Global Information Assurance Certification Paper

Executive Overview

The network security stance of the Academies can best be described as "Ready, Fire, Aim!" As is natural with any young and rapidly growing organization, the Academies attention has been focused on its primary function: providing alternative educational opportunities for children with ADD and ADHD. Management's efforts have been busy developing facilities, recruiting teachers, attracting students, raising funds and putting into place the general infrastructure of the enterprise. With so much that needs to be accomplished, planning is done haphazardly, informally and with little thought. The consequence of this is that key steps required for orderly, thorough implementation are often missed.

The network security stance of the Academies is an excellent example of this. It was decided early on that it was desirable to provide Internet access to the students, email communication with the parents, and information sharing between the various locations. With limited time and funds the ramifications of these decisions were to a large extent overlooked.

For instance, while it was recognized that a firewall was necessary to protect the Akron school's internal network, there were no funds or internal expertise available to properly implement it. To meet the school's need it was decided to solicit the assistance of the Cleveland Linux Users Group to set up a Linux-based firewall. To their credit these volunteers did a reasonable job given their resources and technical background. Unfortunately, they made a critical error and left an unnecessary service running that leaves the entire network exposed to attack at the most damaging level.

At the same time the Academies recruited another volunteer with professional NT administration skills. However, this individual also lacked network security expertise and left another critical vulnerability that can be used to gain access to the highest levels of privilege on the NT network.

Taken together these two holes leaves the Academies completely unprotected from unauthorized access either from the internal network or the Internet. The good news is that no one seems to have noticed this yet.

To remedy these problems the Academies need to sit back, take a breath, analyze what has been done, and what needs to be done.

The first issue that needs to be addressed is to develop an Enterprise Security Policy. This policy provides the framework for all subsequent decisions pertaining to security concerns. It should state the purpose of the resources that the Academies have invested in, their appropriate use, the rights of the system users, the expectations of the Academies, and the consequences for misuse of the Academies resources.

A critical component of the Enterprise Security Policy is a Presumption of Privacy Statement. This document should define who owns the network resources and the associated information. It should clearly state whether or not the Academies would monitor users to verify that no inappropriate use is being made of the Academies resources.

After the policies have been established, the Academies networks should be reviewed to determine how well they conform to the stated policies. The configuration of each network should be analyzed to verify that sufficient protections are in place to protect the Academies.

An initial review of the Academies has been completed. In addition to the policy voids and security holes mentioned above, the following has been found:

- The current deployment of network resources provides little protection for the Academies.
- No enterprise-wide virus protection exists leaving the Academies open to infestation.
- Confidential information such as student records, medical backgrounds, and teacher's tests could be easily obtained without authorization.
- Inadequate incident handling procedures are in place leaving the Academies vulnerable to lost time and even lost data in the event of an emergency.
- No mechanism exists to determine if a security breach has occurred.
- The physical security of critical server resources is extremely lax. This is not only a problem for network security, but it also is a significant risk to the students and teachers.

The remainder of this document provides details supporting the above conclusions. A prioritized list of proposed corrective actions with budgets is also provided. It is strongly recommended that the Academies carefully review the issues uncovered and the solutions proposed. It is vital that the most critical problems be corrected at the first opportunity.

Like charity good security begins at home. Prior to connecting any other schools to the Internet, the suggestions contained within this report should be implemented.

Security Policy Overview

Corporate Security Policy

No formal corporate-wide security policy exists.

The informal policies that are in place recognize two groups of users: students and administrators/teachers. In the event that an activity has not been explicitly approved, it should be denied.

Students are granted limited access to the Internet for Web browsing and downloading files for classroom purposes only. The limits placed on the students rely upon Cybersitter and the teacher visually monitoring the student's activities. Additionally, students are also allowed to access an on-line multiplayer game – Wheel of Time.

Administrators and teachers are granted unlimited access to the Internet for Web browsing, file downloads, and email. No specific guidelines exist for what is deemed appropriate use except an informal understanding that the individual is expected to use discretion and to use the network resources in such a way as to not reflect poorly on the Academy.

Administrators and teachers are allowed the use of email primarily for the purpose of communicating with the parents of students. Since the email is hosted through Yahoo! mail services and not locally, no controls exist on actual usage. While teachers are free to communicate positive feedback to parents without review, they are expected to have any correspondence that may be considered controversial reviewed by the headmaster prior to transmission to the parent. Again, this policy relies on the discretion of the individual teacher and is virtually unenforceable.

Presumption of Privacy Policy

No formal presumption of privacy policy has been published and there does not appear to be a clear consensus as to what the Academies' position should be. This problem is compounded by the use of the free, public mail server because the ownership of such email accounts is ambiguous.

A good presumption of privacy policy should state the Academies' position regarding ownership of the network, systems, software, and data. It should also state if the Academies' would monitor a user's use of the system.

Communication of Security Policies

Consistent with the lack of formal security policies is the lack of any formal mechanism to educate the users of the network as to its appropriate use. Use of the Academies' network resources should be contingent on a statement outlining the Academies' policies signed by the user. Parents of students should also sign a similar statement covering appropriate usage for their child.

Security Policy Conclusions

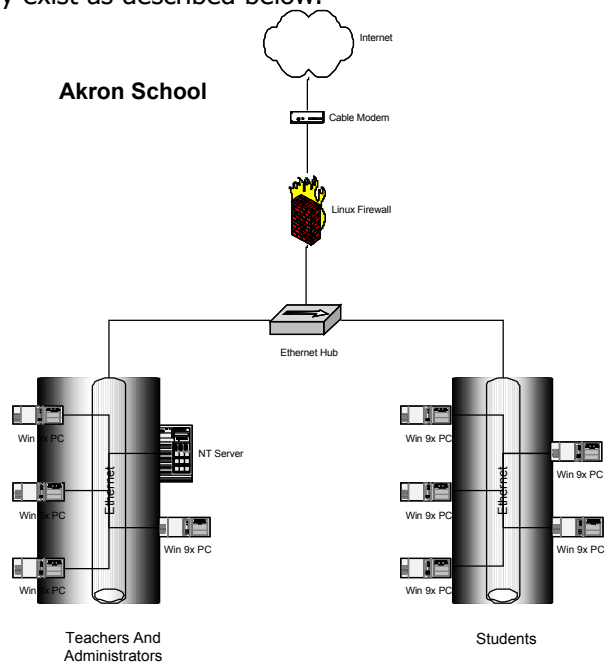
Without any formal security policies in place, the Academies are exposed to a large number of problems. Claims of harassment could be made if individuals improperly used the network to access sites that feature sexual, racially derogative, or hate-speech content. Further, a significant parental backlash could occur if it was discovered that students were visiting such sites.

Without clearly defined security policies it is also difficult, if not impossible, to take any

disciplinary action should any questionable activity occur. The Academies would be unable to assert that an action was inappropriate because it has not established what the network can and cannot be used for.

Network Overview

Two networks currently exist as described below.



The Akron School network is connected to the Internet via a cable modem. Because no router exists between the cable modem and the Linux server, a layer of defense is lost and the firewall must process every packet coming from the Internet.

A Linux server using ipchains to control network traffic protects the internal network. This means that the "firewall" is actually a stateless packet filter. While a lot of traffic can be blocked it is not as effective as either a stateful router or firewall. It is susceptible to mapping through protocol bending techniques such as FIN scans and penetration via fragmented TCP packets.

In addition to acting as the network firewall, the Linux server is also the Web server for the Academies. Currently, it serves up a very limited number of static pages reducing the security risk that this type of setup would otherwise represent. Should the web site be expanded, it is advisable that a separate web server be installed for this purpose.

The TCP ports open from the Linux server to the Internet are:

Port	Service
22/tcp	ssh
23/tcp	telnet
53/tcp	domain
80/tcp	http
113/tcp	auth
3128/tcp	squid-http

The telnet port was originally used for remote administration, but was replaced with Secure Shell (ssh). However, the telnet port was not closed when Secure Shell was installed. So while a more secure mechanism was put in place, the vulnerable one was left behind.

The auth (Identd) service identifies the owner of a TCP connection. Exploits are available that allow an attacker to gain root access by returning invalid data. Sendmail 8.6.9 is especially vulnerable to exploits against this service. Although sendmail is not running on this system, this port is not necessary and should be closed.

Domain services are running on the Linux server, but for no apparent reason. Because it is running Bind Version 8.2.1, it is vulnerable to an external exploit that will provide root access. This service should be blocked immediately and removed from the system.

The TCP ports open from the Linux server to the internal network are:

Port	Service
22/tcp	ssh
23/tcp	telnet
53/tcp	domain
80/tcp	http
113/tcp	auth
3128/tcp	squid-http

As with the external interface, the telnet port has outlived its purpose and should be closed, the Domain service should be closed and removed from the system, and the auth/identd port should be closed.

