

Re: WHERE ARE NT4 OLD PASSWORDS STORED – summary of replies

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-07/0033.html>

From: Russ (*Russ.Cooper_at_RC.ON.CA*)

Date: 07/10/03

Date: Thu, 10 Jul 2003 10:55:39 -0400

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

So the question was, where are the NT 4.0 old passwords stored so password history will work? I've compiled 3 replies together;

1. Tom Geairn pointed out that Bindview had a very good paper that included information about the subject. That paper was published on NTBugtraq in Dec. 1999;

<http://www.ntbugtraq.com/default.asp?pid=36&sid=1&A2=ind9912&L=ntbugtraq&F=P&S=&P=4507>

A prettier version can be seen on Bindview's site here;

http://razor.bindview.com/publish/advisories/adv_WinNT_syskey.html

2. 314ns at free.fr wrote a detailed explanation of the key structure;

```
> Where does NT4 keep the users old passwords
> when the password history option is enabled ?
What an excellent question Steve ! I'm really surprised nobody tried (and published !) the trick
> Also as I do not believe they are in the SAM,
> I would also want to closely
> audit the location where they are kept.
You're guessing wrong : password history IS in the SAM database !
> Any help or avenues of investigation would
> be gratefully received. Else I will have to
> image the whole drive and start checking all
> files for changes.
Please don't !
Well....let's try to understand the structure of the entity that stores the passwords in a NT box
The password hashes in Windows NT are stored in the registry under the SAM database. Precisely, h
Under this key, you will find subkeys that represent RIDs of the users en hex (000001F4 for the B
Now, let's hexadump a "V" Value :
0x0C  Username offset
0x10  Username lenght
0x18  Full Username offset
0x1C  Full Username lenght
0x24  Comment offset
0x28  Commen lenght
0x48  Homedir offset
0x4C  Homedir lenght
0x9C  Password Hashes offset
0xC4  Number of hashes in the history (new undocumented point !!! Warning : the number is revers
```

NT-Bugtraq: Re: WHERE ARE NT4 OLD PASSWORDS STORED – summary of replies

To retrieve the REAL position of an entity, just add 0xCC to the corresponding offset (example :
At the position of the current password hashes, you will find : 16 bytes for the current lanman h
Please note that hashes are encrypted using a DES-EBC algorithm, the DES key is derivated from th
So, where are the old password hashes now ?

Very simple, they are just stored AFTER theses current hashes, but in a weird order (that's the t
How ?

Just that Way :

Current (T) LM hash

Current (T) NTLM hash

(T-1) NTLM hash

(T-2) NTLM Hash

...

(T-n) NTLM Hash

(T-1) LM Hash

(T-2) LM Hash

...

(T-n) LM Hash

Now you should be able to modify the pwdump source code (as i did : believe me, it works fine !)

Have fun!

3. PWDump source and execute can be found in the Samba.org mirrors, one example being;

<http://de.samba.org/samba/ftp/pwdump/>

4. James MacDonald wrote a step-by-step that will let you see the data in question;

Actually they are stored in the SAM, but you have to set yourself up with permissions to read the

1. Create a Scheduler job as follows (you must have admin on the computer).

P:\>at \\yourcomputername 15:49 /interactive cmd.exe

Added a new job with job ID = 1

2. Confirm the job by:

P:\>at

Status	ID	Day	Time	Command Line
--------	----	-----	------	--------------

---	1	Today	3:49 PM	cmd.exe
-----	---	-------	---------	---------

3. Once the command prompt starts up, if you have WHOAMI.EXE from the RESKIT run it and you

C:\WINNT\system32>whoami

SYSTEM

This is very important, it must say SYSTEM, because even admins cannot read the SAM portion of the

4. From this command prompt, type REGEDIT. You can now open the SAM portion of the Registry

HKEY_LOCAL_MACHINE\SECURITY\SAM\Domains\Account\

What you see is a series of hex numbers under Users. Also, under Names you will see the account

5. Select one of account names and open the key. You will see a single hex number under the

6. You now should see two REG_BINARY entries labeled F and V. Open the V entry and note the

7. On NT 4 bring up MUSRMGR (in my case W2K, I went to Manage Computer) locate the account t

8. Go back to the REGEDIT windows and re-check the length of the V REG_BINARY value and you

At this point I believe you will be able to do what you want with the history.

Cheers,

Russ - NTBugtraq Editor

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

Are You "Certifiable"? Summer's Hottest Certification Just Got HOTTER!

With a growth rate exceeding 110%, the TICSAs security practitioner

certification is one of the hottest IT credentials available. And now, for

a limited time, you can save 33% off of the TICSAs certification exam! To

learn more about the TICSAs certification, and to register as a TICSAs

candidate online, just go to

<http://www.trusecure.com/offer/s0100/>

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo