CHAPTER 6

Auditing Windows Operating Systems

The Windows operating system has grown from humble beginnings and evolved into one of the world's most pervasive operating system for servers and clients. This chapter covers the basic components of a Windows server audit and includes a quick audit for Windows clients.

We will discuss the following:

- A brief history of Windows development
- Windows essentials: learning about the target host
- How to audit Windows servers
- How to audit Windows clients
- Tools and resources for enhancing your Windows audits

Background

Microsoft and IBM worked jointly to develop OS/2 in the early 1990s, but the relationship turned sour. Microsoft and IBM split up and went separate directions, with Microsoft later releasing Windows NT in July 1993. Microsoft's server line as we know it today finds its roots in these humble beginnings. Windows NT was the professional version of the Windows operating system targeting company and government organizations.

The server market evolved from Windows NT to Windows Server 2000, Windows Server 2003, and then Windows Server 2008. What this means for the auditor is that many versions of the operating system are used in most large environments. It's highly recommended to find the time to familiarize yourself with the operating systems in your particular environment. Not all utilities work on all systems. In some situations, hosts might exist on your network that are no longer supported by Microsoft. Additional controls should be in place to protect these systems, such as technologies that prevent network attacks or malware propagation.

Microsoft Windows products cover nearly two dozen categories. The Enterprise focus breaks down into Client Infrastructure, Server Infrastructure, and Comprehensive Management. Comprehensive Management is an important strategic focus by Microsoft to integrate management into Microsoft System Center, including Configuration

Manager, Operations Manager, Data Protection Manager, Virtual Machine Manager, and Service Manager. The strategic focus includes simplified management platforms targeting midsize and small businesses, called Microsoft System Center Essentials and Microsoft Intune.

Windows Auditing Essentials

The material in this chapter requires a basic understanding of the components that compose the Windows environment. In addition, your role as an auditor and advisor will significantly improve if you understand how to approach a comprehensive audit of a Windows platform.

Figure 6-1 illustrates how the operating system serves as a vehicle for supporting applications. Many components surrounding the operating system should be considered in a complete review. For example, consider the danger of poorly maintained or configured applications. The more applications you add to the platform, the more potential trouble areas you have as an auditor as you increase your attack surface area. Several chapters in this book are devoted to applications that you might want to consider for your audit. In addition, the hardware, storage, and network affect the performance and protection of the operating system. Finally, the surrounding controls and management of the environment affect the support, risk, compliance, and business alignment of the server.

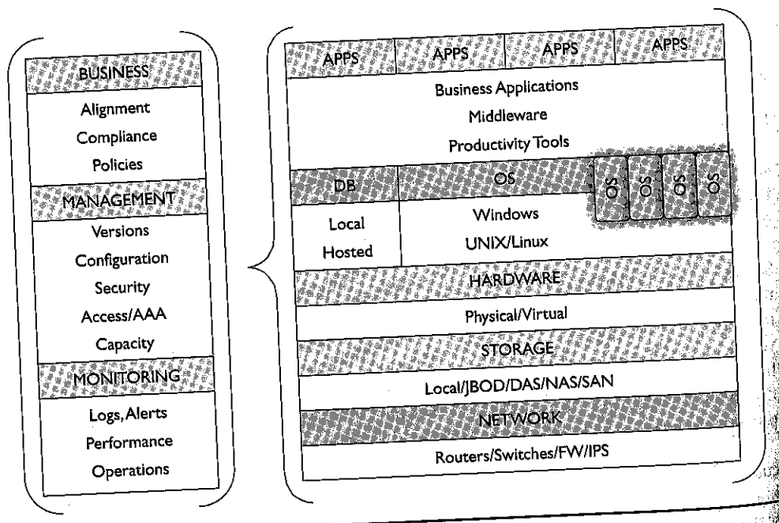

Figure 6-1 Model for auditing hosts

Consider scheduling time on your calendar to use and learn any of the tools discussed in this chapter. You might be surprised at how easy most of them are to use and how much more efficient you become because you know the shortcuts to getting just the information you want. Sometimes it's too easy as auditors to continue using what you've always used because it works, instead of looking at new methods for improving your efficiency. After you've done a little homework, you can ask your company administrators to show you the ropes. Most administrators of any caliber actually enjoy doing this. You can be assured that if you show up to an administrator's office asking about an obscure tool, you'll get his or her attention, and one of you will walk away a little wiser for the visit.

Command-Line Tips

Those of you who are comfortable with the command line on a UNIX machine may appreciate installing UNIX functionality using Cygwin from www.cygwin.com, which allows you to access several utilities such as `ls`, `sed`, `grep`, `more`, and `cat`. It's also possible to create scripts based on these binaries, located in the bin directory, to manipulate the text output from standard Windows utilities. Finally, as long as you understand the risks involved, you power users may even want to add the <drive>:\cygwin\bin directory to the environment path.

NOTE If you like the command line and enjoy scripting, take advantage of the resources located in Microsoft's scripting center website at www.microsoft.com/technet/scriptcenter/default.mspx.

Essential Command-Line Tools

Several tools should be in every administrator's back pocket. Keep in mind that with today's complex firewalls and malware protection, not all these tools may work properly. Test every tool in a lab environment prior to running it on a production network.

NOTE The various tools discussed in this chapter can be powerful. Follow best practices. Learn how these tools work on another computer off the network in a test environment prior to using them on your own computer or production network and systems.

Resource Kit Tools

The Windows 2003 and earlier resource kit tools are beyond this chapter's scope and are not discussed here. Windows 2008 did not ship with a general administration resource kit. Many of the tools you would have found useful have been supplemented with much more robust or powerful tools that are now part of the command line, one of the Remote Server Administration Tools, or are handled by a more powerful Sysinternals tool.

PART II

The old Windows 2003 Resource Kit contains more than 120 different tools for administering and troubleshooting systems, managing Active Directory, configuring security features, and much more. You can still download the Resource Kit tools from Microsoft's website, but you should carefully test any tool that you intend to use to make sure it will not disrupt your environment.

NOTE Microsoft offers outstanding command-line help at http://technet.microsoft.com/en-us/library/cc754340(WS.10).aspx. Type **help cmd** from the command prompt for general information about using the command line in Windows.

