



Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Securing the Network in a K-12 Public School Environment

In many ways, a K-12 public education data network will be designed and constructed in the same manner as any other business data network. While all business networks will have some degree of security built into them, a K-12 school environment presents special needs and requirements. It goes beyond the obvious items such as physical security, routers, sub-netting, firewalls, and anti-virus. These will be addressed as well, but we will be looking at several other very important issues, which incl...

Copyright SANS Institute
Author Retains Full Rights

AD



Securing the Network in a K-12 Public School Environment

Russell Penner
GIAC Security Essentials Certification (GSEC)
Practical Assignment version 1.4b, Option 1

October 25, 2003

Abstract

In many ways, a K-12 public education data network will be designed and constructed in the same manner as any other business data network. While all business networks will have some degree of security built into them, a K-12 school environment presents special needs and requirements. It goes beyond the obvious items such as physical security, routers, sub-netting, firewalls, and anti-virus. These will be addressed as well, but we will be looking at several other very important issues, which include privacy (confidentiality), data integrity, and content filtering.

There are laws in place regarding privacy and the confidentiality of student information. There are repeated concerns with students hacking into school data systems and modifying files. It is also a hot topic regarding having Internet content filtering within schools. We will be doing some comparisons between the United States and Canada in regards to these items. As well, funding always comes up in any conversation pertaining to the public school system, so this will be looked at too. Many decisions that are made are done within the confines of the available funding structure.

Enterprise network hardware

We are all used to seeing large data centres located behind locked doors, maybe even several doors, with alarms; possibly even with a security guard out front. Some of you may have even encountered this setting before starting to actually work in the IT world. What these people were subscribing to even then, was Law #3 of the Ten Immutable Laws of Security. It states "If a bad guy has unrestricted physical access to your computer, it's not your computer anymore"¹ (Microsoft).

However, much more than just the computer room portion of the data network needs to be secured. It extends to the other physical devices as well, such as the routers, hopefully located within a locked wiring closet, and with access for only a limited number of personnel.

Routers play a key role by transferring and routing all the data communication across the network in a proper mode. Each router maintains a routing table and Address Resolution Protocol cache, or ARP cache. ARP caches are mappings that correlate an IP address to a media access control, or MAC address². Routing tables contain a list of all the known hosts on both sides of the router. These are the two means by which a router is able to pass any data communication along to another router on another LAN, and out onto the Internet if needed. If the information within these data files was corrupted by an outside source, then in essence the network could be broken.

Routers are also used for segmenting the corporate network into smaller networks. This is done for security reasons such as isolating networks from each other and for performance reasons such as increasing available routes for data to travel, and increased bandwidth for users. This describes what would be “internal” routers, and you could also use a “border” router for connecting to your ISP³.

In addition to physical security for the routers, we also need to ensure the logical configurations within the routers are not open to attack and possibly compromised. We can achieve this by keeping up-to-date with vendor patches and ensuring there are complex admin passwords. It is also strongly suggested that you keep network configuration documentation current².

Another thing to mention at this point is whether it is a router, a server, a firewall, or many other network devices; they will work for you right “out-of-the-box”. However, these are very insecure default settings, as hackers regularly test for known factory default passwords and settings when they are scanning and probing networks⁴. Many times a system administrator may be rushed into putting the host device on the network. They plan to go back later and reset passwords and lock down the box, but for some reason they never get around to it. It is much better to follow best practices and make the needed changes including passwords, before the device is put onto the network.

Sub-netting

In many large networks the added security of breaking the enterprise’s group of allocated IP addresses into smaller sub networks can be very desirable. The application and data servers can be placed within different sub networks from where users are placed. Access rights can then be managed to control which users have access to what.

This scenario is especially relevant with a K-12 school environment. Within an individual school, staff and students should only have access to required resources and data. As well, in most cases there will be no need for students at school A to have access to resources at school B.

Also, in an effort to reduce your Internet visibility, and increase security, it can be advisable to use private IP addresses (or NAT). These reserved ranges of IP addresses are 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255, and

192.168.0.0 - 192.168.255.255. These private addresses are non-routable out onto the Internet, and provide an added level of protection.

