Windows Administrators Meeting
December 9, 2005
Notes (taken by Steve Kunz)

Meeting Started (9:00)

Announcements

- All future WinAdmin and ExchAdmin meetings will be held in Durham 206. This is a nice newly remodeled room on the second floor of Durham (middle of the east hall) with good seating and audio/video.

- Scout 7.0 will be released in early January (tentative date is January 3, 2006). Kunz and Pruski [ITS] talked about a couple new major changes.

  Scout 7.0 supports "WindowsXP x64 Edition" (a 64-bit OS). Nearly all the current Scout-kits have been verified (and altered as necessary) to install on either the 32-bit or 64-bit platforms. A few "Advanced" Scout-Kits will NOT be ready by release date. See below for details.

  Another major change in this release is the replacement of the current Kerberos 5 library package with "Kerberos For Windows" (the current product from MIT). Users will notice a new "system tray" application called "Leash" installed for management of Kerberos credentials. If the "Kerberos Login" (Advanced Scout-kit) is installed on 32-bit systems, users will see little change other than the new Leash application running. Leash and SideCar will both show Kerberos credentials present. However, if "Kerberos Login" is NOT installed, a login to the desktop will have Leash popping up and requesting credentials for Kerberos authentication at that time.

  Other minor changes include:

  - Changed "Office of Academic Information Technologies" to "Information Technology Services"
  - Changed text on "Advanced" Scout-Kit warning to be "softer"
  - Fixed the "Shift-Click" install to include all components for "Portable Scout-kits"
  - Fixed a bug in "Passive FTP" code relating to load-balanced FTP servers (few people noticed this but it is fixed)

  The "look and feel" of running Scout itself is unchanged.

  A few software kits will NOT be ready by release date on the WinXP x64 (64-bit) systems. The following "Advanced" Scout-kits will NOT be available in early January:

  - OpenAFS (a working "beta" is in-house, so it is "close")
  - Cisco VPN (this is up to Cisco – we've asked, and will ask again)
  - Kerberos Login (Getting Kerb tickets at desktop login time. This requires native-64-bit complied Kerberos from MIT developers.)

WSUS Status

Kunz talked about the status of the WSUS upgrade on the Enterprise SUS server (sus.iastate.edu). Current plans are to install the WSUS software on the existing hardware platform in January, and cut over to WSUS in late January. No client changes should be required since the WSUS service will communicate in "back level" mode to clients that have not upgraded to the new WSUS client software. Since the same system (and DNS hostname and IP number) will be used, the upgrade should be "transparent" to the client systems pointing the SUS server. As was the policy for the current SUS server, all updates will be "approved" without testing. Since this is "WSUS", driver updates and other product updates (such as Office and SQL) will now be available on a "local store".

Kunz will post announcements of the "cutover" date (which will be sometime in late January) when plans are finalized.

LANMAN and NTLMv1

A recent email thread in the CCSG/WinAdmin mailing lists underscored the need to tighten down the authentication protocols available in the Enterprise domain. Since the discussion at the last WinAdmin meeting, no reasons have been presented to allow LANMAN and NTLMv1 as authentication to the Enterprise domain controllers. All present felt the security benefits far outweighed the "backward compatibility" concerns of allowing LANMAN and NTLMv1. Kunz cautioned, however, that 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). We will bring this up in the CCSG meeting/mailings, also.

For people interested in the "hard technical" aspects of this, we are planning to alter the Enterprise domain policy at the following setting:

```
Computer Configuration
  Windows Settings
    Security Settings
      Local Policies
        Security Options
          Network Security: LAN Manager authentication level
```

The current setting is:
  Send LM & NTLM - use NTLMv2 session security if negotiated
We will change it to the following after spring semester ends:
  Send NTLMv2 response only\refuse LM & NTLM

MSI Installer Sharing

A topic that was raised in a CCSG (or "IT Needs") meeting was raised again. There should be some method for colleges/departments to share MSI installers created for software products. If a product does not come bundled with an MSI installer it generally involves some work to produce one. This effort is a needless duplication of effort if multiple departments are interested in the same product (say, for example, and MSI installer for "Mozilla Firefox"). While an "open public drop box" approach is not good from a security standpoint (it would be a great way to box up a trojan and with a product) a cooperative effort with some form of "approval/trust" should be able to be developed. It was suggested this project may be most successfully drive by a wider group (possible by Dan Carlile). Noah Hughes (ECSS) indicated he would contact Dan on moving this idea forward.

Open Discussion

- Steve Heideman (CHEM) offered a tip for those people doing "lab builds". Steve was having a problem with building images on Dell GX620 systems that incorporated VirusScan 8.0i clients. It turned out it was a problem with the version of Ghost he was using. Upgrading from Ghost 8.0 to 8.2 solved the problem. Another person in the meeting reported the same experience.

- Wayne Hauber (ITS) commented that some server-class systems on campus were compromised because of a security flaw in "IBM Director". Similar to the "BackupExec" software flaw, this is a case of older "third party" software installed on systems that is not kept up to date (even though the Windows components are). Any service that exposed ports on a system is suspect for security flaws and people are reminded they should constantly look for upgrades to any such software. This would include things like "Dell OpenManage" and other vendor products that may be "pre-installed" on systems when you get them. Watch for later versions of each product being released and upgrade on a regular basis.

- A question was asked about who could help solve a problem with "MySQL" (a product available via GNU General Public License or as a licensed product) on Windows server platforms. Nobody in the room was working with MySQL on Windows. Wayne Hauber suggested that this was a good question for the Stanford "Windows HiEd" list (a listserv mailing list read by many IT people from large colleges and universities). Send mail to majordomo@lists.stanford.edu and put "subscribe windows-hied" in the ***body*** of the message.

- Kunz took some "open discussion" time to talk about "good security practices" that OU managers may wish to follow. These are not intended to be viewed as "rules of how you must do things" but rather a collection of tips/techniques Kunz and Hauber have collected from Windows seminars, SANS seminars, and security articles/discussions on the web over the last year or two. The list of "Good Ideas" is available at:

  http://www.tech.ait.iastate.edu/win2000/admin/OUManagerSecurity.pdf

Meeting Adjourned (10:00)

Next meeting is scheduled January 13, 2006