Windows Administrators Meeting

January 13, 2006

Notes (taken by Steve Kunz)

Meeting Started (9:00)

Announcements

- The announcement of disabling LANMAN and NTLMv1 protocols in the Windows Enterprise Domain has been made. These old (insecure) protocols will not longer be supported starting May 10, 2006. See the following for more details: http://tech.ait.iastate.edu/win2000/admin/Announce.01.10.06.pdf

- ITS will be having a new series of meetings focused on "Lab Needs" in the future. These meetings will be held once or twice a semester to help lab administrators be aware of current techniques and provide a venue for new solutions to better support lab/multi-user environments. These meetings will deal with multiple platforms (not just Windows). Watch for upcoming announcements.

Status Reports

- Scout 7.0 (for Windows) was released January 4. Steve Kunz [ITS] and Beata Pruski [ITS] talked about the few problems that were reported to ITS.

  - Some users found that the Scout installer would not run when it was deposited in a location where the file path was very long (the Desktop is one instance). The workaround is to simply move the installer to a folder near the root of a drive and launch it from there.

  - Terminal Services installations using MountAFSHome (to map AFS drive letters at login) may run into a problem where a drive does not map as it should. Beata Pruski [ITS] has a workaround for this. Contact her at bapruski@iastate.edu .

  - A bug was found in support for Windows Server 2003 on Scout 7.0 (it does not work on this OS). If anybody really needs this to work a "special build" can be supplied, otherwise it will be fixed in the next release. Contact Steve Kunz (skunz@iastate.edu).

  - One person found an ISP DNS problem exhibited itself with Scout 7.0 (they could get version 4 and 5 Kerberos tickets but not service tickets). Resolving the DNS issue with the ISP provider fixed the problem.

- The Windows WMF vulnerability caused concern until Microsoft (fortunately) released the patch via their update services last Thursday. If you have not installed hotfix KB912919 on all your systems you should do so as soon as possible. See http://www.microsoft.com/technet/security/bulletin/ms06-001.mspx

- The Active Directory "Student Re-Org" is progressing. See: http://tech.ait.iastate.edu/win2000/admin/Announce.01.09.06.pdf

The “Students” OU and college sub-OUs within it have been created. No student user objects have been moved yet. Work on the “Account Sync” process to auto-drop newly registered students into their college OU is in progress.

Microsoft “Windows OneCare”

Kunz talked about a new Microsoft product currently in public beta testing called “Windows OneCare”. This is a future “by subscription” service to handle important system administration tasks that many people find beyond their ability or desire to do. From Microsoft’s web page:

> “The things you should have to help protect your PC, but probably don't because they're such a hassle—stuff like virus scanning, firewall settings, tune-ups, and file backups—all delivered to you in a friendly, easy-to-use package that runs quietly in the background.”

It appears the initial offering is aimed at the “home user” market, but it is probably something Windows administrators should be aware of. The home page for this product is at www.windowsonecare.com .

Open Discussion

Web Wilke (RES H) opened a discussion on Windows “root kits” and how to detect them. Hackers are the obvious worry, but apparently there are more software vendors that are imbedding “hidden services” (like Sony did). Wayne Hauber (ITS) and others discussed the current products people are using to detect Windows root kits. They are:

SysInternals “RootKit Revealer”
http://www.sysinternals.com/SecurityUtilities.html

FSecure “BlackLight” (free beta until March 1, 2006)
http://www.f-secure.com/blacklight/

Wayne commented that many times the best way to detect root kits is not on a running system, but on a “forensic analysis” system examining an image of the infected system’s hard drives.

Wayne Hauber (ITS) mentioned that at the last Security SIG meeting a call went out for volunteers to held work on the “Secure Server” document being prepared by the Security section of AIT. At that meeting there were about 4-5 volunteers and more are welcome. Contact Wayne Hauber (wjhauber@iastate.edu) or Mike Bowman (mbowman@iastate.edu) if you are interested in helping with this important document.

Meeting Adjourned (9:40)

Next meeting is scheduled Febuary 10, 2006