Sysinternals Tools

The Sysinternals tools, bought by Microsoft in 2006, help administrators and auditors perform complex tasks and detailed analysis. You can download Sysinternals tools from the website at www.sysinternals.com. Dozens of tools are available for remote administration, network analysis, process and registry monitoring, and other tasks. Several companies include a subset of these tools as part of the standard build for servers and clients.

Other Tools

Many, many other tools are available as well, some of which are listed here and discussed in the various audit steps. You can script nearly everything in the following audit, and in some cases, you may find that you have commercial configuration management tools that can perform a detailed analysis of the system to the standard set in the following discussions. You will still find it helpful to sample critical servers and individually test them for appropriate controls.

One interesting tool, the Windows Forensic Toolchest (WFT), written by Monty McDougal, serves as a wrapper for command-line tools. It can handle any of the tools listed here or others you may want to add. WFT is referenced as part of the SANS forensic track. You can learn more about it from www.foolmoon.net/security (and you might get a discount if you tell him you learned about it from this book).

Common Commands

Table 6-1 presents a list of command-line tools used throughout this chapter.

Server Administration Tools

Remote Server Administration Tools (RSAT) enable a Windows 7 client to manage roles and features running on Windows Server 2003 and 2008 systems. RSAT is comparable in functionality to the Windows Server 2003 Administrative Tools Pack and Remote Server Administration Tools for Windows Vista. Most of the tools in the Adminpak were used for Active Directory (AD) domain-specific administration. If the subject of the audit is part of the AD infrastructure, these tools may be of use. RSAT allows administrators to perform remote server management functions and includes several great tools that are otherwise difficult to duplicate in functionality.

Tool	Description	Where to Get It
psinfo	List system information, including installed service packs, patches, applications, and drive information	www.sysinternals.com
Systeminfo	List system information	Native command
Pslist	List running processes	www.sysinternals.com
psservice	List all installed services	www.sysinternals.com
cmdkey	Create, list, or delete stored credentials	Native command
Netsh	Display or modify network configuration	Native command
netstat	Provide network information	Native command
psservice	List service information	www.sysinternals.com
Sc	Tool for talking with service controller	Native command
DumpSec	GUI and command-line "Swiss army knife" of the security settings	http://somarsoft.com
tcpview	GUI view of processes mapped to ports	www.sysinternals.com
procexp	Powerful GUI process explorer	www.sysinternals.com
Fport	Command line view of processes mapped to ports	www.foundstone.com/knowledge/ proddesc/fport.html
schtasks	List scheduled tasks at the command line	Native command
bootcfg	List boot partition information	Native command
pendmoves	List file move operations scheduled for the next reboot	www.sysinternals.com
autoruns	List everything scheduled to start when your computer starts up—the GUI version	www.sysinternals.com
autorunsc	List everything scheduled to start when your computer starts up—the command-line version	www.sysinternals.com
rsop.msc	Open the resulting set of security policies on your host when run from the Start | Run box or command line	Native command
secpol.msc	Open just the local computer policy	Native command
Pwdump	Dump Windows password hashes into a format usable by nearly all free and commercial password crackers	http://openwall.com/passwords

Table 6-1 Common Commands Used in this Chapter

NOTE You can easily add the Microsoft Windows RSAT to your desktop or laptop computer. Just visit Google, type **Microsoft Remote Server Administration Tools** in the search field, and follow the link to Microsoft's downloads page. After downloading the installer package onto your computer, you need to run the file as an administrator to install the tools onto your system.

Performing the Audit

The key to a successful audit of Windows servers or clients is to review the host thoroughly by itself and in conjunction with the many other possible connections that pass data to and from the host.

The following audit steps focus only on the host and do not cover extensive reviews of overlying applications or trust relationships with outside systems. Also not covered are data input and data output methods or their validity. You would deal with these on a per-host basis using techniques and tools covered elsewhere in this book. The steps shown here are typical of many server audits and represent a good tradeoff between the number of risks covered and the amount of time it takes to review the host.

NOTE The test steps in this chapter focus on testing the logical security of Windows boxes, as well as processes for maintaining and monitoring that security. However, other internal controls are also critical to the overall operations of a computing environment, such as physical security, disaster-recovery planning, backup processes, change management, and capacity planning. These topics are covered in Chapter 4 and should be included in your audit if they have not already been covered effectively in a separate data center or entity-level controls audit.

Test Steps for Auditing Windows

In an ideal world, you would audit against a reference set of controls and information covering every possible configuration setting. However, we don't live in an ideal world, and most of us don't have that much time per host. The test steps in this chapter are a recommended list of items to evaluate. From experience, we know that debate abounds regarding auditing Windows. Can a Windows server be secured? What makes your steps better than someone else's steps? The steps covered here have worked for several companies.

Many auditing programs fail to balance effective audits and effective time management. Related to time management, notice that we spend a lot of time discussing various ways to script the results. Configuration management tools can also be leveraged by the audit team to review scores of servers very quickly, and some audit packages promise the same. The only concerns here regard ensuring that all of the controls that impact the business are covered, and occasionally validating the results of the tools with your own independent reviews.

Setup and General Controls

The following represents a check of the overall system setup and other general controls to ensure overall system compliance with your organization's policy. These are mostly general, high-level controls, such as making certain that the system runs company-provisioned firewall and antivirus programs.

1. Obtain the system information and service pack version and compare with policy requirements.

Policies were written and approved to make your environment more secure, easily manageable, and auditable. Double-check the basic configuration information to ensure that the host is in compliance with policy. Older operating systems increase the difficulty in managing the server and increase the scope of administrator responsibilities as he or she attempts to maintain control over disparate operating system (OS) versions. Maintaining standard builds and patch levels greatly simplifies the process of managing the servers.

How

You could find this information using built-in command-line tools, hunting through the graphical user interface (GUI), and searching the registry. However, two efficient ways to pull up this information include the Sysinternals tool `psinfo` and the native tool `systeminfo`. Go to sysinternals.com and download the pstool package. Use one of these tools to retrieve this information, and then compare the results with your organization's policies and requirements.

NOTE Download `pstools` from www.sysinternals.com/Utilities/PsTools.html. The tool psinfo is part of this set of tools. You may want to use several tools from Sysinternals for auditing your servers.

2. Determine whether the server is running the company-provisioned firewall.

Failure to use a firewall subjects the client to network attacks from malware, attackers, and curious people.

How

Most of the time, a check of the processes on the system shows that the company-provisioned firewall is installed and running on the system. An easy way to script this check is to run the Sysinternals tool `pslist`. Do this by running `pslist <process name>` on the system, and search for the appropriate running process by specifying the process you want to find.

