Interested in learning more about security?

SANS Institute
InfoSec Reading Room

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

Security Auditing: A Continuous Process

Does your company have internal auditing? Do they think audits are necessary? Are they willing to follow through on an audit, from start to finish? Many think audits are unnecessary and useless. When an audit is completed, the outcome isn't taken seriously. Maybe they are even compromised and manipulated internally. What do you think? Could it take too much time, money, or be an inconvenience. Whatever the reason, there is no excuse for not conducting internal audits. Having timely and thorough audits is a critical pie...

Copyright SANS Institute
Author Retains Full Rights

AD

Security Auditing

A Continuous Process

© SANS Institute 2003, Author retains full rights

Written by Pam Page
GSEC Practical Version 1.4b, Option 1
24 May 2003

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Abstract

Does your company have internal auditing? Do they think audits are necessary? Are they willing to follow through on an audit, from start to finish? Many think audits are unnecessary and useless. When an audit is completed, the outcome isn't taken seriously. Maybe they are even compromised and manipulated internally.

What do you think? Could it take too much time, money, or be an inconvenience. Whatever the reason, there is no excuse for not conducting internal audits. Having timely and thorough audits is a critical piece of an organization but in many cases, they are not being performed, at least in a timely manner. Internal audits are a never-ending process. I would like to help you determine how to successfully configure your W2K file and print server, monitor your server, have an action plan and be prepared for a successful security audit on that server. Although this audit will center on W2K servers, the same principals can be applied to other server audits.

Introduction

A company's networks are its means of communication and information sharing. However, by virtue of "sharing," information security comes under attack everyday. Information security is not only compromised by individuals outside the company, but those inside as well. As information is shared via email, attachments, and network drives dangers imposed by allowing access is heightened. To minimize these dangers, companies need to be aware of unauthorized access and take steps to correct/protect their resources.

In an effort to address security risks and show how they can be mitigated, this paper will demonstrate how proper configuration of your network server(s) will limit access to company data, and how monitoring of this access through auditing will ensure information is safe and any holes in security are plugged. First, we'll look at auditing and how it works, and then gets a little more specific by showing how a properly configured server (W2K server) can aid in the auditing process.

As a System Administrator, a NOS Server Support Technician, an Internal Auditor, and/or a Security Analyst, you will have great insight on protecting W2K servers. I would like to help you follow an outline process on W2K file and print server that will help establish your security baseline, monitor your environment, and prepare you to take action once the audit has been performed.

Again, auditing is a very important process that will uncover any holes in network security. Auditing can be done through informal self audits and formal information technology (IT) audits.

Self Audits

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

When your server is providing service to your company, you will want to develop some type of self-audit procedures to follow on a regular basis. Some software companies have development applications to enhance the monitoring and reporting of the security event logs. These applications provide an agent that runs on each server, which allows the security event log to pass to a collector that combines each server's log. From the collector you can provide security rules that will allow the application to offer such details as sending an alert message that an unauthorized security action has taken place. You can even have the event undone and the initiator's account event locked out. The collectors will send all the daily logs to a consolidator once a day where you will be able to create numerous reports and graphs surrounding your security events. You can also use this for Trends and Analysis.
Know your Company's policies and procedures when performing self-audits. This will enable you to configure your server correctly.
Be aware of the data that resides on your servers and determine if there is information that could be considered to fall under government regulations and guidelines. If you are part of a financial institution you will have the OTS for banking, SEC for mutual funds and variable products. If you have health information that would include the HIPAA guidelines regulated by the HHS. All of these regulations plus additional regulations could add to additional configurations and security settings on your server.

The IT Audit

The purpose of an internal audit is to provide operations management with an independent review of the adequacy and effectiveness of the operations' internal controls. Your internal auditing department will expect you to comply with a standard role of controls and guidelines. They will create a scope of what they are planning to address in their audit and prepare a risk assessment.
What is a risk assessment? As you prepare to begin your audit, you need perform a risk assessment to determine the threats and vulnerabilities creating a risk to the business environment. The degree of the risk is compared with the adequacy and effectiveness of controls in place to mitigate the risk. It requires much detail and past experience to conduct are inspiring audit. Some companies create their own matrixes and scales. Others rely on software driven programs to help determine the risks. The assessment tool market is small and the companies providing the tools are very small companies.
The IT auditors may contact your department at this time and let you know their intentions toward conducting the audit. They may sit down and review the scope and determine who will be their auditees.
The IT auditors will create several individual test cases towards testing the security of the server and its environment.