Anti-virus protection

One concern that every data network, both large and small, will need to address is the issue of anti-virus protection. Over the past couple of years, some of the most damage done to enterprise networks has been by what is known as a mixed-threat attack. This would include attacks such as CodeRed and Nimda. There is a real possibility that one non-secure client workstation could impact or degrade the entire data network for the enterprise. It cannot be stressed enough that the most important item any system or network administrator can do is to stay current with security hotfixes and patches from their vendors.

Within a large K-12 public school board system, you could have several dozen different school sites, each of which may have hundreds of individual desktops. It would very quickly become an impossible task for an IT department to be able to manage each workstation separately.

The only reasonable way to keep control in an environment such as this would be to have it centrally managed. When the school board is reviewing possible solutions for data protection, they need to focus on an entire enterprise strategy. In all likelihood there will not be resources for additional staff to manage an anti-virus solution directly on the desktop. As well, a school environment is much different than a business one. Within many of the schools, there may be students who will actively attempt to circumvent the security efforts made on the desktop. It is also possible a staff member would try and disable software on their desktop, if they felt it would improve performance, or affect another application, or with a claim that it was interfering with student learning.

Unlike a typical business environment, the greatest threat for a K-12 network is from inside. In many cases there is very little consequence for the student who attempts to defeat the security settings on the network.

With any anti-virus software deployment, there should be a focus on a comprehensive solution. It should address the desktop, server, gateway, firewall, and email servers for example. This defense-in-depth approach is essential, as you cannot trust the desktop solution 100%. This is because users will bring their home laptops into their work environment, and schools in an effort to provide additional desktops to the students, will accept and install various donated computers of undetermined origin. With donated hardware in the environment, it is very difficult to have control on an asset management system because you do not always know what is on your network.

Desktop

Must be kept up-to-date and protected at all times with the anti-virus product. Should not be configurable by the user, but managed centrally for control. Try and ensure the desktop solution does not consume large amounts of resources. One possible resolution for desktop performance could be a terminal server / client solution.

Server

A large degree of security for a server can be obtained by securing the operating system and any applications that are being run on it. This however is not a “check once and forget it” situation. A continuous effort must be made as new vulnerabilities are discovered all the time, and new security patches are made available regularly.

HTTP

There should be real-time virus protection configured at the gateway, as many infections are as a result of downloads from the Internet. This can occur from an inappropriate website or from an ftp server, and can be accidental or purposeful.

SMTP and email

With everyone having an email address these days, virus writers have taken advantage of this popularity, and much of their code has been written so it can be distributed through this channel, and executed on the desktop. One of the ways of curtailing this within the corporate network would be to block all executable attachments such as .EXE, .VBS, .COM, PIF, CMD, and .BAT. This is also done to help prevent new viruses and worms that do not yet have a pattern file written for them, from spreading.

Firewall

Firewalls can be described as a filter for all network traffic between the company network and the Internet. They can be either a piece of software or hardware. We may want to consider two types of firewalls; firstly with a firewall to the external world called a border or perimeter firewall. There may also be consideration given to having internal firewalls, where we are protecting various enterprise servers from the internal users. These could assist in reducing or preventing internal data theft. In some environments the greatest threat is from inside the company network.

It is generally agreed that a properly configured firewall would be set to use a “default-deny rule”³. What that means is you would lock down all ports, and then open any desired ports as needed. The firewall would then block any unwanted traffic.

Additional consideration may be given to providing VPN access to remote users, in an effort to protect corporate data. An enterprise Intrusion Detection System (IDS), or an Intrusion Prevention System (IPS) are also considered by many sites, in their efforts to provide defense-in-depth security for their data networks.

Content filtering

Towards the late part of 2000, the United States Congress enacted the Children's Internet Protection Act (CIPA) ⁵. As of July 1, 2001 it became federal law. The requirement under this law was that schools were to adopt an "Internet Safety Policy". To continue to be eligible to receive certain federal funds, (E-rate and Title III technology funding) and discounted rates for purchases of equipment and services for accessing the Internet, schools would need to install filtering technology. A failure to comply could entail funds being stopped or even that funds already received would be required to be paid back ⁶.

A solution for Content Filtering can be either appliance-based or software-based. They both have their place in the content filtering arena. What may be applicable in your environment can be determined by size of your network, bandwidth availability, vendor support, degree of testing, and performance of several products, to name just a few. The products should provide some central management, and reporting tools can also be very valuable.