For many organizations, the firewall is centrally managed and the same across all hosts in a group. You may want to verify the configuration of the firewall on the host.

If you are using the Windows Firewall, learn the `netsh` command set, which allows scripted output and changes to the firewall. Try running `netsh firewall show config` to see the overall configuration of the firewall on the host and whether the firewall is configured for particular adapters. Use `netsh firewall show` to see other available options for the `netsh firewall` tool.

3. Determine whether the server is running a company-provisioned antivirus program.

Running software other than company-provisioned software may cause instabilities in the enterprise software environment on the laptop or desktop. Failure to have antivirus protection may allow harmful code or hacking tools to run on the computer that violate company policy.

How

A visual check of the system tray shows that an antivirus program is installed and running on the system. As mentioned earlier, an easy way to script this check is to run `pslist` from Sysinternals on the system and search for the running process:

```
pslist rtvscan
PsList 1.26 - Process Information Lister
Copyright (C) 1999-2004 Mark Russinovich
SysInternals - www.SysInternals.com
Process information for CA-CDAVIS:
Name  Pid Pri Thd Hnd Priv  CPU Time  Elapsed Time
Rtvscan  244 8 53 569 26212  0:07:16.640  85:27:32.223
```

Depending on the nature of your audit, you also might want to check the configuration of the antivirus program on the host. For many organizations, the antivirus program is managed centrally and is the same across all hosts. One thing to be careful about with antivirus programs is the ability to exclude certain files or folders from monitoring. This is an easy way to get around the antivirus program.

4. Ensure that all approved patches are installed per your server management policy.

If all the OS and software patches are not installed, widely known security vulnerabilities could exist on the server.

How

Use `systeminfo` or `psinfo -s` to pull this information up for you, and then compare the results against the policies and requirements of your organization. You can use the output to compare with existing SMS/SCCM, patchlink, and other patch-management data. You could also compare the output with data from a vulnerability scanner to identify possible disparities.

5. Determine whether the server is running a company-provisioned patch-management solution.

Again, running software other than company-provisioned software may cause instabilities in the enterprise software environment on the laptop or desktop. Failure to have a company-provisioned patch-management solution may prevent the server from receiving the latest patches, allowing harmful code or hacking tools to run on the computer.

How

A visual check of the processes in the Task Manager usually shows that the company-provisioned patch-management system for servers is installed and running on the system. For example, this may be evidenced by the existence of the process in the Task Manager or the output of `pslist`. Some organizations like to enable automatic updates, which is also easily checked by looking for "Automatic Updates" in the Control Panel. You can also verify whether the system shows up on the Microsoft System Center Configuration Manager (SCCM) console and validate the last patch cycle applied to a given machine.

6. Review and verify startup information.

Rogue partitions, processes, or programs in violation of your policies can sometimes be found during system startup. In addition, malware will sometimes make use of the next reboot to install kits deeper into the OS.

How

Several utilities can help you dissect what the next reboot will do to the system. Two excellent tools include `pendmoves`, and `autoruns`. You can use `pendmoves` by itself without any switches to understand what file moves are planned for the next system restart.

`Autoruns` is the GUI version of `autoruns`. When you use `autoruns` from the command line, it might be easier to output it to a comma-separated values (CSV) file with the `-c` switch and view the results inside Excel. It might be difficult to appreciate the power of `autoruns` until you use the GUI `autoruns` version to see the information it's capable of uncovering for you.

Review Services, Installed Applications, and Scheduled Tasks

Running services, installed applications, and automated tasks that are beyond the scope of the server's stated purpose increase the complexity of maintaining the server and provide additional attack vectors. Unknown services, applications, and tasks may be indications that a server was compromised. These should be reviewed routinely.

7. Determine what services are enabled on the system, and validate their necessity with the system administrator. For necessary services, review and evaluate procedures for assessing vulnerabilities associated with those services and keeping them patched.

Enabling network services creates a new potential vector of attack, therefore increasing the risk of unauthorized entry into the system. Therefore, network services should be enabled only when there is a legitimate business need for them.

New security vulnerabilities are discovered and communicated frequently to the Windows community (including potential attackers). If the system administrator is not aware of these alerts and does not install security patches, well-known security vulnerabilities could exist on the system, providing a vector for compromising the system.

NOTE This is one of the most critical steps you will perform. Unnecessary and unsecured network services are the number one vector of attack on Windows servers.

How

The tools shown in Table 6-2 reveal key pieces of information to help you identify services and how they are used. `Netstat` reveals the active sockets on your computer listening for external communications. `Psservice`, `sc`, and `DumpSec` list the running services. Next, you can map the running services to the open ports using `tcpvcon`. Finally, `procexp` is also capable of showing you much of this information but cannot be scripted. It is mentioned here because of its powerful capabilities and because it is free.

These may seem like a lot of utilities, but it's worth your time to look through them to decide what information you need for your audit. In general, if the system is being used in the AD domain, ensure that the Group Policy Object (GPO) policy rules are periodically reviewed. These rules are applied to any system that joins the domain/specific branch.

You can use the native `netstat` command by typing `netstat -an` at the command line. Look for lines containing `LISTEN` or `LISTENING`. The host is available for incoming connections on these TCP and UDP ports. You can find a list of services using such tools as `psservice`, which is very much like the `netstat` service on *NIX systems.

Other utilities that map processes to port numbers include the built-in `sc` (try `sc query type= service`) command and `tcpvcon` from Sysinternals. We recommend `tcpvcon` from Sysinternals. The "Tools and Technology" section a bit later offers information about where to find these tools and more. You can run `tasklist /svc`

Tool	Description	Where to Get It
`Netstat`	Provide network information	Native Windows command
`psservice`	List service information	www.sysinternals.com
`Sc`	Native tool for talking with service controller	Native Windows command
`DumpSec`	GUI and command-line "Swiss army knife" of the security settings	www.somarsoft.com
`Tcpvcon`	CLI view of processes mapped to ports	www.sysinternals.com
`Tcpview`	GUI view of processes mapped to ports	www.sysinternals.com
`Procexp`	Powerful GUI process explorer	www.sysinternals.com

Table 6-2 Tools for Viewing Service Information

if you quickly want to map existing process IDs to running services. If you want to know absolutely everything about a process, download and run the Sysinternals Process Explorer.