Internally, the NT server is used primarily as a file server. It provides user authentication for access to its own services. However, due to the fact that the workstations are all running Windows 95, the NT server is unable to provide much in terms of additional security for the network.

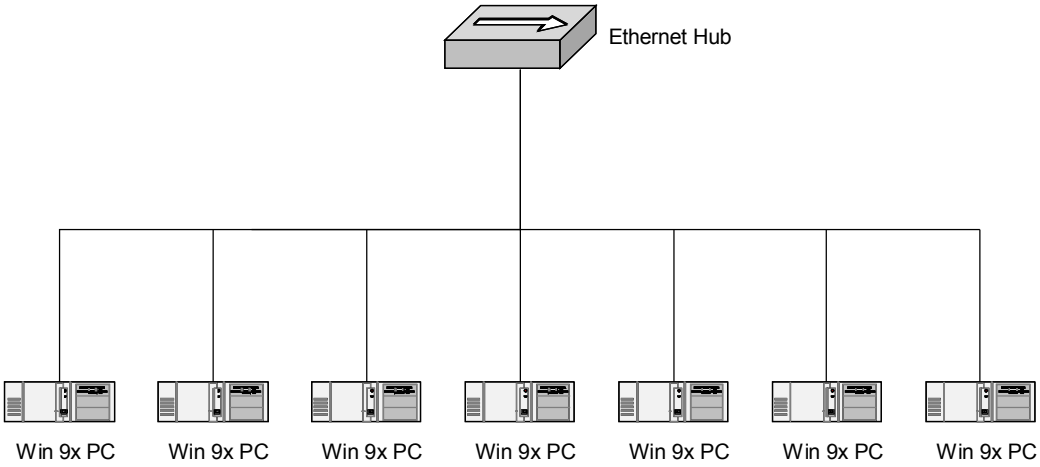
The TCP ports open from the NT server to the internal network are:

Port	Service
135/tcp	loc-srv
139/tcp	netbios-ssn
1032/tcp	iad3

The loc-srv port is used by DHCP to dynamically assign IP addresses to workstations on the internal network. Netbios is used by Windows to resolve system names to IP addresses. Therefore, they are necessary for operation. The iad3 service is usually used to bind TCP to another protocol such as X25. This service should be investigated further to determine the process that has this port open and whether it is necessary.

While it is the intent of the Academies to promote the use of a centralized file server, the teachers believe that storage of their files on an external machine diminishes the security of their files. While this is clearly erroneous, it points up the effect of the current lack of security awareness among the users of the network. The use of Windows 95 means that there is no effective security for the files being stored locally by the teachers. The lack of education regarding security policies and benefits leads the teachers to take a course of action that is diametrically opposed to the proper one.

Administrative Offices



The Administrative office has a simple Windows 95 peer-to-peer network. As such there is no security whatsoever. Access to the Internet is currently done via modems on individual workstations. No firewall security exists at any level. Hence, the Administrative offices are extremely vulnerable to penetration. Since files are shared amongst all PC's within the network, all workstations are exposed even if they are not directly connected to the Internet.

Future Network Plans

Investigations are currently underway to connect the Canton and Parma schools to the Internet and to upgrade the Administrative offices to a DSL connection. The most likely scenario for the Canton location is that it will have an identical configuration to the Akron school. The Parma school will probably be connected via DSL.

Aside from the different connection types, all locations will be configured in a similar manner with the same services being provided. With all locations having full-time connections to the Internet, it will be possible to share information amongst each facility. The most likely scenario will be the establishment of a centralized location for storage of student records. It would also be possible to establish a central mail server for all locations.

Network Summary

The Akron school is extremely vulnerable to being compromised. Security could be further enhanced through the installation of a border router to filter the most easily identified malicious traffic. Upgrading to the most current level of Linux will allow for the use of iptables that can provide stateful protection for the internal network. Any plans to increase the Web services provided should also include a plan to deploy them on a separate server that should reside on a screened sub-network separated from the trusted network.

The Administrative office is in strong need of security hardening. At the very minimum each PC that connects to the Internet should have personal firewall software installed. It would be even better if only one workstation made the connection and the rest of the network was

protected via Network Address Translation.

Before proceeding with connecting the new schools, the problems with the Administrative office should be dealt with. Disconnecting all individual modems, installing a single DSL connection and routing it through a stateful firewall such as Linux running iptables would be the best course of action. The configuration established for the Administrative office could serve as a template for the schools' firewalls.

