Windows Administrators Meeting
June 8, 2012
Notes (taken by Steve Kunz [ITSYS])

Meeting Started (9:00)

Announcements

- Flame malware is in the wild. Microsoft Security Advisory 2718704 has been released "out of band" (which indicates its severity). Systems admins should apply the latest security updates ASAP.
- LinkedIn password list hacked and published. If you use LinkedIn change your password.

Account Sponsor in Master LDAP and AD -- [Steve Kunz - ITSYS]

Steve Kunz [ITSYS] talked about another change coming to the mastered LDAP data in directory.iastate.edu and Active Directory. It has been suggested that it would be valuable to have an attribute contain the sponsor of a sponsored (affiliate) account. An "owner" field already exists (but is empty) in the master LDAP database (directory.iastate.edu) and ITS will populate that field with the sponsor data in the near future.

The next step will be to populate the information onto an AD attribute. Kunz feels it is desirable to have the information on an attribute displayed in Active Directory Users and Computers. While the "manager" field sounds like a candidate, it is unlikely that the "manager" of an affiliate user account is always the "sponsor" of that user's account. A better attribute might be the "info" attribute which appears in the "Notes" area on the "Telephones" tab. If any existing information is there (it is only present on about 20 user objects in the domain) the sponsor info could simply be appended.

Other ideas on an appropriate AD attribute are welcome. Either send email to Steve Kunz at skunz@iastate.edu or post to the WinAdmin list. This topic will be raised again at a future CCSG meeting.

Group Policy Central Store (.admx files) -- Tim Danzer [H SCI]

Tim Danzer [H SCI] gave a presentation on the advantage of placing group policy .admx and .adml template files in a central store in the domain SYSVOL area. This has advantage in that domain SYSVOL storage can be greatly reduced (which in turn reduces AD replication traffic) and common templates are accessible for all in one shared location. The main drawback is that on systems where a local OU admin has modified local copies of these files the central store will "trump" the local modifications. People in the meeting indicated they did not modify .admx files for the most part – but were concerned about what would happen if a previous OU administrator had performed undocumented changes and the new OU was caught by surprise.

This proposal needs to be more widely discussed. A CCSG presentation is certainly in order. Provide feedback to Tim Danzer (tdanzer@iastate.edu) and Steve Kunz (skunz@iastate.edu) or the WinAdmin list.

Tim's PowerPoint show is available at
http://www.tech.its.iastate.edu/windows/admin/GroupPolicyADMX.ppsx

Open Discussion

Beata Pruski [ITSYS] requested that those people using the SCCM imaging system make sure they are using the most current "WinPE" product when deploying systems. Previous versions had a time-zone issue that causes a large number of authentication failures in the domain (and causes DHCP addresses to be blocked by the IDS).

It was asked if it would be possible for the sponsor of an account to be notified that an account needs to be renewed. One department was experiencing renewal messages being ignored and accounts being suspended. Others in the meeting said that they were getting renewal email for accounts they sponsored. The issue may be due to "emeritus professor" accounts which undergo a slightly different renewal process. The Solution Center probably has the best answer to the question.

Jim Wellman [ENGR] asked what to do when Group Policy Objects created by an old OU admin need to be managed by a new OU manager and permissions prevented working on the GPO. Kunz said this is an Enterprise Administrator task and email can be sent to its-ad-admins@iastate.edu indicating the GPO objects, who owned them, and who should now own them. This is a manual process – but some tools are provided by Microsoft to make the job easier. Google "download gpmc sample scripts" and you will find them. They may help you find all GPOs owned by a given user.

Steven Spencer [LAS] asked if anyone knew of a way turn off auto-proxy via a GPO (since the Flame malware used a proxy to inject malware). Nobody knew of a way (other than a direct registry hack).

Meeting Adjourned (10:00)

Next meeting is scheduled for July 13 (provided a sufficient agenda exists).