Windows Administrators Meeting
September 12, 2003
Minutes (taken by Steve Kunz)

Meeting Started (9:05)

Announcements

- Integrated Login – With the release of the Windows Kerberos 5 authentication libraries, the ability to acquire Kerberos 5 credentials for SideCar (and other authenticated services) at desktop login time is now possible. To do this the client system needs to be a member of the "iastate.edu" Windows Enterprise Domain and have some special registry entries configured. A Scout-kit has been prepared that will be available in the "Advanced" Scout-kit list early next week. In addition, a ".reg" registry mod file and instructions will be available on www.sitelicensed.iastate.edu for non-Scout IT administrators. This feature, combined with AFS "Integrated Login" and "AFSMountHome" (available as advanced Scout-kits) allow login, mounting of the users AFS home directory, and AFS authentication at desktop login time (for enterprise domain members).
- Eudora Pro 6.0 – Qualcomm released Eudora Pro 6.0 a week or two ago. The initial release was missing component and an "updated" release was available yesterday. This product is in internal testing at the moment. A Scout-kit will be released in the "Advanced" Scout-kit area early next week for "public testing" (the raw installer will be available on www.sitelicensed.iastate.edu at the same time). The most significant new feature is "junk mail" (a.k.a. "spam") filtering. A "New Features" document is included with the installation.
- HostExplorer 8.0 – HostExplorer 8.0 is nearly prepared for release (probably next week). This version features native Kerberos 5 support for "pass through" authentication. This means that if the Kerberos 5 interface is properly configured and the "Integrated Login" configuration is done (see above), a single sign-on to an Enterprise domain system will result in no sign-on being necessary when connecting to a Vincent workstation (or "Vincentized Linux") workstation. A telnet connection will immediately result in a command prompt at the Unix host.
- Mike Bowman (AIT) announced that no changes to the current port blocking (port 135 at the border routers) are anticipated. More specifically, we do NOT intend to block ports 136-139, 445 at the borders until VPN services are available to the general public (see next announcement). Traffic analysis has indicated there is significant use of file and print sharing to off-campus hosts (this uses ports 136-139,445) that would be interrupted until VPN was available. Unless forced to block these ports for new vulnerabilities, AIT prefers to wait for VPN availability. These port blocks will apply only to the border – traffic on 135-139,445 will remain unblocked between local campus subnets.
- VPN – Telecommunications has a production Cisco VPN server in house, being tested by staff. Scout-kits with the Cisco VPN client for Windows, Macintosh, and Linux are being prepared. Raw client installers will be available on

www.sitelicensed.iastate.edu. This service should be available in 2-3 weeks. At that time AIT will move toward blocking ports 136-139,445 (as per previous section). Windows file and print sharing will no longer work across the campus border at that point unless the external client connects via a VPN connection.

MS03-039 Security Hole (Steve Kunz – AIT)

Microsoft announced yet another security hole in their RPC service (which uses port 135) this week. Patches and scanners have been well announced/discussed on the WinAdmin and CCSG mailing lists. This hole is as severe as MS03-026 and Critical Updates available from Microsoft should be applied to all Windows NT/2000/XP/Server2003 systems ASAP. No known exploit for the hole is in the wild (yet) but it is anticipated it will be a matter of days. Note that the vulnerability scanner for the older MS03-026 issue should not be used after applying the fix for MS03-039 (it will indicate the patch for MS03-026 is missing). Use the new vulnerability scanner released by Microsoft for the MS03-039 hotfix.

Automatic Update for Non-managed Systems (Steve Kunz – AIT)

Steve Kunz (AIT) talked about steps the AIT MicroNet Group is taking to make it easier for "non-managed" Windows systems to be kept patched with critical hotfixes. Using the techniques already documented for the enterprise "SUS server" (at www.ait.iastate.edu/win2000/admin/SUS_User_Kit.zip in the "Configuration Options in a Non-AD Environment" document) it is possible to configure any Windows ME, 2000, XP, and Server2003 systems to automatically apply critical hot-fixes. The AIT MicroNet Group is building a Scout-kit that will perform these "Automatic Update policy settings" on non-managed (or "loosely managed") systems. This Scout-kit will start by warning the user that if they proceed critical hotfixes will automatically be applied to their system at the specified time and that the system will reboot when all users have logged off. They will have an opportunity to "bail out" at that point.

If they proceed, Kunz outlined the following registry settings (as recommended by the AIT MicroNet Group) would be applied:

```
HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU\
    RescheduleWaitTime = 5 (see below)
    NoAutoRebootWithLoggedOnUsers = 1 (don't reboot if someone logged on)
    NoAutoUpdate = 0 (Enable automatic updates)
    AUOptions = 4 (automatic download and install – don't ask first)
    ScheduledInstallDay = 0 (check for updates every day of the week)
    ScheduledInstallTime = <current time> (install at this time – see below)
    UseWUServer = 0 (use Microsoft's update servers, not ours – see below)
```

The "RescheduleWaitTime" option is used when a machine is powered off during the time an update should be applied. When the system is powered up, the "RescheduleWaitTime" value specifies the number of minutes that should elapse after power-up until the updates are applied. Five minutes is the default value from Microsoft (the maximum value is “60”).

The “ScheduledInstallTime” is the time-of-day any installation and reboot occur. The Scout-kit will provide the current time by default and allow the user to change it. Ideally this would be at a time when the system is always “On” and “Not in Use”.

The “UseWUServer” option is set to NOT use our enterprise “SUS” server since a large portion of the target audience is our student community and we do not want them to eventually leave campus with their systems configured to perform automatic updates from our enterprise SUS server (since it will not talk to off-campus systems). For those departmental IT admins who choose to use this technique and KNOW the system will remain “on-campus”, the “UseWUServer” value can be set to “1” (enabled) and the following additional values can be added to point to the Enterprise SUS server:

> WUServer = sus.iastate.edu
> WUStatusServer = sus.iastate.edu

Kunz solicited input from the audience on the above values. Several IT admins already apply similar settings via Group Policy to their systems and remarked these values were pretty close to what they were using. All agreed these values seemed best.

It is hoped an “Advanced” Scout-kit can be available next week. A “.reg” file and instructions will be made available on www.sitelicensed.iastate.edu for departmental IT admin use at the same time.

Open Discussion

Russ Hoffman (STATL) asked if anyone knew of a way for force a remote system to reboot automatically. In particular, this was related to Group Policy causing updates to be applied, but the user of a system refuses the reboot and never logs off (meaning the updates are “staged” but not installed). Comments were made from the audience about using shutdown scripts or scheduled tasks. The best answer seemed to come from Michael Miller (Design), who promised to post his solution to the WinAdmin mail-list.

[Information since the meeting]
Michael Miller posted the following to winadmin@iastate.edu with the Subject of “Poweroff”:

> Per discussion in the meeting this morning to shutdown a group of machines...this is very simplified...I just use this program on a server and set up a batch file to step through each machine....It could probably be scripted to look at a list of machines that could be generated (nightly?) from the OU list...This program can

be run with a GUI (just double-click) or as a command (poweroff /? gives all options). I like the idea of being to travel the OU, look for machines that have the STATE flag set for having downloaded and applied the critical updates, just not re-booted and set it to reboot. Try this link...

http://www.webattack.com/get/poweroff.shtml

So my batch file is just a bunch of lines like

```
poweroff reboot -remote {MACHINE1} -use_nt
poweroff reboot -remote {MACHINE2} -use_nt
```

Thanks, Michael!

Meeting Adjourned (about 10:05)

Next meeting is October 10.