

## Re: net use and LM / NTLM

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2002-04/0177.html>

---

**From:** Mike Coppins ([mike@legolas.com](mailto:mike@legolas.com))

**Date:** 04/13/02

Date: Sat, 13 Apr 2002 01:52:29 +0100

To: [focus-ms@securityfocus.com](mailto:focus-ms@securityfocus.com)

From: Mike Coppins <[mike@legolas.com](mailto:mike@legolas.com)>

At 12/04/2002 14:35, Laura A. Robinson wrote:

> > 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.

The exception (straight to IP) you mentioned would make sense in a Microsoft-twisted point of view, however it entirely negates the point of