

Re: Masses of 529 Errors!

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2007-05/msg00075.html>

- *From:* "Roger Abell [MVP]" <mvpNoSpam@xxxxxxx>
 - *Date:* Fri, 11 May 2007 23:54:28 -0700
-

If the username is not changing, fixed at "anonymous" then at least you are being targetted by (of on the many) dumb probers. If you must have authentication interfaces exposed to the internet then there is not much you can do about this, save perhaps blocking all access for that origin IP – which is just a temp measure that does usually make them go away, although something they just return with another IP. On machines that must have authN interfaces exposed I have seen some events where there are 100s per second for extended periods.

"Bill Glidden" <billyg1943@xxxxxxxxxxxx> wrote in message news:e8uHEpElHHA.680@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Thanks again, Svyatoslav.

I posted here because it looked like a security issue to me. I will have a look at snort.

Cheers,
Bill

"S. Pidgorny <MVP>" <slavickp@xxxxxxxxxx> wrote in message news:%230E7hfElHHA.4960@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

I would analyse traffic coming through the Internet to see if there is a correlation b/wen connection attempts and the failed logon attempt. I would also consider implementing a network intrusion detection system (like Snort –www.snort.org – it's free and runs on Windows) for such monitoring.

Also please post the question to SBS newsgroups.

--
Svyatoslav Pidgorny, MS MVP – Security, MCSE
–= F1 is the key =–

* <http://sl.mvps.org> * <http://msmvps.com/blogs/sp> *

"Bill Glidden" <billyg1943@xxxxxxxxxxxx> wrote in message

Re: Masses of 529 Errors!

news:e8c5btDIHHA.4592@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Thanks, Svyatoslav.

I am running SBS 2K3 with ISA 2004 behind a firewall/router:

Internet -- router -- SBS/ISA -- local LAN

What can I do about this, please?

Cheers,

Bill

"S. Pidgorny <MVP>" <slavickp@xxxxxxxx> wrote in message

news:O9KKrcDIHHA.596@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Splash in a botnets activity?

The access is denied, which is a good thing.
Filling up the logs is something to worry about.

--

Svyatoslav Pidgorny, MS MVP – Security,
MCSE

-- F1 is the key --

* <http://sl.mvps.org> *

<http://msmvps.com/blogs/sp> *

"Bill Glidden" <billyg1943@xxxxxxxx>
wrote in message

news:%23%23a1PiCIHHA.4628@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

I have often seen these errors in the security log at the rate of up to hundreds in a 24 hour period, but in the last 24 hours I had 107,710 of them. Is this something I should be worrying about? Obviously the fact that I know about it means that who/whatever is doing this is unsuccessful. Below is pasted one of the events:

Event Type: Failure Audit

Re: Masses of 529 Errors!

Event Source: Security
Event Category:
Logon/Logoff
Event ID: 529
Date: 11/05/2007
Time: 10:20:37 PM
User: NT
AUTHORITY\SYSTEM
Computer: <my sbs server>
Description:
Logon Failure:
Reason: Unknown user
name or bad password
User Name: anonymous
Domain:
Logon Type: 3
Logon Process: Advapi
Authentication Package:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Workstation Name: <my sbs
server>
User Name: <my sbs
server>
Caller Domain: <my
domain>
Caller Logon ID:
(0x0,0x3E7)
Caller Process ID: 1216
Transited Services: –
Source Network Address: –
Source Port: –

Advice most welcome,
please.

Bill

Re: Masses of 529 Errors!