

## Re: kerberos!

**Source:** <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2004-09/0067.html>

---

**From:** J. Merrill (*jvm\_cop\_at\_SPAMCOP.NET*)

**Date:** 09/13/04

Date: Mon, 13 Sep 2004 09:50:16 -0400  
To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

It's clear that "fallback to NTLM" is necessary in many cases. What is not clear is why it occurs in total silence -- that is, the NTLM username and password for the currently-logged-in user are presented to the other system. If you want to connect as a different user -- as you may have been doing when the initial Kerberos connection attempt failed -- an effort must be made to disconnect and re-connect.

If Windows presented the "connect as" dialog when falling back to NTLM, you would at least know that it was happening without having to understand the contents of this thread.

At 12:37 PM 9/10/2004, David Schenz wrote

>Two important points need to be remembered here: first, in order to join  
>a domain in the first place, NTLMv2 is still necessary (as the joining  
>member is not a part of the Kerberos realm), and second, windows  
>requires NTLMv2 to authenticate when opening a cif share via ip address.  
>[snip]  
>the authentication will fall  
>back to NTLM. I'm certainly glossing over the finer details of Kerberos  
>here, but it gets the point across.  
>  
>So yes, you're certainly right in that it is less secure. Unfortunately,  
>as currently designed, fallback to NTLMv2 is still necessary. I agree  
>that legacy support in Windows needs to be disabled by default. Too  
>often the trade off has been chosen in favor of compatibility over  
>security (causing many of Microsoft's security issues.  
>  
>David

J. Merrill / Analytical Software Corp

-----  
NTBugtraq Editor's Note:

Want to reply to the person who sent this message? This list is configured such that just hitting reply is going to result in the message coming to the list, not to the individual who sent the message. This was done to help reduce the number of Out of Office messages posters received. So if you want to send a reply just to the poster, you'll have to copy their email address out of the message and place it in your TO: field.

-----