At the conclusion of the audit, usually an oral report is conducted with the management, accompanied by a written report. At this time you will need to plan actions to take in response to the report or whether you wish to assume the risks involved.

Getting Started

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Now that the different types of audits have been identified, let's begin setting up a W2K Server environment that will help you be prepared at audit time. Remember, if your servers are set up with auditing in mind, your self audit or formal audit will run smoothly and produce far less findings.

Determine Your Requirements

Let's begin with the architecture. As you start to configure your system think of the following:

- Will the server be connected to the Enterprise network and joined to the domain?
- What function(s) will the server provide; will there be applications running on it?
- What type of hardware will you need?
- Will it be located behind a firewall?
- What protocols will you need?

Remember: Security settings can interfere with the operation of the server's services. Always test your configurations in a test environment before deploying to your production network.

Physical Security

Decide the location of your server. Make sure your server is placed in an environment is to protect your employees and assets. Have a checklist in place and make sure it regularly maintained and followed.
Possibly consider the 3 rings-of-security which is a logical and cost-effective approach to flexible security. Each ring has a definite, separate function but, when combined, provides flexible effective security, at an acceptable cost:

1. The first or outer ring addresses the building and its outer perimeters. These areas are secured with a combination of mechanical locks and electronic access controls. They are also electronically monitored.
2. The second ring of security includes physically separating and locking controlled areas. These areas are secured with a minimum of mechanical locks.
3. The third or inner ring of security includes restricted areas. Entry into these areas is controlled on a need-to-enter basis. These areas are secured with electronic access control. They are also electronically monitored.

Installation/Configuration

While this is a very thorough list there are always additional protections being discovered everyday. There are many web-sites to check for additional protections. These steps are in the installation process that includes security implications:

1. Remove the server from the network, your computer could be attacked or exploited before appropriate patches or configurations are in place.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

2. Create separate partitions for each major portion of the server: operating system, file serving, logs, etc.
3. Format all drives using NTFS. The NTFS file system allows you to control access to files and directories.
4. You will be prompted to enter the computer name and the administrator password. Select a strong password at this time but note you will make additional changes later.
5. Carefully determine the W2K components you wish to install and uncheck all options not needed. Note that Internet Information Server is selected by default during installation and should be unselected if not needed.
6. Install all service packs and hot fixes appropriate to your server. It is extremely important to keep up-to-date on new versions and releases.
7. Install an anti-virus software package and keep it current. Schedule your software to run regularly and frequently. Have a process in place that will detect and alert support immediately when an unknown event takes place.
8. Use the "Custom Settings" to configure your network settings. This is where you will enter your designated IP information, using static IP addresses is much more secure. You will also configure the DNS and WINS on your NIC cards. You will also want to disable the Enable LMHOSTS lookup and select the Disable NetBIOS Over TCP/IP option on the WINS tab.
9. You are now ready to join the domain.

Now that your server has been configured for the network it is time to start configuring and applying numerous security enhancements that will protect your server from internal and external intrusions.

Account Security

1. Verify the Guest account is disabled.
2. It is often suggested to rename the Administrator account and maybe even create a dummy account named "Administrator". While this may be a minimal procedure, it may stop some hackers. Whatever your decision make sure you use a strong password policy.
3. Do not create unnecessary accounts such as test accounts, shared accounts, or generic accounts. If you must create these types of accounts, disable them when not being used, use group policies to assign permissions and audit these accounts regularly.

Authenticated Users Group

Replace the Everyone Group with Authenticated Users on file shares. Everyone means anyone who gains access to your network can access the data.

File System Security

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Note: Most of the W2K operating system security is defined by the using default access permissions granted to three groups: Administrators, Power Users, and Users.

