

## 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/msg01151.html>

---

- *From:* "SteveB" <[newsgroup@xxxxxxxxxxx](mailto:newsgroup@xxxxxxxxxxx)>
  - *Date:* Sat, 13 Sep 2008 17:46:13 -0700
- 

You don't need port 80 open for any SBS functionality. I recommend closing it.

"Siv" <[Siv@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:Siv@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message [news:B260D9D2-7F06-4EE7-8341-DA71513CDE66@xxxxxxxxxxxxxxxxxxx](mailto:news:B260D9D2-7F06-4EE7-8341-DA71513CDE66@xxxxxxxxxxxxxxxxxxx)

Dave,

I have put logging on the Default SMTP Service in protocols (after some help from Teneo) and I will be able to catch the beggars if they try again and we are correct that it is the SMTP service.

I only have the ports opened by the IECW  
SMTP 25  
HTTP 80  
HTTPS 443  
Sharepoint 444  
RWW 4125  
VPN 1723  
TS 3389

All pointing to the same port on the SBS box.

It's a NAT Firewall/modem/router and the open ports are all forwarded to the SBS box.

You mentioned turning off Port 80 in one of your other posts, would that not stop access to Remote Web Workspace or is it only Port 4125 that is used by that?

Siv

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

—  
Martley, Near Worcester, UK

"Dave Nickason [SBS MVP]" wrote:

I don't know if that pins it down to SMTP, but I doubt that SMTP is the only thing on the box using that authentication package. Inetinfo is IIS, so the PID does narrow it down to something that uses IIS – Exchange, OWA, or anything else with a web site. I guess the way I'd word it is that the authentication package, the PID pointing to inetinfo.exe, and the fact that you (hopefully) don't have other services opened to the Internet strongly indicates that it's SMTP. The SMTP or IIS logs should answer everything.

I'm not familiar with that particular router or its logging capabilities, but you could just look at the manual or log into the interface and see what's there.

FYI, WPA2 with a strong key mitigates pretty much all risk from wireless. Really the only major risk would be something that a disgruntled user might do with the key, and you can work around that by changing the key when employees leave.

"Siv" <Siv@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message [news:64CE5372-CEC4-4A5F-B8E9-5BBF999F8788@xxxxxxxxxxxxxxxxxxxx](mailto:news:64CE5372-CEC4-4A5F-B8E9-5BBF999F8788@xxxxxxxxxxxxxxxxxxxx)

Dave,  
Just logged in and checked, yes it is inetinfo.exe. The firewall/router is directly connected to the internet and the server and I am not sure how to set up the firewall logging. It's a Draytek Vigor 2600i. I think you can set up logging and it posts it to a server port. I have never managed to get that working on this model properly.

As 1692 is Inetinfo.exe does that pin it down to SMTP. The post from Teneo

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

seems to indicate that the authentication package type points to SMTP.

He

suggested putting diagnostic logging on SMTP which I have done and if

they

have another go I'll see if I can get their IP and then

complain to

their

ISPs abuse team.

Thanks for the advice,

Siv

--

Martley, Near Worcester, UK

"Dave Nickason [SBS MVP]" wrote:

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 SMPT 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

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

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](mailto: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

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

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  
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\$\br/>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

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

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

what do the  
caller  
Login  
ID and Process ID tell me??

Any help appreciated.

Siv  
--  
Martley, Near Worcester,  
UK