**Windows Administrators Meeting**
April 26, 2002
Minutes (taken by Steve Kunz)

**Meeting Started (9:05)**

**Announcements**

- May 13 – DHCP leases, NetReg registrations, and WINS server registrations for residence halls IP addresses will be flushed/reset. This will NOT affect other non-residence halls ("staff") systems on campus. This is not a NEW process being done – just a different TIME when it is being done (it has been performed in August before the students come back in previous years).
- May 28 – The SMTP service on the pop-servers will be shut down. Only a few people were using this (everyone should be using mailhub.iastate.edu for SMTP service). Some old ("incorrectly configured") email clients are using the pop-servers for this (unadvertised) purpose. This bypasses the E500s (and email virus scanning) for outbound mail. AIT is watching the list of IP addresses using SMTP on the pop-server and will attempt to contact the owners for re-configuration (to mailhub) prior to May 28.
- The SSH client from SSH.com has been site licensed for use at Iowa State University. It has been installed as the SSH client on the Vincent workstations. A Scout-kit installer for the Windows version is being prepared (and will be placed in the "Advanced" Scout-kit area soon). This client has fewer problems than the OpenSSH software (and uses the "version 2" protocol level for SSH). It was commented that another package that people might find of interest is "WinSCP", a secure file transfer utility. A web-search for "winscp" will get you additional information.

**Interesting Info**

- Event logging stats from the Windows 2000 domain controllers: During the week of April 16 to April 22, 1,837,083 login events were processed for 5,674 unique users. Windows login events are triggered multiple times per actual session (for network file access, printer access, etc) so it is difficult to come up with an actual "user session" count. If any Windows admin knows of good software to report on user sessions from event logs feel free to send us the info (skunz@iastate.edu).
- It was discovered that ZoneAlarm Pro version 3.0 would cause problems with a Windows 2000 Pro system finding a domain controller. The latest version fixes the problem. The problem occurs even if the firewall is configured to trust the domain controllers and DNS servers.
- The latest version of Transarc AFS for NT/Windows 2000 fixes the problem of a client going "100% CPU Utilization" when the local network is down. Kunz is working on a Scout-kit to distribute the latest version of this product.

- Kunz mentioned that there is some "experimentation" going on within AIT to enable Apple OS X systems to authenticate to our MIT Kerberos servers and mount AFS home directories. AIT is examining a couple solutions for use in our labs (and hopefully a more general solution for others on campus). The "Apple Solution" (using Active Directory) has also been examined.

**Windows 2000 Enterprise Infrastructure Progress (Kunz)**

- Password-Sync from Windows to Acropolis (the ISU NetID) was activated Tuesday, April 23. If an OU admin "right-clicks" an ISU NetID user object in their OU and selects "Set Password", the password is synched back up to the MIT Kerberos server (setting it for other Acropolis functions). The "Change Password" button on the Windows 2000 Pro client systems will be enabled in the near future (this was disabled by a domain-wide group policy setting because of the lack of synching capability in the past).
- The ISU NetID "pre-population" (discussed in previous meetings) was completed. ISU NetIDs who had not changed their password since April 2000 are now populated into Active Directory with a long random-character password (the actual password cannot be recovered from the MIT Kerberos servers once encrypted and stored). These user objects have a "Description" (viewable with "Active Directory Users and Computers") set to "Change password to use". If someone cannot login with their ISU NetID to a Windows 2000 system in the enterprise domain, first check their "Description" field. If it indicates "Change password to use" they should change their password (via asw.iastate.edu). Their password will be synched and the Description reset to their proper name.
- The OU population process (moving faculty/staff ISU NetIDs into departmental OUs) has been progressing this week. Most OUs doing significant work with Active Directory (having a number of computers within the OU) will be loaded by the end of this week.
- A new document titled "Managing Users Within a College/Departmental Organizational Unit" is available on the Windows 2000 support web page at the following URL: http://www.ait.iastate.edu/win2000/admin/UserMgmtInOUs.pdf . This document should be used by OU managers with ISU NetIDs populated into their OU. It is very important that user objects linked to ISU NetIDs not be renamed or deleted. If an OU manager does not want them in their OU they should arrange to have them moved back into the general user pool.

**LANMAN and NTLM Security Issue (Steve Kunz)**

Kunz talked about the LANMAN and NTLM security issue again. The main concern is whether or not it would be a good idea to cause the domain controllers to stop authenticating via insecure protocols (LANMAN and NTLM). Related Microsoft Knowledge Base articles that have information about how to do this (and the implications of doing it) are at:

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q239869

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q147706

The following articles relate to the Directory Services client on Win9x and ME systems:

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q249841

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q276472

The original proposal was to configure the domain controllers to only speak NTLMv2 and above. However, two groups on campus using "SNAP" servers (a device to share files on disk drives via a variety of protocols) discovered that the product only speaks "NTLM". [If you are using this product and have not emailed Kunz about it, send email to skunz@iastate.edu]

Discussion during the meeting also brought out the fact that certain Apple clients using Apple file sharing techniques against Microsoft Apple services MAY also use down level protocols (unknown at this time). Other products may also be affected.

The final decision was that it was probably safest at this time to go to "Level 1" protocol negotiation on the domain controllers (negotiate to use NTLMv2 and fall back to the other lower protocols if the client cannot do it). This is recommended in SANS documents if the higher security setting causes problems (like it will here).

A question was asked about whether we really need to worry about insecure protocols if we have switched network connections on campus. The answer was "yes", since many buildings still have labs/rooms with hubs, and the advent of "wireless" means we are going back to a "general broadcast" type of environment in certain areas.

It was pointed out that a "replay attack" could still be used to steal credentials off the network on systems not using Kerberos. In this scenario a user using NTLMv2 supplies a valid username and password, getting a securely encrypted credential that could be sniffed and "replayed" to acquire services by someone else. In this case the "hacker" did not need to crack the password – just "borrow" the encrypted credential off the network and "replay" it. The only real solution to this is to upgrade the client to Windows 2000/XP (and thereby use Kerberos).

**Meeting Adjourned (about 10:00)**

Next Windows Administrator meeting is May 10. Kevin DeRoos (ADP) will chair and will discuss progress in the Exchange 2000 project.