Windows Administrators Meeting
November 9, 2007
Notes (taken by Steve Kunz)

Meeting Started (9:00)

Announcements

- A schema extension was done on November 6 for SMS. This was a very minor modification (from an SMS Service Pack) that added one attribute to one SMS object. The goal was to reduce some error messages within the SMS system.
- On Tuesday, November 13, 2007 there will be a change in the "password length" for new passwords on NetIDs. The new length requirement will be "8 character minimum" (instead of the current "5 character minimum"). Two character-set classes (from upper/lower, numeric, special character) will still be required. Existing passwords that are shorter than eight characters will NOT be forced to change – the new rules only affect NEW passwords at the time the user elects to change it themselves (either within Windows, UNIX, or ASW). At a later date (yet to be announced) the AccessPlus system will also move to "8 character minimum" passwords.

Portqry Command from Microsoft [Kunz]

Steve Kunz [ITS] discussed a downloadable command from Microsoft he had recently learned about. This command can assist in diagnosing connectivity and service problems on systems. The command is "portqry.exe" and it is used to query whether a given port (or range of ports) is open on a particular host. The program will indicate whether a system is "listening", "not listening", or "filtering" on a port. This is useful if you are wondering if a particular service is up and getting through a firewall to client systems "on the outside". The "portqry" program does not require a formal install and can easily be carried on a USB keychain device. A companion program called "portqryUI.exe" wraps the command-line version with a nice GUI interface.

A description of "portqry" and links to the download points for "portqry" and "portqryUI" are available in KB310099:

http://support.microsoft.com/kb/310099

Look at the bottom of this article for links to other valuable info, such as "How To Use Portqry.exe to Troubleshoot Microsoft Exchange Server Connectivity Issues", "How To Use Portqry To Troubleshoot Active Directory Connectivity Issues", and "Port Requirements for the Microsoft Windows Server System".

Prepare for Kerberos-4 Demise [Kunz and Pruski]

Steve Kunz [ITS] and Beata Pruski [ITS] talked about upcoming new versions of client programs related to 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)

Here are the software projects the MicroNet group needs to address in the Windows area:

- EMail: New Eudora installs are OK now (already configured for Kerberos-5). We may need to tweak old installs for Kerberos-5 (results in a client behavior change). Kpoprelay will replace SideCar for non-Eudora email apps. People who have never upgraded very old versions of Eudora Pro (which only did Kerberos-4) will have to upgrade by Fall 2008.

- Print: A new version of PCLPR will be needed.

- KerberosLogin: A new version will be needed.

- WinZephyr: New versions of both the client and the server will be needed.

- Scout System: New versions of the server ("ftp.sitelicensed.iastate.edu" a.k.a. "scout.iastate.edu") and client (with removal of SideCar, adding new kpoprelay kit) will be needed.

Progress on Active Directory LDAPS [Kunz]

Steve Kunz [ITS] explained that progress is being made on the LDAPS project on the Enterprise Active Directory domain. This project was first announced in the August 2006 WinAdmin meeting. See "Shutting Down LDAP Simple Binds on Enterprise AD" in the meeting notes here:

http://tech.ait.iastate.edu/win2000/admin/WinAdmin.08.10.07.pdf

A digital certificate to enable LDAPS (from Thawte) has been installed on WINDC4, opening up port 636 on that domain controller for "LDAP secure encrypted binds". Two departments are doing preliminary work on converting their applications from "simple binds" (clear text passwords) to "LDAPS binds". Within the next few weeks ITS will install similar certificates on WINDC1-3, and document knowledge learned by the initial conversions. Following that, 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.

Open Discussion

Russ Hoffman [STAT] asked if there was any information (such as numbers of users at Iowa State who had their passwords compromised) that IT managers could use to convince people of the importance of good ("longer and more complex") passwords. The "sale" of stronger passwords is sometimes difficult because people are not aware of the threat or concerned about the ramifications of a password compromise. Mike

Bowman [ITS] indicated we probably don't have statistics on the total number of compromises that have happened. However, ITS Security has felt that in many "compromised systems" (root-kits and other intrusions) the cause has been a compromised system administrator password.

Dave Orman [CNDE] commented that he felt that AccessPlus security was lax with its current password rules. Mike Bowman [ITS] responded that while the passwords may be currently short and "non-complex", the "bad try lockout" feature alleviates any severe "hacking" ramifications. To date, there have not been a large number of users "locked out" of AccessPlus due to hacking on their accounts.

A good general discussion occurred on the good and bad effects of having AccessPlus use NetIDs (for "one login/password"), the value of long "pass phrases", the value of "second form factor" authentication and good security practices in general. It can generally be said that ITS will be encouraging and providing for stronger security on campus computing systems both now and in the future. Current activities (stronger password rules and more secure LDAP bind methods) are all consistent with that goal.

Meeting Adjourned (10:00)

Next meeting is scheduled for December 14.