Windows Administrators Meeting

January 10, 2003

Minutes (taken by Steve Kunz)

Meeting Started (9:05)

Announcements

- The "DHCP" problem (as discussed in last month's meeting) has been fixed. A solution to the "dropped or delayed" DHCP responses was implemented on Dec 13.

- No additional information is available at this time on site-licensing "Adobe Writer" (or similar products). [Linda Hutchison (AIT) was looking into that following the last meeting and I have no information from her as yet – SLK].

- Ordb – "Open Relay DataBase" (www.ordb.org) - has "blacklisted" our outbound mail servers under their "open mail relay testing service". The Ordb database list is used by some service providers (local ISPs) to block access to blacklisted mail systems. We have contacted (via email) Ordb to attempt to be removed from their list but remain on it at the time this document is being written. The end result seen by ISU email users is that mail SENT to certain email addresses (from mailhub) may bounce (or not be received) because the recipient's site honors the "blacklisted open relay mail server" list from Ordb.

Web Browser Opinions Follow-up (Kunz)

Kunz asked for follow-up feedback on the "Netscape vs. Mozilla" issue raised at the last meeting. There was very little discussion in the email list on testing of Netscape 7.0 and Mozilla. The Windows Scout-kits are in the "Advanced" area (Macintosh kits are still "in progress"). People at the meeting who expressed an opinion still felt Mozilla was the preferred web-browser to distribute. In all likelihood Mozilla will replace Netscape as the AIT-distributed browser.

Exchange 2000 Status (DeRoos – ADP)

The Exchange 2000 project continues to proceed. During the week of December 16 all user objects in Active Directory that were NOT "mailbox-enabled" (i.e. are not Exchange mail users) were "mail-enabled". In addition, all NEW Net-ID-based user objects are now created "mail-enabled".

The act of "mail-enabling" means that the Active Directory "targetAddress" attribute for the user object is set to something similar to "SMTP:joeuser@iastate.edu". [Additional info not presented at the meeting: A few other attributes are also set as follows: "mailNickname" to the user's "NetID", "legacyExchangeDN" to the proper

IASTATE Exchange Organization container name, “internetEncoding” to “1310720” and “MAPIRecipient” to “False” - SLK]

A question was asked (by Greg Wilson, Foundation) as to whether or not the “targetAddress” was going to be of the form “SMTP:joeuser@iastate.edu” if that person had forwarded their mail to somewhere else. The answer is “Yes” - the “iastate.edu” format will always be in the userobject attribute. Mail forwarding will occur as usual after the mail is direct to that address.

ADP has been carefully checking out the work done so far and will soon be setting up a “recipient connector agreement” for existing Exchange 5.5 users. For departments wanting to bring up new Exchange 2000 servers, they can probably do this as soon as ADP is confident that all work done to date is correct.

Open Discussion

Wayne Dowling (ECSS) commented that he as been receiving some email that does not contain the PerlMX (SPAM-detection) mail headers. He wondered how such mail bypassed the central servers. AIT staff indicated it probably came in via departmental servers that bypassed the PerlMX systems. Wayne Hauber (AIT) indicated that if he could be sent a copy of such a piece of mail (with ALL email headers included) the reason could be easily determined.

Jim Wellman (AE EM) asked if any more progress had been made on AIT offering an “ePO” (ePolicy Orchestrator) server that could be used by departments to “push out” anti-virus software and definitions to client systems on campus. Al Day (AIT) replied that Jeff Balvanz is planning a public meeting at the end of January to discuss just such an offering. [Watch the CCSG and WinAdmin email lists for an announcement of the date and time - SLK]

Kunz offered “protecting servers” as a discussion topic. There are many cases of automated password hacking, denial-of-service attacks, etc. being detected on campus. Several methods can be used to detect this. For password hacking one of them is as simple as analyzing the Windows security event logs on your Windows systems. Other “intrusion detection systems” exist. The question of how to protect Windows systems (both client and servers) from intrusion attempts resulted in a long discussion that indicated that several options are available.

Kunz indicated that one simple technique to protect a system from “off-campus” attacks is to move the IP-number to a “non-routable” address (“10.10.<n>.<n>”). In this way the system can be seen within the border-routers (including the Research Park) but not from “outside” on the Internet. Access via ISU PPP (dialup) would continue to work since the PPP server is “on-campus”. Since this is an “IP-number” change (not a “DNS hostname” change) clients on campus should see no difference, but off-campus probes and attacks against the system would be blocked.

Some departmental SNAP-servers (prone to network password-hack attacks) have used this technique.

Greg Wilson (Foundation) said they have contracted with “LightHouse” out of Des Moines” to firewall their site and monitor it. Greg could not quote the monthly price of the service but indicated it was below the cost of high-quality firewall hardware and it relieved their staff from learning and managing a complex firewall system.

Another option is to buy and configure a commercial hardware firewall box. This option tends to be expensive and requires a considerable amount of knowledge on “what to block” and “what to let through” (including knowing what hosts, protocols, and ports are needed on the protected system). Nobody in attendance was currently running a hardware firewall system.

Steve Schallehn (Telecommunications) indicated that Telecomm is considering a “campus wide offering” that departments could use. Steve noted that in the case of “firewall protection” there is generally not a single solution that fits all needs, and that a firewall is simply an “additional layer” in security.

Bill Frazier (AIT) commented that “personal firewall software” is an option. This software has the ability to block access to systems (based on host, protocol, port, etc) and is installed on each system to be protected. Common software is “ZoneAlarm”, “BlackIce”, and “Tiny Personal Firewall”. Software is generally less than $40 for “professional” versions for client systems (and some, like “Tiny Personal Firewall”, are free for individual use). BlackIce offers a “server version” for $400-500 per server (don’t install “personal firewall software” on servers without carefully testing first). AIT staff warned that “personal firewalls” can be effective but like hardware firewalls can be hard to configure correctly to allow desired services through. It is easy to break system functionality.

Kunz talked about a high-quality software firewall product already present on all Windows 2000 Server systems called “IPSec”. This standards-based facility allows a server manager to tightly control the access to all ports on the system. To get into the “IPSec” area on a server use “Programs->Administrative Tools->Local Security Policy” and double-click “IP Security Policies on Local Machine”. Three default policies are present (“Client”, “Server”, and “Secure server”) that can be “assigned” (activated) one at a time. BE CAREFUL and READ about IPSec before doing anything with it. You can easily lock out all network access to your clients. A great deal of information is available on the web about using IPSec on Windows 2000.

Jim Wellman (AE EM) raised a question as to why AIT did not provide documentation on the ports needed to pass through a firewall if we encouraged their use. A discussion ensued about the complexity of documenting all ports for all possible applications. It was argued that ports for common campus services could still be documented. Kunz indicated there was such a document available off AIT’s web site. [Additional information since the meeting: URL for this document is http://www.ait.iastate.edu/pubs/gst302/gst302.pdf].

Meeting Adjourned (about 10:05)

Next meeting is February 14.