

Re: Password cracking / recovery Lotus Notes R6

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-11/0274.html>

From: Joachim Schipper (j.schipper_at_math.uu.nl)

Date: 11/28/05

Date: Mon, 28 Nov 2005 23:05:21 +0100

To: pen-test@securityfocus.com

On Mon, Nov 28, 2005 at 09:20:47AM -0500, Francois Labreque wrote:

> Joachim Schipper <j.schipper@math.uu.nl> a écrit sur 2005-11-25 17:37:16 :

>

>> On Fri, Nov 25, 2005 at 08:38:09AM -0500, Richard Zaluski wrote:

>>> Hello,

>>>

>>> Currently I am working with a client to gain access to a Lotus Notes

> R6

>>> (running on NT) database. We have full access to the box and need to

>>> penetrate the passwords on the data bases.

>>>

>>> Does anyone have tools or techniques they can suggest to achieve this
> goal?

>>>

>>> Thanks....

>>

>> Can't you just sniff them off the wire?

>>

>

> Lotus Notes traffic and passwords and encrypted on the wire.

Yes, I figured that – but, while I know basically nothing about Lotus Notes, every encrypted server I knows of stores the encryption key on the server itself, and very few admins will encrypt or password-protect the key.

I don't know what Lotus Notes uses, but if it's plain SSL and you have the server key, it should be possible to find some tool that will do the decrypting for you (if there's no such tool for Windows, dump the packets and read them in on a *nix system).

Cracking the passwords may help in some cases, but this sound like an attack that is at least theoretically feasible to me. Of course, practical feasibility depends on the OP being able to get hold of a decrypting program for whatever Notes uses.

Joachim

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
