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.

Acceptable Security on Public Access Computer Workstations in Public University Libraries

Providing highly secure workstations in public university libraries requires defining what is acceptable for the working environment and determining what types of security can be implemented to compensate for lesser security at lower layers at the workstation level. I evaluated, analyzed, recommended and implemented changes for the enhancement of a computer lab workstation in one public university library.

Copyright SANS Institute
Author Retains Full Rights

AD

Acceptable Security on Public Access Computer Workstations in Public University Libraries

A Case Study

Name: Cheryl Lytle

Certification: GIAC Security Essentials Certification (GSEC)
Version 1.4b, Option 2

Date Submitted: May 8, 2004

.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Abstract

Providing highly secure workstations in public university libraries requires defining what is acceptable for the working environment and determining what types of security can be implemented to compensate for lesser security at lower layers at the workstation level. I evaluated, analyzed, recommended and implemented changes for the enhancement of a computer lab workstation in one public university library.

Overview

I evaluated current acceptable computing security for a public access workstation in a public state university library with an open computing and teaching lab. Courts have held that public libraries are to offer free and open communication. However, this is "subject to reasonable restrictions as to the time, place, and manner for doing so." [1] Determining what security restrictions are reasonable depends on the specific overall network environment or set-up at the university library and adherence to library principles.

I analyzed the security of a desktop lab PC, running Windows XP Professional, Service Pack 1. Unfortunately, there are several issues common to university libraries which prevent them from hardening the lab workstations as much as would be desired. Instead, my major focus was on improving layers of security before the workstation and evaluating what was acceptable risk on the workstation.

I set up a centralized virus update system to ensure that all lab PCs were adequately protected from virus or worm infection. I deployed a patch-management system that centrally applied operating system-security patches. One problem with the patch-management system was reporting. A centralized imaging, patch-management-reporting and inventory system software was invoked by a team member of the library computing support staff. This allowed a review method of the patch-management system. From analysis of various tools, some recommended improvements to the security of the workstation were determined and are being evaluated. In addition, information on the degree of threat and a clearer picture of how the security compared, to highly secure stations was obtained from the reports I ran from Tenable Nessus Windows Technology; NeWT and The Center for Internet Security Windows Security Scoring Tool (CIS scoring tool). Training of end users was increased. Quality of staff training on security issues was enhanced. Other factors, such as

[1] "Guidelines and Considerations for Developing a Public Library Internet Use Policy." American Library Association Issued June 1998; rev. November 2000. URL:http://www.ala.org/Template.cfm?Section=Other_Policies_and_Guidelines&Template=/ContentManagement/ContentDisplay.cfm&ContentID=13098 (2004).

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

enhancements at the university level in security have also contributed to improved protection. Currently, with the above implementations, downtime due to viruses and operating system vulnerabilities on the workstations has been reduced.

Current acceptable security for the workstations was determined by evaluating the results of the tool reports included in this paper against how the lab is used. This will be discussed in more detail in the following pages. However, since currently acceptable security requirements can change, library system administrators should monitor the workstations frequently to determine any changes in the effectiveness of the security policies. Some suggestions on ways to monitor are:

- Monitor event logs on workstations and active directory for suspicious logins at the workstations.
- Run the list of tools discussed in this report and check for any increases in threats. Evaluate whether changes could be made to increase the security and decrease the threat.
- Keep track of all maintenance done on the workstations, what was done to fix the problem, and what kind of changes could be made now to prevent having to fix the problem in the future.

Before Issues

The goal was to evaluate current acceptable workstation security risks given all the issues facing the public university computing and teaching labs. There are some commonalities among library computer networks that make them attractive targets for hackers.

Anonymity for users of lab workstations in the library is common. “Few public libraries assign specific user accounts to patrons accessing network resources. Almost all assign some generic account for public users. While this makes network administration easier, it also makes use of the network totally anonymous.”[2] There may not be any way to know who sent the latest security threat from the public computer. Also, there may not be any way to trace the sender of harassing e-mail sent to members of the university community. However, all these activities can be traced to the library computer used for this dangerous activity.

> Some attackers will break into a library network just to build a "nest." If they can succeed in gaining administrator rights on a library computer connected to the Internet, they can store software tools on its hard drive. From this computer they can launch more aggressive attacks against other computers and networks on the Internet. Generally, these attackers

[2] Williams, Robert. “Computer and Network Security in Small Libraries.” Texas State Library and Archives Commission. 2001.
URL: http://www.tsl.state.tx.us/ld/pubs/compsecurity/index.html (2004).

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

also store tools allowing them to cover their tracks. Any subsequent investigation dead-ends at the nest, your library's computer. [3]

In addition, the hacker community generally considers libraries easy targets. "Libraries, especially within universities, have the reputation of lacking the security-conscious systems administration staff that operates the computers of other types of computing organizations." [4] The perception of lax security at the university library, whether true or not, means the public workstation may be a target. Due to the perception created by this situation, system administrators are under increasing pressure to make everyone authenticate. However, we must provide computer access to persons from other campuses and members of the local, non-university community.

Besides, the fact hackers are attracted to university libraries, there are various other issues facing public university computing. The transition in the past decade from dumb terminals to fully networked/multimedia workstations has placed extra burdens on university library budgets to allow for increased training and resource allocation for security. However, computers in a public library must also adhere to library principles of public service, user privacy and legal access.[5]

The varied clientele of the university library — public, students, faculty, and staff — can be in conflict with their computing and security needs from one network computing lab. In addition, the patrons of the university library have come to expect the workstations to be available for long hours of use with minimal interference from computer-support administrators.

Protecting information on behalf of the unsuspecting patron is the library's job. Patrons expect their checkout and use privileges to remain private, for use by them only. This is an example of confidentiality. However, if security is too restrictive, the experiences of the user can be frustrating and will have a negative impact on use of the lab. The CIA triangle has various sizes for these different groups (CIA: Confidentiality, Integrity, Availability).[6] For example, library staff may have greater needs for confidentiality, while a patron from the university community may have less information he is concerned about keeping private. Federal Content Filtering Laws have further complicated decisions libraries must make in Internet use. In the past, courts have indicated a public library has

[3] Williams, Robert. "Computer and Network Security in Small Libraries." Texas State Library and Archives Commission. 2001.
URL: http://www.tsl.state.tx.us/ld/pubs/compsecurity/index.html (2004).

[4] Fore, Julie. "Things that go Bump in the Virtual Night." Library Hi Tech. 15 (1997):84-91

[5] Ayre, Lori. "Library Computer and Network Security." Infopeople Project. February, 2003.
URL: http://infopeople.org/howto/security/
The Infopeople Project is supported by the U.S. Institute of Museaum and Library Services under the provisions of the Library Services and Technology Act, administered in California by the State Librarian. (2004).

[6] Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. "SANS Security Essentials with CISSP CBK." The Sans Institute. 2003:pg.295.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

limited access with regard to the First Amendment's intellectual freedom, meaning public libraries offer free and open communication subject to federal, state and local governmental laws on what material is obscene, child pornography or "harmful to minors." Moreover, the legal framework and context of regulation is rapidly changing; federal, state, and local governments have begun to legislate specifically in the area of library Internet use.[7] The American Library Association openly suggests its members actively oppose legislation that exposes them to new liabilities and negatively impacts intellectual freedom.[8] However, what is considered acceptable use and acceptable viewing on library workstations will continue to change.

Of all the workstations in the department, the library lab workstations are the most likely computers to be quarantined on the network due to security problems. Before this analysis was done, I did not have a clear picture of what was the effective security on a lab workstation. I wanted a security snapshot of what was happening when a patron sat down to use a workstation in the computer lab, so that we could truthfully answer any patron's concern: How secure are my communications when I work in the lab? I will describe various tools used to analyze the risks on this computer and will discuss virus and patch management. Education is critical among users and staff; training that supplements the efforts of policies and specific workstation security will be evaluated. The paper follows by discussing briefly other factors in workstation security. In the conclusion, acceptable security risks will be discussed.

