Windows Administrators Meeting
October 11, 2002
Minutes (taken by Vince Oliver and Steve Kunz)

Meeting Started (9:05)

Announcements

- Two new Windows Scout-kits are available in the "Advanced" Scout-kit list. The latest version of the IBM/Transarc AFS client (patchlevel 3.6 2.39) is available. The product provides native AFS file service on Windows NT/2000/XP. A companion product called "MountAFSHome" can be used to automatically mount each logged-in user's AFS home directory on a Windows drive letter. Installation of the MountAFSHome Scout-kit will configure the IBM/Transarc AFS client for "integrated login", meaning the Windows username/password will be used to obtain tokens for AFS (provided the username/password for the Windows system is that same as that for AFS access). This is especially useful for systems that are members of the enterprise Windows 2000 domain ("iastate.edu"). Tokens are discarded and the "non-persistent mount" is removed at logoff.

- It was announced that PerlMX (the enterprise "SPAM flagging system") was placed into production on October 1. Mike Bowman announced that some changes to the PerlMX implementation are being planned which will be announced early next week. Kunz indicated he preferred not to have multiple discussion forums going on for PerlMX, and suggested the CCSG meeting would probably be the best place to center discussions.

  [News since the meeting: On Monday, October 14, AIT proposed that on October 28 (after 5:00 PM) the "Subject:" header no longer be modified. Most users could still filter SPAM based on the "X-Perlmx-Spam: Gauge=…" header inserted by PerlMX. Some email clients (such as Outlook Express and Novell GroupWise) cannot filter based on "X" headers and therefore will be unable to filter SPAM flagged in this fashion. Discussion is open on this proposal via a post to the CCSG, UA, and WinAdmin email groups. Please participate if you have opinions on this proposal.]

Exchange 2000 Status (Kunz)

ADP/AIT ran the "Active Directory Migration Tool" (ADMTv2) against approximately 1,500 ADP Windows accounts last Thursday (Oct 3, 2002). The ADMTv2 utility assists in the migration of Windows accounts from existing NT 4 domains to Windows 2000 Active Directory. One function ADMTv2 has is the ability to copy the "SID history" (for access control) and the existing NT 4 password into Active Directory. This "password migration" was performed on Oct 3, but some problems for those users resulted. While the old NT 4 password correctly became the "Active Directory" password, the ISU Net-ID was incorrectly set to a "random character string" for all 1,500 ADP users.

Kunz feels the reason for the "Net-ID password scramble" was the result of a "bug" in ADMTv2. When ADMTv2 migrated the user information, the "password change" caused by ADMTv2 caused the Windows domain "password change exit" to be activated on the domain controllers. This exit is used to pass Windows password changes up to Acropolis, where they are checked for complexity and "synched" with the Net-ID if the username is linked to an ISU Net-ID. This works properly for all normal Windows "password changes" ("sets" and CTRL-ALT-DEL, for example). However, when the password change initiated by ADMTv2 is passed through the Windows exit it is NOT the correct password (but a "random character string", possibly a portion of a hash of the password). The Acropolis functions said "this is a password of suitable complexity and length and is for an account that is a valid Net-ID, therefore I will change it here, too". The password change was accepted for the ISU Net-ID. Windows 2000 (and ADMTv2) completed the remaining steps to the set the Active Directory password (correctly). Unfortunately the user in question no longer knew the password for the ISU Net-ID in Acropolis.

This bug in ADMTv2 is being reported to Microsoft. Circumvention is being planned (so this does not happen again, should be not get a fixed version from Microsoft). In the future a list of usernames being processed by ADMTv2 will be checked by the password-change exit, and (if on the list) the password change will not be passed up to Acropolis. At this point users being migrated by ADMTv2 can be told their password is either 1) their old NT 4 password or 2) their existing Active Directory password and that they should change it to make them "synch" again.

One of the next steps in the Exchange 2000 project will be to "mail enable" all Windows 2000 user objects based on ISU Net-IDs ("!user" exception accounts will NOT be mail enabled). In addition, the user-object "displayName" attribute will undergo a "format change" (see next section).