Once you have obtained a list of enabled services, discuss the results with the system administrator to understand the need for each service. Many services are enabled by default and therefore were not enabled consciously by the system administrator. For any services that are not needed, encourage the administrators to disable them. The Microsoft snap-in for the management console can be launched by typing **services.msc** from the Run option on the Start menu.

8. Ensure that only approved applications are installed on the system per your server management policy.

Administrators must manage the set of applications installed on their hosts for the following reasons:

- Not all applications play well together.
- Applications may have a dependency that's not installed.
- More applications mean more areas of potential compromise.

Unmanaged or unknown applications also may have configuration or coding issues that make the server vulnerable to compromise. For example, a poorly managed application could be missing patches, could allow access to a privileged process, or could inadvertently create a covert channel for an unprivileged user.

How

Use the results from the output of `psinfo -s`, which includes information about the installed applications. You might also consider looking through Process Explorer. Compare your findings with organizational policy and discuss them with the administrator.

9. Ensure that only approved scheduled tasks are running.

Scheduled tasks can stay hidden for weeks until an administrator takes the time to view the running scheduled tasks on the host. Scheduled tasks created by malicious or unknowing sources could damage host or network resources.

How

Note that reading scheduled tasks from the command line doesn't show you what the task is really going to do. The task can be called anything an attacker wants to call it while setting it up. That being said, you can view tasks from the command line using `schtasks`:

```
The current directory is C:\>
schtasks
TaskName  Next Run Time  Status
========================= ==================== ==========
Malicious Task  12:27:00 PM, 6/13/2011
```

PART II

Administrators should note that running the old `AT` on the command line on this server doesn't list Malicious Task. Get in the habit of using `schtasks` to view tasks. If you really want to understand in-depth exactly what each task does, you need to open the properties of each task independently. From there, you also can see the target file and review several other settings. Choose Start | Search and type **schedule**. Then select Task Scheduler. Alternatively, you could type `taskschd.msc` at the command line to open the Task Scheduler.

Account Management and Password Controls

Account management and password controls are fundamental components of server management. Tracking users over time is a difficult task, and a common method for gaining access to systems that a user should never have had access to in the first place.

10. Review and evaluate procedures for creating user accounts and ensuring that accounts are created only for a legitimate business need. Review and evaluate processes for ensuring that accounts are removed or disabled in a timely fashion in the event of termination or job change.

If effective controls for providing and removing access to the server are not in place, it could result in unnecessary access to system resources. This, in turn, places the integrity and availability of the server at risk.

How

Interview the system administrator, and review account-creation procedures. This process should include some form of verification that the user has a legitimate need for access. Take a sample of accounts from the password file, and review evidence that they were approved properly prior to being created. Alternatively, take a sample of accounts from the password file, and validate their legitimacy by investigating and understanding the job function of the account owners.

You should also review the process for removing accounts when access is no longer needed. This process could include an automated feed from the company's human resources (HR) system providing information on terminations and job changes. Or the process could include a periodic review and validation of active accounts by the system administrator and/or other knowledgeable managers. Obtain a sample of accounts from the password file, and verify that they are owned by active employees, and that those employees' job positions have not changed since the account's creation.

Additional controls may be appropriate in your environment to monitor the use of sensitive administrator accounts. Review these controls if they are determined to be a critical part of your audit.

11. Ensure that all users are created at the domain level and clearly annotated in the active directory. Each user should trace to a specific employee or team.

Most user accounts should be administered centrally by a domain controller, with the possible exception of accounts created on isolated systems that are not a member of a domain (such as some DMZs). This increases network security because account provisioning and deprovisioning can be controlled.

How

You can view the accounts by opening `compmgmt.msc` from the command line or with a tool such as `DumpSec` using the following syntax:

```
DumpSec.exe /rpt=users /saveas=fixed /outfile=users.txt
```

NOTE Download `DumpSec` from www.somarsoft.com. The same executable that launches the GUI is used from the command line. You can include `DumpSec` in a script by including the binary with your script when you run the script. Learn about the different command-line options by going to the help file under Help | Contents and selecting Command-Line options.

Discuss your findings with the administrator, and pay close attention to accounts that should exist outside the domain. The only accounts that should exist outside the domain are the built-in guest and administrator accounts unless required by an application.

12. Review and evaluate the use of groups, and determine the restrictiveness of their use.

Groups can greatly simplify the provisioning and deprovisioning process for adding or removing user access to systems as users join and leave a team. However, old members sometimes hang around inside a group when they leave a team.

How

Review the contents of the groups on the system for appropriate membership while you're looking through the accounts using the method in the preceding step. Remember that in an Active Directory environment, groups can be nested, and you need to check the membership of the nested groups. In general, this is a good time to investigate the use of shared accounts. Such accounts present risk in that you lose accountability for actions taken on the system. However, in some situations, this is unavoidable, such as with certain software on a manufacturing floor. Organizations dealing with personally identifiable information (PII), Payment Card Industry (PCI), or Health Insurance Portability and Accountability Act (HIPPA) should closely examine their use of shared accounts.

Additionally, ensure that the IT security team, investigations team, and appropriate support personnel have administrative access to the server. This may not pertain to all organizations, and there may be some exceptions. These users should be placed into a group and not added as individual users to the server.

NOTE Although mentioned earlier, it bears repeating that it's common to have exception requests that document exceptions to policy. This is fine as long as the requests are documented with the specific accepted risks and the appropriate management sign-off on the request. Many large organizations require the highest levels of management to sign-off on such requests to discourage exceptions to policy.

13. Review and evaluate the strength of system passwords.

If passwords on the system are easy to guess, it is more likely that an attacker will be able to break into that account, obtaining unauthorized access to the system and its resources. A key mitigating control for many organizations is the use of two-factor authentication.

How

All accounts should have passwords. The methods used to test these controls depend on the password-provisioning process and controls enabled on the servers and Active Directory. At a minimum, you should review system settings that provide password controls such as those mentioned in the next step.

You can retrieve and test Windows password hashes in several ways. You should, however, be careful and play it safe. Password dump, or `pwdump`, is one commonly used tool to dump password hashes from systems (see download information in the accompanying note). Different versions work using different methods. The tool works well, but even the latest version may have problems on your server, crashing your system. This has happened to highly customized servers. Test everything in a nonproduction environment first.

NOTE You can download `pwdump` from http://openwall.com/passwords.

