Windows Administrators Meeting
December 14, 2007
Notes (taken by Steve Kunz)

Meeting Started (9:00)

Announcements

- Vince Oliver [ITS] announced that over the semester break WIND3 would be "physically moved" within the ASB machine room and a brief outage may be experienced.

Status Report on Kerberos-4 Demise [Kunz]

Steve Kunz [ITS] gave a status report on the demise of the Kerberos-4 KDCs supported by ITS. Kerberos-5 is the current (modern) Kerberos protocol and all client packages must authenticate via Kerberos-5 by Fall 2008. The current timeline is:

- End of Fall semester 2007: Applicable servers do both Kerb4 and Kerb5
- End of Spring semester 2008: Clients converted to do Kerb5
- Prior to Fall semester 2008: Turn off Kerberos-4 (non-converted clients cease to work)

At this point the most pieces are ready. Current work is being done on:

- Zephyr: A Kerberos-5 version of the Zephyr server is working in test. New versions of the client will be needed once the server is in production.

- Scout System: New versions of the server ("ftp.sitelicensed.iastate.edu" a.k.a. "scout.iastate.edu") and client are being worked on. Scout 9.0 (which will have the ability to use both Kerberos-4 and Kerberos-5 servers) is being prepared for distribution in January.

Progress on Active Directory LDAPS [Kunz]

Steve Kunz [ITS] reviewed the progress being made on the LDAPS project on the Enterprise Active Directory domain

Digital certificates (from Thawte) to enable LDAPS have been installed on all four domain controllers. Some departments have performed software conversions and provided some feedback. Information for "Moodle" and "Apache" are available here:

http://tech.ait.iastate.edu/win2000/admin/UsingLDAPS.pdf

If you have information that will assist in other conversions, please send the instructions to skunz@iastate.edu. Information for configuring "Samba" would be useful if anyone has done that.

Starting in January ITS will contact other system admins that are doing "LDAP simple binds" to Active Directory and assist them in converting their applications.

The last step will be making domain policy changes so that the Enterprise Domain Controllers will no longer accept a "simple bind" form of LDAP authentication.

KeePass Demo [Kunz]

Steve Kunz [ITS] gave demonstration of "KeePass", a password storage application. KeePass is available at http://keepass.info . KeePass is available for:

- Windows 98 up
- PocketPC (KeePassPPC). Pocket PC 2003 up (but not SmartPhone)
- Palm (KeyRing application data converter)
- Blackberry
- Linux & Mac (all versions)

KeePass is a "foundation class" application, and runs without "installation" on a Windows system (making it a good application to put on a portable USB storage device). During the demo Kunz displayed how KeePass could be used to launch a login-page and "auto-type" the username and password, scripting it for varying web-sites (or applications). KeePass is freely distributable under the Gnu licence, and will be available as an "Advanced" Scout-Kit in January. A "Usage Tips" document will be carried with the Scout-Kit giving tips on recommended usage (choosing good pass-phrases, choosing and remembering a good "master pass-phrase", keeping backups, and using KeePass on a USB key-ring storage device).

Kunz offered one important warning as you begin experimenting with KeePass and the "auto-type" features. Do not use "real passwords" until you get the techniques down. In particular, don't do a "Perform Auto-Type" operation without having an "Auto-Type-Window:" parameter specified. You could run the risk of putting a "real password" out clear text on the network (KeePass may launch Internet Explorer with your password as the URL). Use bogus passwords until you get it entering the username/password fields correctly on the web-page you have "pre-launched" with the "Open URL(s)" function.

Use the "First Steps Tutorial" in the KeePass help file for a nice "quick start". KeePass has "plug-ins" to extend the base functionality. Look for those in the "Tools/Plugins" area of KeePass.

Open Discussion

Jim Wellman [AER E] said they experienced a problem last weekend with "false positives" on VirusScan which resulted in some systems having application components deleted. Apparently definitions released Monday ("5180") corrected the problem. People may want to check their ePO logs to see if other systems were affected and restore deleted/quarantined files. Jim also asked if some additional documentation could be written by ITS on how to get reports out of ePO for ISU IT admins. There is a lot of good locally written documents out there, but not much on how to run reports on ePO.

Meeting Adjourned (9:50)

Next meeting is scheduled for January 11.