely via the administrator account which generally has a blank password anyhow and is available only in Safe Mode logon.

Possibly malware or spyware could cause such activity to disable your ability to access shares on your computer from another computer on the network by setting a guest password. To get more details would require process tracking activities to see what processes are running at the time of the failed password changes though that is very difficult on XP Home due to it's lack of ability of advanced logging.

No you can not manage privileges which are also called user rights in XP Home via a GUI as that would take command line tool call NTrights.

If you have not done so yet do a full spyware scan with an additional

Re: Event 627 Failure of Change Password Attempt

program. The free version of Spyware Doctor from <http://pack.google.com> is very good and worth trying. If you can not track it down and everything is working correctly you may want to just live with it. Otherwise you could try using msconfig to try and selectively disable startup items [most likely non Microsoft items] to see if you can narrow down a particular process that is causing the activity.

Steve

http://www.netsquirrel.com/msconfig/msconfig_xp.html
<http://support.microsoft.com/kb/310353>

"kn0tu" <kn0tu@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
<news:7784712C-A0D2-448B-9780-29907C92B7B0@xxxxxxxxxxxxxxxxxxxx>

I am getting dozens of these entries in the Security Log with both Guest and ASPNET. This leads me to believe my machine has been hacked. Is this true?

My machine is a Pentium 4 running XP SP2 Home and is up to date with patches, or so Microsoft Baseline Security Analyzer says. I have a firewall security suite which has a anti-virus component and it is up to date as well with about 276,000 signatures.

The events I am getting are:

Event Type: Failure Audit
Event Source: Security
Event Category: Account Management
Event ID: 627
Date: 10/20/2007
Time: 8:19:42 PM
User: GATEWAY-DESKTOP\Owner
Computer: GATEWAY-DESKTOP
Description:
Change Password Attempt:
Target Account Name: Guest
Target Domain: GATEWAY-DESKTOP
Target Account ID: GATEWAY-DESKTOP\Guest
Caller User Name: Owner
Caller Domain: GATEWAY-DESKTOP
Caller Logon ID: (0x0,0x11346)
Privileges: -

For more information, see Help and Support Center at

Re: Event 627 Failure of Change Password Attempt

<http://go.microsoft.com/fwlink/events.asp>.

I have noticed other things like when I go to My Computer>Manage there is no way to set or modify privileges. Is this restricted in XP Home?

—
kn0tu