Perhaps the easiest way to get your software asset management (SAM) and SYSTEM files is to copy them from the C:\WINDOWS\repair directory. Select the files with the CTRL key pressed, and then CTRL-drag them to another folder or USB drive.

Cracker	Cost	Comments
John	Free	www.openwall.com. A fast brute-force cracker that supports dictionaries and is accessed from the command line.
Rcrack	Free	Code is originally from Zhu Shuanglei at www.antsight.com/zsl/rainbowcrack. Built into a lot of tools such as Cain and Abel (www.oxid.it). You must find, generate, or buy tables.
Ophcrack	Free	Sometimes buggy, but free and quick. Comes with rainbow tables; download at http://ophcrack.sourceforge.net.

Table 6-3 Common Password Crackers

As for cracking the passwords, once you have the hashes, you can attempt to crack the passwords with one of the password crackers listed in Table 6-3. Several of these will take the SAM and SYSTEM files as direct inputs, dump the hashes, and perform the crack.

14. Evaluate the use of password controls on the server, such as password aging, length, complexity, history, and lockout policies.

Password controls are essential to enforcing password complexity, length, age, and other factors that keep unauthorized users out of a system.

How

You'll find the account policies as they affect your system by typing `rsop.msc` at the command line. When the window opens, choose Computer Configuration | Windows Settings | Security Settings | Account Policies. In general, verify that the policies listed in Table 6-4 are set in accordance with your local policies. Some common settings are listed.

Policy	Setting
Minimum password age	1 day
Maximum password age	90–180 days
Minimum password length	8 characters
Password complexity	Enabled
Password history	10–20 passwords remembered
Store passwords using reversible encryption	Disabled, if possible, but understand and test this before making this decision
Account lockout duration	10–30 minutes
Account lockout threshold	10–20 attempts
Reset account lockout after	10–30 minutes

Table 6-4 Account Policies

Review User Rights and Security Options

Microsoft ships with a robust ability to configure user rights and security options. These are only effective, however, if they are configured properly.

15. Review and evaluate the use of user rights and security options assigned to the elements in the security policy settings.

The default installation of Windows Server 2003 has 39 user rights settings and 70 security options. Windows Server 2008 grew to 44 user right settings and 78 security options. These settings and options allow broad, sweeping, and powerful changes to how the host behaves under many different situations.

CAUTION Be careful here. It is possible to lock yourself out, disable critical internal processes, and limit necessary functionality. It's strongly recommended that you thoroughly test any changes you make here in a test environment with any applications that may even possibly depend on the settings running on the system.

How

You'll find the security policies as they affect your system by typing `rsop.msc` or `secpol.msc` at the command line. After the GUI opens, choose Computer Configuration | Windows Settings | Security Settings | Local Policies. Remember that you can export these settings by right-clicking the folder icon and selecting Export List. Another helpful command-line option is to type `gpresult` to get a summary of group policy settings.

Evaluate the settings you found with the policies for your organization. Several guides suggest recommended settings, including Microsoft's website, the built-in security templates, the Center for Information Security guides (www.cisecurity.org), and of course, SANS (www.sans.org). The bottom line here is that you need to decide what your organization is looking to accomplish and audit against these settings. If your organization isn't using these settings at all, you should take the initiative to spearhead a project to look into them. Here are some common settings for both.

Common security options include the following:

- Renaming guest and administrator accounts
- Disabling the guest account
- Choosing not to display the last logged on user
- Prompting the user to change the password before expiration
- Refusing enumeration of SAM accounts and shares by anonymous
- Refusing to store network credentials (be careful with this!)
- Changing local-area network (LAN) manager responses (be careful with this!)

Common user rights assignments include the following:

- Changing who can access the computer across the network
- Defining who can log on locally
- Denying access to the computer from the network

- Denying logon through terminal services
- Defining who can take ownership of file or other objects

Network Security and Controls

Network access to servers must be controlled.

16. Review and evaluate the use and need for remote access, including RAS connections, FTP, Telnet, SSH, VPN, and other methods.

Not all remote access technologies are created equal, and until encrypted networks become the standard, clear-text protocols should be eliminated where possible. Although newer equipment and savvy network administrators can help mitigate the risk of eavesdropping on network traffic, the real risk of catching that traffic still exists, especially on the same broadcast domain.

Certain protocols such as File Transfer Protocol (FTP) and Telnet transmit all information in clear-text, including user ID and password. This could allow someone to obtain this information by eavesdropping on the network. Nonessential remote access connections should be limited or eliminated and clear-text administrative communications eliminated. Exceptions should be limited to business-driven cases on which senior management is willing to sign-off and formally accept the risk of clear-text and remote access.

Modems in particular, or Remote Access Services (RAS) access, bypass corporate perimeter security (such as firewalls) and allow direct access to the machine from outside the network. They present significant risk to the security of the machine on which they reside and can also allow the modem user to access the rest of the network. Allowing dial-in modems to be placed on a production machine is dangerous. Using a virtual private network (VPN) is a much better idea—preferably a VPN with two-factor authentication.

How

View the output of the services and port-mapping tools, and discuss these with the administrator. Ask the administrator about the remote access policies and the different methods of access. Question the need for any clear-text communications that aren't driven by business needs. In some cases, clear-text communications exist and are difficult to remove because of a legacy application, or the traffic just isn't that important. However, where possible, an encrypted protocol should be used instead. For Microsoft hosts, encrypted protocols include the Remote Desktop Protocol (RDP), Citrix (ICA protocol), Secure Shell (SSH), and Secure Sockets Layer (SSL), among many others.

On a Windows server, you can find information about remote access by choosing Start | Administrative Tools | Routing and Remote Access.

NOTE The use of secure protocols is particularly important in a DMZ and other high-risk environments. The auditor may determine that they are of less importance on the internal network. However, it is still advisable to use secure protocols even on internal networks to minimize attacks from within.

17. Ensure that a legal warning banner is displayed when connecting to the system.

A legal logon notice is a warning displayed whenever someone attempts to connect to the system. This warning should be displayed prior to actual login and should say something similar to this: "You're not allowed to use this system unless you've been authorized to do so." Verbiage of this sort may be needed to prosecute attackers in court.

How

Log into your account using each available service that provides access, such as remote desktop, Telnet, and SSH. Determine whether a warning banner is displayed. Interview the system administrator to determine whether the verbiage for this warning banner has been developed in conjunction with the company's legal department.