System Overview

Operating system vulnerabilities

Akron Linux Server – Mandrake Linux Version 6.1

1. User Accounts.
   Several user accounts have been disabled, but still have valid shells specified. These shell specifications should be eliminated. RISK ASSESSMENT – Medium.
2. TCP Service Configuration.
   Several TCP services have been assigned to the wrong port. Their port assignments should be corrected on the off chance that they may be activated in the future. RISK ASSESSMENT: Low – services not activated.
3. File Permissions
   a. /etc/aliases has group and world read permissions – Used by sendmail to establish alternate mail identities for users. A race condition vulnerability existed on older versions of Linux. Also, it can be used to determine users on the system. RISK ASSESSMENT: Low – sendmail is not installed.
   b. /etc/exports has group and world read permissions – Used by NFS (Network File Systems) to specify which file systems to make available to client systems. RISK ASSESSMENT: Low – NFS is not installed.
   c. /etc/fstab has group and world permissions – Used to specify what file systems types can be used on the system. RISK ASSESSMENT: Low – non-administrators cannot modify the filesystem types for the system.
   d. /etc/rc.d has group and world read permissions – Used during the system boot sequence to specify processes and services to be started at boot time. RISK ASSESSMENT: Medium – provides valuable reconnaissance information.
   e. /var/run/utmp has group write permissions – Stores information regarding who is using the system. RISK ASSESSMENT: High – can allow for fake system log entries and modifications to system files.
4. Setuid Programs.
   Several programs relating to uucp (Unix To Unix Copy) have relative pathnames allowing for Trojan programs to be inadvertently executed with elevated privileges. RISK ASSESSMENT: Low – uucp is not used and the programs should be removed.

Workstation Operating System Vulnerabilities

The general use of Windows 9x on the workstations is a substantial vulnerability risk to the entire organization. Windows 9x is designed for personal not corporate use. Its file system is incapable of limiting access to authorized individuals, and it lacks basic user controls. It essentially offers no security and should be considered as compromised out of the box.

Configuration vulnerabilities

Akron Linux Server

The most critical configuration issue for the Linux server relates to the provision of domain naming services. Bind has a long history of vulnerabilities and should only be installed when necessary and never on a firewall. The version installed, 8.2.1, has published exploits in the wild that will provide root access to the server. This is the highest security level on a Linux server so the attacker will have gained complete control of the system. Since this service is so dangerous and is not used, it should be immediately removed from the system. The Academies' ISP has the professional expertise to manage DNS and is the best way to provide these services to the network.

Akron NT Server

The most critical configuration issue for the NT server is that null sessions have not been disabled. The same NetBIOS mechanisms that permit Windows File Sharing may also be used to enumerate sensitive system information from NT systems. User and Group information (usernames, last logon dates, password policy, RAS information), system information, and certain Registry keys may be accessed via a "null session" connection to the NetBIOS Session Service. This information is typically used to mount a password guessing or brute force password attack against the NT target. This issue can be quickly and easily corrected by correcting registry entries, and should be done so immediately.

Administrative Network

The most critical configuration issue for this network is the lack of any firewall protection on the PC's connecting to the Internet. Files shared within the network are therefore being made available to the Internet while any PC is connected to it. Quality, personal firewall software is available at little or no cost, and should be installed on any PC connecting directly to the Internet. When the permanent Internet connection is installed, it should go through a stand-alone firewall to protect the Administrative workstations.

Risks from installed third-party software

Game Hosting

The NT server is also being used as a game server for "Wheel Of Time" from GTI Interactive. The Tech Support pages for Wheel Of Time list several situations that can cause the game to crash. Although there is no documented security risk associated with these crashes, they can nonetheless represent a risk by potential exposing the content of the processor's memory. This may also be an indication of a buffer overflow that could be leveraged into a full-fledged compromise.

Also, according to the Tech Support pages, "Wheel of Time generates a lot more network traffic than conventional deathmatch games due to all the seeking missiles and defensive spells that can be used. A server should have enough processing power to handle bigger games. A P2-266 will host up to 4 players comfortably, but for more players you'll want a bigger system." Given these demands upon the server, consideration should be given to the appropriateness of using the school's primary server for game playing.

Yahoo! Email Hosting

Using a remote host for email services poses several problems. The first issue is that of ownership. Is it the individual's or the Academies' email? Without a clear answer to this question, it may be impossible to ensure that it is used in accordance with the Academies' policies. The second issue is the security of the email hosting service. There are many reports of security breaches at these free mail sites. Finally, there is the issue of availability in the event that the Internet connection is lost or the mail host goes off-line because of technical problems or denial of service attacks.

