

## Re: Disabling LM Hash creation

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2004-09/1143.html>

---

**From:** Steven L Umbach (n9rou\_at\_n0-spam-for-me-comcast.net)

**Date:** 09/30/04

Date: Thu, 30 Sep 2004 15:56:10 GMT

I use Cain and Abel and my experience is that after disabling lm hash and resetting the passwords that the passwords are much more difficult to crack. Try this with lm hash disabled. Change a password to some thing like aT184!\*ir&h and see how long it takes to recover that password. --- Steve

"rusga" <reply2newsgroup@nntp> wrote in message  
news:opse3bf0qjeqwqha@207.46.248.16...

> Hi,

>

> I've pasted this followup here since it's the proper NG to do so.

> It's named "Disabling LM Hash creation" in

> microsoft.public.win2000.registry.

>

> (paste start)

>

> Ok...

>

> What I did was:

>

> a) Changed the key to "NoLMHash" (no spaces).

> b) Rebooted the system.

> c) Changed the passwords.

> d) Tried to crack them with LC4.

>

> ... the setting was now active, but according to LC4, what happened was:

>

> a) The LM and NTLM passwords changed to an \*empty\* state to all users

> affected.

> b) The LM and NTLM hashes \*were created anyway\*.

> c) The LM and NTLM hashes were \*the same for all users\* affected (same

> empty seed).

>

> Now, these few questions arise:

>

> a) Isn't this a worse security scenario?

> b) Shouldn't the key be renamed to "Blank\_LM/NTLM\_Passwords" (or the

> like)?

> c) Am I seeing it wrongly?

>  
> *Regards,*  
> *rusga*  
>  
>  
> *On Wed, 29 Sep 2004 11:05:26 +0100, rusga <reply2newsgroup@nntp> wrote:*  
>  
> *Oops! That's it.*  
>  
> *I'll try it and post back.*  
>  
> *Thank you,*  
> *rusga*  
>  
> *On Thu, 30 Sep 2004 02:39:31 -0700, Mark V <notvalid@nul.invalid> wrote:*  
>  
> *In microsoft.public.win2000.registry rusga wrote:*  
>  
> *Hi,*  
>  
> *In MS checklist*  
> *( <http://207.46.156.156/technet/images/security/prodtech/win2000/wi>*  
> *n2khg/images/win2k45\_BIG.gif ) there's the possibility of*  
> *disabling the creation of LM hashes by creating the following new*  
> *key:*  
>  
> *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\NoLM Hash*  
>  
> *... but, unfortunately, it doesn't seem to work since LC4 cracker*  
> *still get's them.*  
>  
> *What am I doing wrong here?*  
>  
> *I think the KeyName is: NoLMHash*  
> *If you had a SPACE in there (as did your cited (but incorrect)*  
> *article) it would fail.*  
>  
> *There is a Group Policy that would probably be better and easier to*  
> *use.*  
> *KBA 299656*  
> *"How to prevent Windows from storing a LAN manager hash of your*  
> *password in Active Directory and local SAM databases"*  
>  
> *(paste end)*  
>  
> *Regards,*  
> *rusga*