

Mail Server problem / query

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-04/0057.html>

From: Marc Davison (m_davison_at_talk21.com)

Date: 04/13/05

Date: Wed, 13 Apr 2005 22:44:55 +0100 (BST)

To: pen-test@securityfocus.com

Hi all, I hope you can help with this. I have been testing a server for open-relay and found that I could connect from an external machine and send mails using a MAIL FROM (the local domain) and a RCPT TO (the local domain) – now this may seem fine as internal users will need to send mail to other internal users but my query is whether there are mail servers which can be configured to recognise that the connection was an external address and therefore that the MAIL FROM address was invalid. eg I can send a mail from the CEO of the company to his own secretary asking her to copy his hotmail address on all future mails and to the secretary, this mail seems perfectly valid yet me (prospective attacker) outside the company may now receive loads of sensitive mails (assuming the secretary is the type who doesn't like to query things and ask questions) – thanks in advance.

Send instant messages to your online friends <http://uk.messenger.yahoo.com>