An appliance is an all-in-one "black box" that contains it's own software and databases. A software solution would need a separate server running a mainstream operating system, be it Windows, Linux, or Macintosh. One answer to "What is Internet filtering software?" is "software that is designed to enable organizations or individuals to block access to specific types of web content, which may be deemed inappropriate for a user or group of users" ⁷ (N2H2). The better products provide a degree of customization, thus allowing schools to add websites they deem to be objectionable, and categorizing them into groups. Categories that may exist already with the various products could include: Chat, Drugs, Games, Violence, Hacking, Free Mail, Pornography, Sex, Hate, and School Cheating Information.

The question could be asked; "Why manage Internet access". A stop at a popular website that monitors what words are entered into the most actively-used search engines will quickly reveal that the list of top word searches daily on the Internet prominently include searches related to sex, porn, games, MP3 downloads, and music sharing software. ⁸. A survey done by Digital Media Forum shortly before CIPA was enacted indicated that 92% of Americans polled indicated that pornography should be blocked on school computers ⁹. It is well-known and can be proven on any network that just a few workstations downloading MP3 files, or involved in a chat session can cause a performance impact on a corporate network. It is also possible that if a school district did not use content filtering, and minors were exposed to hate, violent, or pornographic content while at school, there could also be legal ramifications for the school district. There is probably a better chance for more productivity in the classroom if access is blocked to the websites that are not relevant to related subjects ¹⁰.

There appears to be a general consensus that content filtering be applied to K-9 classes. There is not nearly as much agreement with regard to high school students. It

is more of a recommendation, and some school sites do not filter all senior high students.

As an additional comparative note between the United States and Canada, at present there is not an equivalent to the CIPA law in Canada. Even so, many jurisdictions in Canada do apply content filtering within the K-12 environment.

Information Assurance

The fundamentals of data security need to be addressed by reviewing the three cornerstones of information assurance. Confidentiality, together with data integrity and system availability, is what makes up this troika.

System availability

The idea of system availability can be looked upon in some ways as an environmental issue. In an effort to ensure enterprise servers are available for the required amount of uptime to meet or exceed the Service Level Agreements (SLA), there are steps that can be taken to help achieve this. This can include purchasing (or leasing) servers that have hot-swappable redundant power supplies, mirroring your system disk when installing your operating system, and adding redundancy such as RAID 5 striping to your data drives. These kinds of steps can reduce the single points of failure that could cause a server to become unavailable. The ability to swap out a failed power supply, or a failed disk drive without turning off the server is very desirable. Having an available uninterruptible power supply (UPS) installed in a data centre, or in front of a critical application server can also serve to increase the availability of the network to the end users. Redundant network systems should also be considered, with additional routers and switches available in fail-over mode, in the event of hardware failure or a Denial of Service (DoS) attack.

Confidentiality

There are laws in place regarding what information about a student may be made available to a third party. In both the United States and in Canada there are federal laws that dictate the parameters to guide this. As well, there are state and provincial laws that are also designed to adhere to the respective federal statutes. In any corporation, there is a requirement that data be kept very secure, and measures are taken to ensure that is the case. It may be trade secrets that if released to a third party could be very damaging to the corporation. A similar concern is the case within a K-12 environment, and the student enrolment information.

In the United States, the Federal law that lays out the rights and permissions regarding the disclosure of student information is called the “Family Educational Rights and Privacy Act (FERPA)”¹¹. Within this document, parents receive certain rights to their children’s education records. These rights are subsequently transferred to the student when they turn 18 years of age. This document also outlines under what circumstances

data can be released to an outside third party, and whether or not written permission from the parent is needed. An example of when permission is not required could include when a student is transferring to another school. That school will require the education records of the arriving student. Other examples may include the need to comply with a legally issued subpoena, or for a potential college or university that may want to accept the student for an upcoming academic year. As well, FERPA states that schools are able to disclose phone numbers, addresses, and place of birth, of a student without permission. A school does however have to relate to the parents and students, on an annual basis, what their rights are under FERPA.

