Global Information Assurance Certification Paper

GIAC Certification GSEC Practical
Kelly R. LeNeave
User Name: k_lenea001
Version 1.4b Option 2 – Case Study in Information Security
February 2004

Case Study: Auditing a Windows Environment

Abstract:
This case study will provide the reader with information and resources necessary to conduct a security audit of Microsoft Windows within a corporate environment. The company for which I work will be given the fictitious name of ACME FS to protect privacy and security. ACME FS is a financial institution where proper information security policies and procedures have already been established and implemented. However, I have identified a weakness within the company's network security practices. A time lapse currently exists between scheduled, third-party network audits. These audits are performed by an external security firm and take place every year to year and a half. Federal regulations mandate that a high level of security be met for financial institutions like ACME FS. To help achieve this level of security these non-biased audits are essential. However within this time lapse, new system vulnerabilities could be uncovered and changes within the company's network environment could occur. Not addressing these vulnerabilities could result in unauthorized network access leading to the potential loss of customer confidentiality and financial assets.

My goal is to take a proactive approach in protecting our company's computer systems from the latest vulnerabilities related to Microsoft Windows, specifically Server 2000 and XP Professional. I will use the resources and knowledge obtained from the SANS training program to ensure that known vulnerabilities are identified and proper updates are applied.

Before

Setting the stage – The Company
ACME FS is a financial institution that provides banking services to a local and growing regional community. This company relies heavily on technology to maintain a competitive edge as a financial service provider.

ACME FS converted its entire database to an in-house system within the last decade. This has allowed for increased efficiency in data processing and an environment that requires the latest technological advancements. With this step toward self-containment, there is a heightened risk for security dilemmas. ACME FS desires to take the necessary security measures to ensure customer confidentiality and availability of financial information. This project is another preemptive action to maintain and improve the highest practices in security.

Setting the stage – The Computing Environment
The company's operating environment consists of 120 computers. Thirteen of these computers are servers running Microsoft (MS) Windows 2000 Server, and the remaining are end-user workstations running MS Windows XP Professional. The operators of the 107 end-user workstations use MS Office 2000/XP and a variety of proprietary financial applications. However, the scope of this security audit will be limited to the MS operating system, MS SQL server, Internet Information Server (IIS), and the MS Office Suite.

Below is a basic breakdown of the server hierarchy. This chart also contains each server's main roll and software applications.

Server Name	Roll
Server1	File server, MS SQL Database Server, Active Directory Domain Controller
Server2	Proprietary database server
Server3	DNS Server
Server4	Public web server – IIS 5, MySQL, PHP
Server5	Development web server – IIS 5, MySQL, PHP
Server6	Building 1 backup file server
Server7	Building 2 backup file server
Server8	Building 3 backup file server
Server9	Building 4 backup fileserver
Server10	Proprietary interface server
Server11	Network storage device
Server12	MS Exchange 2000 mail server
Server13	Backup proprietary database server

Setting the stage – The Security Dilemma
I have identified several security risks associated with the current posture of ACME FS and its computing environment. The main concern is the lengthy time lapse between scheduled third-party security audits. During this time, regular in-house inspections and maintenance of the network have not been taking place. It was not until my training with SANS that I became aware of the many security vulnerabilities that could exist and the importance of maintaining a secure operating environment.

Setting the stage – The Plan
Currently ACME FS has not been verifying that operating system updates have been applied. These critical updates provide patches that are essential to the security of the operating system. One major vulnerability that is checked for during the update process is the CERT® Advisory CA-2003-16 Buffer Overflow in Microsoft RPC. According to Ian A. Finlay of the Cert Advisory Board the negative impact of this vulnerability is that "A remote attacker could exploit this vulnerability to execute arbitrary code with Local System privileges or cause a denial of service." Even though the computers are configured to automatically update, there is always a possibility that this could not occur. For this reason,

there needs to be a process of patch verification within the network. I plan to use the Microsoft Baseline Security Analyzer V1.2 to verify that critical updates have been implemented at least once every three months.

The Microsoft Baseline Security Analyzer, as mentioned above could also be useful when a new computer has been introduced to the network or when a current system has to be rebuilt. Due to the overwhelming number of updates that exist, this tool provides assurance that all updates have been applied.

Microsoft Office updates for end-user workstations are another critical component to a secure computing environment. At the present time, ACME FS has no set regiment for applying these updates. Updates are only applied during the initial installation of the office suite. In some cases, many computers may have not received updates for more than a year. This current state puts ACME FS at severe risk to many exploits, such as execution of malicious macros, buffer overflows, and other program exploits.

Deploying these updates as they are released is imperative to keeping information protected. Microsoft has developed a tool to aid in auditing for these updates. According to Microsoft Office Online, “The Office Update Inventory Tool 2.0 reports on which updates have been applied, which updates are available to be applied, and which updates can be applied only to an administrative image.” The range of updates needed for each computer should be derived from the reports produced by this tool. MS Office updates will be conducted in correspondence with the Microsoft Baseline Security Analyzer at ACME FS.

