

Re: disabling password request when connecting from the LAN

Source:

<http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.networking/2005-01/0110.html>

From: Steve Riley [MSFT] (*steriley_at_microsoft.com*)

Date: 01/03/05

Date: Mon, 03 Jan 2005 14:35:07 -0800

> *Seems the hashing is actually applied to each 7-byte half*
> *individually.*

That's true only for LM "hashes" (I put that in quotes because it really isn't a hash in the true definition of the term). And in networks that still use LM "hashes," it's true that 7 characters is better than 8 because of the way the cracking programs divide the hash in two.

NTLM and NTLMv2 create true hashes of the entire password at once, not two 7-byte halves.

I'm now using a 25-character passphrase on all my accounts. It would take more storage than exists on the planet to store rainbow tables for 25-character phrases; brute-force attacks would take approximately 500,000 centuries even accomodating for Moore's law. :)

Steve Riley
steriley@microsoft.com

> *"Steve Riley [MSFT]" <steriley@microsoft.com> wrote in message*
> *news:32434632402986863949856@news.microsoft.com...*
>
>> *Do you remember exactly what it was you witnessed? Your mention of a*
>> *"BIG computer" leads me to believe you might have seen someone*
>> *demonstrate*
>>
> *rainbow*
>
>> *tables or something simliar--software that precomputes all possible*
>>
> *hashes.*
>
>> *There's really very little defense against something like that. Yes,*
>> *the use of only a password as an authenticator is rapidly reaching*

microsoft.public.win2000.networking: Re: disabling password request when connecting from the LAN

>> *the end of its useful life.*

>>

> *No, not off the top of my head -- I might think of enough*

> *to get a Google search to track it down and if I do then*

> *I will let you know but (you know me pretty well) I was*

> *completely convinced on using at least 15 characters*

> *for all secure systems and have done so every since.*

> *This has the added advantage of disabling the LANMAN hash for THAT*

> *user even if the domain in question does not turn it off for everyone.*

>

> *There are also (very good) arguments that 7 is more secure than 8,9 10*

> *unless you go all the way to 14 but this 'feature' may have changed in*

> *recent OS versions.*

>

> *Seems the hashing is actually applied to each 7-byte half*

> *individually.*

>

>> *Steve Riley*

>> *steriley@microsoft.com*

>>> *"Steve Riley [MSFT]" <steriley@microsoft.com> wrote in message*

>>> *news:31807632402788220414480@news.microsoft.com...*

>>>>

>>>>> *Consider that even a 14 character password with partial complexity*

>>>>> *is not difficult to break (about 10-20 seconds with current*

>>>>> *technology) though.*

>>>>>

>>>> *Herb -- this is a little alarmist since complexity can vary wildly.*

>>>> *What*

>>>>

>>>> *Yes, it certainly alarmed me when I saw it done that easily.*

>>>>

>>>>> *kind of "partial complexity" do you have in mind that would fall so*

>>>>>

>>>> *rapidly?*

>>>>

>>>> *14-characters, upper/lower case, and numbers was the actual case.*

>>>>

>>>> *The password was otherwise highly random.*

>>>>

>>>>> *And what do you mean by "break"? Be more precise: you can guess*

>>>>> *passwords, you can crack hashes.*

>>>>>

>>>> *It was cracked (I believe) -- 20 seconds but it was a BIG computer.*

>>>>

>>>> *One the other hand it was only ONE computer. With distributed*

>>>> *attacks, you can figure it gets worse.*

>>>>

>>>>> *Passwords that fall in 10 to 20 seconds are usually extremely weak*

>>>>>

>>>> *passwords*

>>>>

Re: disabling password request when connecting from the LAN

microsoft.public.win2000.networking: Re: disabling password request when connecting from the LAN

>>>> *that cracking programs have either already generated the hashes for*
>>>> *or can generate the hash instantly -- meaning dictionary words,*
>>>> *words with*
>>>>
>>> *numbers*
>>>
>>>> *appended at the end, obvious substitutions (like zero for O, 4 for*
>>>> *A, and so on).*
>>>>
>>> *Not in this case -- it was highly random.*
>>>
>>>> *Steve Riley*
>>>> *steriley@microsoft.com*