

# Re: Logon failures filling the event log

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2007-08/msg03020.html>

---

- *From:* the\_nextman <[richard.markiewicz@xxxxxxxxxxxxx](mailto:richard.markiewicz@xxxxxxxxxxxxx)>
  - *Date:* Tue, 21 Aug 2007 14:04:09 -0000
- 

On 21 Aug, 14:23, Freaky <[wont...@xxxxxxxxxxxxx](mailto:wont...@xxxxxxxxxxxxx)> wrote:

Got IIS opened to the outside? Either HTTP or HTTPS? Seems like someone/some bot/some viri/etc is trying to attack your webserver.

the\_nextman wrote:

Hi Everyone

Running Small Business Server 2003 Premium at the moment as our office file and Exchange server.

Just got back from vacation and the last two days the event logs have been filled with failed logon attempts (really nice to come back and see the server performance report telling my 7676 critical errors!).

Logon Failure:  
Reason: Unknown user name or bad password  
User Name: zackary  
Domain:  
Logon Type: 3  
Logon Process: Advapi  
Authentication Package:  
MICROSOFT\_AUTHENTICATION\_PACKAGE\_V1\_0  
Workstation Name: [SERVERNAME]  
Caller User Name: [SERVERNAME]\$  
Caller Domain: [MYDOMAIN]  
Caller Logon ID: (0x0,0x3E7)  
Caller Process ID: 1732  
Transited Services: -

Re: Logon failures filling the event log

Source Network Address: –  
Source Port: –

So someone is trying to poke holes in our server? I also notice that the Guest account has been locked out (I've now disabled it).

Do I need to worry? I'm confident that all my users have strong passwords. Anything I can do to stop this? Or should I just ignore it?

Many thanks in advance for any advice or comments.

Cheers, Richard– Hide quoted text –

– Show quoted text –

Thanks, yes IIS is open to the outside:

- Small Business Server default web site (Remote Web Workplace?), Exchange web interface and CompanyWeb all require SSL and 128 bits.
- We also have MS CRM web interface running. No SSL but it only uses Windows Integrated.

We also have a bunch of protocols enabled to support Exchange and CRM (in web service extensions), but nothing that we don't need.

I would really appreciate any advice you might have or any comments. It is gratifying that this person/bot/virus doesn't seem to be getting access but still makes me quite nervous.

Also, does it mean anything that the source address/port aren't getting caught? Usually when my users get their password wrong, it traps the source IP address. Could this indicate the attack is from within the server (like a worm or virus?) or is this information easily hidden?

My experience of IIS 6 is that it is very secure – we also run a server farm (Windows 2003 standard, IIS6) hosting SSL secured, NTLM Sharepoint portals and never see this kind of thing going on.

If I have nothing to worry about that's fine, but I don't really see what I can do to stop this. I don't want to disregard the security

Re: Logon failures filling the event log

Re: Logon failures filling the event log

warnings. As I said, any comment or advice is very much appreciated.

Many thanks in advance, Richard

.