18. Look for and evaluate the use of shares on the host.

Inappropriate or open shares may needlessly compromise personal or company data. You need to identify all shares, shared directories, and permissions. For example, it's not uncommon to find open shares on a network with personal, group ranking, or payroll information. This type of data never should be kept on an open share.

How

Use the Microsoft Management Console (MMC) snap-in under Start | Administrative Tools or by typing `compmgmt.msc` at the command line. When the MMC opens, go to Computer Management | System Tools | Shared Folders to view open shares, sessions, and files.

Alternatively, you can script this with `DumpSec`. The first command lists the shares, and the second lists the shared directories. You still should verify the share permissions manually, especially for manually created shares.

```
DumpSec.exe /rpt=shares /saveas=fixed /outfile=TempFile01
DumpSec.exe /rpt=allsharedirs /saveas=fixed /outfile=TempFile02
```

You also can view a list of shares by running the command `net share`. You can view remotely opened files by running `psfile` from Sysinternals or use the command `net file`. If you have a large set of shares on a server and want to spot-check it for inappropriate content, consider indexing the shared volume using a tool such as `dtSearch`. After the indexing is completed, you can run instant searches across the entire volume. This tool is familiar to forensic examiners and built into several products. You can find out more about it at www.dtsearch.com.

For each share you find, determine whether the permissions are appropriate. Disallow public shares where the NT-authenticated users group has full control permissions.

19. Ensure that the server has auditing enabled per your organization's policies.

Auditing provides evidence in the aftermath of an event and helps with troubleshooting issues on the host. Ideally, an event-correlation engine would filter and produce meaningful data for the system administrator. Until that day comes, it is important that you have auditing enabled to provide a record for what happens on the host.

How

You should view your audit settings manually with the MMC Group Policy snap-in. If you want, you can export the settings by right-clicking the Audit Policy folder icon and selecting Export List. Recommended settings are shown in Table 6-5.

Enable object access auditing only if you know how to use this feature. You should monitor only as much as is necessary to meet your needs. You can quickly fill your logs and tax your system with meaningless overhead if this is misused. Desired Configuration Manager (DCM) from Microsoft can also be helpful for those running SCCM.

You would use the following syntax for `DumpSec` at the command line:

```
DumpSec.exe /rpt=policy /saveas=fixed /outfile=policies.txt
```

20. Review and evaluate system administrator procedures for monitoring the state of security on the system.

If the system administrator doesn't monitor his or her systems for changes or regularly attempt discovering issues in these systems, security vulnerabilities could exist, and security incidents could occur without his or her knowledge. By *monitoring*, we mean actively watching for issues (detection) and actively searching them out (finding vulnerabilities).

Audit Policy	Audit Settings	
Audit account logon events	Success	Failure
Audit account management	Success	Failure
Audit directory service access	Not defined	
Audit logon events	Success	Failure
Audit object access	Not defined or failure	
Audit policy change	Success	Failure
Audit privilege use		Failure
Audit process tracking	Not defined	
Audit system events	Success	Failure

Table 6-5 Common Audit System Settings

Monitoring also provides a snapshot of the current security level of the system (from a network services standpoint). The world of network vulnerabilities is an ever-changing one, and it is unrealistic to create a static audit program that will provide an up-to-date portrait of vulnerabilities that should be checked. Therefore, a scanning tool that is updated frequently is the most realistic mechanism for understanding the current security state of the machine. In addition, if the system administrator has a security patching process in place, this scan will provide at least some validation as to the effectiveness of that process.

How

Interview the system administrator and review any relevant documentation to get an understanding of security monitoring practices. You can perform numerous levels and methods of security monitoring; although they don't all need to be performed, some level of monitoring is important. The monitoring level required should be consistent with the criticality of the system and the inherent risk of the environment (for example, a web server in the DMZ should have more robust security monitoring than a print server on the internal network). The system administrator is responsible for monitoring his or her hosts for issues such as those you have been auditing for throughout the audit steps in this chapter.

If security monitoring is performed, assess the frequency of the monitoring and the quality with which it is performed. Look for evidence that the security monitoring tools are actually used. Review recent results, and determine whether they were investigated and resolved. Leverage the results of the rest of the audit in performing this assessment. For example, if you found significant issues in an area they were supposedly monitoring, it might lead to questions as to the effectiveness of that monitoring.

Network Vulnerability Scanning and Intrusion Prevention

Network vulnerability scanning and monitoring can be a very effective control, particularly when you use correlation tools such as RSA enVision to monitor identified vulnerabilities correlated with attempted attacks.

Network accessible vulnerabilities are dangerous because they can be exploited by anyone on the network. Several great scanners are on the market, such as Qualys and Tenable Network Security's Nessus scanner. Auditing a host with a scan for vulnerabilities lets you see the host from the network's perspective, validates your findings, and can show you things that you didn't find. This is true for both Windows and UNIX systems. Many of these companies offer free trial versions of the scanner prior to purchase. The Nessus scanner is practically free depending on your needs, but you need a host on which to install the scanner. The Qualys scanner is particularly easy to use for Windows users. Both have received positive reviews from industry peers.

Even though many of these tools are designed to have nondisruptive settings and don't require access to the system, you should always inform the appropriate IT personnel (such as the system administrator, the network team, and IT security) that you plan to run the tool, receive their approval, and schedule with them execution of the tool. There is always a chance that the scanning tool will interact in an unexpected fashion

with a port and cause a disruption, so it is important that others are aware of your activities. These tools almost always should be run in a "safe" (nondisruptive) mode in a production environment so that the tools do not attempt to exploit any vulnerabilities discovered. On rare occasions, you will want to run an actual exploit to get more accurate results, but this should be done only with buy-in from and coordination with the system owner and administrator.

21. If you are auditing a larger environment (as opposed to one or two isolated systems), determine whether there is a standard build for new systems and whether that baseline has adequate security settings.

Consider auditing a system freshly created from the baseline. One of the best ways to propagate security throughout an environment is to ensure that new systems are built correctly before moving into testing or production.

How

Through interviews with the system administrator, determine the methodology used for building and deploying new systems. If a standard build is used, consider auditing a newly created system using the steps in this chapter. Here is where something like Microsoft's Configuration Manager best comes into play; you can report on the deviations from the baseline and work on auditing just the deltas. Additionally, this is also the time to ask your virtualization administrators for information about the baselines they use to create virtual servers.

