

Re: 100's of logon errors for MSFTPSVC, event id: 100

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2007-04/msg04054.html>

- *From:* "Mal Osborne" <mal@xxxxxxxxxxxxxxxx>
 - *Date:* Wed, 25 Apr 2007 08:51:18 +0800
-

That is an easy one!

You have FTP exposed to the outside world, hackers have seen it listening on port 21, and are trying a variety of common passwords to see if they can fluke it. If the credentials "Administrator" & "password" could allow FTP access, they would almost certainly have managed by now. If your admin password is a strong one, they probably will not. If you have a user who uses a weak password, hackers may manage to guess it.

If your server is full of child porn, phishing sites, stolen credit card numbers & pirate software, then they have guessed right!

Hackers can also derive a username from an email address, ie, if they have the name fred@xxxxxxxxxxxxxxxx, they can try authenticating against FTP or SMTP (to relay). They use the username "fred", and DNS lookup "somecompany.com" Of course if all of your users have strong passwords the will fail.

All of this hacking activity is done via automated scripts, usually from a machine that hackers have already compromised. Its easy for a script to scan thousands of IP addresses for an FTP server, and try thousands of passwords.

Any site that has FTP enabled *WILL* be hit with password guesses, strong passwords will trump the attacks.

Only real defense if to ensure strong passwords are in use. Getting rid of FTP if it's not needed is reasonable idea as well, but strong password are really essential. Its easier to have strong passwords than try to figure out & block everywhere that hackers may try to authenticate.

Mal Osborne
MCSE Mensa

"Mike Webb" <Mike_Webb@xxxxxxxxxxxxxxxx> wrote in message
<news:%23CDtAuohHHA.5048@xxxxxxxxxxxxxxxx>

Running SBS 2003 Premium, ISA 2004, SQL, WSUS, 2 NIC's and a router,
Symantec Backup Exec 11d, dynamic IP, DDNS service through dyndns.org.

=====

Checking the weekly Server Report I saw this. Checked the System Log and saw this over and over again. Seems to be running every 2 seconds and goes back to at least 11 April (end of my log). What do I check? Am I being hacked?

Re: 100's of logon errors for MSFTPSVC, event id: 100

Mike Webb
Platte River Whooping Crane Maintenance Trust, Inc.
a 501 (c)(3) conservation non-profit organization