

privilege timeout

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2004-12/0550.html>

From: Chris (Chris_at_discussions.microsoft.com)

Date: 12/29/04

Date: Wed, 29 Dec 2004 10:51:05 -0800

I am trying to configure a handful of Windows file servers to timeout user connections (like mapped drives) after a certain amount of idle time and make the user reauthenticate after that time is up. This is trying to mitigate the problem where a user authenticates to a sensitive file server and then walks away from the computer. I do not want to have their computer automatically lock itself...I just want that session to the sensitive file server to timeout and require reauthentication.

My first thought was to have the user's kerberos tickets expire if they're logged on as a domain user. I was able to change the domain GPO to successfully get the tickets expiring, however, the session tickets were automatically reissued if the user tried to connect to the same file server after the ticket expired. Is this due to any sort of credentials caching that can be disabled? (sort of like q299656, perhaps?) Again, my goal is to have these session tickets expire and make the user reauthenticate to generate them again, but I do not want the user to get logged out of their local domain login session.

If the above problem could be solved that would at least solve some of my problems. However, my corporation needs to be able to support employee's accessing these file servers from personal laptops that are not part of the domain either locally or remotely through VPN. I understand that in these cases NTLMv2 is used instead of Kerberos for authentication. Is there anyway to get Kerberos authentication to work in these situations (the user is logging on from a non-domain computer, though they will authenticate using their domain user account) using either built-in Windows Kerberos support or some third party option (MIT's Leash for example)? If not, is there anyway to get sessions authenticated using NTLMv2 to timeout and require reauthentication?

Thanks in advance for your help!

Chris