Another risk associated with the current security state of ACME FS is the absence of auditing for weak passwords, default passwords, and non-existent passwords. Presently, passwords are assessed only when third-party audits are performed. The Tech TV staff report the following information from the SANS Institute, "Easy to guess passwords and default passwords are a big problem, but an even bigger one is accounts with no passwords at all. In practice, all accounts with weak passwords, default passwords, and no passwords should be removed from your system."

Systems with weak or no passwords are easy targets for intruders. Programs such as John the Ripper and @stake LC 4 are often used by intruder in an attempt to break an account. Once an account has been compromised, the intruder has made strides in invading the network. From this vantage point, the intruder has the ability to create his/her own account for future entry and possibly disrupt the availability of information to customers and company.

To mitigate the risks associated with passwords, I plan to use @stake LC4 to audit for weak passwords. By doing this every 3 months, I hope to better follow through on ACME FS’s existing password policy.

Other improvements that could be made to enhance security within the operating environment include auditing systems for unnecessary and unidentified open ports. Unnecessary and unidentified ports may be running services that could be vulnerable to an attack. Malicious programs intentionally installed by an intruder, which provide a backdoor to the system, could cause unauthorized access to the network. If an unexpected port is open, this should be a red flag for a possible unwarranted program. There are numerous ports associated with many well-known programs such as keyloggers and trojans. Below is a table that contains common programs and associated port number.

Program	Port Number
FTP	21
Telnet	23
HTTP	80
SubSeven Trojan	1243
MS SQL Server	1433
Virtual Network Computing	5800
Hack'99 KeyLogger	12223
PCAnywhere	65301

Founstone Super PortScanner

Foundstone's SuperScan 4 is a TCP port scanner that I will utilize to identify unnecessary or unidentified open ports. SuperScan is an essential tool for performing an audit due to its ability to efficiently scan IP addresses and ports as well as produce a detailed report of findings. This information will be important to ACME FS because it will provide clues about what programs are running on our network.

Throughout the course of an operating system's lifetime, new security findings may arise that are not initially addressed by the software vendors. These issues can range from software design flaws to configuration settings that leave many systems vulnerable to an attack. Vendors may not acknowledge these findings as security risks, but many groups such as The SANS Institution, CERT Coordination Center, and many leading experts have deemed such vulnerabilities as risks. Solutions to these potential risks are commonly referred to as "Best Practices."

At the present time, ACME FS does not have a set course of action to address these types of software vulnerabilities. Sites such as SANS and CERT maintain information on security "best practices" that will aid ACME FS in obtaining and remaining current on information security "Best Practices."

During

A beginning – SANS Top Windows Vulnerabilities

My assessment will cover the SANS top 10 windows vulnerabilities, which contain many of the vulnerabilities that I have discussed above. This list contains "the ten most commonly exploited vulnerable services in Windows"(SANS Institute). By auditing for these ten most critical vulnerabilities, I hope to identify

and mitigate risks related to ACME FS's computing environment. Also, the reader should have a greater understanding of how and where to begin an audit of a Windows environment. A detailed list of tools and their availability will follow at the conclusion of the document.

Anyone out there?
This audit will begin with a network discovery, which is the process of mapping-out or identifying all devices on the network. An extremely useful tool in analyzing a network is Insucure's Nmap. Nmap is a free, open source tool designed to explore networks and identify host operating systems, services, and open ports.

ACME FS's network is sectioned into five IP addressing schemes (see diagram below). I will scan each portion of the network for devices and then compare the resultant sets against a list of known devices.

IP Address	Network Section
192.168.1.1 – 192.168.1.255	Building 1
192.168.2.1 – 192.168.2.255	Building 2
192.168.3.1 – 192.168.3.255	Building 3
192.168.4.1 – 192.168.4.255	Building 4
192.168.5.1 – 192.168.5.255	Building 5

From a command prompt within the Nmap directory, I used the following command to run a simple Nmap ping sweep scan. Nmap has a wide variety of options available when performing network scans. Additional information on performing a more in depth scan is available within Nmap's documentation.

Nmap –v –sP –oN output.txt 192.168.1.1-255

Below is a brief summary from the NMAP man pages of the aforementioned command.

> **-sP** – This option is used to do a simple ping sweep scan. This type of scan will show only active hosts on the network.
>
> **-v** – Verbose. Outputs detailed information to the system console.
>
> **-oN** – This option is used to log all details from a Nmap scan to an external file.

After analyzing the results produced from the scan, I was able to single-out four unidentified devices that were not on ACME FS's list of known hardware. To investigate further, I again used Namp to perform a more detailed scan on the hosts in question.

