

Re: net use and LM / NTLM

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2002-04/0173.html>

From: Laura A. Robinson (larobins@bellatlantic.net)

Date: 04/12/02

From: "Laura A. Robinson" <larobins@bellatlantic.net>
To: <focus-ms@securityfocus.com>, "Mike Coppins" <mike@legolas.com>
Date: Fri, 12 Apr 2002 14:35:13 -0400

> At 11/04/2002 17:47, Laura A. Robinson wrote:
> >It depends on several things--
> >
> >First, is it a "net use" to a name, an IP or a GUID?
> >Second, what service pack revision is the NT4 server on in the second
> >scenario?
> >
> >Net use to IP, even in a pure Windows 2000 environment, uses NTLMv2.
> >Other net use is Kerberos in a pure Win2K environment.
> >NT4 SP4+ with Win2k is NTLMv2.
> >
> >Win2k and NT4 (SP4+), will both talk LanMan (LM) authentication unless
> >otherwise specified. I know this from experience. For example, two Win2k
> >machines on the same network, one of which has an LSA registry setting
> >that
> >says "reject NTLM and LM authentication, accept only LM". You get a
> >machine that is a default install of Win2k to try and connect to it, no
> >chance. You'll get "account doesn't exist" in the event log, in true
> >win2k
> >"report any old error" style. Switch off the "reject NTLM/LM" setting,
> >and
> >it works fine.

Hmm. This doesn't jibe with what I just tested. I have one Win2K box which is set to "Send NTLMv2 response only\refuse LM&NTLM", and another Win2K box which is set to the default "Send LM & NTLM responses" sitting on the other side of the room. No issues whatsoever connecting. Of course, that's because Kerberos authentication is used between Windows 2000 machines in a Windows 2000 AD environment except for those odd exceptions like the ones I mentioned.

Now, if you have a Win2K box that is set to refuse downlevel authentication *and* an NT 4 box that isn't configured to use NTLMv2, that's a different story.

As far as the part about NT4 not using NTLM by default, from:

Re: net use and LM / NTLM

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;q239869>

"When you first install the NTLM 2 support files, they are configured to use only LM authentication for backward compatibility with existing servers and domain controllers. Before you enable NTLM 2 authentication for Windows 95/98 clients, verify that all domain controllers for users who log on to your network from these clients are running Windows NT 4.0 service Pack 4 (SP4) or later. (Or, Service Pack 6 if the client and server are joined to different domains.) No domain controller configuration is required to support NTLM 2; the only time domain controllers need to be configured is to disable support for NTLM 1 or LM authentication."

and

"LMCompatibilityLevel – Clients IMPORTANT : For an SP4 client to choose level 3 or greater, the domain controllers for the user's account domains for all users who will use the client (hereafter, "the users' domain controllers") MUST have been upgraded to SP4.

If an SP4 client chooses level 0, which is the default, it will interoperate with earlier servers exactly as it did with Service Pack 3 (SP3).

If an SP4 client chooses level 1, it will interoperate with earlier servers exactly as it did at Service Pack 3 (SP3). In addition, it will negotiate NTLMv2 session security with SP4 servers."

If you go to a Windows 2000 client and look at HKLM\System\CCS\Control\LSA, you'll see that the default setting for authentication is, indeed, "0", which would allow it to use LM and NTLM authentication, so you're correct on that default. I guess I have a tendency to assume non-default settings, sorry about that. :-)

>

> *Win2k has issues with authentication (between LM/NTLM/NTLMv2 and kerberos).*

What issues, aside from those I mentioned (I know of a couple others, but I'm curious as to the ones you reference)?

> *In a domain control environment (ie. a DC and a load of nodes connected to the domain), both windows networking authentication (be it > LM/NTLM/NTLMv2) and kerberos will be sent in some scenarios.'*

Which scenarios (aside from what I mentioned)?

>

> *If what you were saying was the case, then on the NT4 SP4 upgrade, the NT4 > SP4 machine would suddenly not be able to connect to anything.*

That doesn't make any sense. Why would it "suddenly not be able to connect to anything"?

>

> *Have a read:*

> <http://support.microsoft.com/default.aspx?scid=kb:EN-GB;q147706>

>

Yes, from that article:

"Deployment

Because of the above considerations, if it is preferred to deploy NTLMv2, the following steps should be taken:

Upgrade the domain controllers where the accounts for all users that are to use NTLMv2 are stored.

Even before the upgrade of the domain controllers is completed, clients and servers can be upgraded to SP4 and will obtain enhanced security when connecting SP4 to SP4 by setting level 1.

When step 1 is completed, individual systems that have already been upgraded to SP4 can start setting level 3 or greater.

If users in some account domain never need to access resources from downlevel LM clients, that domain's domain controllers can have their level set to 4, and after all of those users' systems have been upgraded to SP4, that domain's domain controllers can have their level set to 5. "

So, I will agree with you that if we're talking plain vanilla, no configuration interaction between a Windows 2000 box and an NT4 box, then yes, downlevel authentication may be used. I think I took the wrong approach in my response, looking at it from the perspective of where Kerberos versus NTLMv2 would be used, as opposed to where LM/NTLM versus NTLMv2 would be used, even though the original question was quite clear that he was looking for information on the latter. :-)

Laura

-
- ***Previous message:*** [CHRIS GRABENSTEIN: "RE: Peculiar login troubles."](#)
 - ***In reply to:*** [Mike Coppins: "Re: net use and LM / NTLM"](#)
 - ***Next in thread:*** [Mike Coppins: "Re: net use and LM / NTLM"](#)
 - ***Reply:*** [Mike Coppins: "Re: net use and LM / NTLM"](#)
 - ***Messages sorted by:*** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)