Windows Administrators Meeting

June 11, 2004

Notes (taken by Steve Kunz)

Meeting Started (9:00)

Announcements

- AIT is experimenting with a Scout-kit for installing and configuring "Spybot Search & Destroy" version 1.3. This product scans for "spyware" (software that transmits personally identifiable information from your computer to some place in the internet without your knowledge). This kit, while "unannounced", is available in the "Advanced" Scout-kit area. If you would like to participate in evaluating this product, feel free to try it. There is no commitment on the part of AIT at this time to offer this product on a permanent basis (however, that is certainly possible depending on testing and feedback). Feedback can be provided to skunz@iastate.edu.

- NAI is public-beta-testing the next version of their antivirus product, VirusScan Enterprise Edition 8.0i. Departmental IT admins are encouraged to download the beta from NAI (http://www.nai.com/us/downloads/beta/mcafeebetahome.htm) and try it. This version has a considerable number of new features and options and AIT would like your input on how this package should be configured once it becomes our production version in the future. If you have any preferences or feedback on features that should be enabled/disabled/configured send email to antivirus@iastate.edu . AIT will be willing to host a group discussion on this product in the future if there is interest.

Fall Computer Inspection Project

Kunz briefly outlined the "Fall Computer Inspection Project". This project is a software product that residence hall people will use while NetReg'ing their systems this fall. Five areas of their system are will be examined:

1. Automatic Updates (they should be enabled)
2. Service Pack level (should be current one for the OS)
3. Critical Hotfixes (a subset of the most important should be installed)
4. Antivirus software (it should be there, be enabled, have current DAT files, and have had a fairly recent "full scan")
5. Weak passwords for local-system accounts (a "commonly used list" will be tested)

Upon conclusion of the tests (which currently run in about 10 seconds) the user is shown a web page indicating problems found and how to fix them. Clean and properly configured systems are presented with a “Congratulations!” screen. Only Windows 2000 and Windows XP systems are examined (all Win9x and WinNT systems will simply “pass all tests” since we have so few of them these days).

When introduced this fall the system will simply “inspect and instruct” but not disallow the NetReg’ing if problems are found. This is a “policy issue” that could not be implemented in time for fall. However, enforcement of “you don’t get on the network if your system is not in this state” is a goal that AIT is working toward. The first audience is “residence halls only starting fall 2004”, though the project scope may expand in the future.

Status Report on Domain Controller Upgrade Project

Kunz gave a status report on the Domain Controller Upgrade Project. A fourth domain controller named WINDC4 (running Windows Server 2003) was introduced on May 8. On Tuesday, June 15, WINDC2 will undergo a hardware/OS upgrade (again, to Windows Server 2003) during the morning. As previously announced in a email to the WinAdmin and CCSG groups, WINDC2 will be demoted from its domain controller role, the hardware swapped, and then it will be promoted to domain controller again. Later this month we will upgrade the operating system on WINDC3 (to Windows Server 2003). Finally, WINDC1 will have a hardware/OS upgrade sometime in mid-July. The final step is to switch the forest/domain to “Server 2003 Functional Level”, which we plan on having done by “the end of summer”.

Discussion of Why "RPC over HTTP" Is Not Offered (an Exchange issue)

Dave Orman (CNDE) raised the question as to why we do not offer/enable “RPC over HTTP”. This capability allows Outlook clients behind firewalls to communicate with Exchange servers over port 80 (HTTP). The response from Vince Oliver (ATS) was that ATS felt that VPN was the proper solution for such issues. Orman indicated that "RPC over HTTP" was simpler to set up than using VPN. Bill Frazier (AIT) indicated there were positive and negative aspects of "RPC over HTTP" that need to be discussed before a decision is made. ATS and AIT will consider the request.

Should We Block Remote Desktop/Terminal Services at Campus Border?