1. Restrict access to directories and files to only those who require access. Create groups for different levels of access and verify any default accesses. It is much easier to maintain and monitor group access than individual access. Remove unnecessary groups but remember to leave access for the System Administrators or a separate administrative group.
2. Disable default "administrative" shares.
3. Restrict access to system files by limiting NTFS permissions. An example would be to change the permissions on all .exe and .com files in this folder so that only a special group can access them.

Local Security Policies

Password Policies:

Configure your company's policy in the Password Policy section of the Account Policies. Some common suggestions are:

1. Enforce Password History Enabled (recommended value is 5)
2. Maximum Password Age Enabled (recommended value is 60)
3. Minimum Password Age Enabled (recommended value is 5)
4. Passwords Must Meet Complexity Requirements (Enabled)
5. Store Password Using Reversible Encryption (Disabled)
6. Minimum password length (Recommended value is 8)

Account Lockout Policies:

Configure your company's policy in the Account Lockout Policy section of the Account Policies. Some common suggestions are:

1. Account Lockout Threshold Enabled (recommended value is 3-5 invalid logon attempts)
2. Account Lockout Duration Enabled (recommended value is 30)
3. Reset Account Lockout Threshold After Disabled (recommended manual reset of accounts)

Audit Policies:

Configure your company's policy in the Audit Policy section of the Local Policies. Some common suggestions are:

1. Audit account logon events - Success and Failure
2. Audit account management - Success and Failure
3. Audit directory service access - No auditing
4. Audit logon events - Success and Failure

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

5. Audit object access - Success and Failure (this item only add to logs when auditing is enabled on specific files or other objects)
6. Audit policy change - Success and Failure
7. Audit privilege use - No auditing
8. Audit process tracking - No auditing
9. Audit system events - Success and Failure

Be aware that in large organizations recording of Success events will cause the logs to fill up rapidly. You may consider just recording Success at certain Domain Controllers or even specific member servers that may hold highly sensitive or confidential information.

User Rights Assignments:

Configure your company's policy in the User Rights Assignments section of the Local Policies. Some common suggestions are:

1. Access this computer from the network - generally workstations only need to have Administrators listed, whereas servers usually must be accessed by many different users from the network.
2. Create permanent shared objects - Administrators only
3. Logon locally - only those who require local access
4. Manage auditing and security log - Administrators only

Security Options:

Configure your company's policy in the Security Options section of the Local Policies. Some common suggestions are:

1. Additional restrictions for anonymous connections - Do not allow enumeration of SAM accounts and shares
2. Disable CTRL+ALT+DEL requirement for logon – Disabled
3. Do not display last user name in logon screen – Enabled
4. LAN Manager Authentication Level - generally workstations may have a more restrictive setting of "Send NTLMv2 response only" or higher, whereas servers usually must support a broader range of clients and should use "Send LM & NTLM - use NTLMv2 session security if negotiated".
5. Message text for users attempting to log on - Many groups place a disclaimer on improper computer use here
6. Message title for users attempting to log on - An appropriate window name for the above message

<u>Default shares</u>

Determine if your company is going to need to use any of the default shares used by the system account, which are: C$, D$, E$, ADMIN$, IPC$, FAX$, NetLogon and PRINT$.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

To disable the default Administrative shares can be done one of two ways. One is to stop or disable the Server service, which removes the ability to share folders on your computer. (However, you can still access shared folders on other computers.) When you disable the Server service (via Control Panel > Administration Tools > Services), be sure to click Manual or Disabled or else the service will start the next time the computer is restarted. The other way is via the Registry by editing HKeyLocal Machine\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters. For Servers edit AutoShareServer with a REG_DWORD Value of 0.

Services

Disable any network services not required. Be aware that many applications installed will require additional services to run that open the server up for exploits. A few services that you will definitely want to disable are: IIS services, FTP services, Network News Transport Protocol (NNTP), Simple Mail Transport Protocol (SMTP), and the World Wide Web Publishing Service.

