Subject: Block Spoofed Emails
Posted by chontay on Wed, 17 Dec 2008 09:52:55 GMT
View Forum Message <> Reply to Message

Hi All

Ok here is my setup.

Internal Exchange Server. NST 3.0 on it as a trial. Local users send/recieve via this.

Also have an external SMTP server hosted. This has a full 3rd Party Mail Server on it with duplicates of internal staff mailboxes and addresses. This has NST 3.0 purchased and running on it.

If internal server goes offline, all staff have a second POP account in Outlook which automtically checks mail on the external box and mail continues as normal.

Now. On a Second internal server I have a POP3 collector application. This collects mail from the hosted box and squirts it into internal Exchange all day long. So if anything on the remote server is missed by clients it is collected automatically at all times.

We are getting loads of spoofed emails using internal staff addresses. How can I block these without blocking legitimate mail which might be sent via a pop account by one of the internal staff?

Basically is there anyway to tell NST to not accept mail addressed domains it hosts?

Thanks

Rob

Subject: Re: Block Spoofed Emails
Posted by James Wilkinson on Thu, 18 Dec 2008 17:48:32 GMT
View Forum Message <> Reply to Message

OK: I'm going to assume that your business domain name is example.com. Convert as appropriate.

It sounds as though you've got @example.com addresses whitelisted. Don't do that.

Next, I don't understand why e-mail from internal users goes through No Spam Today.

I presume that the POP3 collector sends the e-mails straight to Exchange, not through No Spam Today. (If not, why not?)

Do your users ever send e-mail through the POP3 server, and some of it will be to @example.com users (so it goes to NST on the internal server)? If so, put both servers' IP addresses in trusted_networks (in local.cf in sa\ruleset); for example:

trusted_networks 192.168.1.253 10.10.1.253
and give a negative score on ALL_TRUSTED
score ALL_TRUSTED -5
(again, all these rules go in local.cf). See http://wiki.apache.org/spamassassin/TrustPath for more details.

Do your users ever send e-mail using @example.com addresses, but using third-party mail servers (for example, Googlemail?) If so, you may want to use something like
WHITELIST_FROM_RCVD joe@example.com google.com
Or you might want to turn on authenticated (important!) relaying through your external server, and get them to use that. (Hint: use port 587 for this: it avoids some firewall blocks).

You might want to use SpamAssassin to treat anything else apparently from example.com with suspicion: something like
header LOCAL_FROM_EXAMPLE From:addr =~ /\@example.com\$/i
score LOCAL_FROM_EXAMPLE 1.8

You don't really want to give a score high enough that all email apparently from @example.com addresses will get blocked, since some of it is legitimate. Just don't whitelist it, and allow the other SpamAssassin rules to do their job.

Don't forget to run sa-lint.bat from a command prompt after making any changes. If you see nothing between
C:\Program Files\No Spam Today!>sa\spamassassin -x --siteconfigpath="sa\ruleset" --lint
and
C:\Program Files\No Spam Today!>pause
Press any key to continue . . .
then that's good. Otherwise there's a problem.

Hope this helps.