Any violations under FERPA, and the offending institution can lose all their educational funding. Individual states also have their own laws that may assist in compliance with FERPA, as well as individual educational institutions. One long-used practice of associating grades with an individual's Social Security Number (SSN) has been made illegal. According to a document posted at the website for Maricopa Community College in Arizona, internally identifiable numbers should be used for posting all student marks, or else the professors are to refrain from posting marks¹². This practice of using internal numbers is in wide use today.

Within Canada, the act that governs the release of any and all information is called "The Access to Information Act"¹³. This Act however, does govern more than just student information. Under Article 4 of this Act, The Right of Access; any Canadian citizen or permanent resident, has a right to be given access to information that is held within a government institution¹⁴.

Then within each province or territory of Canada, there are separate Acts governing privacy and freedom to information that have been signed into law, over the past several years. This listing can be found under the Department of Justice link for Access to Information and Privacy¹⁵. Each of these provincial access and privacy laws are titled in the vein of "Freedom of Information and Protection of Privacy Act", with slight naming variations from province to province. An example would be the province of Alberta, where its document is referred to the shortened title of FOIP¹⁶.

There were adjustments made to the provisions under Section 17 of the FOIP document during a 1999 review. These changes were directly in regards to student information¹⁷. What these changes indicated was that information previously available before FOIP was enacted; such as a list of graduates or members of a class photos, should continue to be so, and would not contravene the intent the FOIP. This kind of information was deemed to be part of the public domain. Unless a student has specifically requested this information not be made public, there would be no repercussions if it were released.

Any complaints regarding what was or was not revealed in relation to the FOIP guidelines are to be brought forward to the Office of the Information and Privacy Commissioner of Alberta (OIPC)¹⁸. There have already been cases brought forward to OIPC in regards to how and what information can be released within a school setting¹⁹.

To summarize, within jurisdictions in both the United States and in Canada, it is extremely important to what extent student data is revealed to a third party or the public in general. The rules and guidelines in place are for the protection and security of student enrolment information of children under the age of 18. Jurisdictions involved in the teaching of children in a K-12 environment must be cognisant of adhering to these rules in the day-to-day operations regarding student data.

Data Integrity

Student record systems need to be secure. There are regular reports in the news of a student or group of students who have breached the available security surrounding the data systems at their school and attempted to change marks; either for themselves or someone else. These incidents are reported on the evening news, in local and national newspapers, and of course in many online resources. A K-12 school environment or even a post-secondary one, are not immune to these attacks. These incidents are not limited to university students however, as many of them involve senior high school students and middle school students.

Entering the phrase “hacking school grades” into any browser will reveal thousands of links^{20,21}. In many cases there was an attempt by a current student to change marks, either their own or someone else’s. There is at least one case of a high school student in California actually changing his mark “downward”, taking his existing 4.0 GPA and turning it into a 1.9. This case was fairly unique however, as this hacking exercise was sanctioned by the school for a class project. The student was trying to prove the schools’ network was vulnerable and needed to be made more secure²². Sometimes several students are involved in the hacking episode²³. In some cases, a student hacker has charged other students money, for having their marks changed as well²⁴. In another case, not only did the hacking student charge multiple other students money for changing their marks, he also deleted thousands of other files off of the computer system that was hacked. The school district involved had to spend many hours in an attempt to recover this deleted data²⁵. Another high school in California has admitted they were unable to certify, or guarantee to the state, as to the accuracy of their attendance records or student transcripts²⁶.

It is contingent on each jurisdiction to ensure the data under their management is both secure as well as accurate.

Risk Analysis

Risk is inherent in many business processes, and the information technology industry has its share. When we assess risk, we need to look at it in terms of information assurance, and what the effects might be. We can use a risk analysis matrix to assist us in determining the impact or level of threat an action (or inaction) might cause us. You need to look at the level of vulnerability, and to what degree the threat poses, and what the impact might be. A possible question might be “What could happen to this

server if we apply this patch? And what could happen if we do not?" Decisions on the response can then be made dependent on the outcome of the analysis.

Exploits

The incidents involving students hacking into student record systems and changing marks may grab some of the headlines, but other exploit attempts are routinely made upon data networks everywhere, including the K-12 environment. With some of these exploits, many victims may not want to confess that they were successfully attacked. In what is often the case, the vulnerability existed for some time, and there was an available fix, or simple solution. Sometimes a patch may have been available for six months, or the vulnerability could even be an almost-forgotten security hole.

