

# Re: Failed login attempts showing in the security log

---

*Source:*

<http://www.tech-archive.net/Archive/BackOffice/microsoft.public.backoffice.smallbiz/2007-04/msg00049.html>

---

- *From:* "Bagins" <[dejan@xxxxxxxxxx](mailto:dejan@xxxxxxxxxx)>
  - *Date:* Tue, 17 Apr 2007 01:14:12 +0200
- 

Hi Daniel.

You are right, this is some kind of a automated tool attacking (password guessing) SMTP service. You can find more if you review your SMTP logs. IMHO, stopping your SMTP service will not stop attacks, because they are automated and as I can see by now – not very agresiv (only few user names/password combinations tried). If you see only a few IP addresses of attackers in your SMTP logs, try blocking them on the firewall.

names  
retries

info  
8

anonymous  
8

webmaster  
8

admin  
8

root  
8

test  
8

master  
8

web  
5

www  
4

Re: Failed login attempts showing in the security log

DÇ (i guess that this is some chinese word)

3

administrator

4

backup

4

server

4

data

4

Time frame: 13 minutes

Network logon/ IIS/ SMTP

Address (in my case): 142.145.49.58.broad.wh.hb.dynamic.163data.com.cn

I will try to capture some packets for analysis if the attack reoccures so I will have more info on that issue.

Best regards,

Bagins

"Daniel Woodhouse" <daniel@xxxxxxxxxxxxxxxxxxxxxxxx> wrote in message [news:77D5EECC-A00F-4638-B926-B408C3716532@xxxxxxxxxxxxxxxxxxxx](mailto:news:77D5EECC-A00F-4638-B926-B408C3716532@xxxxxxxxxxxxxxxxxxxx)

Hi there

I have a customer who is running SBS2003 Premium. The server is fully patched, latest version of symantec enterprise edition which is all up to date and they have strong password policies enabled. Once or twice a day they are getting numerous login failiures showing in the security log that shows users like "root", "admin", "webmaster" and more trying to login in. I am thinking there is some sort of robot trying to get in using a dictionary attack of some sort. There maybe 20 login attempts in the space of a minute or two. Here is some of the event log messages....

Logon Failure:

Reason: Unknown user name or bad password

User Name: admin

Domain:

Logon Type: 3

Logon Process: Advapi

Re: Failed login attempts showing in the security log

Re: Failed login attempts showing in the security log

Authentication Package: MICROSOFT\_AUTHENTICATION\_PACKAGE\_V1\_0  
Workstation Name: SERVER  
Caller User Name: SERVER\$\br/>Caller Domain: OURDOMAIN  
Caller Logon ID: (0x0,0x3E7)  
Caller Process ID: 908  
Transited Services: –  
Source Network Address: –  
Source Port: –

For more information, see Help and Support Center at

Logon Failure:  
Reason: Unknown user name or bad password  
User Name: test  
Domain:  
Logon Type: 3  
Logon Process: Advapi  
Authentication Package: MICROSOFT\_AUTHENTICATION\_PACKAGE\_V1\_0  
Workstation Name: SERVER  
Caller User Name: SERVER\$\br/>Caller Domain: OURDOMAIN  
Caller Logon ID: (0x0,0x3E7)  
Caller Process ID: 908  
Transited Services: –  
Source Network Address: –  
Source Port: –

For more information, see Help and Support Center at

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: SERVER  
Caller User Name: SERVER\$\br/>Caller Domain: OURDOMAIN  
Caller Logon ID: (0x0,0x3E7)  
Caller Process ID: 908  
Transited Services: –  
Source Network Address: –  
Source Port: –

For more information, see Help and Support Center at

I have tracked process ID 908 as inetinfo.exe. My theory is that someone is trying to log into one of the open ports which will have to be port 25. I have closed the RWW ports but the attempts are still happening. I am

Re: Failed login attempts showing in the security log

closing port 25 this weekend to see if they go away.

I am a bit worried how the workstation name is SERVER which is the name of the actual server.

Any help or guidance on this matter would be much appreciated.

Thanks in advance

Daniel Woodhouse