> Nmap –v –O –oN output.txt <unknown host IP>

The following is a break-down of the additional commands used to identify the unknown hosts.

> **-O** – This option is used to fingerprint the host operation system. Nmap analyzes responses from the remote host and compares them to known fingerprints to provide host identification.

From the results, I was able to gather that these four unknown devices were composed of three MS Windows XP computers and one Hewlett Packard network printer. These devices were newly introduced into the network and had not been logged in ACME FS's list of known hardware.

Internet Information Server (IIS)
Microsoft's Internet Information Server (IIS) has had a history of security related issues which has made it an important aspect to network security. Improperly configured or un-patched installations of IIS could be at severe risk of an attack. I will use MS Baseline Security Analyzer to see that necessary critical updates have been applied. Configuration settings will also be verified by logging onto each web server to inspect security settings.

Upon analyzing the results of the scan, the MS Baseline Security tool showed that two servers were not at a current patch level. After further inspection I was able to determine by running Windows Update Service that the two servers in question were current with all patches released by Microsoft. A note from Microsoft on the Baseline Security Analyzer tool: "It will produce false positives if files scanned were updated by an installation that is unrelated to a security bulletin and/or some security bulletins are not addressed by a file update but a configuration change that cannot be verified." However, I believe the usefulness of this tool far outweighs its flaw in reporting false positives. In a large scale network environment this tool is a must to verify that systems are patched.

Another aspect to securing IIS is proper configuration of extensions and services. This portion will cover disabling WebDAV, removing unnecessary ISAPI extensions, eliminating sample applications, and verifying that proper access permissions are set.

WebDAV is an IIS extension that enables web authors to maintain and upload content remotely to a website. This extension is enabled by default on IIS 5 installations and does not require authentication. Vulnerabilities include the MS IIS WebDAV Remote Compromise Vulnerability. The Internet Security Systems site states that "The impact includes the ability for a remote attacker to run arbitrary code on vulnerable servers."

To check if WebDAV is disabled on IIS systems the following registry key should be verified. This can be done by logging into each web server and executing regedit.exe from the run dialog box. IIS installations with WebDAV disabled will have the following registry values:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters**:**
Value name: DisableWebDav
Data type: DWORD
Value data: 1
(Microsoft Knowledge Base Article – 241520)

Upon inspection, all web servers had the WebDAV extension enabled. ACME FS has determined that this featured is not needed and should be disabled.

ISAPI are programming extensions that include asp, php, ColdFusion, and web service printing. There have been vulnerabilities with these ISAPI programming extensions that careful attention should be taken to ensure that only necessary ISAPI hooks are used.

I was able to gather that ACME FS's web server did not need most of these extensions that were available by default. ACME FS will remove all unneeded items from its web server, excluding the asp and php ISAPI programming extensions, to help reduce any risks that could arise.

> To disable unused ISAPI extension
> 1. Open the Internet Information Services located in the Administrative Tools,
> 2. Navigate to the properties of each web site configured on each web server,
> 3. Select the Home Directory tab, and select the Configuration button.
> From the Application Configuration window a list of active ISAPI hooks will be displayed.
> 4. Simply clicking remove on each item will disable the unneeded ISAPI hook.

A simple, but commonly overlooked feature that is most often found on an IIS installation are sample scripts or sample sites. These samples are packaged with IIS and serve as working demonstrations of IIS's functionality. It has been proven that these applications are not intended to be in a production environment and have had vulnerabilities discovered that could lead to execution or overwriting of files as well as unauthorized access to sensitive data, including the administrator's password (SANS Institute).

To verify if an IIS installation has sample scripts available, navigate to the web root and check for the directories listed in the following table.

Sample	Virtual Directory	Location
IIS Samples	\IISSamples	c:\inetpub\iissamples
IIS Documentation	\IISHelp	c:\winnt\help\iishelp
Data Access	\MSADC	c:\program files\common files\system\msadc

Microsoft TechNet Baseline Security Checklist

If these directories are present, it will be necessary to remove each. Sample script can also be removed through the use of MS's Lock Down Tool for IIS. This tool is a wizard-based application to help secure an IIS web server. After auditing each of ACME FS's web servers, I found that one site, which was used as a development server, had sample applications and scripts available. It will now be ACME FS's practice that all sample applications are removed.

An additional key to securing an IIS installation is setting appropriate ACLs on virtual directories. Not applying the correct ACLs could lead to unwanted script executions causing an intrusion or disclosure of private information. The following is a recommendation by Microsoft of ACLs settings for securing IIS installations.