Windows 2000 UserObject "displayName" Attribute (Kunz)

The people involved in the Exchange 2000 design have requested that the "displayName" attribute (which contains the searchable name for an email user in the GAL/Active Directory for Exchange/Outlook users) be of a modified format. This field is normally not seen with "Active Directory Users and Computers" (where the proper name and description fields are normally viewed).

The current format of the "displayName" is currently similar to:

Steven L Kunz

The new format will be:

Kunz, Steven L [AIT]

The advantage of this format is that the "stem search" applied to the Global Catalog in Outlook clients can be accomplished by "last name", not "first name" (as in the current format). The short abbreviation for the department (when the user is a faculty/staff) is also available to aid in selecting the recipient.

WinAdmin meeting participants had no objection to this change. Barring strong objection from the community reading these minutes this change will be incorporated next week.

Windows 2000 Professional Gold Standard Template (Kunz)

Kunz attended a SANS Institute training session for the "Windows 2000 Professional Gold Standard Security Template" and demonstrated some key concepts from the session.

The template, several accompanying documents, other security templates, and a "CIS Scoring Tool", are available from the following address:

www.cisecurity.org

After registering you can download the file "cis-win.exe", which is an installer that will install all the pieces onto your Windows 2000 Professional system. Several security groups have developed security templates in the past (NIST, NSA, CIS, SANS, etc). The "Gold Standard" template is the "composite best thinking" of all the groups.

After you have installed the product you use the Microsoft Management Console ("mmc") "Security Templates" and "Security Configuration and Analysis" snap-ins. The "Security Templates" snap-in can be used to browse to the Gold Security Standard template (stored by default in "\Program Files\CIS\Templates") and view the settings.

More useful is the "Security Configuration and Analysis" snap-in. Open a "new database" after launching (following the on-screen instructions) and load the Gold Security Standard template (again, stored by default in "\Program Files\CIS\Templates"). You can now view the differences between the template recommendations and your system. By "right-clicking" the "Security Configuration and Analysis" snap-in you can "apply" the template settings. WARNING! There is no "uninstall these settings" function. It was recommended by SANS that you test on an "imaged" (or sacrificial) system before installing this template on a production system. A "high security" system is by nature "diminished in functionality" and some settings may not be tolerable in your situation. You can produce a custom template of your own using the "Gold Standard" as a base starting point (and exporting templates).

Another useful tool distributed with the CIS package is the "CIS Scoring Tool" (available off the "Start->Programs->CIS" program group. Consult the documentation for this tool (in "\Program Files\CIS") for instructions on how to use this tool to tighten down your systems security against a standard security template (such as the "Gold Standard" template).

Windows "net send" SPAM (Kunz)

Several groups on campus are reporting "Windows Messenger Service SPAM". This is NOT related to "MSN Messenger" (a chat/email client from MSN), but rather is use of a long-existing service on Windows NT 4/2000/XP systems called "Messenger". A spammer can send a message to this service on your system using your WINS/DNS name (or IP number) with a command similar to "net send <addr> Hello!". If you have the "Messenger" service running on your system a Windows "popup" will appear with the text "Hello!".

Various discussions are going on relating to how this irritation can be reduced. The simplest way would be to disable the "Messenger" service on your system. Be aware, however, that some departments use Messenger pop-ups for print notification, interprocess messaging, etc. This may NOT be the best solution.

[Information since the meeting: "Messenger" spam is using UDP port 135 to find a random port to send the message on. The best solution may be to block incoming connections on UDP port 135 at the border routers.]

Open Discussion

Jim Wellman (AE EM) reported problems with IBM/Transarc AFS clients a couple weeks ago. The problem was traced (by AIT and Telecomm) to port scans being run against his subnet. When the scanning IP address was blocked the problem went away. Kunz reported similar scans had disabled AFS access on systems within AIT, too. Systems with personal firewall software installed (such at ZoneAlarm or NetworkIce) were protected from this attack.

Meeting Adjourned (about 10:00)

Next meeting is November 8.