ITS Technical Notes

Windows Enterprise Announcement

June 5, 2008 – LANMAN and NTLMv1 to be disabled on Windows Domain Controllers Aug 13

LANMAN and NTLMv1 authentication will be disabled on the Windows Enterprise Domain Controllers August 13, 2008.

Two years ago ITS announced that on May 10, 2006 LANMAN and NTLMv1 authentication protocols would be disabled via "domain policy" in the Windows Enterprise Domain. These are old and very insecure protocols which are used to pass usernames and passwords over the network to the domain controllers.

The "domain policy" change in 2006 did not affect the actual domain controllers - only domain member systems. On August 13, 2008 ITS will complete the disabling of LANMAN and NTLMv1 by disabling the protocols on the domain controllers.

On May 20, 2008 this new "Domain Controller Policy" was temporarily enforced, causing outages for a few systems before it was backed off. If you had systems that experienced problems on May 20, 2008 you should immediately begin taking steps to assure your systems will not be using LANMAN and NTLMv1 on August 13, 2008.

Technical Aspects

A change will be made to the "Default Domain Controller 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. The "Default Domain Policy" will remain unchanged (at the most secure setting, same as since May 10, 2006).