File Type	Access Control Lists
CGI (.exe, .dll, .cmd, .pl)	Everyone – Execute Administrators – Full Control System – Full Control
Script files (.asp, .php)	Everyone – Execute Administrators – Full Control System – Full Control
Include files (.inc, .shtm, .shtml)	Everyone – Execute Administrators – Full Control System – Full Control
Static Content (.txt, .gif, .jpg, .html)	Everyone – Read Administrators – Full Control System – Full Control

It is also a "Best Practice" to create a subfolder for each type of file and set the appropriate ACLs on each folder and have these permissions be inherited to the files contained in each folder (Microsoft TechNet Baseline Security Checklist).

Microsoft SQL Server

Microsoft SQL Server and Microsoft Server Desktop Engine (MSDE) are other important areas that should be considered when performing an audit. Commonly, databases like MS SQL Server serve as a warehouse for information. Oftentimes these databases will contain personal information such as names, addresses, social security numbers, and credit card numbers. This type of information makes databases an appealing target for intruders. Recently, the security community has seen the MS SQL exploit SQLSnake worm, "which inserts itself into a MSSQL database servers with no password protecting the SA (System Administrator) account," according to Riley Hassell of eEye Security. Successful execution of this exploit gives the attacker full control of the targeted PC. This exploit is able to succeed due to the SQL administrator (SA) account having no password.

Auditing of MS SQL Servers will cover checking for the default SA account password, and that every instance of MS SQL Server and MSDE are current with all patches released.

Chip Andrews SQLPing2 will be used to audit for MS SQL administrator accounts that do not have a password. By default the MS SQL Server administrator account is enabled with no password. SQLPing2 works by scanning a given range of addresses for SQL Servers. Once a SQL Server is encountered, it will try to authenticate to the SA account with no password.

Results showed that all SQL Server administrator accounts had a password set. The following are steps that would need to be taken if a SA account did not have a password associated with it.

> Changing the Sa Account Password From the SQL Enterprise Manager
>
> 1. Start the SQL Server Enterprise Manager.
> 2. Right-click 'Microsoft SQL Servers' or your SQL server group
> 3. Select your 'YourServerName (Windows NT)
> 4. Expand the plus (+) sign next to your server name
> 5. Expand the 'Security' leaf
> 6. Select 'Logins'
> 7. Select the Sa account
> 8. Right mouse-click and from the context menu select 'Properties'
> 9. Type in the password and select 'OK'
> 10. At the 'Confirm Password' dialog box in the 'Confirm New Password' section type in the password once again and select 'OK'
> (Hite 2002)

To verify that all computers running MS SQL Server and MSDE are at a current patch level the MS Baseline Security Analyzer will be used. After running the scan, I found that one instance of SQL Server 7 was behind in service packs, but all SQL Server 2000's and Microsoft Server Desktop Engines had all critical updates applied. To resolve the findings, the required service packs will need to be downloaded and installed. MSDE updates can be applied through the use of Windows Update Service.

Windows Authentication

Passwords are another critical component to a secure environment. However, I believe that it is one of the most difficult aspects of security to control. I have found it hard to enforce password complexity requirements. When employees are forced to adhere to a complex password scheme they sometimes resort to writing down and storing their password near their work area.

My audit will include using LC4 to check for weak passwords and a physical spot check of workstations for passwords that may be kept at a user's workstation.

Overall LC4 was able to crack 72 out of 163 passwords within a 48 hour time frame and 38 of these passwords were cracked within the first 2 minutes of the audit. Most of these accounts were cracked through a dictionary style attack. This attack method uses a dictionary word list to generate password hashes to match against the password hash that is being cracked. Also, two accounts with

administrative privileges were compromised within the 48 hour time period. These results showed that even using the passfilt mechanism for enforcing strict password requirements, passwords can still be cracked.

I selected 10 workstations at random to audit for passwords that were being stored near the user's workstation. From this check, I found that one user had a list of passwords stored in the top draw of their desk. I was able to obtain the user's network password and gain network access. ACME FS's course of action will be to educate its users on important security issues which will include proper password procedures.

I also tested for LM authentication, which is the default authentication method used by Windows 2000 Server and Windows XP Professional. The LM authentication method stores an easily breakable hash of the users' password. The hash can be broken by cracking programs such as John the Ripper and LC4 in a matter of moments.

ACME FS is currently using the LM authentication method due to legacy computers still in operation. However, these legacy computers will be replaced within a short period of time. Once these computers have been replaced, ACME FS will implement the NTLMv2 authentication method. The NTLMv2 is a much more secure authentication method which uses a stronger encryption method and makes it extremely difficult for cracking programs to break passwords. The following is the registry key that can be used to check or enable NTLMv2 authentication method on a Active directory Domain Controller.

> HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\LMCompatibilityLevel
> Data type: DWORD
> Value data: 5
> (SANS Institute)

The registry value of five sets the domain controller to refuse any other authentication method other than NTLMv2. To enable Windows XP computers to use the NTLMv2 authentication method, a new computer policy will need to be created.