Virus/Patch Updates During/After

The first concern was for protection against malware: viruses, worms and trojans. Considerable resources were being spent on troubleshooting virus problems. The lab workstations had antivirus programs on them and were set to automatically update, weekly. This allowed us time to evaluate each update before it was installed. However, there was no way of being confident that the definitions were up to date without physically going to every workstation and checking. One wayward station could become infected and cause problems for the whole lab. Other departments on the campus had used Symantec System Center to manage antivirus client workstations with good success. With approval from management this was set up not only on the workstations in the lab, but throughout the department. This greatly reduced the amount of time/labor spent by the computer support group. At one location, you can now monitor the workstations, initiate a scan, and get the history and the version definition date of the virus updates. There is one known security risk with the centrally managed

[7] "Guidelines and Considerations for Developing a Public Library Internet Use Policy." American Library Association . Issued June 1998; rev. November 2000. URL:http://www.ala.org/Template.cfm?Section=Other_Policies_and_Guidelines&Template=/ContentManagement/ContentDisplay.cfm&ContentID=13098 (2004).

[8] "Guidelines and Considerations for Developing a Public Library Internet Use Policy." American Library Association . Issued June 1998; rev. November 2000. URL:http://www.ala.org/Template.cfm?Section=Other_Policies_and_Guidelines&Template=/ContentManagement/ContentDisplay.cfm&ContentID=13098 (2004).

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

software, but so far it has not affected the performance of the software for us. There appears to be a hashed console password for every campus server in the registries of the clients. This means every department on campus is vulnerable to an intruder breaking into the centrally managed server. Answers from Symantec have indicated this is by design so that clients are aware of the centrally managed server. However, the password hash has DES encryption.

All the computer lab workstations have had Microsoft operating systems. Currently, the operating system is Microsoft XP Professional, Service Pack 1. In the timeframe I have been working to improve security in the lab, concerted efforts have always been made to stay with the latest operating systems. However, the same problems that plagued virus updates affected the patch updates for the operating system. Even though the workstations were set to automatically update themselves from the Microsoft website, there were many inconsistencies because there was no centralized configuration point for the updates. Also, there was no way of verifying what patches had been applied or even if they had been applied, without physically going to the workstation. The end result was that we used the "sneaker network" to run around to each workstation and make sure it was patched. Two changes were enforced which improved this situation.

1. We migrated to a Windows 2000 domain with active directory which allowed us to implement group policy objects (GPO/GPOs). A departmental SUS (software update services) server was set up. Group policies were implemented for the computer lab which allowed the workstations to automatically connect to the SUS server, download approved patches and reboot if necessary. If there was a workstation we did not want to update for some reason, we could easily remove it from the group policy; if a new workstation was brought up, it could be easily included. The SUS server also has the added benefit of an administrator centrally controlling explicitly what hot fixes clients are permitted to download. With automatic or Windows Update, this was not possible. We set up the GPO, so that clients would check the SUS server nightly, for new patches.
2. A second issue with the patch-management system was the need for a reporting function. The Microsoft Baseline Security Analyzer tool can be used, but we found it tended to freeze up in graphical mode when analyzing several workstations at one time. We evaluated several systems, but decided to purchase and implement a product used at other departments in the University. The Alteris package offered the most capabilities for our system given the cost of the product. It has some basic reporting capabilities for software installed, along with several other features which we use in the maintenance of the computer lab. If the hot fix shows up in the add/remove programs feature of the Windows XP control panel, then it can be queried from the Alteris package.
    a. A side issue with the Alteris package is the ability to push out updates to machines. This can be used for all sorts of updates,

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

including other-than-critical updates for Windows OS packages as well as other software updates.

Workstation Analysis During

Virus updates and up-to-date patches go a long way toward securing a workstation; however, they are not enough. I evaluated the actual security on the workstation in three areas:

1. What were the current effective security settings on the workstation? This involved items such as policies and security settings. What actually happened when a user logged onto a workstation?
2. How did the lab workstation's effective security settings compare against highly recommended standards for securing a workstation?
3. What were other types of vulnerabilities or risk factors that existed because of weaknesses in security such as open ports?

For an equal comparison, I performed all the tests and ran all the reports on the same workstation in the lab.

To determine the effective security settings on the workstation, I used Microsoft's Group Policy Management Tool, Report 1, for a current view of the effective security settings on the workstation. Please note, this report did not list the local security settings on the workstation. Instead, it only listed GPOs. Workstation security is a combination of GPOs from the active directory, and the local security settings and local group policy, both on the workstation. (Note, local group policy can be set as a GPO through active directory but it is located on the workstation.) If there is a difference on a particular setting for two different security settings, the GPO always wins. (e.g., The GPO says minimum password age on the workstation is 90 days, but the local security policy or local group policy says 0 days, the GPO wins with 90 days.) In addition, the default order of precedence follows the hierarchical nature of the active directory: sites are first, then domains, and then each OU (organizational unit). [9]

Overall, there are five GPOs currently, being applied, and one not being applied.

For users:

- A few account policies are set.
- Extensive auditing is going on.
- A few security options are set.
- Extensive software settings to prevent the Blaster Worm infection are set.

Administrative Templates:

- Several network/system settings are set, including a setting to allow the users to create their own security certificate.

Users/Administrative Templates

- Each workstation environment is very tightly controlled with regard to desktop and application settings.
- The policy is also being applied every 10 minutes.

[9] Microsoft Windows XP Professional Product Documentation. "Step-by-Step Guide to Understanding the Group Policy Feature Set." 2004.
URL:http://www.microsoft.com/windows2000/techinfo/planning/management/groupsteps.asp

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

I used the CIS scoring tool (Report 2) to compare the lab's security settings against a standard. The tool gives a score out of a possible 10 points. The criteria used for scoring are divided into four categories: (1) Service Packs and Hot Fixes, (2) Policies, (3) Security Settings (all, including local security settings), and (4) Available Services, User Rights, File and Registry Permissions, and Other System Requirements.[10] The workstation received a low overall score. Even in the hot fix area, which I thought would be higher with the patch-management GPO, there were missing patches. However, when reviewing the report, the two critical patches that were missing, which the tool checked for, were both released before the patch-management GPO went into effect. Also, one of these patches was for the Blaster Worm infection, Microsoft patch Q833330, which as mentioned earlier a GPO is preventing anyway. Another reason is that the tool is checking for all critical and important hot fixes. We install all critical hot fixes only. The patch-management system is used by all stations in the department and not just the group of managed stations in the computer lab. What is considered important could vary by individual settings on the workstations throughout the department. When I installed the other critical patches the score went up.

In the policies area, as seen earlier in Report 1, the workstations do not have a substantial amount, with the exception of logging. We are currently logging:

- Account logon events. Success, Failure. This has to do with logon requests.
- Account Management. Success, Failure. This includes any sort of maintenance to accounts, such as password changes.
- Directory Service Access. Failure. This is a general category and has to do with any time a user changes an active directory object.
- Logon event. Success, Failure. This is different from account logon events in that it is triggered anytime someone logs in or out of the system.
- Policy change. Success, Failure. These changes are triggered when someone makes a change to policies, such as user rights or audit policies.
- Privilege use. Success, Failure. This logs special rights assignments use, other than an administrator.

We are not using any sort of logging server and currently do not have the manpower to keep up with the analysis of the logs, so while the logs are valuable, they are not being used as they should.

The security settings area received some points in the major security settings area for "restrict anonymous." Giving a DWORD value of '1' to the "restrict anonymous" key limits the access Microsoft's null user can have. The null user is an automatically generated account used by key Microsoft processes, even though it is an account with no credentials. Without restriction, it can enumerate

[10] Shawgo, Jeff and Faber, Sidney "Windows XP Professional Operating System Legacy, Enterprise, and High Security Benchmark Consensus Baseline Security Settings." Version 1.1.3 March 17, 2004. The Center for Internet Security.
URL: http://www.cisecurity.org 2004.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

account names and shares, among other things, which is a major security concern among administrators.

In the available services area, a lot of these changes cannot be made because minor changes could affect performance on the workstation, since this lab is a teaching lab as well as an open computing lab. The classes being taught here often include various technologies and software applications. This requires a certain amount of freedom and access to the operating system, which may be at odds with specific security settings. Other items cannot be changed because of the nature of the internal Windows network. For example, NetBIOS currently needs to be enabled within the domain to allow users to map to their network servers by the name instead of the IP address. Even though the workstation is on a Windows 2000 domain, there is still reliance on a Wins server, which needs NetBIOS. (There is an out-of-forest trust with another library which currently can be set up only with the aid of a Wins server.) However, in some instances changes which cannot be made in the library lab can be made at the university border. In the example above, NetBIOS ports 135, 137-139 are being blocked at the university border. When NetBIOS ports are not blocked, users can obtain much information from the workstation, which can be exploited by attackers. Because the ports are used for file sharing, they can be used to get data by unauthorized individuals. These ports are often called “Scanner Bait” ports. Port 139, file and print sharing, is particularly vulnerable. In addition, NetBIOS creates additional traffic on the network. Because we cannot block this traffic at the workstation at this time, an increased burden is placed on other security levels and a need for heightened awareness by the user at the workstations.