Security patches up to date

Akron Linux Server – Mandrake Linux 6.1

The following vulnerabilities have been identified and corrected by Mandrake since the release of Version 6.1 on September 17, 1999.

Mandrake Advisory	Package	Vulnerability
MDKSA-1999:012	lpr	Allows users to print files for which they don't have read permissions.
MDKSA-1999:013	screen	screen did not use Unix98 ptys (/dev/pts/*), which resulted in its controlling terminal being world-writable.
MDKSA-1999:014	wu-ftpd	Eliminates two potential buffer overflows, which could make the server execute arbitrary code if exploited. Corrected a memory usage condition problem where a user could make the server consume huge amounts of memory eventually rendering the system unusable.
MDKSA-1999:015	ypserv	Fixed a bug that allowed for all admins on a NIS domain to inject password tables into the NIS server. Prevents a user on a NIS domain from changing the login shell and GECOS information (real name, etc.) of other users. Eliminated a potential buffer overflow in the MD5 hash generation.
MDKSA-1999:016	am-utils	Eliminated a potential buffer overflow / remote exploit in the am-utils package.
MDKSA-1999:017	kvirc	Cures the "!nick ../../../etc/shadow" bug which allowed users to access to files they should be able to access.
MDKSA-1999:018	bind	Fixes numerous annoying bugs, ranging from execution of arbitrary code to remote crashing.
MDKSA-2000:000	nmh	Corrects a security bug in MIME headers parsing that can be exploited to trick mhshow into executing arbitrary shell code.
MDKSA-2000:00x	usermode	Eliminates a bug that could be exploited to provide local users with root access.
MDKSA-2000:002 MDKSA-2000:025	gpm	Fixes a bug that could be exploited to provide local users with root access.
MDKSA-2000:009	cdrecord	Eliminates a locally exploitable buffer overflow attack that could be exploited to execute arbitrary commands with the group id of "cdburner".
MDKSA-2000:010	bind	Corrected ownership permissions to limit the damage an exploit could do.
MDKSA-2000:011 MDKSA-2000:038	Xlockmore	Eliminated a buffer overflow in xlock that permitted a user to view parts of the shadowed password file.
MDKSA-2000:013	dhcp	Eliminates a vulnerability in it that allowed for remote exploitation by a corrupt dhcp server, (or an attacker pretending to be a dhcp server). This vulnerability could provide root access on the system running the dhcp client remotely.
MDKSA-2000:014	wu-ftpd	Fixed a function that could jump into shellcode pointed to by the overwritten eip and execute arbitrary commands as root.
MDKSA-2000:015	man	Fixed a problem that allowed the mode of any file on the system to be changed to 0700. Any file on the system could be created or overwritten as root. Local users could read any system file by forcing a copy of it into the whatis database.

MDKSA-2000:016 MDKSA-2000:023	inn	Eliminates a vulnerability that could be used to gain root access on any system with inn installed.
MDKSA-2000:018	dump	Eliminates a buffer overflow exploit in the restore program
MDKSA-2000:027	netscape	Data with a malicious design could allow a remote site to execute arbitrary code as the user of Netscape on the client system.
MDKSA-2000:029	pam	Fixes a problem with the pam_console module that incorrectly identifies remote X logins for displays other than :0 (for example, :1, :2, etc.) as being local displays, thus giving control of the console to the remote user.
MDKSA-2000:031	perl	Corrects a bug that made it is possible to execute a command using ~! passed in the script name to create a suid shell.
MDKSA-2000:033 MDKSA-2000:033-1 MDKSA-2000:036	netscape	Stops Netscape from being turned into a server that serves files on your local hard drive that Netscape has read access to allowing remote people to access them by connecting their web client to port 8080 on your machine.
MDKSA-2000:042	mgetty	Fixes a bug that allows malicious users to overwrite files on the system via a symlink attack which are owned by the user that is invoking faxrunq.
MDKSA-2000:045-1	glibc	Fixes a bug inld.so that could allow local users to obtain root privileges. Also, corrects found in the glibc locale and internationaliztion security checks.
MDKSA-2000:050 MDKSA-2000:050-1	sysklogd	Eliminates a "format bug" that makes klogd vulnerable to local root compromise, as well as the possibility for remote vulnerabilities under certain circumstances.
MDKSA-2000:053	traceroute	Corrects a bug in the traceroute program which causes segfaults and which could potentially be exploited to provide root privilege because the traceroute command is suid root.
MDKSA-2000:054	lpr	Fixes a format string bug in lpr when it calls the syslog facility that may allow a user to gain local root access.