> This can be done by navigating to the security policy for the domain and under the Computer Configuration -> Windows Settings -> Local Policies -> Security Options -> LAN Manager Authentication Level -> set this value to Send NTLMv2 response only\refuse LM.

Internet Explorer

Microsoft's Internet Explorer has had a history of security related issues which makes it a prime target for intruders. A web author could craft a malicious web page to take advantage of a security hole to gather information, execute arbitrary code or completely control a vulnerable system. That is why it is important to stay current with all updates related to Internet Explorer. Again, I will use

Microsoft's Baseline Security Analyzer to audit all network computers to ensure that all critical updates are installed.

From my scan I found that all computers were updated with the latest critical updates. As an additional security measure ACME FS will now implement industry consensus "Best Practices" related to Internet Explorer. The following is a list of "Best Practices" as related to Internet Explorer (SANS Institute).

> To configure the Security settings for Internet Explorer:
>
> 1. Select Internet Options under the Tools menu.
> 2. Select the Security tab and then click Custom Level for the Internet zone.
> 3. Most of the flaws in IE are exploited through Active Scripting or ActiveX Controls. Under Scripting, select Prompt for Allow paste operations via script to prevent content from being exposed from your clipboard.
>
> Note: Active Scripting should not be disabled since it is used by many websites.
>
> ActiveX Controls are not as popular but are potentially more dangerous as they allow greater access to the system.
> 4. Select Prompt for Download signed ActiveX Controls.
> 5. Select Disable for Download unsigned ActiveX Controls.
> 6. Also select Disable for Initialize and script ActiveX Controls not marked as safe.
> 7. Java applets typically have more capabilities than scripts.
> Under Microsoft VM, select High safety for Java permissions in order to properly sandbox the Java applet and prevent privileged access to your system.
> 8. Under Miscellaneous select Disable for Access to data sources across domains to avoid Cross-site scripting attacks.
> 9. Ensure no un-trusted sites are in the Trusted sites or Local intranet zones as these zones are weaker security settings than other zones.
> (SANS Institute)

Windows Remote Access Service

The following audit will focus on Microsoft's specific networking technologies such as NULL sessions and remote registry access. A NULL session is a connection made to a host computer without any form of authentication required. Information that can be enumerated from NULL sessions includes user names, shares, password policies, and groups all of which can aid an attacker in compromising a system (SANS Institute). Since ACME FS's active directory is running in mixed mode, it is possible that it could be vulnerable to NULL session attacks. I will use NetBrute to audit for the NULL session vulnerability.

Results showed 36 computers that are vulnerable to a NULL session attack. The following is the necessary registry key to disable NULL sessions. The following was taken from Microsoft Q Article 246261:

> Use Registry Editor to view the following registry key, and then add the following value to this key, or modify it if the value already exists:
> HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA
>
> Value: RestrictAnonymous

Value Type: REG_DWORD
Value Data: 0x2 (Hex)

Restart the computer after any change to the RestrictAnonymous key in the registry.

My next test was to audit for machines that allowed remote registry access. Accessing the registry via the network is a feature that is available on most all versions of Windows. Typically incorrect permissions set for remote registry access leaves many systems vulnerable to an attack. To audit for this vulnerability, I will use Microsoft's regdump.exe. Regdump.exe attempts to establish an anonymous connection to a remote host's registry. If the attempt is successful, it will be able to download information from the registry.

Running regdump.exe against the computers on the network showed that 40 computers did not have the appropriate permissions set and were vulnerable to a remote registry attack. ACME FS has decided that remote access should be restricted to administrators. The following is an excerpt from Microsoft Knowledge Base article 153183 on how to restrict remote registry access.

1. Start Registry Editor (Regedt32.exe) and go to the following subkey:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control

2. On the Edit menu, click Add Key.
3. Enter the following values:
Key Name: SecurePipeServers
Class: REG_SZ

4. Go to the following subkey:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers

5. On the Edit menu, click Add Key.
6. Enter the following values:
Key Name: winreg
Class: REG_SZ

7. Go to the following subkey:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg

8. On the Edit menu, click Add Value.
9. Enter the following values:
Value Name: Description
Data Type: REG_SZ
String: Registry Server

10. Go to the following subkey.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg

11. Select "winreg". Click Security and then click Permissions. Add users or groups to which you want to grant access.

12. Exit Registry Editor and restart Windows.
13. If you at a later stage want to change the list of users that can access the registry, repeat steps 10-12.

Microsoft Data Access Components
Microsoft Data Access Components is a programming interface used to connect to information sources such as OLE, and ODBC database technologies. Recently, their have been flaws such as buffer overflows that could leave a system vulnerable to an attack (MS Security Bulletin MS03-033). To audit systems that may be vulnerable to an MDAC attack I will uses MS Baseline Security Analyzer.