Ports

Disable any ports not required but never assume your servers are safe! You can find out a list of open ports on your local system by opening the file located at %systemroot%\drivers\etc\services.

Modems

Try to avoid the use of modems with your server at all possible; a modem is one of the easiest ways into the server, the network and the company. If it is absolutely necessary to use a modem make sure it is configured correctly and audited regularly.

Anonymous Access to the Registry

By default, the majority of the registry is secured, but remote access allows the anonymous user too much access. To restrict network access to the registry:

1. Add the following key to the registry:

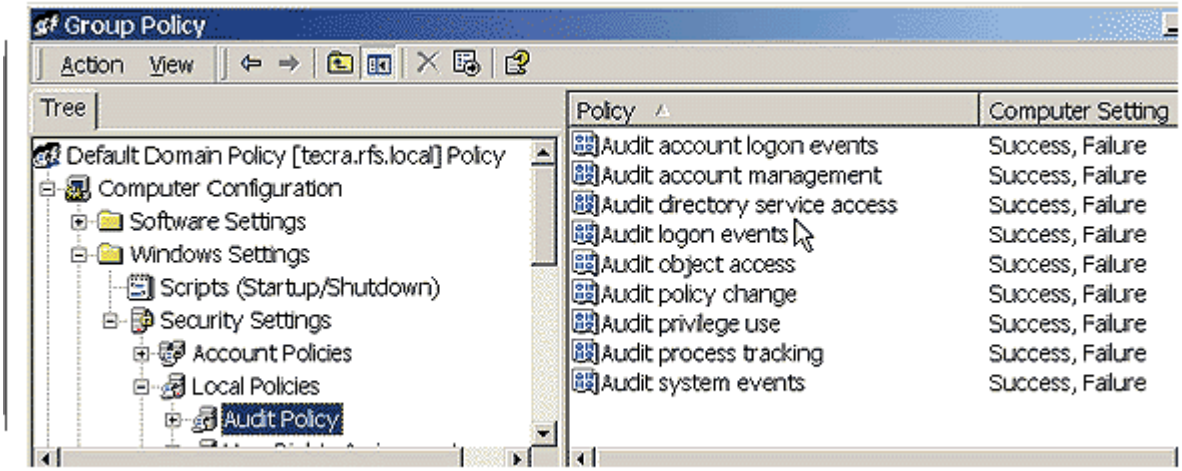
Hive	HKEY_LOCAL_MACHINE \SYSTEM
Key	\CurrentControlSet\Control\SecurePipeServers
Value Name	\winreg

2. Select winreg, click the Security menu, and then click Permissions.
3. Set the Administrators permission to Full Control, make sure no other users or groups are listed, and then click OK.

Enable the Security Event Logging

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The default audit policy is disabled on each audit category. To configure your policies use the Active Directory (AD) Group Policy. In W2K there are nine audit categories:



Categories are located in Active Directory Users and Computers, Group Policy Object (GPO), Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy. Each category can be configured to record successful and unsuccessful events. When you modify a GPO, your configuration changes will apply to all computers in the organizational units (OUs), domain, or sites that you've linked to that GPO. The last policy applied wins.

Restrict the permissions on the logs to allow full access for one special created user group. It is not necessary to use the Administrators group but a few selected users within Security who do not have elevated access. If other users require limited access for troubleshooting or follow-up, limit them to read access only.

Configure logs to a larger size, set writing properties, set the Maximum log size to 10000 to 50000KB and select Overwrite events as needed. Critical systems logs should be archived and backups properly secured.

Prevent the last logged-in user name from being displayed

When you press Ctrl-Alt-Del, a login dialog box appears which displays the name of the last user who logged in to the computer. Doing this makes it easier to discover a user name that can later be used in a password-guessing attack. This function can be disabled using the security templates provided on the installation CD, or via Group Policy snap in.

Set Log on Warning Message

Though setting a log on warning message does not technically restrict an attacker, it significantly increases an organization's ability to prosecute attacks. The specific

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

wording of the message should be provided by your legal counsel: (Example: **This system is restricted to authorized users. Individuals attempting unauthorized access will be prosecuted.**)

Password protect the screensaver

Make sure all of your servers have this feature enabled to prevent an internal threat from taking advantage of an unlocked console. Make sure the wait setting is appropriate for your company. Get your users in the habit of manually locking the server when they walk away from it. You can keep users from changing this setting via Group Policy.

