Windows Administrators Meeting
October 10, 2003
Minutes (taken by Steve Kunz)

Meeting Started (9:00)

Announcements

- Suspended NetIDs – Kunz (AIT) commented that a few OU administrators are finding that some NetID-based user objects are being "mysteriously suspended". If they "unsuspend" them (uncheck "Account is disabled" in the Account Options area) in their Windows OU, they get suspended again. This is probably because the NetID itself has been suspended at the ISU NetID level. The synchronization process forces the status of the NetID-based Windows user object to match the OU status. The suspension is most probably due to a departmental exception account was not renewed on July 1 (it is in the process of being expired). OU managers are reminded that you should not disable/enable NetID-based usernames within your OU as they will not continually be re-synched (see http://www.ait.iastate.edu/win2000/admin/UserMgmtInOUs.pdf). To check on the official status of suspension for any ISU NetID, use the "ShowUserDept.vbs" script (at http://www.ait.iastate.edu/win2000/admin/ShowUserDept.zip). If the term "[inactive]" appears at the end, you should contact the Solution Center to determine why the account is suspended.

- Windows 2003 Server on the Enterprise Domain Controllers – A few people have asked when the Enterprise root domain controllers will be moving to the Windows 2003 Server operating system. Kunz (AIT) announced that a hardware upgrade of WINDC1 and WINDC2 is being planned that will result in all Enterprise domain controllers being upgraded to Windows 2003 Server within a few months. Planned steps in this process are:

  1) Perform the necessary schema update
  2) Introduce an additional domain controller (WINDC4, on new hardware) running Windows 2003 Server.
  3) Introduce two replacement domain controllers (WINDC1A and WINDC2A, on new hardware) running Windows 2003 Server.
  4) Transfer infrastructure roles from WINDC1 and WINDC2 to WINDC1A and WINDC2A.
  5) Decommission WINDC1 and WINDC2.
  6) Upgrade WINDC3 to Windows 2003 Server (retaining the newer hardware).

  Note that this will result in the following final list of Enterprise domain controllers: WINDC1A, WINDC2A, WINDC3 and WINDC4.

- VPN Status Report – Steve Schallehn (Telecommunications) announced the VPN server is still available for testing to members of the CCSG group. There has been a delay in the public roll-out of this offering. There is discussion going on in the technical groups about the security of the username/password used to establish the VPN sessions (relating to Public/Private-key sessions). Telecommunications is working with Cisco on this issue.

- Exchange Status Report – Vince Oliver (ATS) gave a status report on the Enterprise Exchange organization work. ATS currently is well into their Exchange 5.5 migration to Exchange 2000. They have 1,578 mailboxes done with 610 left. CNDE and CARD are also well into their Exchange 2000 departmental upgrades. Any department with an Exchange 5.5 server that wants to move to the Enterprise Exchange organization without manually copying mailboxes later should contact Kevin DeRoos (ATS – kderoos@iastate.edu) ASAP.

- Wayne Hauber (AIT) announced that Mike Broders (AIT) is moving from the Solution Center to the MPC.

Hacked System Forensics (Wayne Hauber – AIT)

Wayne Hauber (AIT) presented a demo on system forensics that he uses to analyze and clean up compromised systems. This presentation included new tools Wayne has found (in addition to the steps outlined in his "Compromised System Forensics" document at http://www.ait.iastate.edu/win2000/admin/Forensics.pdf).

Many times IRC services or "pubstro" (FTP) services are installed on compromised systems to provide a "service" on the compromised system for their purposes. Copyrighted movies, music, and software are common files to deposit and serve off compromised systems.

Wayne started by talking about the use of "nmap" on UNIX system to scan individual systems. Wayne indicated a command like the following could be used:

```
nmap -v -p 1-65535 <host>
```

This will scan a given host on all possible ports to see what services are "listening" on that system. Common "valid" ports for Windows systems are 21, 23, 80, 135, 137, 445, 1372, 1373, and 5000. If you find a port that looks "suspicious" (not a common service port, such as 10001, 33333, etc.) then you should telnet to the system (from another system) to see what answers as follows:

```
telnet <hostname> <port-number>
```

Many times a hacker service will answer the telnet prompt and announce what service it is running.

Wayne said some very useful tools are available at www.sysinternals.com for detailed examination of compromised systems. Some good steps to follow are:

1) Turn on the display of hidden OS files and other hidden files and folders (using "Folder Options" applied to all folders by default).
2) Use "TCPView" (from www.sysinternals.com) to display the open service ports and locate the folder path to the binary supplying the service. Use the "Created" date (not the "Modified" date) to determine when that service was installed. TCPView is a very valuable tool allowing you to watch the activation of communication via "undercover" services back home to their installers.
3) Search for other files and folders created on the same date as any unwanted "undercover" services you find. See if they look like they are more recent than when the system was built (or when you added other valid services).
4) Search "by size" for large files (greater than a mega-byte). Sort the results by size and see what is there. Large numbers of movies and music files will show up on systems compromised to distribute illegal copies of such items. Software installers in one location that you do not own are another sign of "bad things".
5) Use "ProcessExplorer" (from www.sysinternals.com) as another tool to look at processes running on the system that should not be there. Examine where the binaries are. An experiment of killing a suspicious process to see what happens may be a useful experiment.
6) NetRegMon (from www.sysinternals.com) is useful to watch registry reads/updates as they happen.
7) FileMonitor (from www.sysinternals.com) is useful to watch file I/O operations as they happen.

Greg Wilson (ISU Foundation) asked what proactive measures people could take to avoid compromise in the first place. Wayne commented that normal "system hygiene" (keeping the system at current service pack and hot-fix level, current antivirus software, and in some cases firewalling the system) is always a good "first step". Group Policy activating automatic updates helps for AD-domain-member system. AIT is also investigating modifying the NetReg process to verify the state of the system before it is allowed to access the campus network.

Open Discussion

(No time remained due to another meeting scheduled in the room at 10:00 AM)

Meeting Adjourned (about 9:50)

Next meeting is November 14.