

Re: Hacking Attempts ?

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2007-08/msg03814.html>

- *From:* Sunfire Solutions LLC <newsgroups@xxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 27 Aug 2007 19:49:48 -0700
-

I see this from time to time on client's servers, but I've never seen it when it's just a few attempts, usually we'll see it happen hundreds (or thousands) of times. More often than not, we catch it while it's happening and block the IP address, then contact the ISP that controls the IP and forward them the information showing the attack. Some shut the offending server down immediately, some forward it all to a research team.

Make sure that you enhance the logging on all of your virtual directories in IIS Manager and on your SMTP virtual server in Exchange to add all of the options in the advanced view so you can capture all possible data in the logs.

Teneo wrote:

Hi

Im seeing this in clients servers also. Trying to research some 3rd party to give better reporting function, got no idea which 'door' this webmaster is trying.

"Jeff Teel" <jdteel@RMoveThis.sugardog.com> wrote in message
news:Ogci1Cx5HHA.464@xxxxxxxxxxxxxxxxxxxxxxxx

I took a look at my Authentication logs this morning and noticed that I had a "webmaster" username attempt yesterday as well. There were eight attempts with times of:

7:17:25
7:17:26
7:17:28
7:17:29
7:17:45
7:17:47
7:17:48
7:17:50

All attempts mirror the one below except for the times of course.

Event Type: Failure Audit
Event Source: Security
Event Category: Logon/Logoff
Event ID: 529

Re: Hacking Attempts ?

Date: 8/24/2007
Time: 7:17:25 AM
User: NT AUTHORITY\SYSTEM
Computer: SERVER1
Description:
Logon Failure:
Reason: Unknown user name or bad password
User Name: webmaster
Domain:
Logon Type: 3
Logon Process: Advapi
Authentication Package:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Workstation Name: SERVER1
Caller User Name: SERVER1\$\br/>Caller Domain: businessnet
Caller Logon ID: (0x0,0x3E7)
Caller Process ID: 2032
Transited Services: –
Source Network Address: –
Source Port: –

"Colin" <Colin@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:54463927-E34B-41FA-9279-747CC0DF9687@xxxxxxxxxxxxxxxxxxxxx

Hi all,

I read a thread here a few days ago regarding a possible
hacking attempt.
The user trying to logon was 'webmaster', quite a common
hacker logon. I've
just received 3 daily server performance reports from 3
different sites all
reporting the same issue. The most concerning of these
reports is that I have
RWW (and OWA) locked down to certain ISP IP ranges or
from my own IP only.
One system even has a double authentication component. I
find it strange that
all of these servers got hit by a hacker at the same time (2355
hrs). No
systems have been compromised but it seems a bit of a
coincidence that a
'hacker' tried all 3 of my installations at the same time. Has
anyone else
had this behaviour or am I just unlucky that Mr Hacker
decided to pick on me
and 3 of my clients only last night ?

Re: Hacking Attempts ?

Regards Colin.