I used NeWT vulnerability security scanner (Report 3) to determine the workstation’s type and level of risk, compared to the low score it received with the CIS scoring tool. The scan was done from one lab workstation to another, internal to the network. Since this was only done internally, it did not take into consideration any security set at the University border which prevents some of the scanning to get through. Even then, most of the vulnerabilities were low.

Workstation Analysis/ After Recommendations

It is important that administrators be aware of how policies are applied on the workstation. This can be provided in security training for staff. A suggestion would be to have all similar security policies between workstations made through GPOs. Local group policies can also be viewed through active directory, if they are set up as GPOs. This would allow a centralized view of computer lab polices through the active directory of the domain. Local security policies are useful if there is a need to have security policies which are not dependent upon a network, to be implemented, as group policies through active directory are. They may also be useful if there is an isolated security setting specific to one workstation. In this case, the processing time of adding another GPO may cause more work than is necessary. If local security policies are going to be used

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

extensively, a tool should be evaluated which would look at all policies on a workstation and not just GPOs.

As mentioned earlier, there is a lot of log analysis being set on workstations through GPOs. Log analysis on one workstation is probably all that is necessary at this time, or it could be rotated and set through local security settings. A detailed log analysis tool would be beneficial. Currently, personnel resources do not allow for extensive log analysis at each workstation. As mentioned earlier a log server or logging analysis software should be looked into as an alternative. Also, with auto logons enabled at the workstations, extensive analysis of logs would only tell what was happening and not who the culprit was.

GPOs do use processing time on the server, therefore documenting and rating the importance of each policy and what computers or users it affects is necessary. Redundancy and overwritten policies are a waste of server resources.

The patch-management GPO is working; nonetheless, the next time workstations are re-imaged, a check will be made to ensure they are caught up with the pre-SUS server patches. All password and account policies that are being evaluated with the CIS scoring tool really cannot be set any tighter at this time. This would require a major adjustment by patrons, support personnel and management, none of whom are ready to make changes now. I feel this is an acceptable risk given the current purpose and usage of the lab, but, I would like to see more analysis of the workstation security logs.

In the vulnerability scan (Report 3) I evaluated any risk factors that were greater than low. There were four of these and they were all medium risks.

1. The first item was an SMB server that was running on port 445 (plugin ID: 11011). An SMB server is the server service running on a workstation. SMB stands for Server Message Block. It is a protocol which enables file, printer, and serial port sharing. I am evaluating the possibility of removing this service on a workstation. However, this port is being blocked at the University border and use of this port would only be internal.
2. The second item (plugin ID: 10394), involved setting the “restrict anonymous” registry entry to 1. This is something we are doing and was reported on Report 2. Additional investigation showed there was an additional registry key that needed to be changed to ‘1’, to prevent the same type of vulnerability. This registry key is: HKLM\System\CurrentControlSet\Control\Lsa\EveryoneIncludesAnony-mous
3. The third item (plugin ID: 11618) indicated the remote host does not discard TCP SYN packets which have the FIN flag set. This means that a vendor’s hardware or software is not properly handling TCP packets that are sent to it. This may result in an improper connection from a host and

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

an attacker.[11] From the CIS scoring tool report there were three registry entries under the security settings section which should prevent this from happening. I have made these changes and so far believe they will be a good change.

4. The last item involved NetBIOS, and as previously discussed this cannot be filtered or disabled internally, but is blocked at the University border. This policy will be re-evaluated, as plans to eliminate a reliance on Wins and NetBIOS are implemented.

Finally, I looked over some of the other low-risk items and determined if there were any changes that could be made. However, since the risks were all low, I considered them acceptable. Several dealt with NetBIOS, which were eliminated, while several others had to do with finding out information about the host or network, through tools such as traceroute. Since many network tools are run on the network to monitor traffic or troubleshoot campus-wide networking, including traceroute, I did not want to disable or correct any of these vulnerabilities.

- The vulnerability of (plugin ID: 10201) is being protected at the University border, by blocking IANA addresses (Internet Assigned Numbers Authority). These are IP addresses that are of special use. For example, they may be used on an internal only network, but would not appear on the public network. An external user to the network may try to spoof one of these addresses in order to gain access to a network.
- (Plugin ID 11935) indicated the workstation was enabled to do Internet Key Exchange, which is typical of a VPN server (Virtual Private Network). However, I did not agree with this deduction. The reply was sent back on port 500. Lower numbered port numbers are usually assigned, so I needed to find the PID (process ID) to identify what process sent the response. At the workstation, I ran the command, netstat –ano, which identified the PID. I then opened Windows Task Manager and saw that the process is a Windows process called lsass.exe. This is a necessary process to run Windows operating systems; hence I will not kill the process.
- (Plugin ID 10884) is a network time protocol and is also necessary for Windows and other applications. There are some alternative programs to NTP; however I do not consider the risk significant enough to invest the time in using another program.
- I am evaluating (plugin ID: 11765), a Windows registry change for TCP helper.

[11] Finlay, Ian A. "Vulnerability Note VU#464113 TCP/IP implementations handle unusual flag combinations inconsistently." U.S. Cert. Revision 89. May 30, 2003. URL: http://www.kb.cert.org/vuls/id/464113. (2004)

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

To maintain this level of security, all of the above tools should be run periodically, spot checking workstations to make sure we are aware of any changes or enhancements to security that should be implemented. The following are some times when it would be beneficial to re-run the tools:

- whenever there is a change in security settings for a workstation, whether it is a local setting or GPO
- whenever a new image is created for the workstation
- when there is an audit performed at the university level, requiring a check of the security settings to see if there are enhancements that can be made to be more in line with audit settings
- at the very least at each semester change, if it has not been done earlier at one of the instances above

We might also interview staff and patrons to determine what their knowledge of security in the computer lab is and if they feel comfortable with it.

Education During/After

Managing library computer and network security is multifaceted. It involves all users and staff of the library. Security training is critical to successful, acceptable security. "Security training isn't like learning a software application. It's not a step-by-step thing, and it's not skill gained by repetition or judgment. Security training is more a process of familiarization." [12]

Currently, for all users of the computer lab, the lab rules and policies are published on the default home page for browsers with the default login. During this study, additional rules and policies for the University were linked from the library workstation lab page.

There is also a student help desk which is manned when the lab is open. Since the lab is in an open area, the help desk person can constantly monitor, review and answer questions of any patron who is using a workstation. Due to the constant and heavy use of the computer lab, it would be very difficult to have an organized training session for every user of the computer lab. An idea for the future would be a desktop that shows a link to the security policy page, so that the user would never miss the policies. There is some monitoring at the University level on all computers of the University network. Notification is given in the University Policies and Procedures.

There is a separate training session for all new hires in the library computer lab area. This has been enhanced during this study. Some of the items covered include:

- While lab workstations are not backed up, authenticated patrons of the computer lab store their information on library servers that are backed up.

[12] Williams, Robert. "Computer and Network Security in Small Libraries." Texas State Library and Archives Commission. 2001.
URL:http://www.tsl.state.tx.us/ld/pubs/compsecurity/index.html (2004).

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

    - How to operate the backup software, report any problems and store all tapes in a safe and secure location is important to the usage of the workstation for these users.
        - This includes double-checking the process to make sure all backups of software/data are being done.
- Other training information for staff relates to guidelines for making sure sensitive information isn't inadvertently compromised. Some examples include:
    - Keep all passwords secret.
    - Keep network configuration information confidential. Obtain permission before revealing information to a third party.
- Monitor computer lab patrons for inappropriate use of the computer lab, and enforce the policies of the library and the university.
    - Currently the lab workstations do not have any Internet filtering software on them, since they are considered workstations for professional work only and not for use by children. The lab's acceptable use policy parallel's the University's view of illegal use of University owned equipment or use which is not consistent with state and federal laws regarding obscenity, libel, and state and federal laws and University policies regarding political activity, the marketing of products or services, or other inappropriate activities.
    - Reinforce the statement that "People" are the most important component to physical security.[13] If you suspect unacceptable behavior by patrons, do not confront them, even with the likelihood of losing evidence. Notify other library management who will take appropriate action.
- Computer lab employees should be knowledgeable in computer security so they can explain to patrons, how they may provide more protection for themselves while using the computer. This can be in areas such as Internet use, e-mail communications, and backing up and storing their data.

