Windows Administrators Meeting

August 8, 2003

Minutes (taken by Steve Kunz)

Meeting Started (9:05)

Announcements

Frank Poduska announced that we were having some internet problems originating from outside campus this morning (and were continuing at the time this meeting started).

Windows Security and MS03-026 (Wayne Hauber)

Wayne Hauber (AIT) talked about what we have seen so far regarding the MS03-026 RPC vulnerability on campus. This serious Microsoft security flaw was detected and announced starting mid-July.

Wayne started by explaining the seriousness of the RPC vulnerability. Wayne indicated we had one AIT staff member do a "Google" search for the exploit and came up with a command line utility that quickly gave a "system context" command prompt on any non-patched system you pointed it to. He also stated that a preliminary scan of about 4,700 ISU Windows systems indicated that 38% of them were unpatched and vulnerable. Considering we will have thousands more (certainly unpatched) systems arriving on campus Aug 25 with the students, we are just at the leading edge of this issue. Wayne considers the situation for unpatched systems "very dangerous".

Talking about hacking communities in general, Wayne indicated there are two large groups that are threats to our systems. First are the "IRC" communities of organized hackers. These people want to place "pubstro" and "distro" access points (use "Google" for more info on these terms) on as many systems as possible, to serve as publication and distribution points for software, movies, music, etc. The second threat-group is simply "our students", some of whom are frustrated with the bandwidth limitations placed on the residence hall networks. In this case the students are looking for well-connected staff systems to "proxy" a network connection to, bypassing bandwidth limitations. For both groups the RPC vulnerability can be exploited to a great extent to achieve their goals.

Repeating information in a post to the CCSG and WinAdmin mailing lists, Wayne explained that the exploit merely "opens the door" to system compromise. It remains the system administrator's task to determine if the system actually HAS BEEN compromised. Several hacker tools for software serving (such as "serveu", "wupdated", and "firedaemon") are planted in various places on the system and hidden. Many times these tools do not require a great amount of skill to install or use.

Kunz commented that a link to a new document (based on Wayne's info) on "Compromised System Forensics" is available on the Windows 2000 support web page (in the "Security" section) at:

http://www.ait.iastate.edu/win2000/admin/Forensics.pdf

Kunz encourages anyone who is using forensic tools not covered in this doc to send email to Wayne (the email link is included in the document) so this can be an evolving document on how to analyze compromised systems.

Departmental admins (such as Mike Long from CARD and David Orman from CNDE) commented that systems that appeared to be a current critical hotfix level still showed they were susceptible to the RPC attack by the analysis tools. Kunz indicated that other people had reported the same evidence. This has been reported to Microsoft.

Kunz talked about Windows Update tools techniques. He indicated he has personally found it beneficial sometimes to use the "Windows Update" control panel and "turn off" automatic updates, and then immediately turn them back on. This seems to "reset" the checking on what updates are applied and which are not. Sometimes "lost" updates appear again after this action is taken.

Beata Pruski (AIT) remarked that if you delay in applying hotfixes and service packs, and then apply a great many all at once, problems may result (such as losing keyboard and mouse control). She also commented that Shavlik (http://shavlik.com) who provided the original "hfnetchk" utility used by Microsoft offers an expanded version of that product (still "for free"). They also offer hfnetchkpro (for a fee).

A question came up about the number of "authentication failures" that appear in system security logs. Kunz indicated that without VPN (and firewalling the university to block outside Windows file-sharing access) there will be many such entries. Enterprise intrusion-detection systems are actively detecting and blocking a wide range of outside (and inside) scans, account hacking, DOS, and intrusion attempts, but the limits on "what is unacceptable" means that a certain amount will be allowed through until they are block. Whenever VPN is a service (which allows off-campus systems to connect as "on-campus" via authenticated/encrypted means) the amount of "off-campus" intrusion detected will be greatly reduced.

Wayne Hauber went into more detail about forensic tools used to analyze a system for possible compromise. The Linux "nmap" utility can be used to see what ports a system is listening on. The command "nmap –v –p 1-65535 <ip>" will scan the specified Windows IP for all open ports. The same function can be provided on the Windows machine itself with the "fport" command. Suspicious ports can be directly telneted to, so see if a suspicious service answers the call. Wayne posted a document with these and other techniques in the mailing that went out Thursday to the CCSG and WinAdmin lists. Refer to the "Compromised System Forensics" document above, too.

Wayne Hauber asked what people felt about a policy (such as Microsoft enforces) that prevents systems without a certain base level of security and anti-virus protection from connecting to the network (using "Connection Manager" tools). Kunz expanded on the question and asked how people might feel about a regular "enterprise scan" for vulnerable systems (on a variety of fronts). Both these techniques are "two-edged swords", since many feel "any scan is bad". On the other hand "any compromise is bad". Little discussion ensued from the group.

Mike Bowman (AIT) asked if there were better ways for AIT to get out critical information to people other than what we are using. Mailing lists (CCSG, WinAdmin, MacOSX, etc) reach IT departmental admins, but that is a subset of the larger community of computer users. What about the AIT web page? The top level university web page? The "Inside Update" newsletter? Mass emailings? People with ideas on what would work can email mbowman@iastate.edu with their ideas.

Kunz concluded by indicating people that have concerns about systems that appeared to be compromised should contact Wayne Hauber (AIT) at wjhauber@iastate.edu. As this exploit continues to expand in scope we should expect Wayne to be very busy, however. People with policy suggestions or concerns relating to system blocking, information dissemination, etc. should contact Mike Bowman at mbowman@iastate.edu.

Meeting Adjourned (about 10:30)

Next meeting is September 12.