There are various kinds of exploits that can allow an attack to be perpetrated against a system. There are software bugs; with the security hole most often being a buffer overflow. Often due to short timelines to production, and the sheer number of lines of codes, a team of programmers are never able to discover and correct every vulnerable line of code before it is released to market.

Additional exploits include system configuration bugs such as default configurations, and having unnecessary services left running. If you put any Windows or Unix server on your network right "out-of-the-box" and do not lock it down in a secure fashion, you are leaving yourself very vulnerable. This goes as well for leaving services you are not intending to use, still running on the server. It is considered a best practice if you disabled the unneeded services, as these can also leave possible holes.

Some typical security holes can easily be found with web server attacks, flaws in CGI scripts, and lately in the news; web browser attacks. These can be with Java, ActiveX, HTTP headers, or JavaScript for example. As well, Denial of Service (DoS) attacks can be made against a network at any time.

Other ways for exploits to be made against a network could include allowing users (or even lazy administrators) to use easy-to-guess or even blank passwords, or for an attacker to use social engineering to obtain a password for a different user.

System administrators need to be always vigilant. They need to continue to apply security patches, use best practices, request that users are trained properly, and stay abreast of the changes and challenges that occur regularly in the IT field.

Impact

Even short outages due to a successful attack can have an expensive impact on a data network. Whether it was a loss of revenue, loss of reputation or credibility, or just a "simple" inconvenience for an hour or two, there is a cost. Within many schools there is a limited number of PCs available in the computer labs. With no prior warning, if students are unable to access their assignments online, or access the Internet to follow

along during a class, when can this class catch up with their school subjects? The lab is booked for the next class already, and the affected students are supposed to be going on to their next class as well. Also worthy of mention are the dozens, or hundreds, maybe thousands of employees that were unable to do their jobs during the outage.

Cost Effectiveness

Within a K-12 public educational environment, cost will always be an issue. There is never going to be an unlimited amount of funds available, be it for products, software, or even staff resources. With the source of monies being from the taxpayer, either in the form of government funding, or even fundraising, there is often the need to do more with less. One of the more effective ways to approach this concern is to request an educational discount, when approaching a vendor in regards to their products. Many vendors desire a presence in the community, and will often provide deep discounts in an effort to gain a foothold within another public education institution.

As well, there is also the concern with justifying the expense. Many school boards have multiple platforms of operating systems, namely Windows, Apple, and some flavours of Unix for example, running within their environment. This is not unusual in itself, as there is a heterogeneous nature in today's networks. It may be advisable however, to reduce the number of versions of different OSES to be supported. Many IT departments within the K-12 world are not overly large, due to the fact that dollars spent on IT are sometimes seen as dollars that could be better spent in the classroom instead. Sometimes some hard questions need to be asked such as "how many versions of Windows (or Unix) can we realistically support?" with the resources available.

Until recently, it may have been OK to use desktops running Windows 95 within the classroom setting. Often times these were legacy desktops, and this was done to increase the number of available PCs in the classroom. It has not been advisable for some time however, for this platform to be used in the administrative setting. This was due to the inability to lock down the OS, and the concerns with the security of data and also privacy issues. Now that Microsoft is dropping support for Win95, it is no longer advisable to even have this OS in the classroom²⁷.

There is always going to be a focus on whether or not the results of the expenditure will be directly realized in the classroom. Consideration may need to be given to looking at some automated solutions. There is not going to be the opportunity, or the ability, to continually purchase the "best-of-breed" in every situation. However, responsible decisions will need to be made in order for the K-12 network to be made as secure as possible.

Conclusion

Within the parameters of the resources available to a K-12 educational institution, all effort must be made to ensure it is operating in a secure environment, regarding the

data stored and created within its domain. Many concerns are the same as any other business data network. There are however, some unique challenges and efforts that need to be made within a K-12 public school environment. We need to at all times, protect the information available about a student. We have seen where some actions that are taken by the system, are dictated by federal law, in regards to the welfare of minors. Some actions are due in part to best practices. There are also some other actions dictated by available funds and staff resources, and the struggle to find an even balance.

