ITS Technical Notes

Windows Enterprise Announcement

Mar 28, 2006 – LANMAN and NTLMv1 will be disabled May 10, 2006

The LANMAN and NTLMv1 protocols will be disabled on the Windows Enterprise Domain on **Wednesday, May 10, 2006**. The actual time of day for this change will be at 1:00 PM. This is the week between the end of Spring Semester 2006 and the start of Summer Session 2006.

These are old and very insecure protocols which are used to pass usernames and passwords over the network to the domain controllers. Modern operating systems (Windows 2000/XP/2003) use NTLMv2 or Kerberos (more secure protocols). Older operating systems (Windows 95/98/98SE/ME/NT) will be affected if they use Enterprise domain-authenticated resources).

This is typically a very difficult transition in a university environment. Many times it is not known what breaks until the protocols are disabled. As mentioned in the past, problems may arise in the following areas:

- Windows 95/98/98SE/ME systems will no longer be able to perform network authentication for file or print services hosted on systems that are members of the Windows Enterprise Domain. This means, for example, a Windows ME system will not be able to map a network drive from an Enterprise-member server or workstation.

- Old "SNAP" servers (a multi-protocol file server) that are members of the Windows Enterprise domain will cease to serve Windows files.

- Old SAMBA server software (released prior to later code which does modern protocols) will cease to work. (See below)

Please analyze your systems for reliance on LANMAN or NTLMv1 and upgrade prior to May 10, 2006. If you have concerns about this issue please email skunz@iastate.edu (or start a discussion on winadmin@iastate.edu) as soon as possible.

If you suspect you are having problems related this change after 1:00 PM, Wednesday, May 10, 2006 contact the ITS Solution Center by phone at 515-294-4000, email at solution@iastate.edu, or in person at 196 Durham Center.

Technical Aspects

A change will be made to the "Default Domain Policy". The Security Policy Setting of "Network security: LAN Manager authentication level" will be changed from the current setting of "Send LM& NTLM use NTLMv2 session security if negotiated" to the most secure setting of "Send NTLMv2 response only\refuse LM & NTLM". Since authentication occurs at the domain level, departmental overrides for domain authentication will have no effect.

Additional Information for SAMBA Servers

Samba 2.2 (or earlier) is probably not suitable in an Active Directory environment. Samba 3.0.14a can be configured to use NTLMv2. From the "smb.conf" man page for samba 3.0.14a as distributed with Debian GNU/Linux 3.1:

> client ntlmv2 auth
>
> [...]
> If enabled, only an NTLMv2 and LMv2 response (both much more secure than earlier versions) will be sent. Many servers (including NT4 < SP4, Win9x and Samba 2.2) are not compatible with NTLMv2.
> [...]

(Thanks to D. Joe Anderson for providing this information)