Backups

With the configuration you have set up on this server and its potential data, it is extremely important that you do regular backups of your server. You can use a combination of incremental and full backups. And make sure these tapes are *secured*. Keep your backups in a separate, secure location. Ideally this location would be in a separate building from the original computer in case of a fire or other disaster. And know who should have access to tapes. Maintain a current and accurate list of those authorized to handle the tapes.

Testing Security Settings

Now that you have the system(s) configured, you need to test the settings to see if there are still things you can on from the outside. Listed are possible tools you can use to determine exposures but not all tools are freeware so you will have to incur additional costs:

- **Superscan (Port Scanner)** is a freeware tool for W2K and WinNT which will perform a UDP and TCP port scan.
- **RPCDump** You will use this tool to help you determine which RPC services have which ports open. This is available from the Microsoft Windows 2000 Resource Kit.
- **Netstat** You will use this tool on the local host to identify its open ports. This comes with W2K and WinNT.
- **Fport** A great tool from www.foundstone.com to use in the testing used to scan the system to see what is open.
- **Microsoft Baseline Security Analyzer** evaluates your system's configurations and provides a report with specific recommendations to improve the security. It will also recommend missing hotfixes and configuration changes. You will want to run this regularly to explore new vulnerabilities. Remember it is only a baseline.
- **Internet Security Scanner** is a network security scanner that can be used for W2K.

Additional considerations

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Any time you are connected to a network you run the risk of an internal or external intrusion. You will have to use additional security measures to isolate these systems. Here are a few suggestions but there are many more:

- Consider implementing IPSec
- Use the encrypting file system (EFS) to encrypt sensitive files
- Validate permissions on application directories
- Configure system dumps

Be aware there are no hard and fast answers of how to secure or harden your W2K. Use good administration practices, run only minimal services only related to that server, use strong passwords and use the concept of “least privileged” to set. And last but not least, continuous monitoring and review of security and procedures through audit processes is imperative to maintaining a security environment.

Summary

This paper has defined and illustrated how proper configuration and planning serves as an initial step in the auditing process, and will ensure your company’s information is secure. The cost in time and money is significant. However, budgeting for security controls and monitoring is necessary to minimize/eliminate risks imposed by a system subjected to penetration through the everyday elements of uncertainty associated with networked information.

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References:

1. Information Technology Services. "UCB Windows 2000 Server Security Guidelines." http://www.colorado.edu/its/windows2000/adminguide/w2ksecguidelines.html (24 May 2003)

2. Microsoft Technet. "Windows 2000 Server Baseline Security Checklist." http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/w2ksvrcl.asp (24 May 2003)

3. Information Technology Services. "IT Security Information." http://www.colorado.edu/its/security/ (24 May 2003)

4. Cox, Phillip. "Hardening Windows 2000." 30 March 2001. http://www.systemexperts.com/tutors/HardenW2K101.pdf (24 May 2003)

5. Smith, Randy Franklin. "Auditing Windows 2000." *Security Administrator* 20 July 2000. http://www.ntsecurity.net/Articles/Index.cfm?ArticleID=9633&pg=1&show=493 (24 May 2003)

6. "Windows 2000 Checklist." http://www.labmice.net/articles/securingwin2000.htm (24 May 2003)

7. Schreider, Tari. "Risk Assessment Tools: A Primer." Information Systems Control Vol. 2 (2003): 23-25.

8. Cuneo, Eileen Colkin. "Beyond Compliance." InformationWeek (24 Feb. 2003): 20-22.

9. Mandia, Kevin & Prosise, Chris. Incident Response: Investigating Computer Crime. California: Osborne/McGraw-Hill, 2001.

10. Aelita EventAdmin 6.1: Event Management and Security Auditing. Ohio: Aelita Software Corporation, 2001.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 20th, 2013

Upcoming SANS Training

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

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