IOWA STATE UNIVERSITY
IT Services Technical Notes
IT

Windows Administrators Meeting

September 11, 2009
Notes (taken by Steve Kunz)

Meeting Started (9:00)

Announcements

(None)

Granular Password Settings V2 [Steve Kunz - ITSYS]

Steve Kunz [ITSYS] talked about the second version of the Granular Password Settings plan. Minor modifications to the first version incorporated feedback from previous presentations of the plan to the CCSG, WinAdmin, and ITLC groups. All details of the current plan are in the “Planning for Password Setting Objects (PSOs)” document available here:

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

Kunz indicated that there are two changes from the previous version:

1) Colleges and departments will supply a list of OUs (not groups) for PSO application.
2) A sixth “stock PSO” was suggested with a 16 character minimum password length and 180 day expiration. In the above document it is “PSO4”.

The question was asked if the “shadow group creation” script would load the group from the users in all nested OUs. The answer is “Yes”.

If you have any feedback after reading the above document please contact Steve Kunz (skunz@iastate.edu).

Open Discussion

Jim Wellman [AER E] asked if there was any need for stronger password settings given the account lockout facility. Among the answers given was that there were needs expressed during the Active Directory design process years ago relating to contracts that required certain password expiration policies. Currently ITS is aware of one set of compliance needs for the PCI (credit card) system admins. Also, while it may be hard to come up with proof that eight-character passwords can be cracked quickly it is still not considered secure to have an infinite-life eight-character password in this day and age.

Jim Wellman [AER E] asked if there was any thought being put into multi-factor authentication (SmartCards or other tokens). Mike Bowman [ITSEC] answered that ITS is currently looking at a couple of products that support “passcode tokens” (where a multi-digit passcode retrieved from a small physical device must entered in addition to your username and password). ITS is currently looking at a solution for its own needs, but hopefully the solution will scale out in our distributed-management environment.

Wayne Hauber [ITSEC] wants to make people aware that Microsoft has a critical hotfix out (MS09-048) that will not apply to Windows 2000 systems even though the exploit can result in a denial of service. See the “Frequently Asked Questions” section of the hotfix document under the topic “If Microsoft Windows 2000 Service Pack 4 is listed as an affected product, why is Microsoft not issuing an update for it?”:

http://www.microsoft.com/technet/security/bulletin/MS09-048.mspx

This may be a good time to consider moving those old Windows 2000 systems up to a more modern operating system.

Jim Wellman [AER E] commented that they had recently gone through an interesting exercise of printer deployment using group policy preferences. Jim indicated he will arrange to get a document going on tips on how to do this. [Info since the meeting: Jim has emailed Kunz some notes. Kunz and Wellman will develop a TechNote soon]

Meeting Adjourned (10:00)

Next meeting is scheduled for October 9.