

Re: Login Errors Seem to indicate we are being hacked?

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2008-09/msg01115.html>

- *From:* "Dave Nickason [SBS MVP]" <gw@dibble.com>
 - *Date:* Sat, 13 Sep 2008 15:55:59 -0400
-

Does your firewall logging allow you to see what port these login attempts are hitting? I've been getting a good number of them recently myself. I think they're attempts to log into SMTP to relay spam. If you look in task manager and find PID 1692, is it inetinfo.exe? (Note that PIDs may change after a reboot). I've got ISA configured so it only allows SMTP and RWW, and I use RWWGuard for RWW security, so I'm confident that in my case it can't be anything but SMTP.

I configured Exchange not to allow relay from outside, even with authentication. While I certainly don't appreciate the bad guys trying to authenticate to Exchange, there's nothing they could do even if successful. And with 2-factor authentication for RWW, I'm absolutely confident that no one is getting in that way.

I tend to get a whole bunch of these over a few days or a week, then none for a while, then they start up again.

"Siv" <Siv@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:60D337F0-493E-443E-88B1-116ADF2BB5D8@xxxxxxxxxxxxxxxxxxxx

Hi,

In the logs this morning for one of my clients I have had about 500 failed logins in teh Security logs. I looked at the Security Event Log and filtered for failures and there were hundreds of attempts in very quick succession some using the same user name (and presumably different passwords) and then loads of different user names one after the other which sounds like a brute force attempt to gain access.

We use very strong passwords so I am not worried they will have got in, but I would like to ascertain how they were doing it as no IP addresses were quoted so they weren't getting in via the net (unless they were somehow hiding their IP Address). The typical log entry looks like this:

Event Type: Failure Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 529
Date: 12/09/2008
Time: 12:29:41
User: NT AUTHORITY\SYSTEM
Computer: SERVER01

Re: Login Errors Seem to indicate we are being hacked?

Description:

Logon Failure:

Reason: Unknown user name or bad password

User Name: pentium

Domain:

Logon Type: 3

Logon Process: Advapi

Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0

Workstation Name: SERVER01

Caller User Name: SERVER01\$

Caller Domain: MOUNTAINASH

Caller Logon ID: (0x0,0x3E7)

Caller Process ID: 1692

Transited Services: –

Source Network Address: –

Source Port: –

For more information, see Help and Support Center at

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

How do you interrogate the above entry into a meaningful explanation of how they were logging in. Ie what is a logon type 3 and what do the caller Login ID and Process ID tell me??

Any help appreciated.

Siv

--

Martley, Near Worcester, UK