Akron NT Server – NT 4.0 Service Pack 6a

The following vulnerabilities have been identified and corrected by Microsoft since the release of Service Pack 6a on November 30, 1999.

Microsoft Security Bulletin	Package	Vulnerability
MS99-055	Server	Eliminates a security vulnerability that could cause a Windows NT machine to stop responding to requests for services.
MS99-056	Syskey	Fixes a vulnerability that allows a particular cryptanalytic attack to be effective against Syskey, significantly reducing the strength of the protection it offers.
MS00-004	Rdisk	Rdisk creates a temporary file during execution that can contain security-sensitive information, but does not appropriately restrict access to it. Under certain conditions, it could be possible for a malicious user to read the file as it was being created.
MS00-005	RTF Files	Corrects a vulnerability that could be used to cause email programs to crash.
MS00-008	Registry	Release of a tool that installs tighter permissions on three sets of registry values. The default permissions could allow a malicious user to gain additional privileges on an affected machine.

MS00-052	**Relative Shell Path**	Eliminates a vulnerability that could enable a malicious user to cause code of his choice to run when another user subsequently logs onto the same machine.
MS00-070	**LPC Ports**	Fixes vulnerabilities identified in the Windows NT 4.0 and Windows 2000 implementations of LPC and LPC ports that could allow a range of effects, from denial of service attacks to, in some cases, privilege elevation.
MS00-083	**Netmon**	If a malicious user delivers a specially malformed frame to a server that was monitoring network traffic, and the administrator parsed it using an affected parser, it would have the effect of either causing Netmon to fail or causing code of the malicious user's choice to run on the machine.

Sensitive data storage procedures

Initially only data of limited sensitivity was stored on the NT server. However, as the Academy has developed, this situation is changing. Individualized Education Plans (IEP's) contain sensitive, confidential medical information for many students. It is a critical responsibility of the Academies to protect the privacy of this data.

Additionally, the teachers should be instructed to store their critical files on the central server. This data could potentially include student information, grades, and tests. Central storage on the server will go a long way in enhancing the security of this information. Encryption would add an additional layer of protection.

Data sent over the Internet

Currently, the only data originating from the Academies and traveling across the Internet is email. Since the email is primarily addressed to parents, it would be difficult, but not impractical, to set up encryption procedures. GnuPGP is a open source, free software package that could be used for email encryption. WinPT is a freeware product that could be used as a Windows front-end for GnuPGP. However, the support costs for this could be prohibitive.

As the other locations get permanent connections to the Internet, it would be beneficial to link the various locations. In this case encryption becomes imperative. The practice of sending encrypted data between two authenticated Internet servers is called tunneling. The proper name for the tunnel is a Virtual Private Network or VPN.

Three basic tunneling solutions are available to the Academies. Two, PPTP and SSH, can be implemented with the existing Linux servers. The third option would be to install a commercial VPN server in a screened sub-network attached to the firewall.

The primary advantage of PPTP is that it has been included in all Microsoft Windows products since Windows 95 so everybody has a client that supports it. Earlier versions from Microsoft were considered weak from a security point because of weak password hashing, an attacker could masquerade as a server, poor encryption implementation, and a clear-text control channel. Microsoft has since release an updated version that addresses most of these issues, but it is still considered weak because it is still vulnerable to off-line password attacks.

SSH has a long history of providing encrypted sessions over untrusted networks. Three versions currently exist: the original open source version (SSH1), a commercial version (SSH2), and a new open source version OpenSSH. SSH1 and SSH2 are incompatible with one another, but OpenSSH is compatible with both of the other versions. All versions of SSH are available at no cost to academic institutions. The primary benefits of SSH are strong encryption, port

forwarding, strong authentication, agent forwarding, and data compression. However, there are Trojan versions of SSH in the wild so it is important to get the distribution from a reliable source.

There's been an explosion of VPN products in the commercial marketplace. Some take the form of a network appliance that combines hardware and software into a single device while other products are software only. The primary advantage to the commercial VPN's is ease of management and better technical support. The primary disadvantage is that the commercial vendors often sacrifice cross-product compatibility in the pursuit of product uniqueness. Also, proprietary client software is usually required, and there is often a license fee for this software.