This audit showed that no computer was vulnerable to an MDAC attack. However, if a system was vulnerable, simply running MS Windows Update on the exposed system would install the necessary patch.

Windows Scripting Host
Microsoft developed the Windows Scripting Host (WSH) to automate many windows tasks targeted to aid system administrators. However, by default there is no mechanism to prevent malicious scripts that utilize the WSH from running. Malicious scripts can be crafted to take full control of the targeted computer once it has been run. In the case of the VBS.LoveLetter.A and VBS.NewLove.A worms, it enabled the virus writer to automate actions that ran a direct script execution without end-user intervention (Symantec). "Best Practice" recommends that files with the .vbs, .vbe, .js, .jse, and .wsf extension should by default open in a text editor such as Windows notepad once executed. Users requiring the use of a script would have to explicitly specify the filename of the script as an argument for the WSH scsript.exe or wscript.exe (SANS Institute). By changing the default behavior, the risks of a potentially malicious script from executing are reduced.

Currently ACME FS's computer systems are configured to run all scripts without any means of verification. ACME FS will take the aforementioned "Best Practice" and apply it to all servers. End-user workstations have been determined to not need the functionality of WSH and therefore will have this feature disabled. The following are the necessary steps required to change the default behavior of script execution.

Changing default behavior:
From Windows Explorer select Tools-> Folder Options->File Types. One by one select each extension from the list that the default behavior will be changed. For scripts that take advantage of the WSH we will need to change the default behavior for the following extensions: .vbs, .vbe, .js, .jse, and .wsf. Then select the change button and from the Open With window select notepad as the default action. Click OK to close the Open With window and select OK once each extension's default action has been changed.

Disabling WSH:
The program, Noscript.exe, will disable the Windows Scripting Host; this will prevent viruses from executing automated scripts.
Note: Disabling the WSH will prevent all the scripts from running on the system.

1. Download Noscript.exe to a folder on the hard disk.
2. Double-click the Noscript.exe icon. The Norton Script Disabler/Enabler appears.
    If the WSH is currently enabled on the system, you will be prompted as to whether you want to disable it. To do so, click Disable, and then click OK.
    If the WSH is currently disabled on the system, you will be prompted as to whether you want to enable it. To do so, click Enable, and then click OK.

The following are optional command-line parameters to Noscript.exe:

/silent
This suppresses the enable/disable dialog and automatically disable WSH. If WSH has already been disabled, Noscript will do nothing.

/silent /on
This suppresses the enable/disable dialog and automatically enables WSH. If WSH has already been enabled, Noscript will do nothing. The "/on" parameter must be used in conjunction with the "/silent" switch; it cannot be used by itself. (Symantec)

Microsoft Outlook and Outlook Express
Outlook is the default mail client used throughout ACME FS's computer systems. Outlook Express is also available on all systems as it is part of the Microsoft operating system. There has been many security related issues that have been exposed that make it a high priority because it is used on most MS operating systems. Recently, exploits targeted at Outlook and Outlook Express can cause a denial of services, propagation of internet worms, and buffer overflows which leads to code execution of the attacker's choice. These attacks usually arrive via email and take advantage of systems that do not have the appropriate patches installed.

Auditing for necessary critical updates related to Outlook Express and Outlook can be performed by using MS Baseline Security Analyzer and Microsoft Office Inventory Tool 2.0 respectively.

Results from MS Baseline Security Analyzer showed that all occurrences of Outlook Express had the latest security patches and product upgrades. MS Office Update Inventory Tool 2.0 will be utilized to determine if MS Outlook has the latest patches installed. An advantage to using the MS Office Update Inventory Tool 2.0 is the ability to also perform checks on all MS Office programs for critical updates.

Upon completion of the MS Office audit, I found that many workstations did not have the appropriate patches installed. To address this matter, an administrative

image of MS Office XP will be created and deployed to all work-stations. By creating a baseline install of Office, it will ensure all workstations have the identical patch level. Any subsequent updates will be applied through the use of MS OHotFix.exe. The following are the steps necessary to create an administrative image of Office XP and install updates that may be released at a later time:

> Creating an administrative image:
> 1. Create a share on a network server for the administrative installation point.
> 2. On a computer that has write access to the share, connect to the server share. The computer must be running a supported operating system: Microsoft Windows 2000 or later, Microsoft Windows NT® 4.0 Service Pack 6a, Microsoft Windows Millennium Edition (Windows Me), or Microsoft Windows 98.
> 3. On the Start menu, click Run, and then click Browse.
> 4. On the Office XP CD, double-click setup.exe and add /a to the command line.
> 5. Enter the organization name that you want to define for all users who install Office from this administrative installation point.
> 6. Enter the server and share you created as the installation location.
> 7. Enter the 25-character Volume License Product Key and click Next.
> 8. Accept the end-user license agreement and click Install.
> (Office XP Resource Kit)
>
> Maintaining with OHotFix.exe
> To apply a client update file using OHotFix, you first extract the individual MSP files from the client update EXE package and then run OHotFix from a command line to deploy the update to the computer.
>
> You can extract the files from the client update file by using a command line similar to the following:
> C:\path to update file\MyUpdate.exe /c
> /t:C:/folder for extracted files
> (Microsoft Office XP Online)

Windows Peer to Peer File Sharing

Peep to Peer (P2P) file sharing programs are used to download and or distribute many types of files. Problems associated with P2P programs are those such as the legitimacy of downloaded programs (viruses), release of sensitive information, saturation of bandwidth, and the potential of distributing copyrighted materials.

