

RE: MS RAS (pptp + MSCHAPv1)

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-01/0176.html>

From: Todd Towles (toddtowles_at_brookshires.com)

Date: 01/28/05

Date: Fri, 28 Jan 2005 08:07:24 -0600

To: "Maria Da Re" <pentestml@yahoo.it>, <pen-test@securityfocus.com>

Don't forget about this – <http://www.securiteam.com/tools/6F00X000AU.html>

Might come in handy also. Beyond your normal sniffer, I might search for other numbers that may lead to hidden backdoor devices.

> -----Original Message-----

> **From:** Maria Da Re [<mailto:pentestml@yahoo.it>]

> **Sent:** Thursday, January 27, 2005 3:41 PM

> **To:** pen-test@securityfocus.com

> **Subject:** MS RAS (pptp + MSCHAPv1)

>

> **Hi!**

>

> *I will execute a penetration test on Windows 2000 systems*

> *responding in dial-up on different telephone numbers with*

> *pptp protocol handled by Microsoft RAS (Routing and Remote*

> *Access) server.*

>

> *I think to proceed with an analysis composed by these*

> *steps:*

>

> *1) Fingerprint with ppp, trying to use&verify the many*

> *authentication protocol available such as CHAP, MSCHAPv1,*

> *MSCHAPv2; very probably the protocol is MS-CHAPv1.*

>

> *2) Trying to take advantage of this vulnerability:*

> *www.securityfocus.com/bid/5807. Any suggestion? There are*

> *other vulnerability?*

>

> *3) Trying to bruteforcing the passwords with pptp-bruter.*

> *There are other good tools for doing this?*

>

> *Because i can't access to the shared telephone line, i can't*

> *try man in the middle attacks (decrypting credentials or*

> *implement a fake server to steal*

> *credentials)*

>

SecurityFocus Penetration: RE: MS RAS (pptp + MSCHAPv1)

- > *Have you some suggestions? There are other types of attacks*
- > *to try or tools to use?*
- >
- > *Thanks for sharing your experience*
- >
- > --
- > *M. Da Re*
- >
- >
- >
- >
- > _____
- > *Nuovo Yahoo! Messenger: E' molto più divertente: Audibles,*
- > *Avatar, Webcam, Giochi, Rubrica... Scaricalo ora!*
- > *<http://it.messenger.yahoo.it>*
- >