

## Re: Question about the "Microsoft Exchange Server Best Practices Analyzer Tool" and open relaying

**Source:**

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2004-10/0431.html>

---

**From:** Tony (*noreply\_at\_noemail.net*)

**Date:** 10/01/04

Date: Fri, 1 Oct 2004 08:56:57 -0500

I am using a smarthost to forward outgoing mail. One of my concerns is the possibility if a client were to pick up some kind of a trojan ( I am running AV software on all clients) and use the exchange server to relay spam. I already have port 25 blocked for clients on the ISA server so the only conduit would be if a trojan used the default gateway (the exchange server) to route mail bypassing the Outlook client. I may be being a bit overly paranoid here, and thought I had everthing set up correctly until MS's Exchange testing tool put it out as a big flag that it is set up as a open relay.

Tony

"Lanwench [MVP - Exchange]"

<lanwench@heybuddy.donotsendme.unsolicitedmail.atyahoo.com> wrote in message news:eV7oOtzpEHA.324@TK2MSFTNGP11.phx.gbl...

> *Tony wrote:*

>> *The guest account is disabled. I did a telnet in to the mail server  
>> from my workstation on the lan side and was able to relay a message  
>> from a forged email address to another email address in another  
>> domain. I am not overly concerned with somebody externally using the  
>> server as an open mail relay because I have another mail relay server  
>> that scans for virus and spam that port 25 from the internet goes to  
>> and this server hands off the mail to the exchange server. But I am  
>> concerned that the MS tool lists it as open and I can just telnet in  
>> from the lan side and send out. I am a bit of a mail server newbie  
>> and just want to make sure I am not sitting on a potential problem  
>> here. It is my understanding that Outlook talks to Exchange with RPC  
>> and I should not need 25 open to any of the lan clients at all.*

>>

>> *Tony*

>

> *On a client on the LAN, set up a test OE account, with a POP account you*

> *can*

icrosoft.public.windows.server.sbs: Re: Question about the "Microsoft Exchange Server Best Practices Analyzer Tool" and open relay

> *access from somewhere (even if it isn't your Exchange mailbox – best not  
> to  
> use that if you ask me) and specify your Exchange server's local IP or  
> name  
> as the SMTP server, no authentication. Try to send a message to a  
> non-domain  
> address and see what happens. It shouldn't work; you should get a bounce  
> message.*  
>  
> *I'm presuming you're not forwarding all mail to a smarthost for outbound  
> mail, right? But are resolving via DNS and sending directly?*  
>  
> *If your Exchange server isn't exposed directly to the Internet, you're  
> right, nobody on the Internet can even get to it no matter what your relay  
> settings are.*  
>>  
>>  
>> *"Douglas Boyd [MSFT]" <dboyd@online.microsoft.com> wrote in message  
>> news:NHnFjdypEHA.404@cpmsftngxa06.phx.gbl...*  
>>> *Tony*  
>>>  
>>> *Is the guest account enable on the server? Have you tried telnet to  
>>> port 25  
>>> and tried to drop mail for a bogus domain to verify the test ?*  
>>>  
>>> *Doug Boyd  
>>> dboyd@online.Microsoft.com*  
>>>  
>>> *This post is provided "AS IS" with no warranties and confers no  
>>> rights*  
>  
>  
>

Re: Question about the "Microsoft Exchange Server Best Practices Analyzer Tool" and open relay