ITS Technical Notes

Windows Enterprise Announcement

Jan 10, 2006 – LANMAN and NTLMv1 will be disabled in Enterprise Domain

The decision has been made to disable LANMAN and NTLMv1 protocols on the Windows Enterprise Domain on **Wednesday, May 10, 2006**. This is the week between the end of Spring Semester 2006 and the start of Summer Session 2006.

Discussions have been held for some time in the WinAdmin meeting about disabling LANMAN and NTLMv1 authentication protocols on 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. Modern operating systems (Windows 2000/XP/2003) use NTLMv2 or Kerberos (more secure protocols).

Recently, no "show stopper" reasons have been given to continue use of LANMAN or NTLMv1. All Windows administrators expressing an opinion in recent months felt the security benefits far outweighed the "backward compatibility" concerns of continuing to allow LANMAN and NTLMv1.

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.

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.

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.