

Re: Another security question/issue.

## Re: Another security question/issue.

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2008-03/msg03007.html>

---

- *From:* [robbie.desutter@xxxxxxxx](mailto:robbie.desutter@xxxxxxxx)
  - *Date:* Thu, 27 Mar 2008 00:26:11 -0700 (PDT)
- 

As of yesterday, I'm also getting security warnings on my SBS2003 server about failed logins of the "user" mdaemon:

Source : Security  
Event : ID 529  
Last Occurrence : 3/27/2008 2:52 AM  
Total Occurrences : 5  
Logon Failure:  
Reason: Unknown user name or bad password  
User Name: MDaemon  
Domain:  
Logon Type: 3  
Logon Process: Advapi  
Authentication Package: MICROSOFT\_AUTHENTICATION\_PACKAGE\_V1\_0  
Workstation Name: servername  
Caller User Name: servername\$\br/>Caller Domain: domainname  
Caller Logon ID: (0x0,0x3E7)  
Caller Process ID: 2552  
Transited Services: -  
Source Network Address: -  
Source Port: -

I don't have Mdaemon email service on the server, so this is a hack attempt??? or????

Any feedback is welcome.

Btw: why is Source Network Address not mentioned?

Kind regards,  
rds

On 27 mrt, 03:29, "kj [SBS MVP]" <KevinJ....@xxxxxxxxxxxxxxxxxxxx>  
wrote:

Please post the complete events including event id and accounts numbers.  
There should really be nothing in there that would be an issue for public

Re: Another security question/issue.

Re: Another security question/issue.

posting.

For the Mdaemon, that would be typical of a third party email product. If it exists on your SBS server then it should be by intent, not by accident.

The first event is missing the username and logon process appears 'munged'..

In example 2, advapi is IIS if that helps.

sbsstarter wrote:

Here are posts of the failed login attempts:

22 occurrences  
Logon Failure:  
Reason: Account currently disabled  
User Name:  
Domain:  
Logon Type: 3  
Logon Process: Authz  
Authentication Package: Kerberos  
Workstation Name: MYSERVER-SBS  
Caller User Name: MYSERVER-SBS\$  
Caller Domain: MYSERVER  
Caller Logon ID: (0x0,0x3E7)  
Caller Process ID: 876  
Transited Services: -  
Source Network Address: -  
Source Port: -

--and--

Logon Failure:  
Reason: Unknown user name or bad password  
User Name: MDaemon  
Domain:  
Logon Type: 3  
Logon Process: Advapi  
Authentication Package:  
MICROSOFT\_AUTHENTICATION\_PACKAGE\_V1\_0  
Workstation Name: MYSERVER-SBS

Re: Another security question/issue.

Re: Another security question/issue.

Caller User Name: MYSERVER-SBS\$  
Caller Domain: MYSERVER  
Caller Logon ID: (0x0,0x3E7)  
Caller Process ID: 1492  
Transited Services: -  
Source Network Address: -  
Source Port: -

and, no I have not changed the administrator account password, but I have changed the password of the active administrative user account.

"kj [SBS MVP]" wrote:

sbsstarter wrote:

Ok; I get daily hits to the disabled admin account. Event log tells me they are denied access. First, I was told the reason the attempts are higher than my lockout policy is because policies don't apply to admin account - correct? How can I find out who is making these attempts and how I can deny that individual access? The most annoying instance happens very close to the same time every morning at about 4:00 a.m. The logs don't give an address of the user trying the attempted logins. What are my options?

Post an example of your failed logon attempt.

Is your administrator account 'disabled' by choice, or are you saying it's disabled by lockout policy?

While this may be an external cause, it may also be an internal

Re: Another security question/issue.

driven event. Did you change the administrator password lately?

Policy applies to all accounts, but the administrator has some protections against denying the true administrator (person) from gaining access to the server.

Second, if the account is obviously disabled, why would a hacker keep attempting to access it? It's not going to work...right?

Third, I've been noticing fail authentication attempts with the user name MDAemon. Is that an actual service that I need to deal with, or is it an attempt at unauthorized access?

Post one of these too.

Finally....if I've closed all ports except 25 TO the SBS box from my external firewall appliance, why am I still seeing failed authentication attempts on a daily basis? Is it possible to attempt a login through port 25 which is designated for exchange?

--  
/kj

--  
/kj- Tekst uit oorspronkelijk bericht niet weergeven -

- Tekst uit oorspronkelijk bericht weergeven -

Re: Another security question/issue.

Re: Another security question/issue.