

Exchange 2003 (SBS2K3) Messages Pending Submission Queue Filling Rapidly

Source:

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange.admin/2004-05/4285.html>

From: Schyler (*schyler_jones_at_hotmail.com*)

Date: 05/27/04

Date: 27 May 2004 12:43:17 -0700

I'm working on a Windows Small Business Server 2003 that was apparently the victim of an "authenticated relay" attack. The Guest account had been enabled and was apparently this way for several days.

As one can image the problem was discovered when the server started to slow to a crawl and disk activity was hot and heavy. In Exchange System Manager (ESM) under queues, thousands of messages in scores of queues were found). Looking at the messages in these queues it was pretty obvious that much of the mail was NDRs so the first thing after disabling Guest and shutting off the open router ports to this server (including port 25), was to disable NDRs.

I then attempted to clean the queues by stopping the SMTP service, renamed the Program Files\Exchsrvr\Mailroot\vs1\BadMail and Program Files\Exchsrvr\Mailroot\vs1\Queue folders and restarted SMTP service. The queues started as being empty but within seconds began filling up again.

I actually tried the above steps several times and also froze all the queues, which enabled me to determine that it was the Messages Pending Submission (MPS) queue that was feeding of all them. Even with the queues frozen, the MPS queue keeps going and going like the Duracel Bunny (or is it Eveready?) Where the heck are those messages coming from?

I next followed the procedures outlined in <http://support.microsoft.com/?id=324958#3> to clean out the queues (and confirm the server was not an open relay), but the number of messages never seemed to stabilize, though the suggestion to make the SBS SMTP connector forward all messages to [99.99.99.99] was useful in that it forced messages into one queue vs. one for each domain the server was queuing mail for.

I also read an interesting article at <http://www.vamsoft.com/orf/authattack.asp>, which prompted me to remove the relay settings under the SMTP Virtual Server properties – I

removed both the Server's LAN IP and it's loopback address, and cleared the "Allow authenticated computers..." option. Still the MPS queue continues to grow. There are no 1708 messages in the Security Log so I have no idea where these messages are coming from.

Does anyone know how messages get into the MPS queue? Are they stored on disk somewhere? They are definitely not in Program Files\Exchsrvr\Mailroot\vs1\Queue as one might think. The server is also not running any virus protection or other 3rd party products related to Exchange. This is SBS2K3 Standard, installed in 5/7/04. The server tested negative for an open relay and all other user accounts (a whopping 5) have strong passwords.

sj