

Re: e-mail address mining tool?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-11/0100.html>

From: Tomasz Nidecki (*tonid_at_hakin9.org*)

Date: 11/07/05

Date: Mon, 7 Nov 2005 09:14:30 +0100

To: pen-test@securityfocus.com

-----BEGIN PGP SIGNED MESSAGE-----

Hash: MD5

Sunday, November 6, 2005, 6:36:48 PM, Eyal wrote:

- > *I'm not aware of any tool which can test emails against an address file.*
- > *The most efficient approach to achieve this functionality is to write a*
- > *simple script which sends the SMTP VRFY command for each entry in an address*
- > *file.*

- > *Note that some mail servers do not support this command in order to thwart*
- > *spammers.*

Hi, everyone.

Well, to be exact, almost no servers support this command nowadays. qmail definitely doesn't. AFAIK, Postfix doesn't either, at least it didn't the last time I checked. Neither did Exim. Only Sendmail, in its standard config, responds to the VRFY command. I don't know about commercial, Windows mailservers, but I found the VRFY command supported in very few cases. Therefore I would not base anything on its output.

Also, testing the existence of the user is rarely done on the level of mail envelope. Therefore, you cannot expect the mailserver to either reply right after sending the RCPT TO command that the user doesn't exist or reply in such way after DATA is sent. The only thing you can expect, is that if the user address is invalid, you will receive a mailer daemon reply to the MAIL FROM address.

But... This is also not certain. Some mailservers use a default account for a given domain, eg. qmail, which I specialise in. If such a setup is made, all mail to inexistant users in a given domain is directed to a chosen existant account. Therefore you will not receive any answer from the mailserver, if a bad e-mail address is given in RCPT TO, since mail will be delivered to an existing user.

SecurityFocus Penetration: Re: e-mail address mining tool?

Therefore, there is no tool and there will be no such tool. Which is good, because if there was, spammers would have a much easier life making databases of existing users, so they can sell them later on.

Cheers,

-- --

Tomasz Nidecki, Sekr. Redakcji / Managing Editor
hakin9 magazine <http://www.hakin9.org>
mailto:tonid@hakin9.org jid:tonid@tonid.net

Do you know what "hacker" means?
<http://www.catb.org/~esr/faqs/hacker-howto.html>

Czy wiesz, co znaczy slowo "haker"?
<http://www.jtz.org.pl/Inne/hacker-howto-pl.html>

-----BEGIN PGP SIGNATURE-----

Version: 2.6

iQCVAwUAQ28M6ER7PdagQ735AQE90gP9EXVRDGUNNQdWgSCHDeYItm7AuZzj0JYF
ExOhwTC/863ATjCC18b3lGD+qCKvC3ud4q213HqFOUkEGEraWboxVziQluwbnWqz
zjdlxfdj0JHPEP5aqTwS2JE34CvCXqMoN+tVVALD/RvcqqCYQr8jzNn+Q9uzePc2
x2FsceCmFSs=
=m5Ng

-----END PGP SIGNATURE-----

Audit your website security with Acunetix Web Vulnerability Scanner:

Hackers are concentrating their efforts on attacking applications on your website. Up to 75% of cyber attacks are launched on shopping carts, forms, login pages, dynamic content etc. Firewalls, SSL and locked-down servers are futile against web application hacking. Check your website for vulnerabilities to SQL injection, Cross site scripting and other web attacks before hackers do! Download Trial at:

http://www.securityfocus.com/sponsor/pen-test_050831
