

Re: Can Somone Tell Me If We Have a Hacker?

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2006-06/msg00139.html>

- *From:* "Funkadyleik Ssynwhanker" <youreallywantoemailmepunk?@winblows.gov>
 - *Date:* Wed, 28 Jun 2006 09:17:19 -0500
-

"razor" <razor@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:A9FDA3C4-9A81-46ED-81C2-23BBA3D08AEF@xxxxxxxxxxxxxxxxxxxx

I wish we could track the IP, but it is not in the logs and we currently don't have any IDS or other tools to track that—unless there is something in W Server 2003 that we don't know about. Our Cisco Pix 515e firewall does not track IPs either.

The IP is in the text log (usually created here
/%windows%/System32/IISLogs/ftpsvc/). The Event log is not the only source of logging folks.

Just turn logging on and track all the fields and you will get that.

Usually though, these are from hacked boxes in China or Korea or something. Depending on what you are doing you can shitcan the entire pacific rim on your firewall to never see that stuff again. If it's developers that need the access, nobody else has any business knowing it's there let alone trying to get in. So be ruthless with your firewall rules or "deny all" except for the ISPs your developer uses and you just cut your potential pool of attacker IPs from 65 billion to a couple million.

They aren't trying to brute force, they are trying a short (compared to all combos) list of "common" ones such as "Password" "Passw0rd" etc. Watch the logs and they will come in with French and German spellings of "Administrator" too.

Those types of attacks DO work. You'd be suprised how many optimistic beginners out there do that stuff thinking no one will find their FTP site. "He he I will put some numbers in the word "password", nobody will _ever_ think of that!"

Re: Can Somone Tell Me If We Have a Hacker?

Thanks for the insight into the odds of breaking our password. Those are pretty good odds in our favor.

sd

"GobLox" wrote:

Keep in mind that changing passwords often only really protects you from someone on the inside or someone who has already broken the password. In the second case, chances are its too late then. Dictionary attacks? Put a number or two in there and you are safe... Brute force? Glance at your logs – with a 6–8 character password the odds are on your side Considering a 6 Letter password is 30Million combinations? You've got time to notice a brute–force attack and just ban the IP rather than "firewall" your FTP AKA "disable the FTP server" which is probably not an option.

"Steven Burn" wrote:

Been getting quite a few of these myself everything from IIS to FTP to SMTP (most common is my SMTP server). As with yourself however, I tend to use quite complex pw's that are changed twice daily.

--
Regards

Steven Burn
Ur I.T. Mate Group
www.it–mate.co.uk

Keeping it FREE!

"razor" <razor@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:7BF4A62E-0BE8-4A57-AD23-147AA71AB5C3@xxxxxxxxxxxxxxxxxxxx

Hello--

I am pasting an event log from our IIS/web server that repeats about

Re: Can Somone Tell Me If We Have a Hacker?

50
times every day during non-business hours.
Our SQL administrator
seems to
believe that someone is trying to hack into
our system via FTP.

Can somone tell me if the below is a hacker,
and what we can do about
it?

Event Type: Warning
Event Source: MSFTPSVC
Event Category: None
Event ID: 100
Date: 6/25/2006
Time: 12:45:25 PM
User: N/A
Computer: PWARDELLIIS
Description:
The server was unable to logon the Windows
NT account 'Administrator'
due

to

the following error: Logon failure: unknown
user name or bad
password.

The

data is the error code.

For more information, see Help and Support
Center at

<http://go.microsoft.com/fwlink/events.asp>.

Data:

0000: 2e 05 00 00

Many thanks,

sd

Re: Can Somone Tell Me If We Have a Hacker?