NOTE Consider discussing an approval process for new standard builds in which an auditor would look over the changes and perform a full audit of new images. This is a great way for the audit team to create a working relationship with the Windows server team.

22. Perform the steps from Chapter 4 as they pertain to the system you are auditing.

In addition to auditing the logical security of the system, you need to ensure that appropriate physical controls and operations are in place to provide for system protection and availability.

How

Reference the steps from Chapter 4, and perform those that are relevant to the system being audited. For example, the following topics are likely to be pertinent:

- Asset inventory
- Physical security
- Environmental controls
- Capacity planning
- Change management

- Backup processes
- Disaster recovery planning

How to Perform a Simplified Audit of a Windows Client

The following steps provide a very quick method for verifying the image used for provisioning new computers for the end user. This audit isn't designed to cover or catch everything, but it does give the auditor a quick view of the client's health. These checks lean heavily on the Microsoft Baseline Security Analyzer and your external scanner of choice. If you would like a more comprehensive view of the system, you can perform many of the steps in the preceding section pertaining to servers.

Perform the following steps using a freshly built computer and through interviews with a local technician responsible for provisioning new computers.

1. Determine whether the client is running the company-provisioned firewall.

Running software other than company-provisioned software may cause instabilities in the enterprise software environment on the laptop or desktop. Failure to have a firewall subjects the client to network attacks from malware, attackers, and curious people.

How

Usually, a visual check of the processes in the Task Manager shows that the company-provisioned firewall is installed and running on the system. An easy way to script this check is to run `pslist` from Sysinternals on the system and search for the service. See the same step executed for servers in the preceding section for more information.

If you are using the Windows Firewall, learn the `netsh` command set, which allows scripted output and changes to the firewall. Try running `netsh firewall show config` to see the overall configuration of the firewall on the host and whether the firewall is configured for particular adapters. Use `netsh firewall show` to see other available options for the `netsh firewall` tool.

2. Determine whether the client is running a company-provisioned antivirus program.

Running antivirus software other than company-provisioned software may cause instabilities in the enterprise software environment on the laptop or desktop. Failure to have antivirus software may allow harmful code or hacking tools to run on the computer that violate company policy.

How

A visual check of the system tray shows that antivirus software is installed and running on the system. As mentioned earlier, an easy way to script this check is to run `pslist` from Sysinternals on the system and search for the specific running process. Be wary of

customized configurations such as excluding directories and files from normal protections offered by the antivirus software.

3. Determine whether the client is running a company-provisioned patch-management solution.

Again, running software other than company-provisioned software may cause instabilities in the enterprise software environment on the laptop or desktop. Failure to have a company-provisioned patch-management solution may prevent the client from receiving the latest patches, allowing harmful code or hacking tools to run on the computer.

How

A visual check of the processes in the Task Manager usually shows that the company-provisioned patch-management system for client computers is installed and running on the system. For example, this may be evidenced by the existence of the process in the task manager of `pslist`. Some organizations like to enable automatic updates, which is also easily checked by looking for Automatic Updates in the Control Panel.

4. Determine whether the client is equipped with the minimum recommended service pack, hotfixes, and software.

Failure to install the latest hotfixes and service packs as recommended by Microsoft or other software vendors you use in your environment may allow harmful code to run on the computer or prevent legitimate software from working properly.

How

Perhaps the easiest way to check this is with the utility `psinfo`. This utility has several powerful switches that allow for checking for installed software or hotfixes and then outputting the information into a comma-separated file that opens nicely in Excel. Keep in mind that the `pstools`, `psinfo` included, are designed to be run remotely to manage hosts across the network. The options allow for checking against all computers in the local domain, in a file, or on a single host. The following is a partial output of `psinfo`:

```
The current directory is C:\PERL>
psinfo
PsInfo v1.73 - Local and remote system information viewer
Copyright (C) 2001-2005 Mark Russinovich
SysInternals - www.SysInternals.com
System information for \\CA-CDAVIS:
Uptime:      0 days 10 hours 42 minutes 25 seconds
Kernel version:   Microsoft Windows XP, Multiprocessor Free
Product type:     Professional
Product version:        5.1
Service pack:     2
Kernel build number:    2600
Registered organization:
Registered owner:       Christopher Davis
Install date:     4/19/2006, 1:57:31 PM
IE version:       6.0000
```

5. Ensure that the client has all the following according to the Microsoft Baseline Security Analyzer (MBSA).

The MBSA does a great job of auditing a single host quickly for some of the more grievous errors we commit as administrators. For example, we know that incomplete patch installations may cause instabilities in the enterprise software environment on the laptop or desktop. MBSA will check for this and many other common mistakes, such as the following:

- **Active accounts with blank or weak passwords** Blank and weak passwords create easy targets for attackers.
- **Using file systems older than NTFS** Older file systems are easier to compromise because they don't support granular file permissions.
- **Autologin enabled** Autologin allows attackers to boot directly and easily into the computer.
- **Guest accounts enabled** Guest accounts usually have weak passwords and are easily compromised.
- **Anonymous access** Anonymous access allows attackers to access and profile the computer without an audit trail.
- **Logon auditing** When enabled, logon auditing provides an audit trail of who has attempted to log onto the computer.
- **IIS enabled** IIS is complicated to configure securely correctly, and some users won't take the time to do this, even if they know they should.

How

Download MBSA from http://technet.microsoft.com/en-us/security/cc184924.aspx and run the tool. Consult the results of the MBSA scan for possible errors. You should get back results stating the following:

- No incomplete software update installations were found.
- No users have blank or simple passwords.
- All hard drives are using the NTFS file system.
- Autologin is not configured on the computer.
- Guest account is disabled on the computer.
- Computer is properly restricting anonymous access.
- Logon success and logon failure auditing are both enabled.
- IIS is not running on the computer.

6. Scan the system using a commercial-grade network scanner.

Remotely scanning the computer allows you to have a more complete picture of the computer's possible avenues of compromise than you get by simply checking everything locally to the host.

How

Several great scanners are on the market. You need to scan your hosts. Auditing a host with a scan for vulnerabilities

- enables you to see the host from the network's perspective.
- validates your findings.
- may show you issues that you didn't find during the normal audit.

This is true both for Windows and UNIX systems. Many companies offer free trial versions of the scanner prior to purchase. The Nessus scanner is practically free depending on your needs, but you need a host on which to install the scanner.