One technique to audit for P2P programs is by using a port scanner. Typically, most P2P programs operate on a set port which can be detected by a port scanner. Foundstone's SuperScan 4 will be used to scan the entire range of ACME FS's IP addresses for known ports associated with P2P file sharing programs. Not only can SuperScan 4.0 detect P2P programs running on hosts, it can also detect other programs running on ports that may act as a gateway for intruders. The following is a listing of ports used by some popular P2P files sharing programs.

eDonkey	Gnutella	Kazaa
Tcp 4661	Tcp/udp 6345	Tcp 80
Tcp 4662	Tcp/udp 6346	Tcp/udp 1214
Upd 4665	Tcp/udp 6347	
	Tcp/udp 6348	

(SANS Institute)

Results of the port scan showed that there were no instances of P2P programs running. However, the scan did produce several instances of anonymous ftp access, PCanywhere hosts, unnecessary MS Window services, and SSH sessions. All findings will be investigated further to determine the need of each.

Simple Network Management Protocol (SNMP)
SNMP is used by administrators to configure and communicate with remote devices such as printers, routers, and other networking devices. Many devices with SNMP enabled utilize a poor mechanism to authenticate users through the use of a community string. The community string can be thought of as a password. However, most vendors set the community string to "public" or "private" which is commonly known by most attackers. Risks associated with SNMP include the ability for an attacker to reconfigure or shut down devices causing a disruption of service.

To audit for devices running SNMP I will use Foundstone's SNScan 1.04. From scanning the entire range of ACME FS's IP address block, two MS Windows 2000 servers were identified as running SNMP service. It has been determined that SNMP on these servers is not necessary and will be ACME FS's practice to disable it. Removing SNMP requires the following steps to be taken.

From the Windows 2000 Control Panel.
Double click the Add/Remove Programs icon.
Select Add/Remove Windows Components.
Check the Management and Monitoring Tools box.
Click the Details button.
Uncheck the Simple Network Management Protocol box and click OK.

Conclusion:
From this audit of ACME FS's network I have found that it is important to have an ongoing strategy for addressing security. The information security field is an ever-changing world that demands an ongoing effort. ACME FS will perform tests approximately every three months of the network to make sure that a high level of security is maintained. These tests will include many of the ones discussed in this paper. I will also be sure to include any test that would aid in discovering new threats. Also from this audit, ACME FS will develop a security checklist based on the SANS top 10 list that will serve as a guide when introducing new computers into the network.

I tested for the SANS top 10 Windows vulnerabilities which included assessing both the servers and workstations. Some of these tests included checking for password policy compliance, SQL vulnerabilities, and IIS security settings. Most incidents were moderate in risk, however addressing these issues have helped ACME FS become a more secure computing environment. This project truly demonstrated that information security is an on-going practice. If limited to the annually scheduled third party audits, ACME FS could put itself at risk. And with the nature of the information that ACME FS handles, it is of the utmost importance that all possible steps are taken to ensure the privacy of customer information.

From my audit I did verify that Windows 2000 Server and XP Professional were being updated with the latest operating system critical updates released by Microsoft. However, Microsoft Office updates were not being applied as much as needed. From my research, I learned how to resolve MS Office security issues by utilizing the Microsoft Office Update Inventory tool. This patching tool enables updates to be automatically applied to susceptible Office installations. Another weakness that I identified was that many computers were vulnerable to a NULL session attack. By using a tool such as NetBrute a disgruntled employee could use this program, which would reveal to them usernames and network shares. With access to this information, the intruder could be more apt to launch a successful attack. To combat this weakness, I applied the necessary registry sessions that would prevent the release of sensitive information. Before the audit, ACME FS did not have a procedure for implementing industry "Best Practices". This audit showed that programs such as IIS, Outlook, and Internet Explorer were not being properly configured as recommend by "Best Practice". It will now be ACME FS's intention to stay current on this type of information and to implement any changes that relate to the computing environment.

Sites such as SANS, Carnegie Mellon Software Engineering Institute, and NIST's Computer Security Resource Center (csrc.nist.gov) are excellent resources that will be used by ACME FS's information technology team. By utilizing the resources provided by these security websites, ACME FS will be taking a proactive approach in gaining knowledge of the latest security issues.

