

Re: Discovering users by RCPT TO

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-01/0088.html>

From: Kiril Todorov (*voland_at_shadowblade.net*)

Date: 01/13/05

To: pen-test@securityfocus.com

Date: Thu, 13 Jan 2005 14:04:57 +0200

Andres Molinetti wrote:

> I'm currently over a pen-test and I have found that their SMTP Server
> (SendMail) does not have VRFY or EXPN methods available, which was the
> most probably thing to happen taking into account the server has been
> through some hardening before.

>

> Testing for Open Relay, I realized that the server answers different to
> existing users and non-existing users, when trying to deliver mails
> using RCPT TO:

>

> E.g:

>

> rcpt to: asdfasdf@domain

> 550 5.1.1 asdfasdf@domain... User unknown

> rcpt to: bin@domain

> 250 2.1.5 bin@domain... Recipient ok

> rcpt to: nobody@domain

> 250 2.1.5 nobody@domain... Recipient ok

> rcpt to: oper@domain

> 550 5.1.1 oper@domain... User unknown

> rcpt to: root@domain

> 250 2.1.5 root@domain... Recipient ok

>

> Is this ok or is it information disclosure? Is there any way to fix it?

> It is Sendmail...

>

> Thanks in advance,

>

> Andres Molinetti

> CISSP

That's a common practice.

The main reason is the tons of windows zombie machines, used for spamming at random names @ domain name.

All mails are send from fake addresses, so after 2-3 waves of such spamming the mail server's queue gets approximately 30-40K mails.

The server is busy sending out bounces to nonexistant addresses.. well

SecurityFocus Penetration: Re: Discovering users by RCPT TO

you get the picture.