Regardless of the funds available, due diligence needs to be taken to provide multiple layers of protection, or redundancy, within this environment. This effort is called defense-in-depth, and the application of this strategy is still very fundamental to a safe and secure K-12 network.

References

1. Microsoft Corporation, Microsoft Security Response Center, "The Ten Immutable Laws of Security", - URL: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/esays/10imlaws.asp> (October 25, 2003).
2. Ruth, Andy., and Hudson, Kurt., with Microsoft Corporation. January 2003. "Security+ Certification Training Kit", Microsoft Press, Chapter 4: Network Infrastructure Security.
3. Pastore, Michael. "Security+ Study Guide", February 2003, Sybex. Chapter 3: Infrastructure and Connectivity.
4. McClure, Stuart., Scambray, Joel., and Kurtz, George. "Hacking Exposed: Network Security Secrets & Solutions, 4th Edition", McGraw-Hill Osborne Media. Chapter 9: Network Devices.
5. United States Congress, The "Children's Internet Protection Act" (Pub. L. 106-554), (CIPA document), (It is part of the House Appropriations bill H.R. 4577. It may also be cited as the Miscellaneous Appropriations Act, 2001) URL: http://www.fcc.gov/wcb/universal_service/chipact.doc (October 25, 2003).
6. St. Bernard Software. "The Internet Access Management Solution of choice used in Education and Libraries, iPrism v3.4". July 2003. URL: http://www.stbernard.com/products/docs/ip_education.ppt ., pgs 4-7. (October 25, 2003).
7. N2H2, Filteringinfo.org. "About Internet filtering". URL: <http://www.filteringinfo.org/about.php> (October 25, 2003).

8. Wordtracker. "Keywords to improve search engine placement and ranking. Find top internet marketing keywords". URL: <http://www.wordtracker.com> (October 25, 2003).
9. Bridis, Ted. "Congressional panel says no to filters". The Wall Street Journal Online, October 18, 2000. URL: http://zdnet.com.com/2100-11_2-524852.html (October 25, 2003).
10. St. Bernard Software. "The Internet Access Management Solution of choice used in Education and Libraries, iPrism v3.4". July 2003. URL: http://www.google.ca/search?q=cache:IKikNaVsvmsJ:www.stbernard.com/products/docs/ip_education.ppt+%22why+manage+internet+access%22&hl=en&ie=UTF-8 (October 25, 2003).
11. U.S. Department of Education. ED.gov, "Family Educational Rights and Privacy Act (FERPA)". URL: <http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html> (October 25, 2003).
12. Office of General Counsel, Maricopa Community Colleges, Arizona. "State Law Prohibits Use of SSNs". URL: <http://www.dist.maricopa.edu/legal/dp/inbrief/ssnprohibited.htm> (October 25, 2003).
13. Department of Justice Canada. "Access to Information Act (R.S. 1985, c. A-1)", URL: <http://laws.justice.gc.ca/en/A-1/index.html> (October 25, 2003).
14. Department of Justice Canada. "Access to Information Act (R.S. 1985, c. A-1)", Chapter A-1, Article 4, Right of Access. URL: <http://laws.justice.gc.ca/en/A-1/8.html#rid-97> (October 25, 2003).
15. Department of Justice Canada. "Access and Privacy Laws and Commissions Canadian Provinces and Territories". URL: <http://canada.justice.gc.ca/en/ps/atip/provte.html> (October 25, 2003).
16. Government of Alberta, Canada. "Freedom of Information and Protection of Privacy". URL: <http://www3.gov.ab.ca/foip> (October 25, 2003).
17. Government of Alberta, Canada. "Freedom of Information and Protection of Privacy". Bulletin Number 4: Disclosure of Personal Information. (revised October 2003). URL: http://www3.gov.ab.ca/foip/guidelines_practices/bulletins/bulletin4.cfm#Does (October 25, 2003).
18. Office of the Information and Privacy Commissioner of Alberta. "OIPC home page". URL: <http://www.oipc.ab.ca/home/> (October 25, 2003).
19. Office of the Information and Privacy Commissioner of Alberta. "OIPC Order F2002-010". URL: <http://www.oipc.ab.ca/home/DetailsPage.cfm?ID=1073> (October 25, 2003).