Vince Oliver (ATS) raised the question as to whether or not we should block Remote Desktop and Terminal Services at the campus border (similar to the NetBIOS and authentication blocking we currently do). The concern this would address is access to server “login windows” for hacking from off-campus. These services would still work when used with a VPN client. Several people in the room felt this would break needed functionality, since many times off-site staff on non-university systems use this functionality to get access to their desktop office systems or servers. A VPN client may not be available on the client system. The general consensus at the meeting seemed to be that we should not do this. The point was made that there are other ways to get a username/password prompt for such hacking and we cannot close them all (one way being the VPN client itself). Anyone having feedback (positive or negative) may send email to skunz@iastate.edu .

Security Issues

Kunz raised (again) several security issues that relate to policy settings on the Enterprise forest/domain. These are:

1. Allowing LANMAN/NTLM authentication
2. Allowing anonymous enumeration (RestrictAnonymous)
3. Retaining the SID-History

The level of encryption allowed on Windows authentication is currently fairly weak. We currently will negotiate for NTLMv2 and above, but allow LANMAN and NTLM if that is all the client is capable of. These "backward compatible" protocols are very insecure (almost "clear text") and Microsoft recommends you eliminate them ASAP. However, this will break functionality for anything using them (such as SNAP servers, Win9x systems, and WinNT systems prior to SP3). In our environment we probably cannot change our current domain policy but people should be aware they can tighten it down locally on their servers where possible. Most Win9x clients using authentication to shares or printers would need to install the "Directory Services Client" from Microsoft (free) which makes such systems use NTLMv2. More information is available at
http://support.microsoft.com/?kbid=239869
http://support.microsoft.com/?kbid=175641
http://web.mit.edu/ist/topics/windows/server/winmitedu/security.html

Allowing "anonymous enumeration" is another security issue which allows outside (unauthenticated) users to enumerate usernames and shares on systems within the domain. This information is the first stage in a hacking attack. Microsoft recommends the most restrictive value ("No access without explicit anonymous permissions"), however this will break some functions on older operating systems. The default setting allows all anonymous access (bad). Our current domain policy is a compromise between the two ("Do not allow anonymous enumeration of SAM accounts and shares"). While we would like to move toward the more restrictive setting we probably cannot do so without a good deal of "pain". For more information see
http://support.microsoft.com/?kbid=246261
http://web.mit.edu/ist/topics/windows/server/winmitedu/security.html

Storing the LANMAN hash and retaining the "SID-History" is another security issue. Microsoft says these should only be allowed as a "transition" tool to Windows 2000/XP and they should be removed/disabled ASAP. Many common hacker tools extract password hashes using these password stores and crack passwords easily. Again, disabling it breaks some older software products. For more information see
http://support.microsoft.com/?kbid=299656

It is VERY IMPORTANT to recognize the security holes the “backward compatibility features” introduce. You may be able (using the above and other information from Microsoft) to lock down systems within your OU much tighter than can be allowed on the Enterprise domain as a whole. It would be worth experimenting with.

Kunz talked about current thinking within Microsoft on “password complexity”. Microsoft currently recommends “pass-phrases” of twenty or more characters. These phrases should be easy to type and remember, but not “common” phrases everyone uses. An example would be “I took my dog for a walk on the Titanic at 2:00.” Research is showing that people with short but complex passwords find they are hard to remember and type, so they write them down and never change them. Also, any passwords shorter than 15 characters are easily cracked from the LANMAN hash (passwords longer than 15 characters are much harder to crack using that method).

Finally, Kunz talked about physical security for systems. He held up a “keyboard logger”, a small $30 device that captures all keyboard input when plugged between the keyboard and the system (hard to notice). “Social Engineering” combined with this device can compromise your powerful password when you login to such a system (which could be your own system in an insecure area). Software keyboard loggers are also readily available to those who can install software. Be aware of these devices when logging into any system in insecure areas or systems you do not own or manage carefully.

Open Discussion

(No time left for Open Discussion)

Meeting Adjourned (about 10:15)

Next meeting is scheduled July 9.