Anti-virus software protections

Anti-virus protection is done at the Academies on an individual basis with no enterprise-wide coordination. Each person is responsible for updating their own workstation. It is very unlikely that all PC's have up-to-date virus protection at any point in time.

The plus side of using Yahoo for email services is that it reduces the risks associated with an email borne virus propagating through the organization. However, it does not eliminate the risk of an individual PC being infected by email. Also, floppy disk drives are available at each PC. Therefore, it is possible for infected documents to be introduced either inadvertently or deliberately by inserting disks from the outside.

It is imperative that an enterprise virus protection mechanism be put in place. Virus infection is the most likely attack that an organization will suffer and is often used as the first beachhead in a compromise.

For best coordination, the primary server should be located at the Administrative office and secondary servers should be located at each school. The primary server would be responsible for updating each secondary server and the workstations at the Administrative office. The secondary servers would be responsible for updating the workstations at their locations. At a minimum updates should be done on a weekly basis with the capability of performing emergency updates if needed.

The need for enterprise virus protection will be heightened as the various locations are networked together and if an internal email system is installed. The integrity of each location is going to be dependent on the integrity of every other location. An attacker can use vulnerabilities in one system as a lily pad from which to spring to the other systems. And while VPN's provide secure channels of communication across the Internet, they are nothing more than trusted conduits from one system to another. They do not provide any protection from malicious actions originating at the opposite end of the tunnel.

Backup policies and disaster preparedness

A good disaster plan should identify the critical functions and resources of the enterprise network, identify the possible contingencies that may arise, develop response strategies, and have been tested and revised as needed.

Of these factors, the only measure that has been taken by the Academies is to develop a backup strategy. A full backup is done on a daily basis of the Akron school's NT server via Seagate Backup Exec. A backup is taken off premise each week. Aside from this backup procedure, there is no disaster preparedness in place.

Another issue that needs to be considered is where does the valuable data reside. Currently, much of the Academies' critical information is being stored on the teachers' workstations.

Therefore, the backup is the responsibility of each teacher, and it is unlikely that it is being done properly.

It is recommended that an enterprise backup procedure be put in place. First, the teachers should be required to store all dynamic or critical files on the NT server where it can be effectively backed up. Second, a backup of the standard configuration of each PC should be performed and stored. That way in the event of a system failure or corruption, the PC's backup can be quickly restored, and the dynamic information will be immediately available. Other critical resources such as the Linux server should be identified and included in the backup procedures.

Different contingencies entail different responses. A hard disk drive crashing on a workstation may only require restoring a backup. If the hot water radiator above the NT server bursts, it may be necessary to replace the server. And if an attacker compromises the system, the decision must be made whether to just restore the system to a clean state or to preserve the evidence of the attack for forensics and legal action. All these possibilities should be identified and planned for in advance.

It is strongly recommended that a centralized logging system be installed. Currently, it is necessary for someone to manually review each log on each system to determine if any problems have occurred. This task will become more difficult as the additional schools come on line. Reviewing logs is after-the-fact problem identification. Centralized logging assists in several ways. First, notification of the problem can be done on a timelier basis. Second, some logging tools also monitor performance metrics and can take actions such as warning an administrator if a disk drive fills up past a threshold level. Third, centralized logging tools can provide for various notification techniques based on the severity of the problem, the time of day and the day of week.

Finally, just as fire drills are conducted for the students, mock failures should be done as practice for a real incident.

Other issues/vulnerabilities

Physical Security

The physical security of the Akron school servers' needs substantial improvement. My visit was announced and expected, but I was nonetheless surprised by how easily I could gain access to the facility, server room and server without being challenged by anyone I encountered. I think this should be a critical concern for the security of the network, but also for the safety of the students, teachers and administrators at the school.

As a test of physical security, I chose to see at what point I would be challenged regarding my presence and purpose. I was able to walk in the front door, down to the ground level, through the school and to the server room without impediment even though I walked past several staff members. The server room was unlocked and unmonitored. I proceeded to connect to the network and worked for 30 minutes before my contact met with me. During that time several staff members came in, but no one made an attempt to verify that I was authorized to be in the building much less working on the system. At the end of my day, I could not find my contact so the computer lab was left unlocked and unmonitored.

The servers are currently in the same room as the computer lab used by students. A partition separates the servers from the lab. The computer lab door has a lock and all exterior walls appear to extend to a fixed ceiling. This allows the lab to be physically secured fairly well. However, the servers are poorly secured from individuals using the lab. A permanent wall

extending to the fixed ceiling and a locking door should be installed to prevent unauthorized access to the servers.