For all employees of the department a new presentation was developed. Some of the items included:

- Relay security goal.
- Explain terminology of security vulnerabilities, e.g. viruses, worms, and trojans.
- Explain some things they can do as users to reduce their risk while using workstation computers.
- Explain how virus and patch update programs work.
- Explain how backups of their data work.
- Answer any questions they may have in regard to how secure they are when they work at a computer lab workstation.

[13] Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. "SANS Security Essentials with CISSP CBK." The Sans Institute. 2003:pg.260.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Other Factors

As on many university campuses, students and employees are bringing in their personally owned laptops and using them on the campus wired and wireless networks. This computer lab is no exception. If these machines are not properly maintained with patches and virus updates, they can transfer files with malicious code of various types to the lab workstations. The same issues occur with home users connecting through VPN clients to the lab network.

Reliance on physical security is even more crucial for library workstations. Some of the items that are currently being used are:

- There are alarms for all entries into the lab area. One alarm is always set, while the other is right next to the help desk station and is only unset when the monitor is there. Effectively, there is only one entrance for patrons to go in and out.
- The help desk is physically in the lab and is always staffed when the lab is open.
- All servers and network equipment are separated in a staff-only closet and designated enclosed area. Some smaller equipment is placed in locked cabinets next to the help desk station.
- All backup tapes are stored in staff-only area and locked.
- Keys used in securing equipment or media are stored in a controlled location.

One recommendation for physical security would be to have a BIOS password. This is currently being tested to make sure it would not interfere with training or teaching access issues.

There is always the chance that patrons will push the boundaries of freedom from an internal workstation in the lab. As in some of the issues previously mentioned these individuals may be true hackers or they may be just inquisitive students testing what they know and seeing what they can do on a reasonably open computer. Fortunately, the University currently monitors packet activity through the use of Snort. They have Snort watching traffic from the residence halls to campus (and out), as well as traffic from the labs to the Internet (and residence halls). The help desk assistant in the computer lab may not be able to notice anything unusual about activity from a patron, but if the workstation is causing a problem on the network, there is a good chance it will be picked up through the University monitoring of packet activity. It should also be noted, along with intrusion detection devices, intrusion prevention systems such as Tipping Point Systems are being used by the University.

Lab workstations are not backed up and patrons are warned not to store data on them. All workstations are identical, for the most part. This allows administrators to re-image the machines as often as necessary. Re-imaging of workstations is often quicker and easier than troubleshooting and also gives the assurance that the machine's hard drive is "clean".

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

A crucial consideration is that resources at public university libraries are largely dependent on state public funds. The lack of resources is one of the most common and potentially most dangerous threats to the lab security. Education and influence of management and the chain of command is crucial to keeping computer/network security not far from the forefront of funding managers' agendas.

Summary and Conclusions

The imaging/inventory management software was implemented by a group member in the Information Technology group of the department. I implemented the centralized virus management system and increased training and security awareness among patrons. I set up the group policies to implement the patch-update system as well as monitor its effectiveness and ran all the tools to analyze the workstation. Currently and during this case study I have been responsible for management of the computer lab. However, all the actual work that is involved in keeping it in good working order is a team effort.

While the lab workstation is what is being evaluated here, all security in the network is interrelated. Prevention and detection begins at the border to the university. Perimeter, device and server security are all critical and they directly impact the workstation in the computer lab.

> Creating a secure public access workstation is a process made up of many discrete procedures. Furthermore, these steps are interdependent with other features of your secure system, such as network security and user issues. In this age of the Internet, a computer is only very rarely a self-contained unit.[14]

Since this paper focuses on securing a public access computer, one should also remember that to truly secure that computer, one should secure the total network environment, and one must have a way to evaluate and maintain the security.

The goal in the computer lab is to offer faculty, staff, students and the public an open and secure computing environment for all educational, research and administrative purposes. In order to do this, we are creating a certain freedom to roam in the pasture and to experiment without doing harm to ourselves or to others. We are only able to do this by setting up the layers of security for protection.

[14] Ayre, Lori. "Library Computer and Network Security." Infopeople Project. February, 2003.
URL: http://infopeople.org/howto/security/
The Infopeople Project is supported by the U.S. Institute of Museaum and Library Services under the provisions of the Library Services and Technology Act, administered in California by the State Librarian. (2004).

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

To conclude:

- Dependence on any one method of security is not enough, particularly in an open computing environment.
- Acceptable security can be secure enough for all users in the lab, if they are aware of the risks. If necessary, they can provide additional security for themselves, through awareness and training provided by the information technology support group.
- If anything, less hardened workstations need greater monitoring and maintenance, in order to offer a free and open secure computing environment. At some point, inadequate resources may prevent us from keeping the computer lab as open as it is.

List of Reports from Analysis Tools

Report 1
Report Generated from Microsoft Corporation Group Policy Management Console, Group Policy Results

Report 2
Reports Generated from Windows Security Scoring Tool –v2.2.12
© 2001-2004 Kerry Steele SecurePointe
The Center for Internet Security http://www.cisecurity.org/sub_form.html

Report 3
Reports generated from NeWT, Nessus Windows Technology version 1.5© 2003 Tenable Network Security
http://www.tenablesecurity.com/newt.html

List of References

1. Ayre, Lori. "Library Computer and Network Security." Infopeople Project. February, 2003. URL: http://infopeople.org/howto/security/ The Infopeople Project is supported by the U.S. Institute of Museums and Library Services under the provisions of the Library Services and Technology Act, administered in California by the State Librarian. (2004).

2. Biever, Erik. "Securing Public Workstation by Maintaining Software Centrally." Library Hi Tech. 15 (1997):27-29.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

3. Brakel, Garvin. “Public Workstation Security.” Library Hi Tech. 15 (1997):24-26.

4. Brinkman, Carol. Roubieu, Amanda. “Planning and Record Keeping for Computer Maintenance and Management.” Reference Services Review. 29(2001): 72-80.

5. Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. “SANS Security Essentials with CISSP CBK.” The Sans Institute. 2003.

6. Finlay, Ian A. “Vulnerability Note VU#464113 TCP/IP implementations handle unusual flag combinations inconsistently.” U.S. Cert. Revision 89. May 30, 2003. URL: http://www.kb.cert.org/vuls/id/464113. (2004).

7. Fore, Julie. “Things that Go Bump in the Virtual Night.” Library Hi Tech. 15 (1997):84-91.

8. Lynch, Clifford. “The Changing Role in a Networked Information Environment.” Library Hi Tech. 15 (1997):30-38.

9. Shawgo, Jeff and Faber, Sidney. “Windows XP Professional Operating System Legacy, Enterprise, and High Security Benchmark Consensus Baseline Security Settings.” Version 1.1.3 March 17, 2004. The Center for Internet Security URL: http://www.cisecurity.org (2004).

10. Williams, Robert. “Computer and Network Security in Small Libraries.” Texas State Library and Archives Commission. 2001. URL:http://www.tsl.state.tx.us/ld/pubs/compsecurity/index.html (2004).

11. “Guidelines and Considerations for Developing a Public Library Internet Use Policy.” American Library Association . Issued June 1998; rev. November 2000. URL:http://www.ala.org/Template.cfm?Section=Other_Policies_and_Guideline&Template=/ContentManagement/ContentDisplay.cfm&ContentID=13098 (2004).

12. Microsoft Windows XP Professional Product Documentation. “Step-by-Step Guide to Understanding the Group Policy Feature Set.” 2004. http://www.microsoft.com/windows2000/techinfo/planning/management/groupsteps.asp .