20. Google. I used a Google search for “hacking school grades”. URL: <http://www.google.ca/search?q=hacking+school+grades&ie=UTF-8&oe=UTF-8&hl=en&btnG=Google+Search&meta=> (October 25, 2003).
21. Microsoft Corporation. I used an MSN search for “hacking school grades”. URL: <http://www.msnsearch.com/results.aspx?q=hacking+school+grades&FORM=SMCRT> (October 25, 2003).
22. Legon, Jeordan. CNN. “Student gets ‘A’ for hacking school computer”. December 18, 2002. URL: <http://www.cnn.com/2002/TECH/internet/12/17/student.hack/> (October 25, 2003).
23. Akizuki, Dennis. The Mercury News. “High school suspends student hackers who changed grades”. March 6, 2003. URL: <http://www.siliconvalley.com/mld/siliconvalley/5335721.htm> (October 25, 2003).
24. Ananova. Orange. “Hacker charged \$5 a time to change grades on school computer”. June 6, 2002. URL: http://www.ananova.com/news/story/sm_602783.html?menu=news.technology (October 25, 2003).
25. Quinn, Kevin. ABC13 Eyewitness News. Security News Portal. “Yet another Student jailed for allegedly hacking school’s computers and changing grades”. May 20, 2003. URL: <http://www.securitynewsportal.com/cgi-bin/cgi-script/csNews/csNews.cgi?database=JanZ%2edb&command=viewone&id=65&op=t> (October 25, 2003).
26. Jones, Donna. Santa Cruz Sentinel. “Hackers threaten confidential student records”. May 28, 2003. URL: <http://www.santacruzsentinel.com/archive/2003/May/28/local/stories/05local.htm> (October 25, 2003).
27. Microsoft Corporation. “Windows Desktop Product Life Cycle Support and Availability Policies for Businesses”. (Updated October 22, 2003) URL: <http://www.microsoft.com/windows/lifecycle.mspx> (October 25, 2003).



Upcoming SANS Training

[Click Here for a full list of all Upcoming SANS Events by Location](#)

SANS Singapore 2009	Singapore, Singapore	Jul 06, 2009 - Jul 11, 2009	Live Event
SANS Rocky Mountain 2009	Denver, CO	Jul 07, 2009 - Jul 13, 2009	Live Event
SANS SOS London 2009	London, United Kingdom	Jul 13, 2009 - Jul 18, 2009	Live Event
SANS Future Visions 2009 Tokyo	Tokyo, Japan	Jul 15, 2009 - Jul 17, 2009	Live Event
SANS IMPACT 2009	Kuala Lumpur, Malaysia	Jul 27, 2009 - Aug 01, 2009	Live Event
SANS SEC563: Mobile Device Forensics Debut	Baltimore, MD	Jul 27, 2009 - Jul 31, 2009	Live Event
SANS Boston 2009	Boston, MA	Aug 02, 2009 - Aug 09, 2009	Live Event
SANS Atlanta 2009	Atlanta, GA	Aug 17, 2009 - Aug 28, 2009	Live Event
SANS WhatWorks in Virtualization and Cloud Computing Security Summit 2009	Washington, DC	Aug 17, 2009 - Aug 21, 2009	Live Event
SANS Virginia Beach 2009	Virginia Beach, VA	Aug 28, 2009 - Sep 04, 2009	Live Event
SANS SCDP SEC556: Comprehensive Packet Analysis - Sept. 2009	Ottawa, ON	Sep 09, 2009 - Sep 10, 2009	Live Event
SANS Critical Infrastructure Protection at Oceania CACS2009	Canberra, Australia	Sep 10, 2009 - Sep 11, 2009	Live Event
SANS Network Security 2009	San Diego, CA	Sep 14, 2009 - Sep 22, 2009	Live Event
SANS SCDP Cutting Edge Hacking Techniques - June 2009	Ottawa, ON	Sep 15, 2009 - Sep 15, 2009	Live Event
SANS WhatWorks Summit in Forensics and Incident Response	OnlineDC	Jul 06, 2009 - Jul 14, 2009	Live Event
SANS OnDemand	Books & MP3s Only	Anytime	Self Paced