Similar criteria should be established for the server rooms of the other locations. Specifically, the server room should have permanent walls extending beyond any drop ceilings and doors that are locked at all times.

prioritized list of security vulnerabilities

1. No network security and presumption of privacy policy established. These policies provide the framework for the security stance of the Academies and define what actions need to be taken. A firewall is the implementation of the network security policy. It is not the policy itself.
2. A highly insecure version of bind is installed on the Akron school's Linux firewall that is exposing the entire school to a security compromise.
3. Workstations at the Administrative offices are connecting directly to Internet without any firewall protection thus exposing internal file shares to the world.
4. Null sessions are allowed on the Akron server's NT server. This makes it very easy to enumerate other points of potential vulnerability on the server that can lead to privilege escalation.
5. No enterprise-wide virus protection mechanism exists making it a virtual certainty that the Academies are not prepared to withstand a virus attack.
6. iad3 is running on the Akron school's NT server and the process that owns it is not known.
7. The Akron school's Linux firewall is not stateful which means it does not protect against stealth attacks that rely on bending protocol standards such as FIN scans and fragmented packet attacks.
8. The telnet and auth services are running unnecessarily on the Akron school's Linux server.
9. No reviews of system logs are being done.
10. Physical security for the Akron school is weak and poorly enforced.
11. Inadequate disaster preparedness.
12. Lack of an individual with basic security awareness.

A prioritized list of recommended fixes with budgets

1. Prepare a Network Security Policy. A basic questionnaire can be provided which will help gather the information required to formulate this policy. BUDGET: 8 – 12 internal man-hours for information gathering and discussion. 4 hours security consulting at $175/hour - $700. 1 hour legal review at $175/hour - $175. TOTAL ITEM BUDGET: $875
2. Prepare a Presumption of Privacy Policy. Sample policies can be provided for review and discussion. BUDGET: 2 – 4 internal man-hours for review and discussion. 2 hours consulting at $175/hour - $350. 1 hour legal review at $175/hour - $175. TOTAL ITEM BUDGET: $525
3. Remove bind from the Akron school's Linux server. BUDGET: 1 hour security consulting at $175/hour - $175. TOTAL ITEM BUDGET: $175
4. Install ZoneAlarm on the 3 Administrative PC's that connect to the Internet. BUDGET: 1.5 hours at $175/hour - $262.50. TOTAL ITEM BUDGET: $262.50
5. Eliminate null sessions on the Akron school's NT server. BUDGET: ½ hour security consulting at $175/hour - $87.50. TOTAL ITEM BUDGET: $87.50
6. Install InoculateIT Advanced Edition on each of the school's NT servers. BUDGET: (3) copies of InoculateIT at $695 each - $2085. 9 hours (3 hours/school) security consulting at $175/ hour – $1575. TOTAL ITEM BUDGET: $3660.
7. Determine reason iad3 is running on the Akron school and eliminate it if possible. BUDGET: 2 hours security consulting at $175/hour - $350. TOTAL ITEM BUDGET: $350
8. Upgrade the Akron's Linux firewall to Redhat Linux Version 7.0 and upgrade from ipchains to iptables. BUDGET: Redhat Linux Version 7.0 - $30. 4 hours security consulting for installation and system hardening (including elimination of the telnet and auth services) at $175/hour - $700. 2 hours security consulting for development of the iptables access control rule set at $175/hour - $350. TOTAL ITEM BUDGET: $1080.
9. Install a centralized logging system based on Event Log Monitor from TNT Software with a pager for after hours emergency notification. BUDGET: (3) NT servers at $329/each - $987. (3) Linux servers at $45/each - $135. (1) pager at $50. 9 hours (3 hours/school) security consulting at $175/hour - $1575. TOTAL ITEM BUDGET - $2757.
10. Enforce that the computer lab / server room is locked whenever no one is present to monitor the room. BUDGET: No expense involved - $0.
11. Develop incident handling plan. BUDGET: 24 hours security consulting at $175/hour - $4200. TOTAL ITEM BUDGET: $4200.
12. Send part-time MIS administrator to SANS Level One Security Essentials training. BUDGET: Course fee - $1,859. Airfare - $250. Hotel (4 nights at $179/night) - $716. Meals (4 days at $45/day) - $180. TOTAL ITEM BUDGET: $3005.

TOTAL BUDGET FOR ALL ITEMS: $16,977