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Report 1 Group Policy Results on Test computer

Information containing userids and references to the computer has been scrubbed

Data collected on: 3/31/2004 4:46:25 PM

hide all

Summaryhide

Computer Configuration Summaryhide

Generalhide

Computer name	
Domain	
Site	Default-First-Site-Name
Last time Group Policy was processed	3/31/2004 4:02:40 PM

Group Policy Objectshide

Applied GPOshide

Name	Link Location	Revision
Local Group Policy	Local	AD (21), Sysvol (21)
Prevent MS Blaster Execution		AD (52), Sysvol (52)
Default Domain Policy		AD (26), Sysvol (26)
slabs		AD (4), Sysvol (4)
susOuter	/xxxComputers/Labs/OuterLab	AD (6), Sysvol (6)

Denied GPOshide

Name	Link Location	Reason Denied
New Group Policy Object	/xxxComputers/Labs/OuterLab	Empty

Security Group Membership when Group Policy was appliedhide

BUILTIN\Administrators
Everyone
\Debugger Users
BUILTIN\Users
XXX\TESTPC$
XXX\Domain Computers
NT AUTHORITY\NETWORK
NT AUTHORITY\Authenticated Users

WMI Filtershide

This data is available only from computers running Windows XP Service Pack 2 or later.

Component Statushide

Component Name	Status	Last Process Time
Group Policy Infrastructure	Success	3/31/2004 4:02:45 PM

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

EFS recovery	Success (no data)	1/15/2004 9:57:14 AM
Registry	Success	1/15/2004 9:57:09 AM
Security	Success	1/15/2004 9:57:14 AM

User Configuration Summaryhide

Generalhide

User name	XXX\testid
Domain	test.edu
Last time Group Policy was processed	3/31/2004 4:39:49 PM

Group Policy Objectshide

Applied GPOshide

Name	Link Location	Revision
Local Group Policy	Local	AD (6), Sysvol (6)
Default Domain Policy	xxx.univ.edu	AD (1), Sysvol (1)
SXXX	test.edu/xxxUsers/Labs	AD (66), Sysvol (66)
SXXX	xxx.univ.edu/xxxUsers/Labs/InnerLab	AD (66), Sysvol (66)

Denied GPOshide

Name	Link Location	Reason Denied
Prevent MS Blaster Execution	test.edu	Empty

Security Group Membership when Group Policy was appliedhide

XXX\Domain Users
Everyone
BUILTIN\Administrators
BUILTIN\Remote Desktop Users
BUILTIN\Users
LOCAL
NT AUTHORITY\INTERACTIVE
NT AUTHORITY\Authenticated Users

WMI Filtershide

This data is available only from computers running Windows XP Service Pack 2 or later.

Component Statushide

Component Name	Status	Last Process Time
Group Policy Infrastructure	Success	3/31/2004 4:39:50 PM
Registry	Success	1/15/2004 10:04:16 AM

Computer Configurationhide

Windows Settingshide

Security Settingshide

Account Policies/Password Policyhide

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Policy	Setting	Winning GPO
Enforce password history	0 passwords remembered	Default Domain Policy
Maximum password age	0 days	Default Domain Policy
Minimum password age	0 days	Default Domain Policy
Minimum password length	5 characters	Default Domain Policy
Password must meet complexity requirements	Disabled	Default Domain Policy
Store passwords using reversible encryption	Disabled	Default Domain Policy

Account Policies/Account Lockout Policyhide

Policy	Setting	Winning GPO
Account lockout duration	15 minutes	Default Domain Policy
Account lockout threshold	5 invalid logon attempts	Default Domain Policy
Reset account lockout counter after	5 minutes	Default Domain Policy

Local Policies/Audit Policyhide

Policy	Setting	Winning GPO
Audit account logon events	Success, Failure	Default Domain Policy
Audit account management	Success, Failure	Default Domain Policy
Audit directory service access	Failure	Default Domain Policy
Audit logon events	Success, Failure	Default Domain Policy
Audit policy change	Success, Failure	Default Domain Policy
Audit privilege use	Success, Failure	Default Domain Policy
Audit system events	Success, Failure	Default Domain Policy

Local Policies/Security Optionshide
Network Accesshide

Policy	Setting	Winning GPO
Network access: Do not allow	Enabled	Default Domain Policy

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

anonymous enumeration of SAM accounts and shares

Network Securityhide

Policy	Setting	Winning GPO
Network security: Force logoff when logon hours expire	Enabled	Default Domain Policy

System Serviceshide

Messenger (Startup Mode: Manual)hide

Winning GPO	Default Domain Policy

Permissions

Type	Name	Permission
Allow	Everyone	Full Control

Auditing

No auditing specified

Public Key Policies/Autoenrollment Settingshide

Policy	Setting	Winning GPO
Enroll certificates automatically	Enabled	[Default setting]
Renew expired certificates, update pending certificates, and remove revoked certificates	Disabled	
Update certificates that use certificate templates	Disabled	

Public Key Policies/Encrypting File Systemhide

Propertieshide

Winning GPO	[Default setting]

Policy	Setting
Allow users to encrypt files using Encrypting File System (EFS)	Enabled

Certificateshide

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Issued To	Issued By	Expiration Date	Intended Purposes	Winning GPO
Administrator	Administrator	12/17/2005 3:09:34 PM	File Recovery	Default Domain Policy

For additional information about individual settings, launch Group Policy Object Editor.

Public Key Policies/Trusted Root Certification Authoritieshide

Propertieshide

Winning GPO	[Default setting]

Policy	Setting
Allow users to select new root certification authorities (CAs) to trust	Enabled
Client computers can trust the following certificate stores	Third-Party Root Certification Authorities and Enterprise Root Certification Authorities
To perform certificate-based authentication of users and computers, CAs must meet the following criteria	Registered in Active Directory only

Software Restriction Policieshide

Winning GPO	Prevent MS Blaster Execution
Enforcement	

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Policy	Setting
Apply software restriction policies to	All software files except libraries (such as DLLs)
Apply software restriction policies to the following users	All users

Designated File Types

File Extension	File Type
ADE	Microsoft Access Project Extension
ADP	Microsoft Access Project
BAS	BAS File
BAT	MS-DOS Batch File
CHM	Compiled HTML Help file
CMD	Windows NT Command Script
COM	MS-DOS Application
CPL	Control Panel extension
CRT	Security Certificate
EXE	Application
HLP	Help File
HTA	HTML Application
INF	Setup Information
INS	Internet Communication Settings
ISP	Internet Communication Settings
LNK	Shortcut
MDB	Microsoft Access Application
MDE	Microsoft Access MDE Database
MSC	Microsoft Common Console Document

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

MSI	Windows Installer Package
MSP	Windows Installer Patch
MST	MST File
OCX	ActiveX Control
PCD	Photo CD Image
PIF	Shortcut to MS-DOS Program
REG	Registration Entries
SCR	Screen Saver
SHS	Scrap object
URL	Internet Shortcut
VB	VB File
WSC	Windows Script Component

Trusted Publishers

Allow the following users to select trusted publishers	End users
Before trusting a publisher, check the following to determine if the certificate is revoked	None

Software Restriction Policies/Security Levelshide

Policy	Setting	Winning GPO
Default Security Level	Unrestricted	Prevent MS Blaster Execution

Software Restriction Policies/Additional Ruleshide
Path Ruleshide

%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%

Security Level	Unrestricted
Description	
Date last modified	8/15/2003 11:12:00 AM
Winning GPO	Prevent MS Blaster Execution

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%*.exe

Security Level	Unrestricted
Description	
Date last modified	8/15/2003 11:12:00 AM
Winning GPO	Prevent MS Blaster Execution

%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\System32*.exe

Security Level	Unrestricted
Description	
Date last modified	8/15/2003 11:12:00 AM
Winning GPO	Prevent MS Blaster Execution

%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%

Security Level	Unrestricted
Description	
Date last modified	8/15/2003 11:12:00 AM
Winning GPO	Prevent MS Blaster Execution

