

ITS Technical Notes

Windows Enterprise Announcement

Dec 9, 2005 – Proposal to disable LANMAN and NTLMv1 in Enterprise Domain

Discussions have been held for some time in the WinAdmin meeting about disabling LANMAN and NTLMv1 authentication protocols on the Enterprise domain. Recently, no “show stopper” reasons have been given to continue to allow these old and very insecure protocols (which are used to pass usernames and passwords over the network to the domain controllers). All Windows administrators expressing an opinion felt the security benefits far outweighed the “backward compatibility” concerns of continuing to allow LANMAN and NTLMv1.

This is typically a very difficult transition for a university environment to do. Many times you will not know what breaks until you disable the protocols. As mentioned in the past, this will be things like old “SNAP” servers (a multi-protocol file server) or old SAMBA server software (released prior to later code which does modern protocols).

If you have concerns about this please email skunz@iastate.edu (or start a discussion on winadmin@iastate.edu) as soon as possible. ITS will probably move forward with a date of “soon after the end of spring semester” (probably after the Tuesday after the end of final week) for disabling LANMAN and NTLMv1 on the Enterprise domain. A more formal announcement will be coming out soon (probably early January).