Windows Administrators Meeting

November 14, 2003

Minutes (taken by Steve Kunz)

Meeting Started (9:05)

Announcements

(None)

VPN Service Availability (Steve Schallehn – Telecommunications)

Steve Schallehn (Telecommunications) announced VPN service is currently available and considered in "full production mode". Windows Cisco VPN clients are currently available in the "Advanced" Scout-kit list and on www.sitelicensed.iastate.edu. Macintosh and Linux clients will be coming soon. Windows clients are the first to be released since Windows users are the most affected by the upcoming port blocks at the campus border (see next section).

To connect to the ISU VPN server a special "profile" must be used that contains a "group username and password". Scout will configure this profile into your VPN client for you after installation. For people manually installing from www.sitelicensed.iastate.edu, the "Required Profile" link contains the profile and instructions on where to place it to perform manual configuration. An ISU NetID and password (from the Enterprise "IASTATE" domain) must also be used to establish the VPN connection.

Diane Brotherson (ATS) asked if this was a "partial solution" (as she had heard). The answer was "Yes, in the future we will be changing to "certificate-based connection authentication". The "group username and password" will not longer be used, replaced by a certificate (from a new certificate server being installed by AIT). The ISU NetID will still be required with certificate-based connections.

A comment was made about whether the Windows VPN client would eventually move to the "Current" Scout-kit list. Kunz said this was debated within AIT but he was felt that since most people targeted by Scout are already "on-campus", it would not be appropriate to imply they should all use the VPN client to connect (by having it in the "Current" list). Steve Heideman (Chemistry) remarked that the warning Scout gives when installing "Advanced" kits may be too strong and cause people concern when installing "Advanced" kits. The current warning says these kits are "being tested" and you should "Use CURRENT software if at all possible". Kunz agreed and will change the Scout "Advanced" warning message in the future. Bill Frazier (AIT) commented that VPN Server resources are a concern when too many unnecessary connections are made. IP numbers devoted to VPN connections and server resources are the issue here.

Dave Orman (CNDE) remarked that a local firewall is installed with the Cisco VPN client and this may be one good benefit for on-campus use. Steve Schallehn (Telecommunications) remarked that wireless systems also represent a good on-campus use (since the VPN client will encrypt the traffic).

See http://www.ait.iastate.edu and click " Virtual Private Networking (VPN) Service Now Available" for the official announcement on VPN service availability.

New Windows Port Blocking at Campus Border Effective Nov 18 (Kunz, Lustgraaf)

With the availability of the new VPN service, AIT and Telecommunications will quickly block a few additional ports for security purposes. NEW port blocks effective November 18, 2003 are:

136-139 (UDP & TCP) NetBIOS Name, Datagram, Session services
445 (TCP only) Directory Services (Active Directory)
593 (TCP only) HTML RPC endpoint-mapper

People should note the above are ADDITIONS to the following existing port blocks (which have been in effect for some time now):

69 (UDP & TCP) TFTP
135 (UDP & TCP) DCOM RPC endpoint-mapper
4444 (TCP only) Slammer back-door

Kunz gave some statistics on why the additional port blocks are needed. Using statistics from the intrusion detection system on the three Windows Enterprise domain controllers, NetBIOS authentication failures were tallied from early December 2002 until now. During that time AIT saw:

1,229 unique hosts with a large number of authentication failures (hackers)
2,826,255 failures from those hosts (2,300 avg. hacks per hacking host)
Only 146 (11.9%) of those hosts were "on-campus" systems
Only 59,470 (2.1%) hack attempts came from those on-campus hosts

Kunz commented that these numbers would be MUCH larger if the intrusion detection systems managed by AIT had not been in place. In general once a scan is made for Windows systems and large-scale authentication failures begin to be seen, the offending host is blocked at the campus borders.

Using the above numbers it can be seen that most of the problem comes from off-campus hosts attempting Windows authentication ("good-guess common passwords", "brute force", or otherwise). Blocking these ports at the campus border will protect all campus Windows systems (whether they are members of the Enterprise Windows domain or not).

Jim Wellman (AE EM) indicated the information given out is very complex for the common user and it is difficult to tell if this affects them. Could AIT provide a list of applications that will be affected? Kunz (and others) commented the general statement “Windows file and print sharing” and “any application that uses Windows authentication” is the most accurate statement, since there may be many applications we don’t know about. It was agreed that announcement could be reviewed to make it more clear on who would certainly be affected by this change. Mike Bowman (AIT) will carry this comment back to the AIT User Services staff.

See http://www.ait.iastate.edu and click "Specific Traffic from Off-Campus Blocked as of November 18" for the official announcement on new port blocks November 18.

Jan 6, 2004 Kerberos 4 Shutdown and Security Tightening (Kunz, Hascall)

Kunz reminded everyone of the upcoming “security tightening” that will occur January 6, 2004. At this time clear-text authentication to FTP and Telnet sessions for AIT-provided services will no longer be allowed. In addition, the Kerberos 4 authentication port will be disabled (forcing “Kerberos 5 only” authentication). The recent upgrade of several Scout-kits relate to this security upgrade.

At a previous CCSG meeting the question was asked about what would be done for those people who use web-authoring products like “FrontPage”, “GoLive”, “DreamWeaver”, and the like. These products do not support encrypted authentication. The answer is in a new AIT-provided product called “KFTPD” (a “Kerberos FTP Daemon” proxy from University of Washington). Running KFTPD (available for Windows right now, Mac OS-X and other UNIX derivatives in the future) and configuring a clear-text FTP client to use it allows encrypted authentication. Windows KFTPD is currently available on the “Advanced” Scout-kit list.

John Hascall noted that remote XWindows access will be possible after January 6 using an XWin32 upgrade.

See http://www.ait.iastate.edu/security/encryption/ for detailed information on the Jan 6, 2004 Kerberos 4 shutdown and security tightening implications

Windows Domain Controller Upgrade Plans (Kunz)

Kunz gave a status report on the upgrade plans for the Windows Enterprise domain controllers. The upgrade project has been approved and the hardware upgrade of WINDC1 and WINDC2 is in the works. All three Enterprise domain controllers will be upgraded and a fourth domain controller (WINDC4) will be added. Conversion to Windows 2003 Server is planned (see previous month's minutes for more details).

Kunz reminded everyone the plan is to introduce two replacement domain controllers for WINDC1 and WINDC2 (WINDC1A and WINDC2A, on new hardware), transfer infrastructure roles from WINDC1 and WINDC2 to WINDC1A and WINDC2A, and finally decommission WINDC1 and WINDC2. This will result in WINDC1 and WINDC2 "going away". People should be aware that if they are targeting processes to specific IP numbers or hostnames belonging to WINDC1 and WINDC2 these processes will probably break when WINDC1 and WINDC2 are decommissioned.

Jim Wellman (AE EM) remarked that this would affect people with personal firewalls on systems, since you need to punch through holes to the domain controllers for domain authentication. Kunz agreed this may be a problem, but we will have several weeks when the old and new systems will both be on the network, allowing conversion time for firewalled clients.

Open Discussion

(Little time remained and no one had any pressing Open Discussion items to raise)

Meeting Adjourned (about 10:05)

Next meeting is December 12.