

## Re: Cached NT/W2k passwords

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2004-05/0115.html>

---

**From:** Kurt Grutzmacher (*grutz\_at\_jingojango.net*)

**Date:** 05/22/04

Date: Fri, 21 May 2004 20:24:05 -0700

To: John Madden <chiwawa999@yahoo.com>, pen-test@securityfocus.com

John Madden wrote:

>Hi All,

>

>Has anyone been able to decrypt the hash password from  
>the cached login on NT or W2K ?

>

>We're is it located ? In the registry ? If so what's  
>the key....

>

>I've been looking around the only thing I can find is  
>how to disable this feature :(

>

>

For WindowsXP and some 2K (I think SP4 fixed this particular issue, memory dump the lsass process and search for the hex string "76 78 01 26". A little ways further down and voila, cleartext password for currently logged in user. It's in unicode format, btw.

I think the latest rumor is that XP SP2 is going to clear this issue up so if anyone can find the hashes in the registry (ala lsadump for stored services passwords) then we'll be back in business after everyone starts patching.

Need a tool to dump process memory? pmdump of course.

<http://ntsecurity.nu/toolbox/pmdump/>

Arne also has Pstoreview which may help you a little.

<http://www.ntsecurity.nu/toolbox/pstoreview/>