

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/msg01287.html>

- *From:* "Dave Nickason [SBS MVP]" <gwdibble@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 15 Sep 2008 18:09:44 -0400
-

The syslog settings would be to send the router's log info to an external log server. Does it keep a log locally that you can read from the interface? As an example, my Sonicwall keeps a log that I can read from the regular UI, as well as having the ability to report to a syslog server or e-mail out the log info.

"Siv" <Siv@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
<news:348D2A59-0578-47C1-9CBD-58E278FF44C7@xxxxxxxxxxxxxxxxxxxx>

Dave,

I logged in and had a look at the router settings, the only thing I can see that looks like logging is an entry called "SysLog Access Setup" you can tick to enable this and then there are two boxes to fill in, one is "Server IP Address" and the other is "Destination Port" which is prefilled with "514"?

How that relates to getting logs I do not know unless you telnet into that port somehow??

Siv

--

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.

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

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

> 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
> 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.

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

>> 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
>> > Description:
>> > Logon Failure:
>> > Reason: Unknown user name or bad password
>> > User Name: pentium
>> > Domain:
>> > Logon Type: 3

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

>>> 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
>>
>>