

## Re: Filtering email headers generated from internal network (Sensible?)

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-05/0015.html>

---

**From:** Joachim Schipper ([j.schipper\\_at\\_math.uu.nl](mailto:j.schipper_at_math.uu.nl))

**Date:** 05/10/05

Date: Tue, 10 May 2005 10:19:51 +0200

To: pen-test@securityfocus.com

On Mon, May 09, 2005 at 11:23:16AM -0700, anyluser wrote:

- >
- > *IMO there's a balance between sec through obscurity*
- > *(STO) and flat out information leakage. Just as most*
- > *things in security, this as much a balance as any*
- > *other.*
- >
- > *Generally speaking sec through obscurity implies (to*
- > *me) that you're relying on the obfuscation for more*
- > *then it's really worth. If you think it'll keep you*
- > *safe, you're using STO. If you're realistic about*
- > *your expectations then do a CBA (cost/benefit*
- > *analysis) and make your decision as to whether or not*
- > *it's worthwhile.*
- >
- > *IMO if there's a mail routing infrastructure behind*
- > *your borders then you should obscure it to the*
- > *outside, if you have the time. That'*
- >
- > *Granted it wont make you secure but it'll least keep*
- > *your infrastructure details relatively private, which*
- > *being the paranoid lot we probably are is a good*
- > *thing. :)*

You'll need to analyze what you want to cut out, though. While I fully agree that cutting out Received: headers may be somewhat useful [1], cutting out X-Virus-Scanned headers seems sensible [2], cutting out User-Agent isn't all that much good. In the overwhelming number of cases, people use Outlook, and Outlook's idea of HTML is pretty noticeably different from anything not made by Microsoft. And it's the biggest one, so guessing people use Outlook is usually a safe bet.

Other mailers are probably recognizable by, at least, their HTML implementation as well. However, since Outlook is the most often exploited, hiding Outlook is most useful.

SecurityFocus Penetration: Re: Filtering email headers generated from internal network (Sensible?)

There are a couple of notes I'd like to make, though.

[1] If you end up with a broken Received: path, this will break a lot of stuff, and might cause your e-mail to be rejected as spoofed. Check the message-ID; the first receiving mail server may well be encoded in there. Ripping out the message-ID is not advised, as it makes tracking mail much more difficult.

[2] Though I do not see much benefit in scanning outgoing mail, then telling no-one that you did it. Not that any sane person wouldn't use his own scanner as well...

Looks to me like you have to be very, very careful here, or stuff will break. But it might work.

Joachim

- 
- application/pgp-signature attachment: stored