%systemroot%\system32\wins\dllhost.exe

Security Level	Disallowed
Description	worm variant
Date last modified	8/18/2003 9:41:41 PM
Winning GPO	Prevent MS Blaster Execution

msblast.exe

Security Level	Disallowed

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Description	Prevents execution of msblast.exe binary in any location.
Date last modified	10/7/2003 11:30:17 AM

patch.exe

Security Level	Disallowed
Description	Prevents execution of worm variant binary
Date last modified	10/7/2003 11:30:34 AM
Winning GPO	Prevent MS Blaster Execution

penis32.exe

Security Level	Disallowed
Description	Prevents execution of variant of MS Blaster binary.
Date last modified	8/18/2003 4:32:54 PM
Winning GPO	Prevent MS Blaster Execution

psexesvc.exe

Security Level	Disallowed
Description	
Date last modified	9/10/2003 11:30:50 AM
Winning GPO	Prevent MS Blaster Execution

scvhost.exe

Security Level	Disallowed
Description	
Date last modified	9/10/2003 11:30:58 AM
Winning GPO	Prevent MS Blaster Execution

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

teekids.exe

Security Level	Disallowed
Description	Prevents execution of variant of MS Blaster binary.
Date last modified	8/18/2003 4:32:47 PM
Winning GPO	Prevent MS Blaster Execution

winhlpp32.exe

Security Level	Disallowed
Description	
Date last modified	9/10/2003 11:31:13 AM
Winning GPO	Prevent MS Blaster Execution

winppr32.exe

Security Level	Disallowed
Description	Sobig.F virus binary
Date last modified	8/20/2003 5:56:38 PM
Winning GPO	Prevent MS Blaster Execution

Administrative Templateshide

Network/Offline Fileshide

Policy	Setting	Winning GPO
Allow or Disallow use of the Offline Files feature	Disabled	sxxxlabs
Prohibit user configuration of Offline Files	Enabled	sxxxlabs

Prevents users from changing any cache configuration settings.

System/User Profileshide

Policy	Setting	Winning GPO

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Add the Administrators security group to roaming user profiles	Enabled	sxxxlabs
Delete cached copies of roaming profiles	Enabled	sxxxlabs
Do not check for user ownership of Roaming Profile Folders	Enabled	Local Group Policy
Wait for remote user profile	Enabled	Local Group Policy

System/Windows Time Servicehide

Policy	Setting	Winning GPO
Global Configuration Settings	Enabled	Local Group Policy
Clock Discipline Parameters		
FrequencyCorrectRate	4	
HoldPeriod	5	
LargePhaseOffset	1280000	
MaxAllowedPhaseOffset	300	
MaxNegPhaseCorrection	54000	
MaxPosPhaseCorrection	54000	
PhaseCorrectRate	1	
PollAdjustFactor	5	
SpikeWatchPeriod	90	
UpdateInterval	30000	
General Parameters		
AnnounceFlags	10	
EventLogFlags	2	
LocalClockDispersion	10	
MaxPollInterval	15	

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

MinPollInterval	10

System/Windows Time Service/Time Providershide

Policy	Setting	Winning GPO
Configure Windows NTP Client	Enabled	Local Group Policy

NtpServer	clock2.univ.edu
Type	NTP
CrossSiteSyncFlags	2
ResolvePeerBackoffMinutes	15
ResolvePeerBackoffMaxTimes	7
SpecialPollInterval	60
EventLogFlags	0

Policy	Setting	Winning GPO
Enable Windows NTP Client	Enabled	Local Group Policy
Enable Windows NTP Server	Disabled	Local Group Policy

Windows Components/Windows Updatehide

Policy	Setting	Winning GPO
Configure Automatic Updates	Enabled	susOuter

Configure automatic updating:	4 - Auto download and schedule the install
The following settings are only required	
and applicable if 4 is selected.	
Scheduled install day:	0 - Every day
Scheduled install time:	00:00

Policy	Setting	Winning GPO
No auto-restart for scheduled Automatic Updates installations	Disabled	susOuter

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Reschedule Automatic Updates scheduled installations	Enabled	susOuter
Wait after system startup(minutes):	30	

Policy	Setting	Winning GPO
Specify intranet Microsoft update service location	Enabled	susOuter
Set the intranet update service for detecting updates:	http://sus.univ.edu	
Set the intranet statistics server:	http://sus.univ.edu	
(example: http://IntranetUpd01)		

User Configurationhide

Administrative Templateshide

Control Panelhide

Policy	Setting	Winning GPO
Force classic Control Panel Style	Enabled	SXXX

Control Panel/Displayhide

Policy	Setting	Winning GPO
Hide Appearance and Themes tab	Enabled	SXXX
Hide Desktop tab	Enabled	SXXX
Hide Screen Saver tab	Enabled	SXXX
Hide Settings tab	Enabled	SXXX
Prevent changing wallpaper	Enabled	SXXX

Control Panel/Display/Desktop Themeshide

Policy	Setting	Winning GPO
Load a specific visual style file or force Windows Classic	Enabled	SXXX
Path to Visual Style:		
To select Luna type:		

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

%windir%\resources\Themes\Luna\Luna.msstyles

To select a different visual style, type:

ie: \\<server>\share\Corp.msstyles

To select Windows Classic, leave the box

above blank and enable this setting

Policy	Setting	Winning GPO
Prevent selection of windows and buttons styles	Enabled	SXXX
Prohibit selection of font size	Enabled	SXXX
Prohibit Theme color selection	Enabled	SXXX
Remove Theme option	Enabled	SXXX

Control Panel/Printershide

Policy	Setting	Winning GPO
Prevent deletion of printers	Enabled	SXXX

Desktophide

Policy	Setting	Winning GPO
Don't save settings at exit	Enabled	SXXX
Prevent adding, dragging, dropping and closing the Taskbar's toolbars	Enabled	SXXX
Prohibit adjusting desktop toolbars	Enabled	SXXX
Prohibit user from changing My Documents path	Enabled	SXXX
Remove My Documents icon on the desktop	Enabled	SXXX

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Remove the Desktop Cleanup Wizard	Enabled	SXXX

Desktop/Active Desktophide

Policy	Setting	Winning GPO
Disable Active Desktop	Enabled	SXXX
Disallows HTML and Jpg Wallpaper		

Policy	Setting	Winning GPO
Prohibit changes	Enabled	SXXX

Network/Offline Fileshide

Policy	Setting	Winning GPO
Prohibit user configuration of Offline Files	Enabled	SXXX
Prevents users from changing any cache configuration settings.		

Policy	Setting	Winning GPO
Synchronize all offline files when logging on	Disabled	SXXX

Shared Foldershide

Policy	Setting	Winning GPO
Allow shared folders to be published	Enabled	SXXX

Start Menu and Taskbarhide

Policy	Setting	Winning GPO
Add Logoff to the Start Menu	Enabled	SXXX
Clear history of recently opened documents on exit	Enabled	SXXX
Do not keep history of recently opened documents	Enabled	SXXX
Force classic Start Menu	Enabled	SXXX

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Lock the Taskbar	Enabled	SXXX
Prevent changes to Taskbar and Start Menu Settings	Enabled	SXXX
Remove Balloon Tips on Start Menu items	Enabled	SXXX
Remove Favorites menu from Start Menu	Enabled	SXXX
Remove My Documents icon from Start Menu	Enabled	SXXX
Remove user's folders from the Start Menu	Enabled	SXXX
Turn off personalized menus	Enabled	SXXX
Turn off user tracking	Enabled	SXXX

Systemhide

Policy	Setting	Winning GPO
Prevent access to registry editing tools	Enabled	SXXX

System/Group Policyhide

Policy	Setting	Winning GPO
Group Policy domain controller selection	Enabled	SXXX
When Group Policy is selecting a domain controller to use, it should:	Use any available domain controller	

Policy	Setting	Winning GPO
Group Policy refresh interval for users	Enabled	SXXX
This setting allows you to customize how often Group Policy is applied		

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

to users. The range is 0 to 64800 minutes (45 days).	
Minutes:	10
This is a random time added to the refresh interval to prevent	
all clients from requesting Group Policy at the same time.	
The range is 0 to 1440 minutes (24 hours)	
Minutes:	15

System/User Profileshide

Policy	Setting	Winning GPO
Exclude directories in roaming profile	Enabled	Local Group Policy
Prevent the following directories from roaming with the profile:	My Documents;Recent;FrontPageTempDir;Cookies;Application Data\Real; Application Data\Received Files	
You can enter multiple directory names, semi-colon separated,		
all relative to the root of the user's profile		