7. Evaluate physical security controls during a walk-through.

Physical security controls are required usually according to some company policy, and just as important, they help to protect computers from easy physical compromise. There are three common areas for improving physical security inside the building:

1. Cable locks should be used on laptops.
2. Users should be logged out of their workstations.
3. Passwords should not be written down anywhere.

How

Conduct a random walk-through of the work site once during working hours and once after working hours. During the walk-through, observe the use of cable locks, users logged out of their workstations, and whether or not passwords are written down in plain site.

Cable locks may not be an issue if other controls are in place, but most companies can relate to the occasional laptop "walking off" the job site. Cable locks are cheap and a great deterrent to "honest thieves."

Users should show the company some love and log out of their workstations by pressing WINDOWS KEY-L. This key combination quickly locks the computer and prevents others from walking behind the user and using the user's privileges.

Users quite often write down passwords and place them in readily available or obvious locations. There are too many stories of people who never intended to be dishonest, but then they couldn't resist the "open password" and got into trouble. Consider the use of second-factor authentication tokens or free utilities such as `keepass` (http://keepass.sourceforge.net) that store passwords inside an encrypted vault.

Tools and Technology

Several of the tools mentioned in this chapter are free and easily accessible. You are encouraged to download them and play with them on your personal machine, but be careful. Some of them are powerful and should be tested in the bulletproof superman testing network prior to use in a production environment. Table 6-6 lists some of the tools you might consider as you look into auditing Windows.

PART II

Resource	Website
Microsoft Script Center	www.microsoft.com/technet/scriptcenter/default.mspx
Microsoft Command-line Reference	http://technet.microsoft.com/en-us/library/cc754340(WS.10).aspx
Microsoft Sysinternals Tools	http://www.sysinternals.com (Redirects to Microsoft Technet)

Table 6-6 Tools and Technology: Auditing Windows

Knowledge Base

The following table shows additional resources where you can obtain information about Windows environments and related controls. Microsoft has a tremendous amount of information on its website for general consumption. Additionally, the community of helpful enthusiasts and social forums continues to grow.

Resource	Website
Microsoft Server and Tools	www.microsoft.com/servers/home.mspx
Microsoft TechNet	www.technet.com
Microsoft System Center	www.microsoft.com/systemcenter
Windows Intune	www.microsoft.com/online/windows-intune.aspx
Microsoft Tech-Ed Online	www.msteched.com
Windows Products	www.microsoft.com/windows/products
TCP/IP Fundamentals for Windows	http://technet.microsoft.com/en-us/library/cc307741.aspx
Secure Windows Server	http://technet.microsoft.com/en-us/library/dd548350(WS.10).aspx
Windows Firewall with Advanced Security	http://technet.microsoft.com/en-us/library/dd772715(WS.10).aspx
Microsoft Security Assessment Tool	http://technet.microsoft.com/en-us/security/cc185712.aspx
Microsoft Baseline Security Analyzer	http://technet.microsoft.com/en-us/security/cc184924.aspx
The Center for Information Security	www.cisecurity.org
Computer Security Resource Center	http://csrc.nist.gov
KeePass Password Tool	http://keepass.sourceforge.net

Master Checklists

The following tables summarize the steps listed earlier for auditing Windows servers and clients.

Auditing Windows Servers

Checklist for Auditing Windows Servers	
❑	1. Obtain the system information and service pack version, and compare with policy requirements.
❑	2. Determine whether the server is running the company-provisioned firewall.
❑	3. Determine whether the server is running a company-provisioned antivirus program.
❑	4. Ensure that all approved patches are installed per your server management policy.
❑	5. Determine whether the server is running a company-provisioned patch-management solution. Using the patch-management solution, validate the patched history of the client, if possible.
❑	6. Review and verify startup information.
❑	7. Determine what services are enabled on the system and validate their necessity with the system administrator. For necessary services, review and evaluate procedures for assessing vulnerabilities associated with those services and keeping them patched.
❑	8. Ensure that only approved applications are installed on the system per your server management policy.
❑	9. Ensure that only approved scheduled tasks are running.
❑	10. Review and evaluate procedures for creating user accounts and ensuring that accounts are created only when there's a legitimate business need. Also review and evaluate processes for ensuring that accounts are removed or disabled in a timely fashion in the event of termination or job change.
❑	11. Ensure that all users are created at the domain level and clearly annotated in the active directory. Each user should trace to a specific employee or team.
❑	12. Review and evaluate the use of groups, and determine the restrictiveness of their use.
❑	13. Review and evaluate the strength of system passwords.
❑	14. Evaluate the use of password controls on the server, such as password aging, length, complexity, history, and lockout policies.
❑	15. Review and evaluate the use of user rights and security options assigned to the elements in the security policy settings.
❑	16. Review and evaluate the use and need for remote access, including RAS connections, FTP, Telnet, SSH, VPN, and other methods.
❑	17. Ensure that a legal warning banner is displayed when users connect to the system.
❑	18. Look for and evaluate the use of shares on the host.
❑	19. Ensure that the server has auditing enabled per your organization's policies.
❑	20. Review and evaluate system administrator procedures for monitoring the state of security on the system.
❑	21. If you are auditing a larger environment (as opposed to one or two isolated systems), determine whether a standard build is available for new systems and whether that baseline has adequate security settings. Consider auditing a system freshly created from the baseline.
❑	22. Perform the steps from Chapter 4 as they pertain to the system you are auditing.

Auditing Windows Clients

Checklist for Auditing Windows Clients

- ❑ 1. Determine whether the client is running the company-provisioned firewall.
- ❑ 2. Determine whether the client is running a company-provisioned antivirus program.
- ❑ 3. Determine whether the client is running a company-provisioned patch-management solution.
- ❑ 4. Determine whether the client is equipped with the minimum recommended service pack, hotfixes, and software.
- ❑ 5. Ensure that the client has all the following according to the Microsoft Baseline Security Analyzer (MBSA).
- ❑ 6. Scan the system using a commercial-grade network scanner.
- ❑ 7. Evaluate physical security controls during a walk-through.

2011

IT Auditing: Using Controls to Protect Information Assets

Second Edition

Chris Davis
Mike Schiller
with Kevin Wheeler

New York • Chicago • San Francisco • Lisbon
London • Madrid • Mexico City • Milan • New Delhi
San Juan • Seoul • Singapore • Sydney • Toronto