

RE: Spoofed email?

Source:

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange2000.general/2005-03/0183.html>

From: Mike (*Mike_at_discussions.microsoft.com*)

Date: 03/08/05

Date: Tue, 8 Mar 2005 09:27:01 -0800

Aaron,

Yes, it makes perfect sense. I found the setting and ticked the checkbox. Does Exchange automatically reject those emails that don't "match up?" I ask because I could not find any other settings to go along with the checkbox.

Also, I have Sybari Antigen on the Exchange box that also does Reverse DNS, which I have enabled.

Thanks again for taking the time.

Cheers,

Mike

"Aaron Tiainen" wrote:

> *Mike,*
>
> *There is an option in the SMTP Server to Perform a reverse DNS lookup on*
> *incoming messages, under the Advanced button on the Delivery Tab.*
> *Alternatively, get yourself something like Mail Marshal which can do a whole*
> *lot more.*
>
> *By reciever i mean who the mail was sent to... lets say an email from*
> *abc@yourdomain.com was sent to def@otherdomain.com. Lets say the email*
> *originated from the ip address of 10.1.1.1. The reciever at otherdomain.com*
> *will recieve the email but can deliver it as user def doesn't exist. It then*
> *says, lets send a message back to abc@yourdomain.com and say it couldn't be*
> *delivered, even though it didn't originate from you. What the reverse look*
> *up will do, is say right, we got an email from yourdomain.com. Then it will*
> *say whats the ip address for the mail server for yourdomain.com which might*
> *be 20.1.1.1. It will then say, hold on, the ip address in the email, doesn't*
> *match the correct ip address of the senders domain. I can't remember what*
> *exchange does at this point, but i'm using mail marshal which i've got setup*
> *to say... I don't want that email, and doesn't accept it.*
>

> *Hope this makes sense.*
>
> *"Mike" wrote:*
>
>> *Aaron,*
>>
>> *Thanks for taking the time. When you say the "receiver" do you mean our*
>> *Exchange box? How do I go about doing a "reverse lookup?"*
>>
>> *Thanks,*
>>
>> *Mike*
>>
>>
>> *"Aaron Tiainen" wrote:*
>>
>>> *Mike,*
>>>
>>> *My two cents. The reason why you got this email is that somebody externally*
>>> *to the organisation can send email as if it came from abc@yourdomain.com. If*
>>> *the reciever recieves the email and it can't be delivered, then it will send*
>>> *a reply back to your email address because it thinks you sent the email.*
>>>
>>> *What the reciever should be doing is performing a reverse lookup on the*
>>> *incomming mail. What that does is verify the domain name against the ip*
>>> *address it was sent from. This does stop a large amount of crap.*
>>>
>>> *Hope this helps. And, if anybody thinks i am wrong.. .please tell me :)*
>>>
>>> *Thanks*
>>>
>>> *Aaron*
>>>
>>> *"Mike" wrote:*
>>>
>>>> *Greetings,*
>>>>
>>>> *I have a user that occasionally will get a message from Exchange saying:*
>>>>
>>>>
>>>>
>>>> *Your message did not reach some or all of the intended recipients.*
>>>>
>>>>
>>>>
>>>> *Subject:*
>>>>
>>>>
>>>>
>>>> *The following recipient(s) could not be reached:*
>>>>

>>>>
>>>>
>>>> <email address> on 3/7/2005 1:16 AM
>>>>
>>>> *The e-mail account does not exist at the organization this
>>>> message was sent to. Check the e-mail address, or contact the recipient
>>>> directly to find out the correct address.*
>>>>
>>>> <our Exchange box#5.1.1>
>>>>
>>>>
>>>>
>>>> <email address> on 3/7/2005 1:16 AM
>>>>
>>>> *The e-mail account does not exist at the organization this
>>>> message was sent to. Check the e-mail address, or contact the recipient
>>>> directly to find out the correct address.*
>>>>
>>>> <our Exchange box#5.1.1>
>>>>
>>>> *The list will be a bunch of email addresses that do not exist in our domain.
>>>> The thing is, he never sent the email in the first place. Is this a case of
>>>> spoofing?*
>>>>
>>>> *We are running Exchange 2000 SP3 on a WIN2K server, with Outlook 2003. We
>>>> also have Sybari Antigen with Spam Filtering running on the Exchange box.*
>>>>
>>>> *Any help is appreciated. Thanks in advance.*
>>>>
>>>> *Mike*
>>>>
>>>>
>>>>