Policy	Setting	Winning GPO
Limit profile size	Disabled	SXXX

Windows Components/Internet Explorerhide

Policy	Setting	Winning GPO
Disable AutoComplete for forms	Enabled	SXXX
Disable caching of Auto-Proxy scripts	Enabled	SXXX
Disable changing color settings	Enabled	SXXX
Disable changing default browser check	Enabled	SXXX
Disable changing font settings	Enabled	SXXX

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Disable changing history settings	Enabled	SXXX
Disable changing home page settings	Enabled	SXXX
Disable changing link color settings	Enabled	SXXX
Disable importing and exporting of favorites	Enabled	SXXX
Disable the Reset Web Settings feature	Enabled	SXXX
Do not allow AutoComplete to save passwords	Enabled	SXXX
Identity Manager: Prevent users from using Identities	Enabled	SXXX

Windows Components/Internet Explorer/Offline Pageshide

Policy	Setting	Winning GPO
Disable adding channels	Enabled	SXXX

Windows Components/Internet Explorer/Toolbarshide

Policy	Setting	Winning GPO
Disable customizing browser toolbar buttons	Enabled	SXXX
Disable customizing browser toolbars	Enabled	SXXX

Windows Components/Windows Explorerhide

Policy	Setting	Winning GPO
Turn off caching of thumbnail pictures	Enabled	SXXX

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Report 2
Reports Generated from Windows Security Scoring Tool –v2.2.12
© 2001-2004 Kerry Steele SecurePointe
The Center for Internet Security
Note: Information containing userids and references to the computer has been scrubbed

THE CENTER FOR INTERNET SECURITY℠

Windows Security Scoring Tool - v2.1.12

Computer Name	**:**
Template	**: CIS-WinXP-HiSec-v1.0.2.inf**
Scan Time	**: 03/30/2004 13:18:49**

Description	**Value**	**Score**
Service Pack	1	1.25
Hotfixes Needed	1	0
Non-Expiring Passwords	5	0
Policy Mismatches	11	0
Event Log Mismatches	3	0
Restrict Anonymous	1,1	1.25
Security Options Mismatches	31	0
Available Services Mismatches	14	0
User Rights Mismatches	14	0
Other System Requirements Mismatches	0	0
Permissions Mismatches	36	0
Overall Score		**2.5**

Click Here for SecEdit Details

Description	**Mismatches**	**Total**
User Rights	14	38
Group Membership	1	8
Registry Permissions	9	11
NTFS Permissions	27	27
Services	14	90

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Password Policy	5	6
Account Lockout Policy	2	3
Event Log Settings	3	4
Audit Policy	4	5
Security Options	31	81

1 THE CENTER FOR INTERNET SECURITY SM

Windows Security Scoring Tool - v2.1.12

Service Report - Non-Default Installed Services

Altiris Client Service (AClient) -- Running

Application Layer Gateway Service (ALG) -- Stopped

ASP.NET State Service (aspnet_state) -- Stopped

Windows Audio (AudioSrv) -- Running

Background Intelligent Transfer Service (BITS) -- Running

COM+ System Application (COMSysApp) -- Stopped

Cryptographic Services (CryptSvc) -- Running

DefWatch (DefWatch) -- Running

Error Reporting Service (ERSvc) -- Running

Fast User Switching Compatibility (FastUserSwitchingCompatibility) -- Stopped

Help and Support (helpsvc) -- Running

Human Interface Device Access (HidServ) -- Stopped

IMAPI CD-Burning COM Service (ImapiService) -- Stopped

IPv6 Internet Connection Firewall (Ip6FwHlp) -- Stopped

Machine Debug Manager (MDM) -- Running

Network Location Awareness (NLA) (Nla) -- Running

Symantec AntiVirus Client (Norton AntiVirus Server) -- Running

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

NVIDIA Driver Helper Service (NVSvc) -- Running

OracleClientCache80 (OracleClientCache80) -- Stopped

OracleOraHome92ClientCache (OracleOraHome92ClientCache) -- Stopped

IPSEC Services (PolicyAgent) -- Running

Remote Desktop Help Session Manager (RDSessMgr) -- Stopped

Remote Registry (RemoteRegistry) -- Stopped

sasrfc Service (sasrfcService) -- Stopped

Secondary Logon (seclogon) -- Running

Shell Hardware Detection (ShellHWDetection) -- Running

System Restore Service (srservice) -- Running

SSDP Discovery Service (SSDPSRV) -- Running

Windows Image Acquisition (WIA) (stisvc) -- Stopped

MS Software Shadow Copy Provider (SwPrv) -- Stopped

Terminal Services (TermService) -- Running

Themes (Themes) -- Running

Time Service (TimeServ) -- Running

IBM AFS Client (TransarcAFSDaemon) -- Running

Upload Manager (uploadmgr) -- Running

Volume Shadow Copy (VSS) -- Stopped

WebClient (WebClient) -- Running

Portable Media Serial Number Service (WmdmPmSN) -- Stopped

WMI Performance Adapter (WmiApSrv) -- Stopped

Automatic Updates (wuauserv) -- Running

Wireless Zero Configuration (WZCSVC) -- Running

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

THE CENTER FOR INTERNET SECURITY

Windows Security Scoring Tool - v2.1.12

User Report - Accounts with Passwords older than 90 days.

Account Name: Administrator

Password Age (since last changed): 364 days, 7 hours, 50 minutes

Privilege: Administrator

Home Directory:

Comment: Built-in account for administering the computer/domain

Flags:

- The logon script executed.

- The password should never expire on the account.

- This is a default account type that represents a typical user.

Logon Script Path:

Auth Flags (operator privileges):

Full Name:

User Comment:

Workstations:

Last Logon: 11/20/2003 3:50:55 PM

Last Logoff: 1/1/1970

Account Expires: True

Maximum Storage: Unlimited

Bad Password Count: 0

Number of Logons: 10

Logon Server: * (any server)

Password Never Expires: True

Account Name: ASPNET

Password Age (since last changed): 138 days, 0 hours, 35 minutes

Privilege: User

Home Directory:

© SANS Institute 2004, Author retains full rights.

Comment: Account used for running the ASP.NET worker process (aspnet_wp.exe)

Flags:

- The logon script executed.

- No password is required.

- The user cannot change the password.

- The password should never expire on the account.

- This is a default account type that represents a typical user.

Logon Script Path:

Auth Flags (operator privileges):

Full Name: ASP.NET Machine Account

User Comment: Account used for running the ASP.NET worker process (aspnet_wp.exe)

Workstations:

Last Logon: 1/1/1970

Last Logoff: 1/1/1970

Account Expires: True

Maximum Storage: Unlimited

Bad Password Count: 0

Number of Logons: 0

Logon Server: * (any server)

Password Never Expires: True

Account Name: HelpAssistant

Password Age (since last changed): 364 days, 2 hours, 37 minutes

Privilege: Guest

Home Directory:

Comment: Account for Providing Remote Assistance

Flags:

- The logon script executed.

- The user's account is disabled.

- The user cannot change the password.

- The password should never expire on the account.

- This is a default account type that represents a typical user.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Logon Script Path:

Auth Flags (operator privileges):

Full Name: Remote Desktop Help Assistant Account

User Comment:

Workstations:

Last Logon: 1/1/1970

Last Logoff: 1/1/1970

Account Expires: True

Maximum Storage: Unlimited

Bad Password Count: 0

Number of Logons: 0

Logon Server: * (any server)

Password Never Expires: True

Account Name: lab

Password Age (since last changed): 363 days, 2 hours, 10 minutes

Privilege: User

Home Directory:

Comment:

Flags:

- The logon script executed.

- This is a default account type that represents a typical user.

Logon Script Path:

Auth Flags (operator privileges):

Full Name: Lab Test

User Comment:

Workstations:

Last Logon: 4/2/2003 4:14:13 PM

Last Logoff: 1/1/1970

Account Expires: True

Maximum Storage: Unlimited

Bad Password Count: 0

Number of Logons: 2

Logon Server: * (any server)

Password Never Expires: False

© SANS Institute 2004, Author retains full rights.

Account Name: SUPPORT_388945a0

Password Age (since last changed): 364 days, 2 hours, 35 minutes

Privilege: Guest

Home Directory:

Comment: This is a vendor's account for the Help and Support Service

Flags:

- The logon script executed.

- The user's account is disabled.

- The user cannot change the password.

- The password should never expire on the account.

- This is a default account type that represents a typical user.