The SANS training program has instilled in me the belief that information security should be a high priority. I have also had to opportunity to use a variety of software programs to evaluate network security that I had not previously been exposed to before SANS. Programs such as Nmap, Microsoft Baseline Security Analyzer, and NetBrute are essential tools that help ensure that security measures are being implemented and are effective. I have a heightened awareness of how important it is that we at ACME FS do everything possible to ensure that our customer's information stays safe and secure.

Bibliography

"Alerts" Internet Security Systems. 17 Mar. 2003 11 Feb. 2004 http://xforce.iss.net/xforce/alerts/id/advise144

Finlay, Ian A. "CERT® Advisory CA-2003-16 Buffer Overflow in Microsoft RPC" 17 July 2003. 23 Jan. 2004 http://www.cert.org/advisories/CA-2003-16.html

Hassell, Riley. "Spida or Digispid.B.Worm SQL Worm Analysis" eEye Digital Security 22 May 2002. 5 Feb. 2004. http://www.eeye.com/html/Research/Advisories/AL20020522.html

Hite, Don. "Changing The SQL Server Sa Account If The Password Is Unknown" myITforum.com 21 May 2002. 5 Feb. 2004. http://www.myitforum.com/articles/14/view.asp?id=2816

"How to disable or remove the Windows Scripting Host" Symantec 4 Mar. 2004. http://www.symantec.com/avcenter/venc/data/win.script.hosting.html

"How to Restrict Access to the Registry from a Remote Computer" Microsoft Knowledge Base 26 Feb. 2004. 4 Mar. 2004. http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q153/1/83.ASP&NoWebContent=1

"How to Use the RestrictAnonymous Registry Value in Windows 2000" Microsoft Knowledge Base 22 Aug. 2003. 4 Feb. 2004.

http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q246/2/61.ASP&NoWebContent=1

"IIS 5.0 Baseline Security Checklist" Microsoft TechNet 2001 5 Feb. 2004 http://www.microsoft.com/technet/security/chklist/iis5cl.mspx

J.D. Meier, Alex Mackman, Michael Dunner, Srinath Vasireddy, Ray Escamilla and Anandha Murukan. "How To: Use the Microsoft Baseline Security Analyzer" MSDN Jun. 2003. 11 Feb. 2004 http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/HTBaseAnal.asp

Microsoft Knowledge Base Article - 241520 "How to Disable WebDAV for IIS 5.0" Microsoft 24 Mar. 2003. 4 Mar. 2004. http://support.microsoft.com/default.aspx?scid=kb;en-us;241520

Microsoft Office Online. 11 Nov. 2003. Microsoft. 10 Feb. 2004 http://www.microsoft.com/office/ork/2003/journ/offutoolv2.htm

Microsoft Office XP Online "Installing Client Update Files with OHotFix" Microsoft 13 Dec. 2001. 4 Mar. 2004. http://www.microsoft.com/office/ork/xp/journ/Ohotfix.htm

"Microsoft Security Bulletin MS03-033" Microsoft TechNet 20 Aug. 2003. 4 Mar. 2004. http://www.microsoft.com/technet/security/bulletin/MS03-033.mspx

Office XP Resource Kit “Creating an Administrative Installation Point” 4 Mar. 2004. http://www.microsoft.com/resources/documentation/office/xp/all/reskit/en-us/depb01.mspx

TechTV Staff. “FBI Releases List of Top 20 Computer Risks” TechTV 1 Oct. 2001. 10 Feb. 2004 http://www.techtv.com/news/security/story/0,24195,3350889,00.html

“The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus” SANS Institute 8 Oct. 2003 2 Feb. 2004 http://www.sans.org/top20/#w1

Program Resources

Microsoft Baseline Security Analyzer v1.2
http://www.microsoft.com/technet/security/tools/mbsahome.mspx

Office Update Inventory Tool 2.0
http://www.microsoft.com/office/ork/2003/journ/offutoolv2.htm

@Stake LC4
http://www.atstake.com/products/lc/

Foundstone INC Superscan 4
http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/superscan.htm

Insecure NMAP
http://www.insecure.org/nmap/

Microsoft IIS Lockdown Tool 2.1
http://www.microsoft.com/downloads/details.aspx?FamilyID=DDE9EFC0-BB30-47EB-9A61-FD755D23CDEC&displaylang=en

Chip Andrews SQLPing2
http://www.sqlsecurity.com/DesktopDefault.aspx

Microsoft regdump.exe
Microsoft Server Resource Kit

Symantec Noscript.exe
http://securityresponse.symantec.com/avcenter/venc/data/win.script.hosting.html

Microsoft OHotfix.exe
http://www.microsoft.com/office/ork/xp/journ/Ohotfix.htm

Foundstone INC SNScan
http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/snscan.htm