Logon Script Path:

Auth Flags (operator privileges):

Full Name: CN=Microsoft Corporation,L=Redmond,S=Washington,C=US

User Comment:

Workstations:

Last Logon: 1/1/1970

Last Logoff: 1/1/1970

Account Expires: True

Maximum Storage: Unlimited

Bad Password Count: 0

Number of Logons: 0

Logon Server: * (any server)

Password Never Expires: True

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

3 THE CENTER FOR INTERNET SECURITY SM

Windows Security Scoring Tool - v2.1.12

Security Hotfix Report

Scan performed Tue Mar 30 13:18:50 2004

Shavlik Technologies Network Security Hotfix Checker, 3.86

Using XML data version = 1.1.1.970 Last modified on 3/29/2004.

* WINDOWS XP SP1

Warning MS02-055 Q323255

Warning MS03-023 Q823559

Warning MS03-030 Q819696

Note MS03-030 Q819696

--> Patch NOT Installed MS03-051 Q813380

--> Patch NOT Installed TOOL03-039 Q833330

* INTERNET EXPLORER 6 SP1

Information

All necessary hotfixes have been applied.

* WINDOWS MEDIA PLAYER 9.0 GOLD

Information

All necessary hotfixes have been applied.

* MDAC 2.7 SP1

Information

All necessary hotfixes have been applied.

The CIS Scoring Tool uses the Microsoft Network Security Hotfix Checker (HfNetChk), which is licensed to CIS by Shavlik Technologies

http://www.shavlik.com

© SANS Institute 2004, Author retains full rights.

Tenable NeWT Security Reports
Report 3

Start Time: *Fri Apr 09 14:54:36 2004* **Finish Time:** *Fri Apr 09 14:56:01 2004*

Information containing userids and references to the computer has been scrubbed

9 Open Ports, 14 Notes, 10 Infos, 0 Holes.

epmap (135/tcp)	Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. **Solution : filter incoming traffic to this port.** **Risk factor : Low** Plugin ID : 10736 Port is open Plugin ID : 11219
netbios-ssn (139/tcp)	The domain SID can be obtained remotely. Its value is : An attacker can use it to obtain the list of the local users of this host **Solution : filter the ports 137 to 139 and 445** **Risk factor : Low** **CVE : CVE-2000-1200** **BID : 959** Plugin ID : 10398 The host Security Identifier (SID) can be obtained remotely. Its

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

	value is : An attacker can use it to obtain the list of the local users of this host **Solution : filter the ports 137-139 and 445** **Risk factor : Low** **CVE : CVE-2000-1200** **BID : 959** Plugin ID : 10859 Port is open Plugin ID : 11219 An SMB server is running on this port Plugin ID : 11011 It was possible to log into the remote host using a NULL session. The concept of a NULL session is to provide a null username and a null password, which grants the user the 'guest' access To prevent null sessions, see MS KB Article Q143474 (NT 4.0) and Q246261 (Windows 2000). Note that this won't completely disable null sessions, but will prevent them from connecting to IPC$ Please see http://msgs.securepoint.com/cgi-bin/get/nessus-0204/50/1.html All the smb tests will be done as "/" in domain CVE : CAN-1999-0504, CAN-1999-0506, CVE-2000-0222, CAN-1999-0505, CAN-2002-1117 BID : 494, 990 Plugin ID : 10394 The remote native lan manager is : Windows 2000 LAN Manager The remote Operating System is : Windows 5.1 The remote SMB Domain Name is : Plugin ID : 10785

cap (1026/tcp)	Port is open Plugin ID : 11219

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

	Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this port: UUID: 1ff70682-0a51-30e8-076d-740be8cee98b, version 1 Endpoint: ncacn_ip_ [1026] UUID: 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1 Endpoint: ncacn_ip_tcp: [1026] UUID: 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1 Endpoint: ncacn_ip_tcp: [1026] **Solution : filter incoming traffic to this port.** **Risk Factor : Low** Plugin ID : 10736

commplex-main (5000/tcp)	The remote host is running Microsoft UPnP TCP helper. If the tested network is not a home network, you should disable this service. **Solution : Set the following registry key :** **Location :** **HKLM\SYSTEM\CurrentControlSet\Services\SSDPSRV** **Key : Start** **Value : 0x04** **Risk Factor : Low** **CVE : CVE-2001-0876** **BID : 3723** Plugin ID : 11765 Port is open Plugin ID : 11219

general/udp	For your information, here is the traceroute to :

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

	Plugin ID : 10287

general/tcp	The remote host does not discard TCP SYN packets which have the FIN flag set. Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules. **See also :** **http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html** **http://www.kb.cert.org/vuls/id/464113** **Solution : Contact your vendor for a patch** **Risk factor : Medium** **BID : 7487** Plugin ID : 11618 The remote host uses non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host. An attacker may use this feature to determine traffic patterns within your network. A few examples (not at all exhaustive) are: 1. A remote attacker can determine if the remote host sent a packet in reply to another request. Specifically, an attacker can use your server as an unwilling participant in a blind portscan of another network. 2. A remote attacker can roughly determine server requests at certain times of the day. For instance, if the server is sending much more traffic after business hours, the server may be a reverse proxy or other remote access device. An attacker can use this information to concentrate his/her efforts on the more critical machines. 3. A remote attacker can roughly estimate the number of requests that a web server processes over a period of time. **Solution : Contact your vendor for a patch** **Risk factor : Low**

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

	Plugin ID : 10201 The remote host accepts loose source routed IP packets. The feature was designed for testing purpose. An attacker may use it to circumvent poorly designed IP filtering and exploit another flaw. However, it is not dangerous by itself. **Solution : drop source routed packets on this host or on other ingress** **routers or firewalls.** **Risk factor : Low** Plugin ID : 11834 resolves as . Plugin ID : 12053 The remote host is running Microsoft Windows XP Plugin ID : 11936

isakmp (500/udp)	The remote host seems to be enabled to do Internet Key Exchange. This is typically indicative of a VPN server. VPN servers are used to connect remote hosts into internal resources. In addition, The remote host seems to be configured to force all communications across port 500 for both the source and destination port. That is, we sent the machine a packet from a random port greater than 1024. The machine sent the reply back to port 500. NOTE: This sort of behavior has been observed on Microsoft machines. **Solution: You should ensure that:** **1) The VPN is authorized for your Companies computing environment** **2) The VPN utilizes strong encryption** **3) The VPN utilizes strong authentication** **Risk factor : Low** Plugin ID : 11935

ntp (123/udp)	

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

	A NTP (Network Time Protocol) server is listening on this port. **Risk factor : Low** Plugin ID : 10884

general/icmp	The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine. This may help him to defeat all your time based authentication protocols. **Solution : filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).** **Risk factor : Low** **CVE : CAN-1999-0524** Plugin ID : 10114

unknown (1037/tcp)	Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this port: UUID: 7e8952d8-1b50-101b-8952-204c4f4f5020, version 1 Endpoint: ncacn_ip_tcp:0.0xx147[1037] UUID: 2131bed0-5484-11d2-b6c6-006097221e3d, version 1 Endpoint: ncacn_ip_tcp:0.0xx147[1037] Annotation: AFS session key interface **Solution : filter incoming traffic to this port.** **Risk Factor : Low** Plugin ID : 10736

unknown (1038/udp)	

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

	Distributed Computing Environment (DCE) services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries. An attacker may use this fact to gain more knowledge about the remote host. Here is the list of DCE services running on this port: UUID: 7e8952d8-1b50-101b-8952-204c4f4f5020, version 1 Endpoint: ncadg_ip_udp:[1038] UUID: 2131bed0-5484-11d2-b6c6-006097221e3d, version 1 Endpoint: ncadg_ip_udp:[1038] Annotation: AFS session key interface **Solution : filter incoming traffic to this port.** **Risk Factor : Low** Plugin ID : 10736

netbios-ns (137/udp)	The following 5 NetBIOS names have been gathered : = Workgroup / Domain name = This is the computer name = Workgroup / Domain name (part of the Browser elections) = This is the computer name The remote host has the following MAC address on its adapter : If you do not want to allow everyone to find the NetBios name of your computer, you should filter incoming traffic to this port. **Risk factor : Medium** **CVE : CAN-1999-0621** Plugin ID : 10150

© SANS Institute 2004, Author retains full rights.

Last Updated: May 23rd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced