Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Auditing a File Server - Microsoft® Windows Server™ 2003

An Auditor's Perspective

Practical Assignment Version 3.0

(Option 1 – Device, System or Application Auditing)

© SANS Institute 2004, Author retains full

Auditor: Tamer Eltoni
Date: May 2004

Submitted in partial fulfillment for the requirements for GSNA certification

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract

The role of file servers in organizations is growing rapidly and so is the need to protect the business data. Whether it's a missing file, server crash or any unforeseen disaster; in fact anything that limits access to data is disruptive and costly to any organization.

In this assignment a security audit is been performed on a file server for JK Enterprise Financial Department. The main purpose of the file server is to allow network clients within the department's Local Area Network (LAN) to access the stored files, therefore saving them from having to physically transfer data from one computer to another.

Due to the wide range of features and functions that the file server has, a number of these items have been selected to limit the scope of the audit. The objective of the audit is to examine these items at a single point in time to make sure it is configured appropriately according to system role as a file server and according to the organization's policy and standards.

© SANS Institute 2004, Author Retains Full Rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Acknowledgement

I would like to take this opportunity to express my sincere gratitude to all people who have given me invaluable assistance, advice and guidance throughout the course of this assignment.

First and foremost, I want to express my deep appreciation to all the staff in SANS for their continuous direct and indirect help. This assignment, simply put, would not have been possible without the endless support from Gary Anderson and Lara Corcoran. There has been no question posted to them to which they failed to give their full assistance.

Next, no person deserves more thanks than John Green for giving such a professional course during SANS 2004 Conference in Darling Harbour- Sydney (Track 7). He had deep influence upon my auditing skills.

Last, but far from least, I want to thank my parents not only for having me in the first place, but also for believing in me all these years no matter what I have chosen to do.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Table of Contents

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Introduction

JK Enterprise is one of the leading professional services organizations that help companies in a broad range of solutions such as taxes, corporate finance, enterprise project management and other business critical-performance issues.

Many of the servers installed at JK Enterprise are configured with the default security settings. This poses a large security risk and a potential financial loss for the entire enterprise.

The impact of a malicious attacker or virus could result for example in a denial of service (DoS) attack, which would make certain servers or machines unavailable. In the worst case, such attacks could compromise confidential corporate information. Therefore, the financial implications and the operational consequences must be mitigated to save the organization from the impact of such risks.

JK's Finance department have designed and deployed a file server responsible for the storage and management of data in a central location. The main purpose of the file server is to allow network clients within the department's Local Area Network (LAN) to access the stored files, therefore saving them from having to physically transfer data from one computer to another.

Notes: JK (Just Kidding) Enterprise is a fictitious name that is used for the purpose of publishing this document without exposing the real organization.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1 Research in Audit, Measurement Practice and Control

Section A: Identifying the system to be audited

The following sections detail the current environment, system to be audited, scope of the audit and what is beyond the scope.

Current Environment

The file server is physically located in the corporate secured data center and is part of the finance department's LAN. The corporate security policy implies that files should be only accessed during working hours (9 am to 5 pm). Therefore, no one is expected to access the server in non-working hours without a formal approval from the management.

The server is storing corporate confidential data which can cause big harm to the organization if exposed to competitors. It is used for home directories, departmental shares and corporate shares.

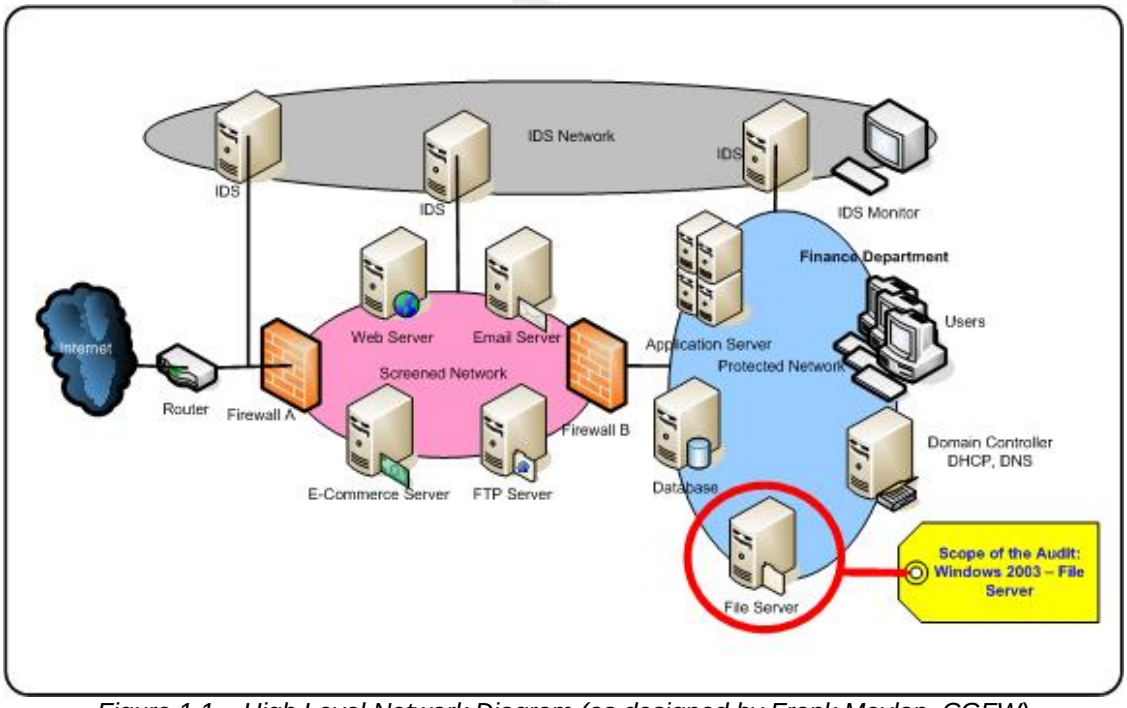


Figure 1.1 – High Level Network Diagram (as designed by Frank Meylan, CGFW)

A maximum storage of 100GB is allowed per user. However, the file server storage capacity needs are growing by 30% annually to accommodate the size of

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

departmental and corporate shared data growth. Daily incremental and weekly full backups are scheduled and done with the tapes send offsite.

All the departments of JK enterprise have their own LANs associated to them and are separated from the DMZ by a firewall. The circled area in *Figure 1.1* indicates the portion of the scope.

System to be audited

The system audited in this assignment is a File Server running on Microsoft Windows Server 2003 Standard Edition version 5.2 (*Figure 1.2*). Winver command was used to get the version and build of the operating system (Start → Run → type winver).

Figure 1.2 – Audited Windows Version

Scope of the Audit

A system security audit for the finance department file server will be preformed in this assignment. The objective of the audit is to examine the system at a single point in time to make sure it is configured appropriately according to its role as a file server, best practices and to the organization's policy. Out of all the functions and features of the file server the following list is the scope of the audit:

- Strong Password Policy
- Restricted Login hours
- User's Disk Quota Management
- Virus Auto-Protect
- Windows Server 2003 Shadow Copying Feature

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Notes: The targeted server is a standalone server with a file server role.

Out of Scope

Anything other than the scope defined above is considered out of scope; however it's important to reconfirm the following:

- The audit will not address the client operating system.
- The audit will only focus on the server roles (files server).
- For a complete security implementation this audit should be part of an overall security audit which should address security at multiple levels. (Security is as weak as the weakest link). The scope does not address auditing:
    - Physical Security
    - Written Security Policies and Procedures
    - Network Architecture Security
    - Perimeter Security Architecture
    - Application security outside of the File Server function and role
    - Backup and restoration

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Section B: Most Significant Risks to the System

In this section we evaluate the most significant risks to the file server. Figure 1.3 shows the cause and effect relationship of threats, vulnerability, and risks.

The threat is the trigger that, if the organization is vulnerable, will cause the risk to materialize and result in damage to enterprise assets [7.].

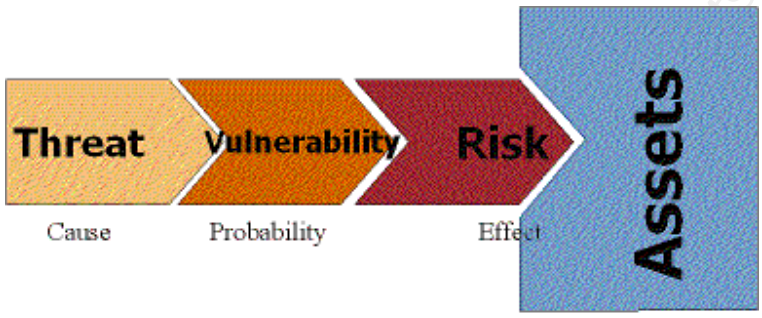


Figure 1.3 - Cause and Effect Relationship [7.]

Threats, Vulnerabilities and Risks are all related. For example, the lack of an antivirus solution makes the file server more vulnerable to the threat of malicious code, which in turn increases the risk of having a denial of service, the risk of losing the data stored on the server, and ultimately the risk of losing customers. The lack of an uninterruptible power supply (UPS) increases a system's vulnerability to the threat of a power failure, thus increasing the risk of data loss or perhaps even physical damage to equipment.

Threats

The following table lists some of the threats and their capacity to inflict damage on the file server.

Table 1.1: Threats

No.	Threat Description	Capacity to inflict damage
1.	Attacks resulting from missing updates and patches	High (70% or Above)
2.	Malicious code infection	High (70% or Above)
3.	Accidental deletion of documents	High (70% or Above)
4.	Un-Authorized Access	Medium (50% to 69%)
5.	Power Failure	Low (Below 50%)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Affected Assets

The chart below covers the majority of assets likely to be vulnerable to risks and the organization should consider in a risk assessment. There may be some additional assets for a corporate or government organization to consider.

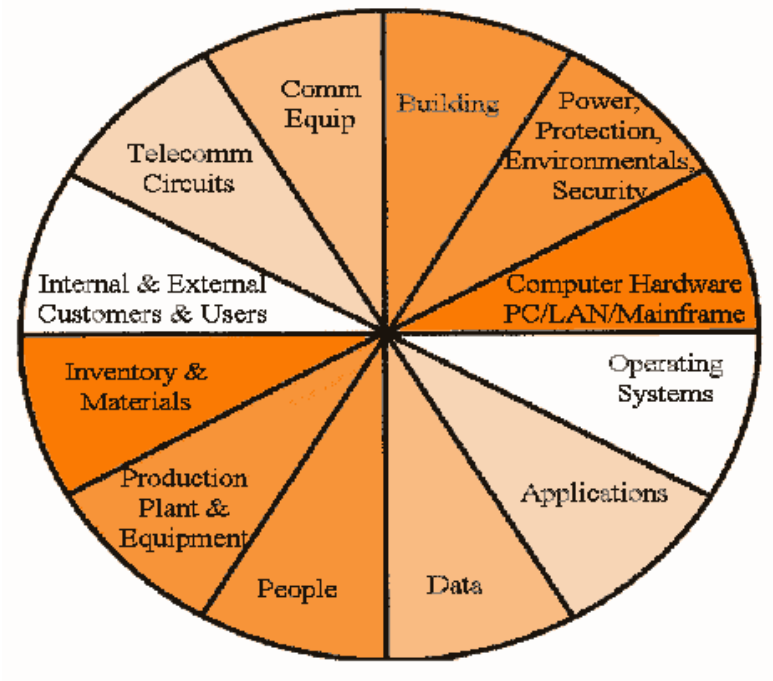


Figure 1.4 – Organization's Assets Chart [7.]

The file server directly affects the organization's data and service. The following table lists the types of assets that are directly affected by the role of the file server.

Table 1.2: Assets

No.	Asset Affected
1.	User's Data
2.	Finance Department's Data
3.	Corporate Confidential Information
4.	Department Services
5.	Shared Applications
6.	Operating System
7.	Computer Hardware

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Major Vulnerabilities

The following table contains several vulnerabilities that could affect the audited file server.

Table 1.3: Vulnerabilities

No.	Vulnerability	Degree of Exposure	Potential impact
1.	Missing Updates and Patches	High	Can result in multiple harmful effects on the server's role such as denial of service, exposure of confidential information, etc.
2.	Lack of Antivirus Solution	High	Results depend on what harm the virus causes but can reach to Denial of Service, exposure of confidential data, loss of data, etc.
3.	Untrained Personnel	High	Results in the loss or miss use of corporate data
4.	Weak Passwords	Medium	Unauthorized access which can cause the exposure of confidential data and the loss of data integrity
5.	Insufficient Disk Space	Medium	File server not able to perform its role for the users. (Denial of Service)
6.	Lack of UPS	Low	Data loss and physical equipment loss

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Section C: Current State of Practice

By securing the environment according to industry best standards, JK Enterprise can ensure that the deployment of Windows Server 2003 File Server operates in a known manner. Hence, using security recommendations that have been tested to provide known levels of functionality will greatly reduce the potential impact of risk on the organization.

After conducting a thorough search on the web and in book libraries for best practices and file server checklists the following references where found to be useful for the audit and to help in building the checklist:

References

No.	Reference	Type	Benefit of the Reference
1.	*Microsoft Windows Server 2003 Security Guide.* Microsoft.20-02-2004. http://www.microsoft.com/technet/security/prodtech/win2003/w2003hg/sgch06.mspx	Security Guide	Guidelines for hardening a file server
2.	*Microsoft Windows Server 2003 File Server Role.* Microsoft.20-02-2004. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/serverroles/fileserver/default.asp	Article	Guidelines for planning deploying and maintaining a file server
3.	*Securing a Windows 2003 Server.* Microsoft.20-02-2004. http://www.microsoft.com/technet/security/guidance/secmod214.mspx	Checklist	File Server hardening steps
4.	*Best practices for securing Microsoft Windows Server 2003* ZDNET.20-02-2004. http://techupdate.zdnet.com/techupdate/stories/main/Best_practices_for_securing_Windows_Server_2003.html	Article	Best Practices to secure Microsoft Windows Server 2003
5.	*Securing a Windows 2003 Server.* Microsoft.01-03-2004. http://www.microsoft.com/technet/security/guidance/secmod122.mspx	Article	File Server Hardening
6.	*How to install and run windows automatic updates.* University of Wyoming. 03-03-2004. http://uwadmnweb.uwyo.edu/ITR/documents/1068.htm	Article	Steps to install windows updates

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

7.	BCOE-200 DRII course: *Introduction to the Principles of Risk Management*	Online Course	Risk Management
8.	Tulloch, Mitch. *Windows Server 2003 in a Nutshell.* O'Reilly & Associates. 2003	Book	Helps in creating the Audit Checklist
9.	Shea, Brian. *Have you locked the castle gate.* Addison-Wesley Pub Co. 2002	Book	
10.	Habraken, Joe. *Absolute Beginner's Guide to Networking.* Que. 2003	Book	Understanding networking with windows 2003
11.	Boswell, William. *Inside Windows Server 2003.* Aw Professional. 2003	Book	Understanding more about windows 2003
12.	Honeycutt, Jerry. *Introducing Microsoft Windows Server 2003.* Microsoft Press. 2003	Book	More understanding of Windows 2003
13.	Williams, Robert and Walla, Mark. *The Ultimate Windows Server 2003 System Administrator's Guide.* Addison-Wesley Pub Co. 2003	Book	Guidelines on windows 2003 administration
14.	*Technical Overview of Windows 2003 Server files services.* Microsoft.01-03-2004. http://download.microsoft.com/download/1/1/3/113f6ce1-a87e-4740-a30d-1dcb72a39a72/FileOverview.doc	Article (document)	Technical Overview of the features of the file service in Windows 2003 server
15.	*What's new in file and print services.* Microsoft.01-03-2004. http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/fileandprint.mspx	Article	List of the new file server features in windows 2003 server
16.	*Windows Server 2003 Guided Tour.* Microsoft.04-03-2004. http://www.microsoft.com/windowsserver2003/evaluation/features/guidedtour/default.mspx	Guided Tour	Step-by-Step guided tour about new features and enhancements
17.	*Setting up & managing a file server in Windows 2003.* WindowsNetworking.04-03-2004. http://www.wown.com/articles_tutorials/File_Server_Windows_2003.html	Conference , Audit Checklists	How to set up a file server
18.	*VirusScan 7.1.0 for Windows – Guide to*	Checklist	Mcafee antivirus

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	Installation and Configuration. The University of Edinburgh. 04-03-2004. http://www.ucs.ed.ac.uk/usd/iss/ol/issues/viruses/anti-virus/vs7_1home2.html#configure		installation and configuration checklist
19.	*Mcafee VirusScan 7.1 Setup Instructions*. Duke University. 04-03-2004. http://www.aas.duke.edu/comp/documentation/mcafee/mcafee7x/	Guide	Mcafee setup & configuration steps
20.	*Maximizing Web Server Availability*. DELL. 15-03-2004. http://www1.us.dell.com/content/topics/global.aspx/power/en/ps1q02_graham?c=us&cs=555&l=en&s=biz	Recommendations	Maximizing Availability
21.	*The Audit Process : Audit Reporting.* AuditNet. 15-03-2004. http://www.auditnet.org/reporting.htm	Audit Reports	Audit Reports Templates
22.	*Security Awareness Web Based Courses.* Native Intelligence, Inc.15-03-2004. http://nativeintelligence.com/courses/whyaware.aspx	Article	Security Awareness

Arsenal of Tools

The following list of tools where used for the audit:

- Windows Update
- Shadow Copy Previous Version Client
- Dumpsec
- L0pht Crack (LC4)
- Microsoft Baseline Security Analyzer (MBSA)
- Eicar

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2 Audit Checklist

Section A: Basic System Information

Before creating the audit checklist, it's important to collect information about the server to which the audit will be preformed.

System Information: For windows system information open the command prompt (Start → Run → type cmd) and run the following command:

```
C:\>systeminfo > sysinfo.txt
```

Results will be directed to a text file with the name sysinfo.txt under the c: drive. Figure 2.1 shows a sample of the output. For more details refer to Appendix A.

```
C:\>systeminfo

Host Name:                 SERV2003
OS Name:                   Microsoft(R) Windows(R) Server
2003, Standard Edition
OS Version:                5.2.3790 Build 3790
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
```

Figure 2.1 –Sample output of the System Information

Notes: Windows Server 2003 also includes the System Information utility (msinfo32.exe) utility. This can also be run from the command line, or launched from the Program menu (Start Programs Accessories System Tools System Information). This is a heavy-duty GUI tool that will show you everything from the OS version to environment variables to the file names and versions of every Internet Explorer file on your system [2].

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Server Role: Click 'Start' button then click 'Manage Your Server' A Window will get launched showing the server roles installed. File Server is the role configured for the audited server.

Figure 2.2 - Server Role

Virus Protection Solution: McAfee VirusScan Enterprise Version 7.1.0 is used to provide comprehensive protection from viruses, worms, Trojans and other malicious code affecting the fileserver.

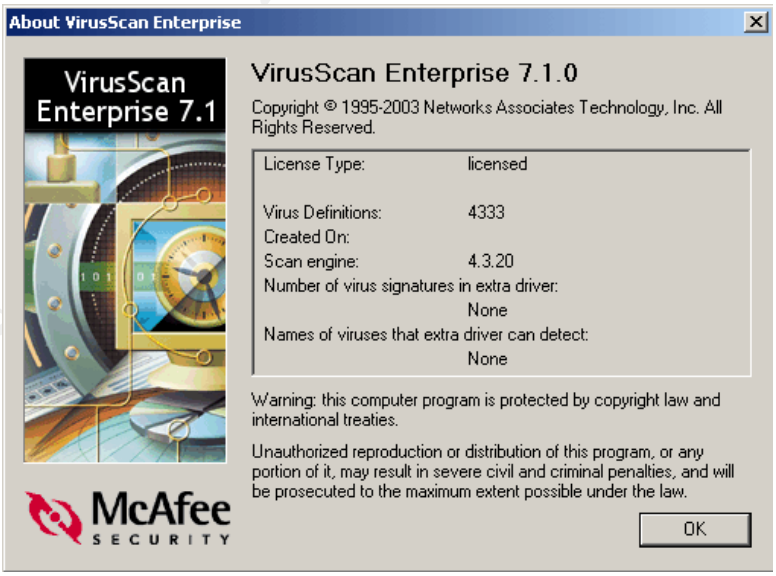


Figure 2.3 – Virus Protection Software Version

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Section B: Audit Checklist

Product: File Server **Audit Date:** _____
Auditor: _____ **Checklist Version:** GSNA-V-3.0

Item Number	Description	Check
1.	Identify Installation Of Required Service Packs and/or Updates	❑
2.	Check System Time and Date	❑
3.	Ensure Shadow Copies Feature Enabled	❑
4.	Confirm Storage Area For Shadow Copies Is On A Separate Volume On Another Disk	❑
5.	Ascertain Network Client Machines Can Use Shadow Copies Of Shared Folders	❑
6.	Ascertain Network Clients Able To Restore Files	❑
7.	Confirm Restriction on Login Hours	❑
8.	Check Password Complexity	❑
9.	Check User's Disk Quota Restriction	❑
10.	Confirm File System Format (NTFS)	❑
11.	Verify File Shares Permissions	❑
12.	Confirm that Server Is Free From Known Malicious Code	❑
13.	Check Virus Auto-Protection	❑
14.	Confirm that Virus Protection Solution Scans Archived Files	❑

Notes:

- It's highly recommended to have a written managerial approval on scope, activities performed, resources allocated and expected outcome before starting the audit.
- Tools required for auditing that will be running on the targeted server should be installed by the system administrator or at least under his presence and under his guidance.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Section C: Audit Checklist Details (Audit Procedures)

ITEM 1 - Identify Installation of Required Service Packs and/or Updates

Reference:
- [3.] Subtitle: File Server Hardening Steps
- [6.] Subtitle: Procedure > Windows 2000

Degree of Exposure: High

Risk: Latest Service Packs and Updates are not installed on the system. *(Vulnerability [1] see page 12)*

Risk Impact: The absence of service packs and updates makes the system vulnerable to all types of threats (Denial of Service (DoS), System Crash, unauthorized access, malicious code infection, etc.) that are protected by patches and windows updates.

Testing Procedure:
a. Logon as administrator to the file server
b. Click 'Start' button then select 'All Programs'
c. Click 'Windows Update'
d. Internet Explorer will get launched pointing to the following URL: http://windowsupdate.microsoft.com/en/default.asp
e. Under the 'Welcome to Windows Update' (right side) click 'Scan for updates' (see Figure 2.4)

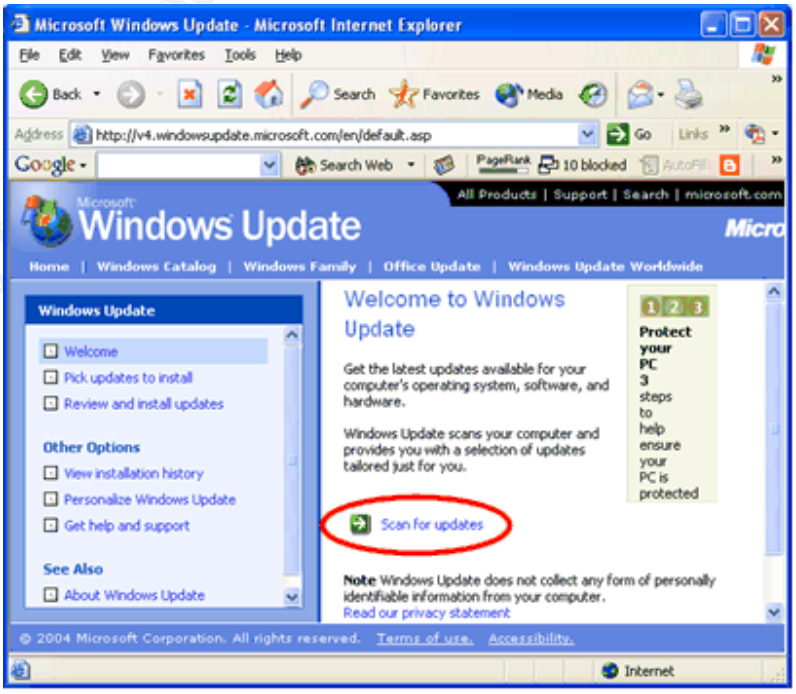


Figure 2.4 - Windows Update Site

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

f. After the 'Scan for Updates' is conducted a report with the results will be presented on the site
g. Under 'Pick Updates to Install' link on the left frame, click on the 'Critical updates and Service Packs' to review a summary of all the missing critical updates
h. Take screen shot by pressing 'Alt + Print Screen'
i. Document your findings in the audit report

Compliance:	Pass or Fail
Compliance Criteria:	The 'Scan Review' should result into Zero (0) Critical Updates and Service Packs.
Test Nature:	Objective
Control Objectives:	Minimizing system exposure to known published security threats.
Evidence:	See Part 3
Findings:	See Part 3

Notes: Evidence and Findings for all the select items in the Check List are found in Part 3 - The Audit.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

ITEM 2 - Check System Time and Date

Reference: Not found as a result of the research, but is a result of personal auditing experience.

Degree of Exposure: Low

Risk: Wrong system time and date.

Risk Impact: Inaccuracy in tracking events and logs and hence can be a cause to misleading problem solving or auditing.

Testing Procedure:

a. Logon on to the file server
b. Click 'Start' button then select 'Control Panel'
c. Click 'Date and Time'
d. Compare the system date and time with the actual present date and time
e. Click on the Time Zone tab verify that the correct time zone is been selected ((GMT+04:00) Abu Dhabi, Muscat)

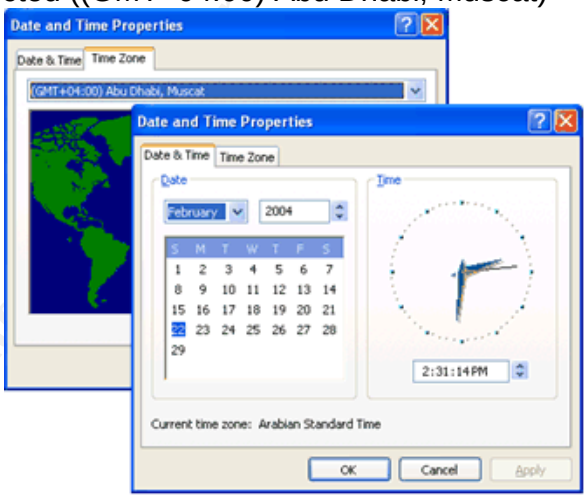


Figure 2.5 - System Date and Time

f. Take screen shot by pressing 'Alt + Print Screen'
g. Document your findings in the audit report

Compliance: Pass or Fail

Compliance Criteria: System date and time are correct and time zone configured according to the appropriate zone of the hosting country.

Test Nature: Objective

Control Objectives: Accurate date and time to avoid any confusion specially when checking logs.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

ITEM 3 - Ensure Shadow Copies Feature Enabled

Reference:

- [16.] Subtitle: Intelligent File Services
- [12.] Chapter 11. File Services – Subtitle: Shadow Copy Restore.
- [11.] Chapter 16. Managing Shared Resource. Subtitle: Volume Shadow Copy

Degree of Exposure: High

Risk: User accidentally deleting or overwriting files. *(Vulnerability [3] see page 12)*

Risk Impact: Loss of critical and important documents can have a bad business impact, in addition to the effort required to create or get these documents back again.

Testing Procedure:

Test 1 – Confirming that the shadow copy feature is enabled

a. Logon as administrator to the file server
b. Click the 'Start' button then click 'Manage Your Server'
c. Click the 'Manage this file server' link next to the 'File Server' role
d. The 'File Server Management' tool appears
e. In the right window pane, click 'Configure Shadow Copies' (see Figure 2.6)

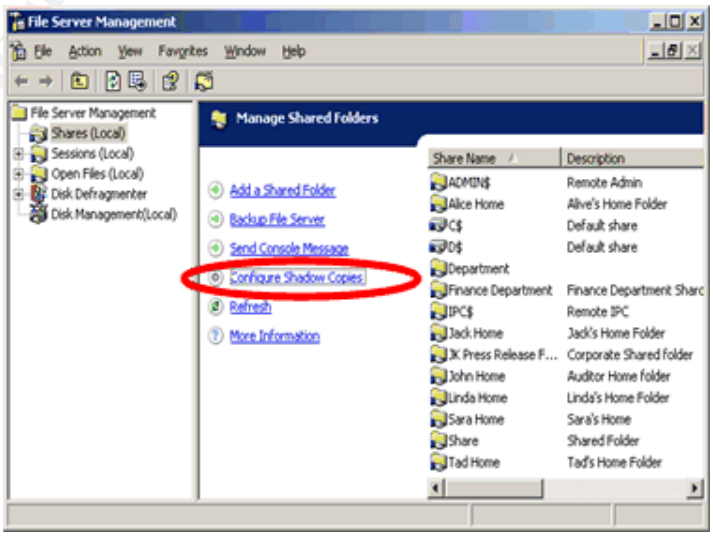


Figure 2.6 – File Server Management

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

f. Take screen shot by pressing 'Alt + Print Screen'
g. Document your findings in the audit report

Test 2 – Shadow Copy Feature (Stimulus/Response)

a. Click the 'Start' button, click 'Run'. In the Open dialog box type "\\localhost\auditshare". Click 'OK'
b. Click the 'File' menu, select 'New' and click 'Text Document'. Give the document a name (Shadow Audit.txt)
c. Double-click the new text document, type "Shadow copy auditing", then save and close the text document
d. Right-click on the folder icon in the Title bar and select Properties
e. Select the Previous Versions tab which lists the versions of the share available through shadow copies
f. Take screen shot by pressing 'Alt + Print Screen'
g. Document your findings in the audit report

Compliance: Pass or Fail

Compliance Criteria:

- Test 1: Shadow Copies of selected volumes should be created and enabled.
- Test 2: The text document created in sub-step (b.) will have a pervious restorable version.

Test Nature: Objective

Control Objectives: Provide point-in-time copies of files on a volume, allowing users to view the contents of shared folders as they existed at points of time in the past. Users can recover files that they accidentally delete or overwrite.

Evidence: See Part 3

Findings: See Part 3

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

ITEM 4 – Confirm Storage Area for Shadow Copies Is On a Separate Volume on another Disk

Reference:
- [8.] Chapter 3. Task Map. Subtitle: Configure Settings for Shadow Copies.
- Windows Server 2003 Help - Best Practices: Shadow Copies of Shared Folder

Degree of Exposure: Moderate

Risk: Single point of failure and high I/O load.

Risk Impact: Can cause hard disk failure or at least shadow copies to be deleted.

Testing Procedure:
a. Logon as administrator to the file server
b. Click the 'Start' button then click 'Manage Your Server'
c. Click the 'Manage this file server' link next to the 'File Server' role
d. The 'File Server Management' tool appears
e. In the right window pane, click 'Configure Shadow Copies'
f. Click 'Settings' (Figure 2.7)

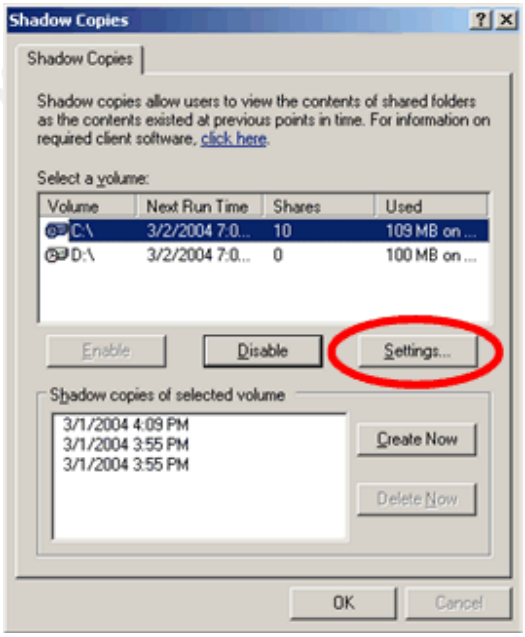


Figure 2.7 - Shadow Copies configuration

h. Take screen shot by pressing 'Alt + Print Screen'
i. Document your findings in the audit report

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Compliance:	Pass or Fail
Compliance Criteria:	Shadow copy storage should be configured to be stored on another volume on a separate disk.
Test Nature:	Objective
Control Objectives:	To prevent shadow copies from being deleted due to high I/O and to avoid a single point of failure.
Evidence:	See Part 3
Findings:	See Part 3

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

ITEM 5 - Ascertain Network Client Machines Can Use Shadow Copies Of Shared Folders

Reference:

- [8.] Chapter 3. Task Map. Subtitle: Install Shadow Copy Clients.
- [16.] Subtitle: Intelligent File Services
- Windows 2003 Help - Checklist: Deploy Shadow Copies of Shared Folder

Degree of Exposure: Moderate

Risk: Previous Version Client not compatible with windows XP (all Network clients run windows XP). *(Vulnerability [3] see page 12)*

Risk Impact: Inability to restore deleted or overwritten files which can cause the loss of critical and important documents that can have a bad business impact.

Testing Procedure:

Test 1- Previous Versions Client Setup on Windows XP Clients

Install the Previous Version Client so that networked Windows clients can use shadow copies of shared folders.

a. Logon as administrator to the file server
b. Click the 'Start' button, and then click 'Run'. In the Open dialog box type:

    %systemroot%\system32\clients\twclient

c. Click 'OK'
d. A Windows Explorer window opens with a list of supported platforms for the Previous Versions Client
e. Double-click the x86 folder
f. Copy the twcli32.msi file to the client machine
g. On the client machine, logon as administrator
h. Double-click the twcli32.msi file
i. Click the 'Finish' button

Test 2 – Previous version tab installed (Stimulus/Response)

a. Logon as administrator to the client machine
b. Click the 'Start' button, and then click 'Run'. In the Open dialog box type "\\serv2003\auditshare"
c. Enter user name and password. Click 'OK'

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

d. Click the 'File' menu, select 'New' and click 'Text Document'. Give the document a name (Shadow Audit Client.txt)
e. Right-click on the file icon and select 'Properties'
f. Click the 'Previous Versions' tab which lists the versions of the share available through shadow copies
g. Take screen shot by pressing 'Alt + Print Screen'
h. Document your findings in the audit report

Compliance: Pass or Fail

Compliance Criteria:

- Test 1: Pervious version client installed successfully on the client machines.
- Test 2: 'Previous Version' tab added to file properties window of the shared folders.

Test Nature: Objective

Control Objectives: To be able to use the shadow copy feature from network client running Windows XP.

Evidence: See Part 3

Findings: See Part 3

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

ITEM 6 - Ascertain Network Clients Able To Restore Files

Reference:
- [8.] Chapter 3. Task Map. Subtitle: View a Previous Version of a File
- [8.] Chapter 3. Task Map. Subtitle: Restore a Previous Version of a File

Degree of Exposure: High

Risk: Network clients not able to restore deleted or over written files.

Risk Impact: Loss of critical and important documents can have a bad business impact in addition to the rework required to create or get these documents again.

Testing Procedure: **Test 1 – Network clients restoring previous versions of files (Stimulus/Response)**

a. Logon as administrator to the client machine
b. Click the 'Start' button, and then click 'Run'. In the Open dialog box type "\\serv2003\auditshare"
c. Enter user name and password. Click 'OK'
d. Click the 'File' menu, select 'New' and click 'Text Document'. Give the document a name (Shadow Audit Client.txt)
e. Double-click on the text document and type "My first document." 'Save' and close the document
f. The creation of shadow copies does not occur in real-time. Shadow copies are created on a scheduled basis or when manually initiated
g. Logon as administrator to the file server
h. Click the 'Start' button then click 'Manage Your Server'
i. Click the 'Manage this file server' link next to the 'File Server' role
j. The 'File Server Management' tool appears
k. In the right window pane, click 'Configure Shadow Copies'
l. Click 'Create Now'
m. Logon as administrator to the client machine
n. Double-click on the text document and change the text to read "My second shadow copy". 'Save' change and close the text document
o. Right-click on the text document and select 'Properties'. Click the 'Previous Versions' tab
p. Look for a previous version of the text document. If available click View to see the document as it appeared when the last shadow copy was created

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

q. Close the previous version of the text document. Click 'Restore' and then click 'Yes'. The previous version should get restored
r. Take screen shot by pressing 'Alt + Print Screen'
s. Document your findings in the audit report

Test 2 – Network clients restoring deleted files (Stimulus/Response)

a. Repeat steps (a – m) as in Test 1 in this item with the exception of changing the file name to (Shadow Audit Client2.txt)
b. Right-click on the text document and select 'Delete'
c. Right-click on the files folder and select Properties. Click the 'Previous Versions' tab
d. Look for a previous version of the folder. If available click View to see the deleted document appear in the folder
e. Close the previous version of the folder. Click 'Restore' and then click 'Yes'. The deleted document should get restored

Compliance:	Pass or Fail
Compliance Criteria:	▪ Test 1: Successfully restoring previous version of overwritten files. ▪ Test 2: Successfully restoring previous version of deleted files.
Test Nature:	Objective
Control Objectives:	Restoring deleted and pervious versions of files.
Evidence:	See Part 3
Findings:	See Part 3

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

ITEM 7 - Confirm Restriction on Login Hours

Reference: Result of personal experience to be able to comply with the organization's policy in accessing the file server.

Degree of Exposure: Low

Risk: User accessing the server in non-approved hours. *(Vulnerability [3] see page 12)*

Risk Impact: Users violating the organizations security policy.

Testing Procedure:

Test 1 – Checking Logon hours for users

This test requires the installation of Dumpsec on the file server.

a. Logon as administrator to the file server
b. Click the 'Start' button, and then click 'All Programs'. Under the 'System Tools' menu click 'DumpSec'
c. Somarsoft DumpSec application should get launched
d. Under the report menu select 'Dump Users as Table'

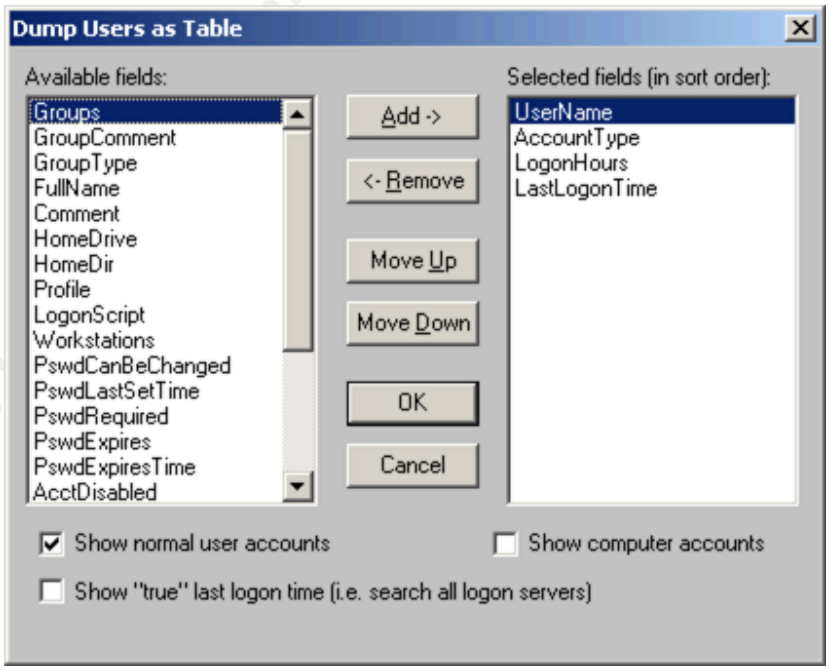


Figure 2.8 - Creating users table for login hours access

e. Add 'UserName', 'AccountType', 'LogonHours' and 'LastLogonTime to the 'Select fields (in sort order):' list
f. click 'OK'

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

j. Take screen shot by pressing 'Alt + Print Screen'
g. Document your findings in the audit report

Test 2 – Users not able to access the file shares in non working hours (Stimulus/Response)

a. During non-working hours (before 9 am, after 5 pm) record the timing in the audit report
b. Logon to the system using a user account that is not supposed to have access during non-working hours
c. Take screen shot by pressing 'Alt + Print Screen'
d. Document your findings in the audit report
e. Logon to the system as administrator
f. Click the 'Start' button, and then click 'All Programs'. Under the 'System Tools' menu click 'DumpSec'
g. Somarsoft DumpSec application should get launched
h. Under the report menu select 'Dump Users as Table'
i. Add 'UserName', 'AccountType', 'LogonHours' and 'LastLogonTime to the 'Select fields (in sort order):' list
j. Click 'OK'
k. Take screen shot by pressing 'Alt + Print Screen'
l. Document your findings in the audit report
m. Click the 'Start' button and then click 'Run', type eventvwr in the text box and press 'Enter'
n. Click on 'Security' (left-side) then search in the events to find the status of your login event
o. Repeat steps c & d

Compliance:	Pass or Fail
Compliance Criteria:	▪ Test 1: All accounts set according to the company's policy of accessing hours. Access limited to working hours. ▪ Test 2: Access denied in non approved hours. User not able to login to the system in non-working hours.
Test Nature:	Objective
Control Objectives:	Login hours controlled. Access restricted to specific hours.
Evidence:	See Part 3
Findings:	See Part 3

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

ITEM 8 – Check Password Complexity

Reference:
- [3.] Subtitle: File Server Hardening Steps

Degree of Exposure: Moderate

Risk: Passwords can be retrieved using password cracking software. *(Vulnerability [4] see page 12)*

Risk Impact: Password can be easily cracked; therefore intruder will gain unauthorized access.

Testing Procedure:

Test 1 – Audit User Account Passwords Complexity using dictionary method

This test requires the installation of L0pht Crack on the file server.

a. Logon as administrator to the File Server
b. Click the 'Start' button, 'Program Files', 'LC4' then select 'LC4'
c. LC4 Wizard will get launched click 'Next'
d. Confirm that 'Retrieve from the local machine' radio button is selected then click 'Next'
e. Select 'Common Password Audit'
f. Keep the default selected items in the reporting style and click 'Next' then click 'Finish'
g. Take screen shot by pressing 'Alt + Print Screen'
h. Document your findings in the audit report

Test 2 – Confirm that Windows 2003 restricts that the user creates complex passwords (Stimulus/Response)

a. Logon as administrator to the File Server
b. Click the 'Start' button, 'Administrative tools' then select 'Computer Management'
c. Expand the 'Local Users and Groups' tree and select 'Users' (left hand side)
d. On the right hand side right click on the 'Administrator' entry and select 'Set Password
e. Enter a simple password (abcd) and click 'OK'
f. Take screen shot by pressing 'Alt + Print Screen'
g. Document your findings in the audit report

Compliance: Pass or Fail

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Compliance Criteria:	▪ Test 1: LC4 not able to crack user account passwords using word dictionary method. ▪ Test 2: Not possible to set a password that is not complex (More than eight characters, Alphanumeric and contains uppercase letters).
Test Nature:	Objective
Control Objectives:	User accounts have strong passwords that cannot be cracked easily.
Evidence:	See Part 3
Findings:	See Part 3

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

ITEM 9 - Check User's Disk Quota

Reference: [11.] Chapter 15. Managing File System. Subtitle: Quota

Degree of Exposure: Moderate

Risk: Server running out of disk space. *(Vulnerability [5] see page 12)*

Risk Impact: Server disk space getting filled to capacity and hence affecting overall performance. Users misusing disk space and wasting organization's resources.

Testing Procedure:

Test 1 – Confirm that quota management is enabled

a. Logon as administrator to the File Server
b. Click the 'Start' button, and then click 'Windows Explorer'
c. Under 'My Computer' right click on the 'C' drive, click 'Properties'
d. Select the 'Quota' tab
e. Take screen shot by pressing 'Alt + Print Screen'
f. Document your findings in the audit report
g. In the 'Quota' tab click on the 'Quota Entries…' button
h. Repeat steps e. & f.
i. Repeat steps a to h with all fixed drives

Test 2 – Confirm limitation on user's disk space (Stimulus/Response)

a. Login to the user account created for auditing from a client machine
b. Click the 'Start' button, and then click 'Run'. In the Open dialog box type \\serv2003\John Home
c. Enter user name and password. Click 'OK'
d. Copy a folder that exceeds 100MB in size to 'John Home'
e. Monitor the file transfer till an error occurs
f. Take screen shot by pressing 'Alt + Print Screen'
g. Document your findings in the audit report
h. If the folder gets copied successfully right click on the copied folder and select 'Properties'
i. Repeat steps f. & g

Compliance: Pass or Fail

Compliance Criteria:

- Test 1: 'Enable Quota Management' checked and a disk space limit is specified. Under the 'Quota Entries' users should have a set limit for their disk space.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Test 2: User should not be able to copy files more than 100 MB. A copying file or folder error should popup stating that there is not enough free disk space and recommending deleting one or more files to free disk space, and then try again.

Test Nature: Objective

Control Objectives: Restrict user disk quota to 100 MB and so prevent the users from exceeding the file space assigned. Hence, preventing file server from filling to capacity without warning.

Evidence: See Part 3

Findings: See Part 3

ITEM 10 – Confirm File System Format (NTFS)

Reference: [13.] Chapter 9. Permissions Security, Folder Sharing, and Dfs

Degree of Exposure: Low

Risk: Less file system stability and no restriction on the access of individual files and directories. *(Vulnerability [5] see page 12)*

Risk Impact: Low stability can cause the system to crash. Due to less access restrictions, file and directory sharing is limited and unsecured.

Testing Procedure: *This test requires the installation of Microsoft Baseline Security Analyzer on the file server.*

a. Logon as administrator to the File Server
b. Click the 'Start' button, 'Program Files' then select 'Microsoft Baseline Security Analyzer'
c. Click on 'Scan a Computer' link then click 'Start Scan'
d. Locate 'Windows Scan Results' category
e. Click 'Result details' in the 'File System' section
f. Take screen shot by pressing 'Alt + Print Screen'
g. Document your findings in the audit report

Compliance: Pass or Fail

Compliance Criteria: All hard drives are using the NTFS file system.

Test Nature: Objective

Control Objectives: Secured File system to allow control and restricted access to individual files or directories.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

ITEM 11 – Verify File Shares Permissions

Reference:
- [12.] Chapter 5. Security Services – Subtitle: Effective Permissions
- [11.] Chapter 16. Managing Shared Resource. Subtitle: Configuring File Sharing

Degree of Exposure: Low

Risk: Unauthorized users having access to shared directories. *(Vulnerability [4] see page 12)*

Risk Impact: Loss of data confidentiality and integrity due to unauthorized access.

Testing Procedure: *This test requires the installation of Dumpsec on the file server.*

a. Logon as administrator to the file server
b. Click the 'Start' button, and then click 'All Programs'. Under the 'System Tools' menu click 'DumpSec'
c. Somarsoft DumpSec application should get launched
d. Under the report menu select 'Dump Permissions for All Shared Directories'
e. Copy all the content by pressing Ctrl + C
f. Paste the content to a word document press Ctrl+V
g. Manually review all the share permissions and confirm that they comply with organization's policy for shared directories
h. Document your findings in the audit report

Compliance: Pass or Fail

Compliance Criteria: All shares permission are configured according to the organization's policy for shared directories.

Test Nature: Objective

Control Objectives: Access to files and folders restricted to authorized users.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

ITEM 12 – Confirm That Server Is Free From Known Malicious Code

Reference:	▪ [3.] Subtitle: File Server Hardening Steps ▪ [18.] Subtitle: Step 5 Update Virus Scan ▪ [18.] Subtitle: Step 7 Configure On-Demand Scan and Scan your system ▪ [19.] Subtitle: Install VirusScan 7.1
Degree of Exposure:	High
Risk:	Server files infected by malicious code (virus, Trojan, worms, etc.). *(Vulnerability [2] see page 12)*
Risk Impact:	File server and all other systems on the network can get infected and so is vulnerable to all risks created by malicious code such as denial of service, loss of data, etc.
Testing Procedure:	a. Logon as administrator to the File Server b. Click the 'Start' button, 'Program Files', Network Associates then select 'VirusScan On-Demand' c. Highlight 'All Local Drives' by clicking on the icon d. Click 'Scan Now' e. Take screen shot by pressing 'Alt + Print Screen' f. Document your findings in the audit report
Compliance:	Pass or Fail
Compliance Criteria:	Antivirus software reports that the server is free from any malicious code after conducting the scan.
Test Nature:	Objective
Control Objectives:	Files stored on the server are not infected by malicious code. Server free from any known malicious code.

© SANS Institute 2004, Author Retains Full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

ITEM 13 – Check Virus Auto-Protection

Reference:
- [3.] Subtitle: File Server Hardening Steps
- [18.] Subtitle: Step 6 About On Access Scan
- [19.] Subtitle: Configuring VirusScan 7.1

Degree of Exposure: High

Risk: Antivirus software not able to automatically detect malicious code. *(Vulnerability [2] see page 12)*

Risk Impact: File Server can get infected by malicious code and so is vulnerable to all risks created by that malicious code such as denial of service, loss of data, etc.

Testing Procedure:

Test 1 – Check On Access scan enabled

a. Logon as administrator to the File Server
b. Click the 'Start' button, and then select 'Network Associates' click 'Virus Scan Console'
c. Take screen shot by pressing 'Alt + Print Screen'
d. Document your findings in the audit report

Test 2 – Antivirus Software detecting malicious code Automatically (Stimulus/Response)

a. Login to the user account created for auditing from a client machine
b. Disable any antivirus software on the client machine
c. Open the following URL (http://www.eicar.org/anti_virus_test_file.htm) in the web browser
d. At the bottom of the page right-click on the eicar.com.txt link and download the antivirus test file "eicar". It is safe to use this file, because it is not a virus, and does not include any fragments of viral code
e. Click the 'Start' button, and then click 'Run'. In the Open dialog box type \\serv2003\John Home
f. Copy the antivirus test file "eicar" to John Home folder
g. Logon as administrator to the File Server
h. Take screen shot by pressing 'Alt + Print Screen'
i. Document your findings in the audit report

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Compliance:	Pass or Fail
Compliance Criteria:	▪ Test 1: Antivirus software configured to Auto-Protect the file server from malicious code. On Access scan feature enabled. ▪ Test 2: Antivirus software automatically detects Eicar as a virus and cleans the server from the file.
Test Nature:	Objective
Control Objectives:	Auto-Protect the server from any malicious code. Antivirus solution automatically detects and cleans the server from malicious code.
Evidence:	See Part 3
Findings:	See Part 3

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

ITEM 14 – Virus Protection Solution Scans Contents of Zipped Files

Reference:
- [3.] Subtitle: File Server Hardening Steps
- [18.] Subtitle: Step 7 Configure On-Demand Scan and Scan your system
- [19.] Subtitle: Install VirusScan 7.1

Degree of Exposure: High

Risk: Server not scanning Archives (e.g. ZIP files). *(Vulnerability [2] see page 12)*

Risk Impact: File Server can get infected by malicious code and so is vulnerable to all risks created by that malicious code such as denial of service, loss of data, etc.

Testing Procedure:

Test 1 – Check Archive Files Scanning Configuration

a. Logon as administrator to the File Server
b. Click the 'Start' button, and then select 'Network Associates' click 'VirusScan On-Demand'
c. Click on the 'Detection' tab
d. Take screen shot by pressing 'Alt + Print Screen'
e. Document your findings in the audit report

Test 2 – Antivirus Software Automatically detecting malicious code in Archive Files (zip) (Stimulus/Response)

a. Open the following URL (http://www.eicar.org/anti_virus_test_file.htm) in the web browser
b. At the bottom of the page click on the eicar_com.zip link to download the antivirus test zip file "eicar". It is safe to pass around, because it is not a virus, and does not include any fragments of viral code
c. Click 'Save'
d. A warning message should appear
e. Take screen shot by pressing 'Alt + Print Screen'
f. Document your findings in the audit report
g. If no warning message appears go to the folder where you have saved the zip file
h. Repeat steps e & f

Compliance: Pass or Fail

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Compliance Criteria:	▪ Test 1: Antivirus software configured to scan zipped files for malicious code. Scan inside archive files feature enabled. ▪ Test 2: Antivirus software automatically detects Eicar zipped file as a virus and cleans the server from the code.
Test Nature:	Objective
Control Objectives:	Protect the server from any malicious code stored in archived files.
Evidence:	See Part 3
Findings:	See Part 3

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3 The Audit

Product:	File Server	**Audit Date:**	01- 03 - 2004
Auditor:	Tamer Eltoni	**Checklist Version:**	GSNA-V-3.0

Item Number	Description	Check
1.	Identify Installation Of Required Service Packs and/or Updates	☑
2.	Check System Time and Date	❑
3.	Ensure Shadow Copies Feature Enabled	☑
4.	Confirm Storage Area For Shadow Copies Is On A Separate Volume On Another Disk	☑
5.	Ascertain Network Client Machines Can Use Shadow Copies Of Shared Folders	☑
6.	Ascertain Network Clients Able To Restore Files	☑
7.	Confirm Restriction on Login Hours	☑
8.	Check Password Complexity	☑
9.	Check User's Disk Quota Restriction	☑
10.	Confirm File System Format (NTFS)	❑
11.	Verify File Shares Permissions	❑
12.	Confirm That Server Is Free From Known Malicious Code	❑
13.	Check Virus Auto-Protection	☑
14.	Confirm that Virus Protection Solution Scans Archived Files	☑

Notes:

- Out of the checklist items in Part 2 the above ten items were selected as the scope of the audit.
- For the test procedure please refer to Part 2.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Auditing ITEM 1 - Identify installation of required Service Packs and/or Updates

(For test details See Part 2 page 19)

Evidence: After conducting the scan it was found that one Critical update is Missing, Security Update for Windows Server 2003 (KB828028). See figure 3.1.

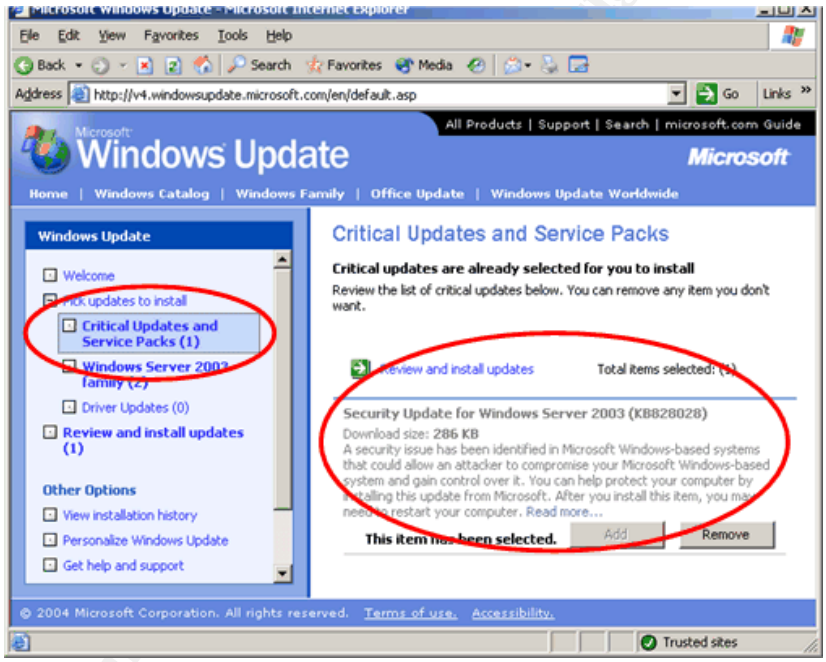


Figure 3.1- Critical updates missing

Findings: **Compliance** = **Failed** ✕

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Auditing ITEM 3 - Ensure Shadow Copies Feature Enabled

(For test details See Part 2 page 22)

Evidence:

Test 1 – Confirming that the shadow copy feature is enabled

As shown in figure 3.2. Shadow Copying is enabled for both volumes (**C**) and (**D**)

Test 2 – Shadow Copy Feature (Stimulus/Response)

A Shadow Copy of the document is created and can be restored which proofs that the shadow copy feature is functioning as expected. See figure 3.3.

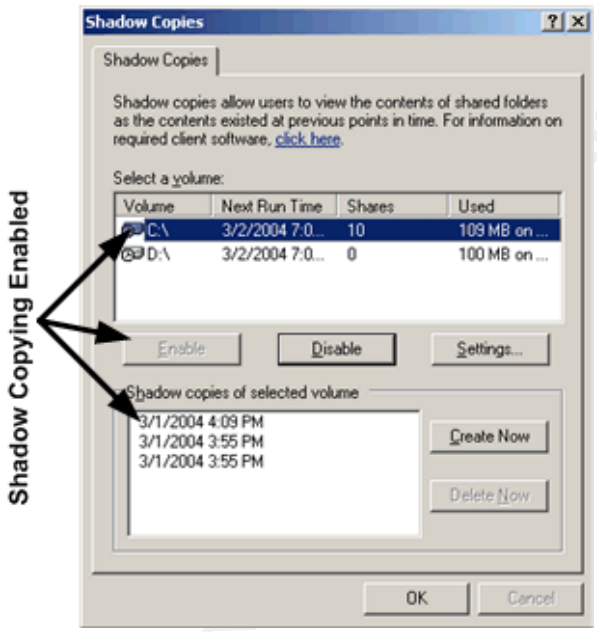


Figure 3.2 – Shadow copy enabled

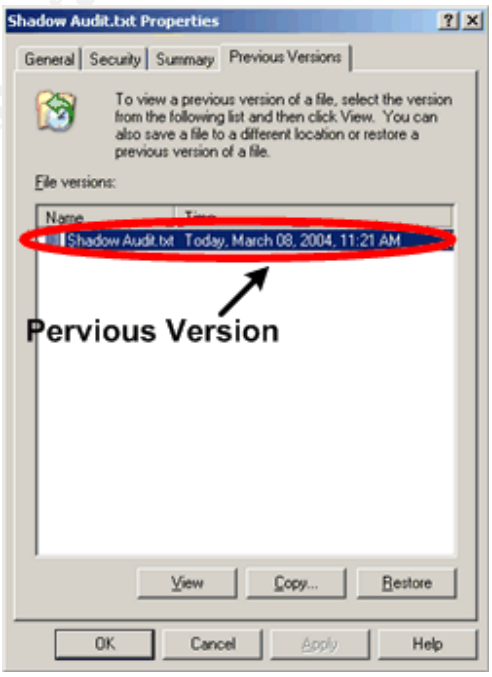


Figure 3.3 – Pervious Version of Document

Findings:

Test 1 Compliance = **Passed** ✔

Test 2 Compliance = **Passed** ✔

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Auditing ITEM 4 - Confirm Storage Area for Shadow Copies Is On A Separate Volume on another Disk

(For test details See Part 2 page 24)

Evidence: The shadow copy is stored on the same volume. As its shown in figure 3.4 volume(**C**) shadow copy is being stored on the same volume (**C**).

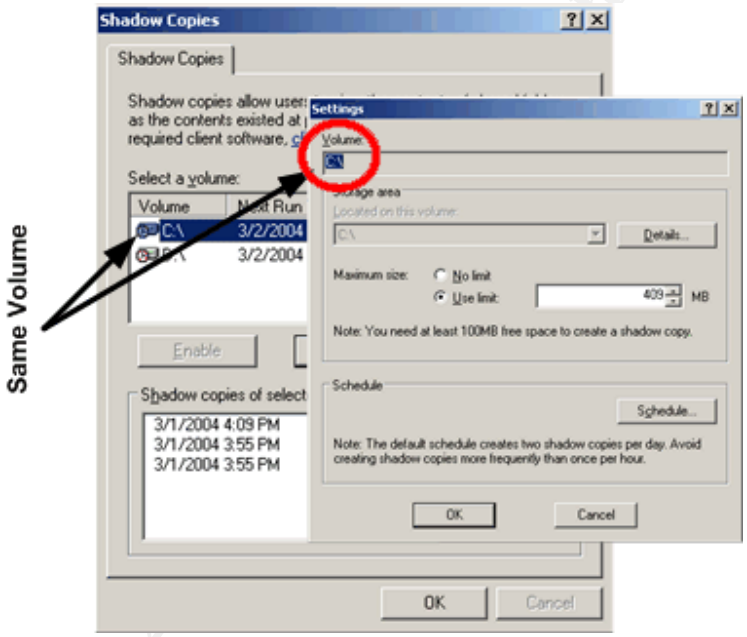


Figure 3.4 – Storage area of shadow copies

Findings: **Compliance** = **Failed** ✕

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Auditing ITEM 5 - Ascertain Network Client Machines Can Use Shadow Copies Of Shared Folders

(For test details See Part 2 page 26)

Evidence:

Test 1- Previous Versions Client Setup on Windows XP Clients

'Previous Versions' client was installed successfully on Windows XP.

Test 2 – 'Previous Versions' tab installed (Stimulus/Response)

After installing the Previous Versions client on Windows XP, documents available under network shares protected by shadow copies had a new tab Previous Versions added to the document's properties window. See figure 3.5.

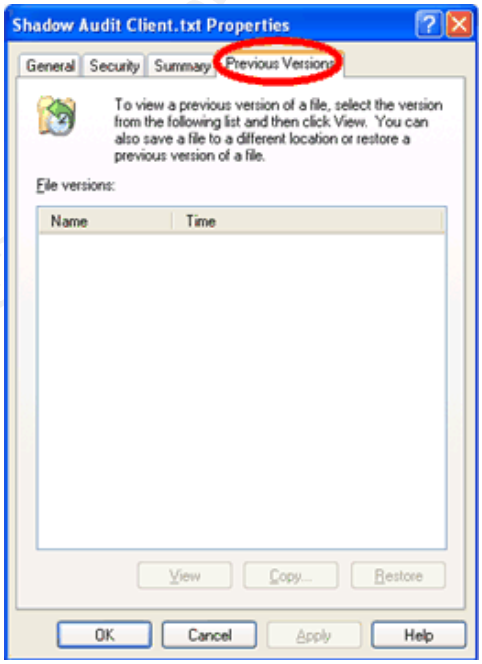


Figure 3.5 – Previous Version Tab

Findings:

Test 1 compliance = **Passed** ✔

Test 2 compliance = **Passed** ✔

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Auditing ITEM 6 - Ascertain Network Clients Able To Restore Files

(For test details See Part 2 page 28)

Evidence:

Test 1 – Network clients restoring previous versions of files (Stimulus/Response)

In the 'Previous Version' tab under the 'Properties' of the document a shadow copy was created. When viewing this copy the previous written text was found as shown in figure 3.6. It was possible to restore the previous version of the document and replace the modified document.

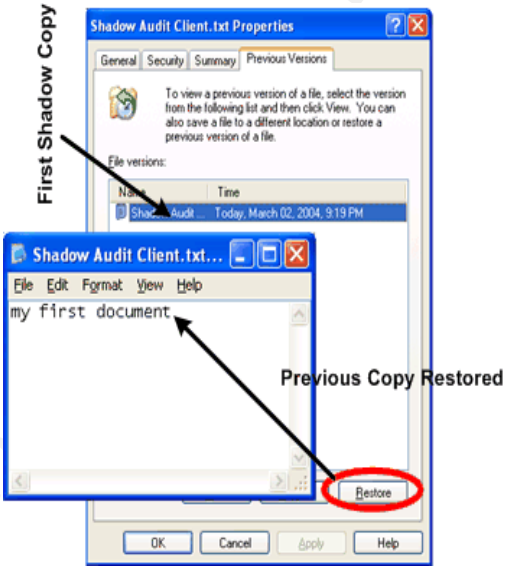


Figure 3.6 – Previous copy restoration

Test 2 – Network clients restoring deleted files (Stimulus/Response)

Even though the document was deleted from the folder and the folder ended to contain only one document; it was possible to restore the deleted document by restoring the previous version found under the 'Previous Version' tab in the folders properties. See figure 3.7.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

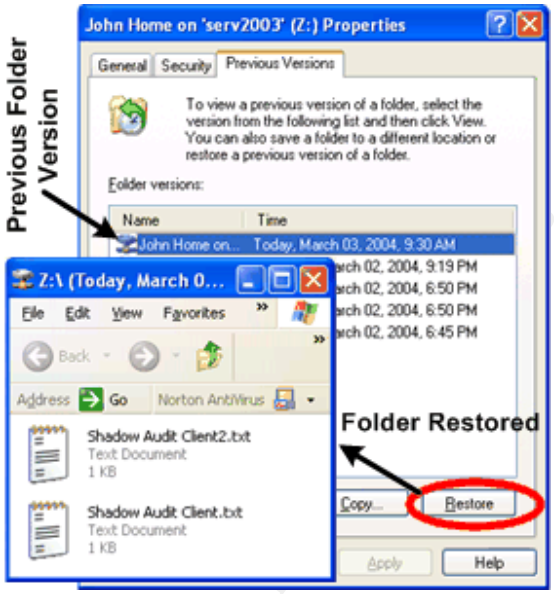


Figure 3.7- Deleted version restoration

Findings: **Test 1 Compliance** = **Passed** ✔

Test 2 Compliance = **Passed** ✔

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Auditing ITEM 7 - Confirm Restriction on Login Hours

(For test details See Part 2 page 30)

Evidence:

Test 1 – Checking Logon hours for users

It was found that there is no login restriction on any of the users as the 'LogonHour' column in the report generated by DumpSec showed the word 'All', which means all hours access. See figure 3.8.

Test 2 – Users not able to access the file shares in non working hours (Stimulus/Response)

It was possible to login to the system in non-working hours using a user's account that should be prevented access at that hour. By check the systems event viewer the events properties showed the time of a successful access which was after working hours as in figure 3.9.

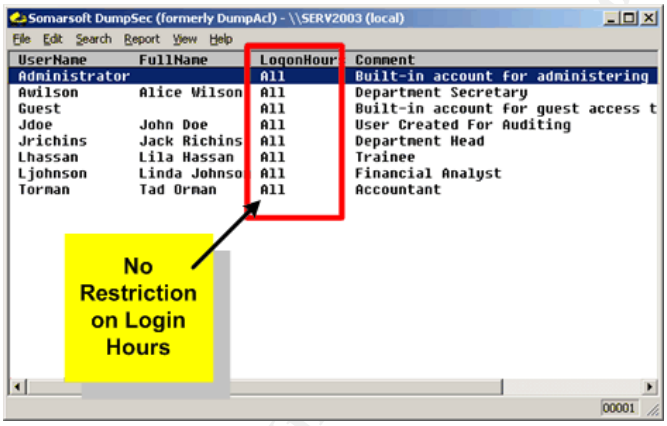


Figure 3.8 – Allowed login hours

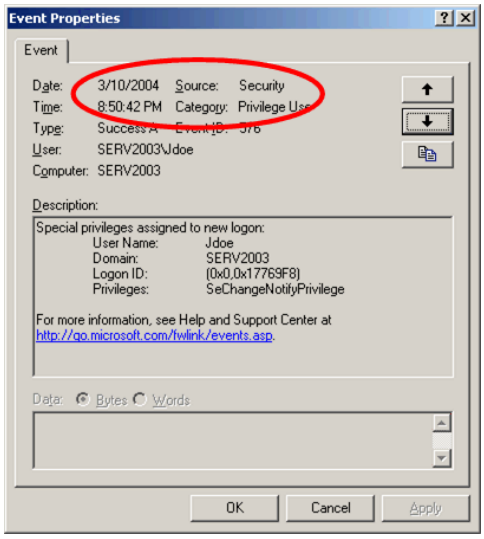


Figure 3.9 – Login time

Findings:

Test 1 Compliance = **Failed** ✗

Test 2 Compliance = **Failed** ✗

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Auditing ITEM 8 – Check Password Complexity

Evidence: (For test details See Part 2 page 32)

Test 1 – Audit User Account Passwords Complexity using dictionary method

L0pht Crack software was not able to retrieve any of the user accounts passwords found on the local machine using the word dictionary method, which proofs that passwords are complex to a certain level. (Brute Force attack was not possible due to the unavailability of the commercial edition of L0pht Crack).

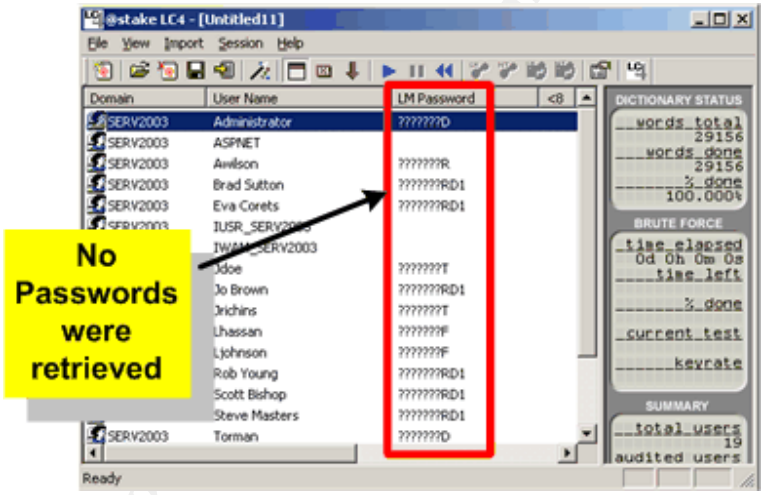


Figure 3.10 – No passwords cracked

Test 2 – Confirm that Windows 2003 restricts that the user creates complex passwords (Stimulus/Response)

The user was restricted from creating a password that is less than eight characters, alphanumeric and has uppercase letter. Therefore, avoiding the existence of simple passwords.

Figure 3.11 – Password doesn't meet policy requirements

Findings: **Test 1 Compliance** = **Passed** ✔ **Test 2 Compliance** = **Passed** ✔

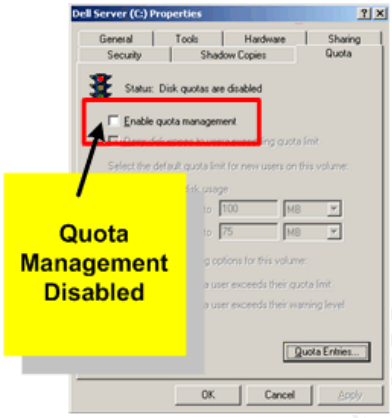
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Auditing ITEM 9 - Check User's Disk Quota

(For test details See Part 2 page 34)

Evidence: **Test 1 – Confirm that quota management is enabled**

Volume disk space Quota Management is disabled as was found under volume's 'Properties' in the 'Quota' tab as in figure 3.12. Hence, 'Quota Entries' showed no limits on any of the shares see figure 3.13. Therefore there will be no limitation on the share disk size of each user.



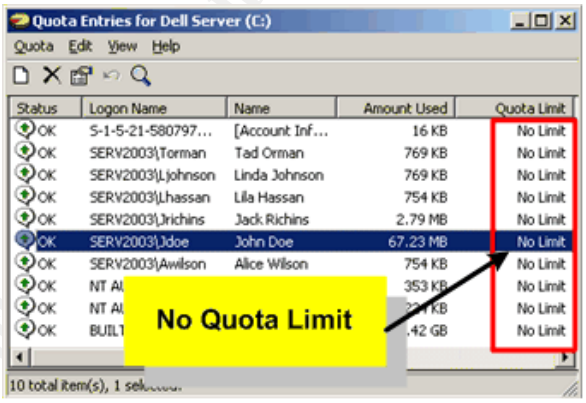


Figure 3.12 - Quota Management *Figure 3.13 – No quota Limits*

Test 2 – Confirm limitation on user's disk space (Stimulus/Response)

It was possible to copy data that exceeded 100 MB without any restriction. The data copying was done to a share that should have a limitation of 100 MB in data size. See figure 3.14.

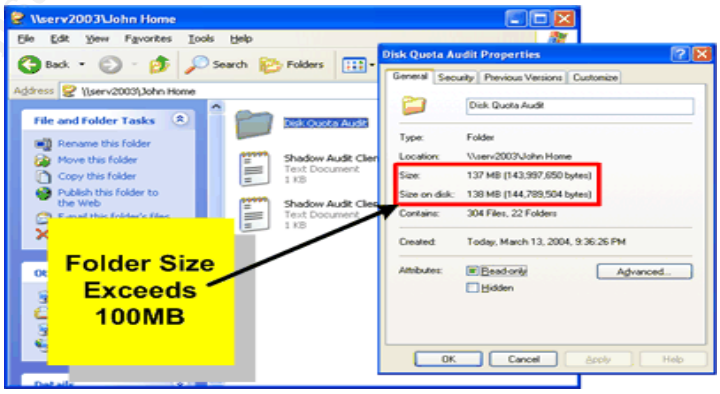


Figure 3.14 – Data size exceed 100MB

Findings: **Test 1 Compliance** = **Failed ✕**

Test 2 Compliance = **Failed ✕**

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Auditing ITEM 13 – Check Virus Auto-Protection

(For test details See Part 2 page 38)

Evidence: **Test 1 – Check On Access Scan enabled**

The On-Access Scan feature is enabled as shown in figure 3.15. This feature detects malicious code immediately as it accesses the server.

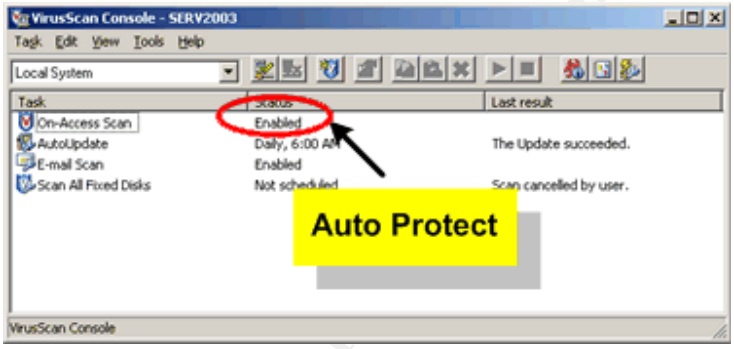


Figure 3.15 – Virus auto-protect enabled

Test 2 – Antivirus Software detecting malicious code Automatically (Stimulus/Response)

Eicar file was automatically detected as a virus once downloaded to the server, which proofs the antivirus protection solution can automatically detect malicious code as shown in figure 3.16.

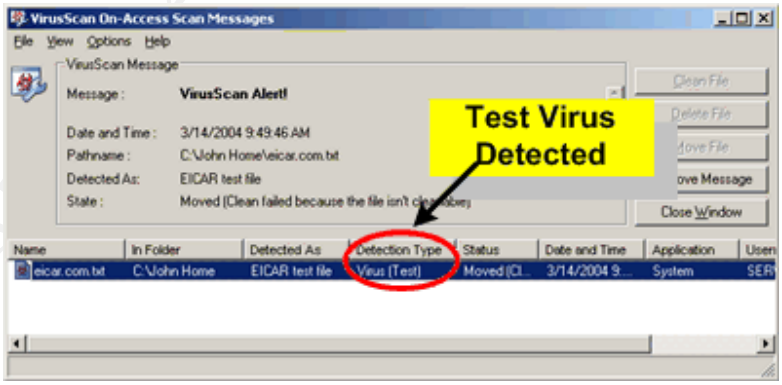


Figure 3.16 – Virus detected

Findings: **Test 1 Compliance** = **Passed** ✔

Test 2 Compliance = **Passed** ✔

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

bAuditing ITEM 14 – Virus protection Solution scans contents of zipped files

(For test details See Part 2 page 40)

Evidence: **Test 1 – Check Archive Files Scanning Configuration**

Scan inside archives files option is disabled as seen in figure 3.17 and so the antivirus will not detect malicious code found in archives such as zip files.

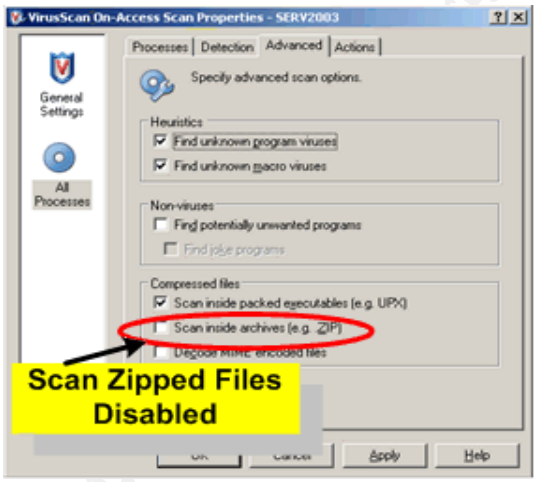


Figure 3.17 – Archive files scanning disabled

Test 2 – Antivirus Software Automatically detecting malicious code in Archive Files (zip) (Stimulus/Response)

The eicar compressed file (.zip) was not detected as a virus although it contains the eciar file which indicates that the antivirus doesn't scan archive files for malicious code. See figure 3.18.

Figure 3.18 – Eicar zipped file

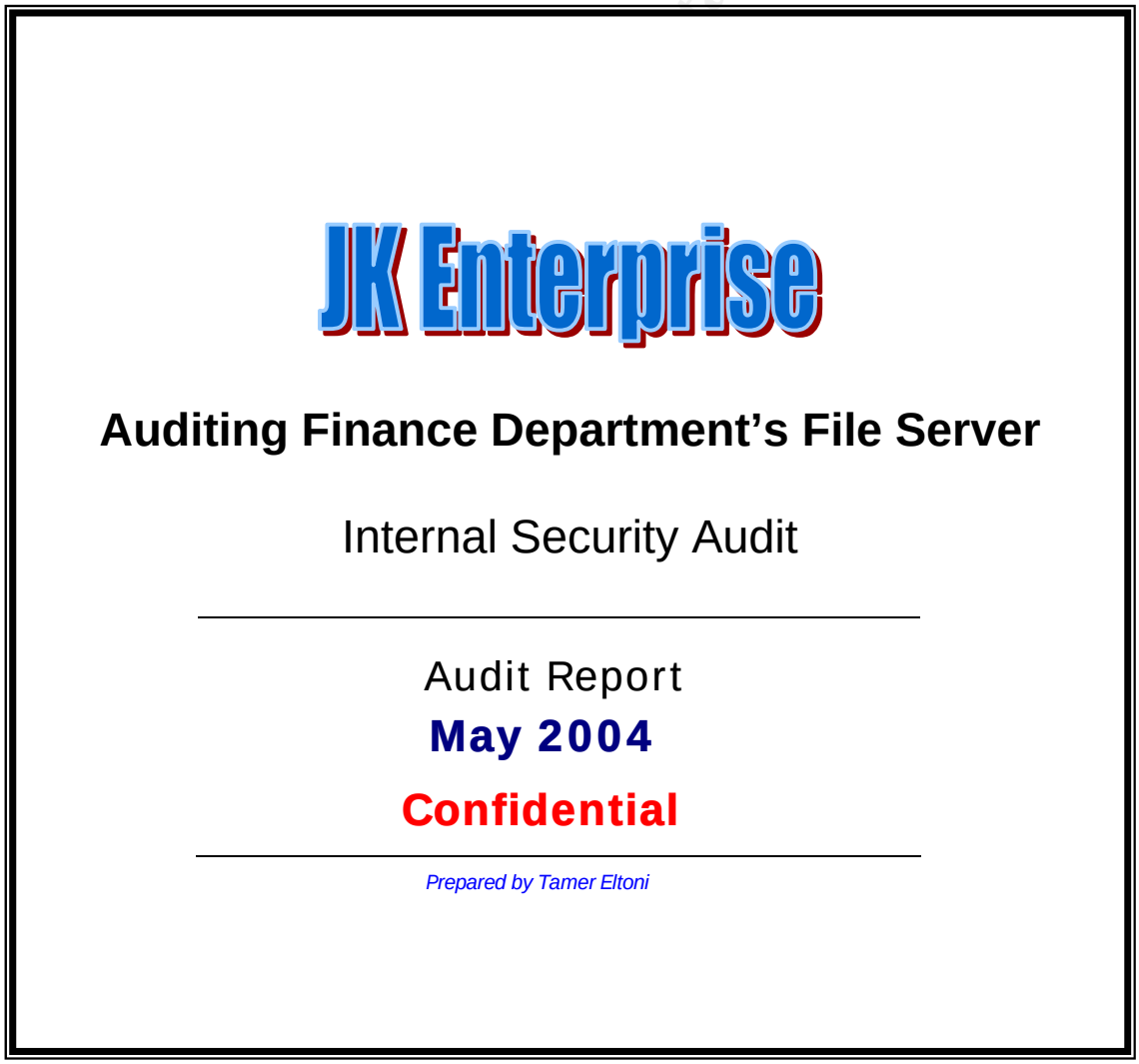
Findings: **Test 1 Compliance** = **Failed ✕** **Test 2 Compliance** = **Failed ✕**

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

4 Audit Report

The audit report communicates the results of the audit work. For that reason alone it is perhaps one of the most important parts of the audit process. It is important because it is what the department and senior management sees, and in some cases may be the only product of the audit that management receives. If written and communicated well, it can act as a positive change agent prompting management to take corrective action. [21.]

Section A: Cover Page



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Section B: Executive Summary

As businesses come to increasingly depend on continuous access to their data (including systems formerly misunderstood as non-critical), ensuring that this data is secure and available on demand are of paramount importance.

The inability to access critical data on demand is a business-killer. To fight this problem, JK Enterprise ran an internal security audit on its finance department's file server to ensure that the server is fulfilling the security and availability measures required.

The objective of the audit, which is to examine the server at a single point in time to make sure it is configured appropriately according to its role as a file server, best practices and organization's policy, was successfully achieved.

The scope of the audit was covered by running ten audit items testing the following features:

- Strong Password Policy
- Restricted Login hours
- User's Disk Quota Management
- Virus Auto-Protect
- Windows Server 2003 Shadow Copying Feature

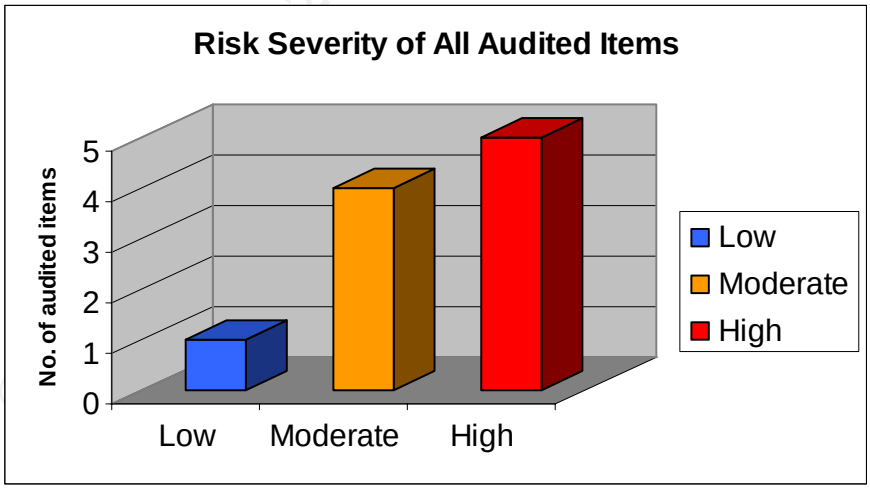


Chart 1 – Risk severity of audited items

After conducting the audit it was found that results of five items had a high risk severity, four moderate and finally one with a low risk severity as shown in chart 1.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

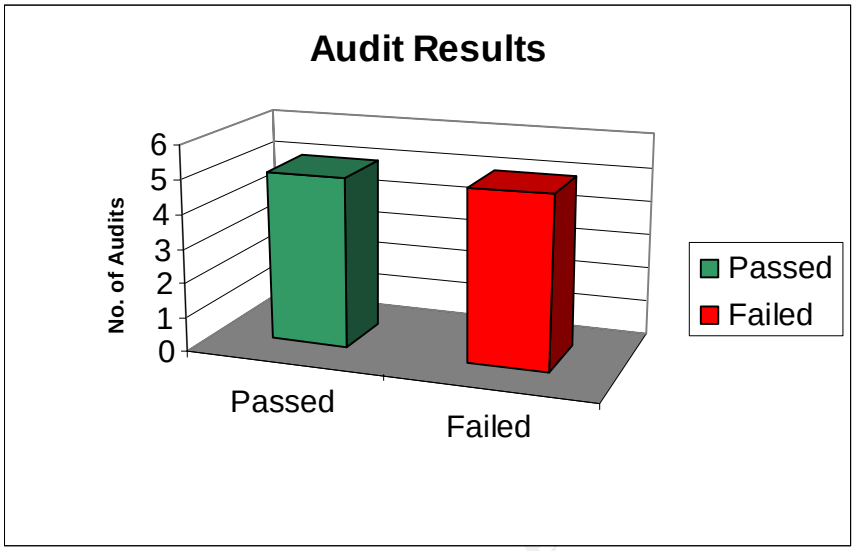


Chart 2- Audit Results

Five out of the ten audited items met the compliance criteria and passed the audit, as represented in chart 2. Meanwhile, the remaining unsuccessful five items included three items with high risk severity. See chart 3.

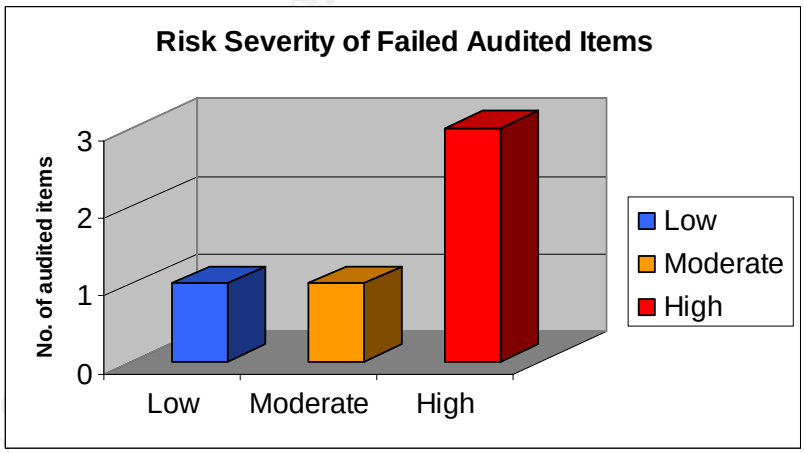


Chart 3 – Risk severity of failed items

Notes: This report represents a security audit performed for JK Enterprise. It contains confidential information about the state of the audited system. Access to this information by unauthorized personnel may allow them to compromise the audited system.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Section C: Audit Findings

A ten item audit checklist was conduct to the finance department's file server and the results were as shown in table 4.1.

Table 4.1: Audit Results

Item Number	Description	Results	Risk Severity
1.	Identify installation of required Service Packs and/or Updates	Failed ☒	High
3.	Ensure Shadow Copies Feature Enabled	Passed ☑	High
4.	Confirm Storage Area For Shadow Copies Is On A Separate Volume On Another Disk	Failed ☒	Moderate
5.	Ascertain Network Client Machines Can Use Shadow Copies Of Shared Folders	Passed ☑	Moderate
6.	Ascertain Network Clients Able To Restore Files	Passed ☑	High
7.	Confirm Restriction on Login Hours	Failed ☒	Low
8.	Check Password Complexity	Passed ☑	Moderate
9.	Check User's Disk Quota Restriction	Failed ☒	Moderate
13.	Check Virus Auto-Protection	Passed ☑	High
14.	Confirm that Virus Protection Solution Scans Archived Files	Failed ☒	High

Compliant Audit Findings

Five of the ten audit items passed the audit by meeting the compliance criteria; which shows that the administrators and the security team are doing a great job in handling these items. The compliant findings are:

- Shadow Copies Feature Enabled (for details on the audit evidence and findings refer to Part 3 page 44)
- Network client machines can use shadow copies of shared folders (for details on the audit evidence and findings refer to Part 3 page 46)
- Network clients able to restore previous versions of files (for details on the audit evidence and findings refer to Part 3 page 47)
- Password Complexity (for details on the audit evidence and findings refer to Part 3 page 50)
- Virus Auto-Protection functioning properly (for details on the audit evidence and findings refer to Part 3 page 52)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Non-Compliant Audit Findings (audit exceptions)

However, the other five items need special care to avoid and mitigate the risk that can be a result of their existence. Recommendations and cost for managing each risk is found below:

ITEM 1 - Installation of Required Service Packs and/or Updates

For details on the audit evidence and findings refer to Part 3 page 43.

Finding

After conducting the audit on the checklist **item 1**, the result **failed** the compliance criteria (see page 20).It was found that Security Update for Windows Server 2003 (KB828028) is missing.

Risk

Windows Server 2003 (KB828028) update fixes a security issue that has been identified in Microsoft Windows-based systems that could allow an attacker to compromise Microsoft Windows-based system and gain control over it. For more details on the missing update and its impact refer to the following URL: http://www.microsoft.com/downloads/details.aspx?FamilyID=3D7FFFF9-A497-42FF-90E7-283732B2E117&displaylang=en

Recommendation

System Security does not rely solely on technology; it also depends on people and processes. Systems must be monitored and maintained over time, and one of the most critical maintenance tasks that an administrator must perform is updating or patching the system. Automatic download and notification of windows updates must be enabled.

Cost

Table 4.2: Item 1 risk mitigation cost

No	Description	RATE ($)		Qty	Cost ($)
		Setup	Per Day		
1	Internet access cost (already covered)	0	0	317KB	0
2	Installation and testing of patch file	0	250	2 hours	62
				Total	**$62**

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

ITEM 4 – Storage Area for Shadow Copies Is On a Separate Volume on another Disk

For details on the audit evidence and findings refer to Part 3 page 45.

Finding

After conducting the audit on the checklist **item 4**, the result **failed** the compliance criteria (see page 25). It was found that the Shadow Copies are stored on the same volume as the original copy.

Risk

The storage of shadow copies on the same volume can cause hard disk failure or at least the overwriting of the shadow copies due to the high I/O load on the hard disk.

Recommendation

Shadow copies are a low-cost way to recover files from many accidents caused by human error, such as inadvertent editing, corruption, and deletion.

While shadow copies cannot replace your current backup solution—for example, shadow copies cannot protect you from data loss resulting from media failures—shadow copies should reduce the number of times you need to restore data from tape. Therefore, for higher availability shadow copies should be stored on separate hard disks.

Cost

Table 4.3: Item 4 risk mitigation cost

No	Description	RATE ($)		Qty	Cost ($)
		Setup	Per Day		
1	Hard Disk Configuration & Management	0	250	2 hours	62
2	Shadow Copies Configuration	0	250	1 hour	31
				Total	**$93**

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

ITEM 7 - Restriction on Login Hours

For details on the audit evidence and findings refer to Part 3 page 49.

Finding

After conducting the audit on the checklist **item 7**, the result **failed** the compliance criteria (see page 31). For better monitoring and control over the file server JK has set a policy of restricting access to working hours. It was found that there are no restrictions on login hours to the file server. Meanwhile, the organization's policy restricts access to the data in non-working hours.

Risk

Users accessing server in non-working hours and so are violating the organization's security policy.

Recommendation

Setting and configuring the operating system (Windows Server 2003) to restrict user's access to working hours.

Cost

Table 4.4: Item 7 risk mitigation cost

No	Description	RATE ($)		Qty	Cost ($)
		Setup	Per Day		
1	Configuring User Access to login hours	0	250	4 hours	125
				Total	**$125**

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

ITEM 9 - Check User's Disk Quota

For details on the audit evidence and findings refer to Part 3 page 51.

Finding

After conducting the audit on the checklist **item 9**, the result **failed** the compliance criteria (see page 34). It was found that there are no limits on the disk space the user's can use.

Risk

Users misusing disk space and wasting organization's resources causing server disk space getting filled to capacity which can affect overall performance.

Recommendation

Enabling quota management in order to be able to limit the disk space used by each user according to organization's policy and user needs.

Cost

Table 4.5: Item 9 risk mitigation cost

No	Description	RATE ($)		Qty	Cost ($)
		Setup	Per Day		
1	Configuring User's Disk Space (Disk Quote management)	0	250	4 hours	125
				Total	**$125**

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

ITEM 14 – Virus Protection Solution Scans Contents of Zipped Files

For details on the audit evidence and findings refer to Part 3 page 53

Finding

After conducting the audit on the checklist **item 14**, the result **failed** the compliance criteria (see page 41). It was found that the anti virus protection solution does not detect malicious code stored/hidden in zipped files.

Risk

Antivirus engine not scanning zipped files, which can cause the file server to get infected by malicious code and so being vulnerable to all risks created by that malicious code such as denial of service, loss of data, etc.

Recommendation

The role of antivirus solutions is to prevent users from writing/accessing files containing infected/suspicious code and inform the administrator in case virus-infected or virus-suspicious files are found or if any errors occur.

Therefore, the anti virus should be properly configured and enabled to scan all types of files including zipped files in order to perform its full function. This will help to ensure that users who connect with infected machines to the corporate file servers do not spread viruses to others on the network.

Cost

Table 4.6: Item 14 risk mitigation cost

No	Description	RATE ($)		Qty	Cost ($)
		Setup	Per Day		
1	Anti Virus Configuration	0	250	1 hour	31
				Total	**$31**

© SANS Institute 2004, Author Retains Full Rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Section D: Audit Recommendations

The implementation of this audit should be performed as part of a larger security audit. Computer system running Windows Server 2003 File Server comprises only part of the overall environment. Additional measures should be taken to secure the perimeter network, internal network, other host computers, applications, and the client environment. In addition, policies, procedures, and physical access to critical computers should be addressed and audited in separate assignments.

It's crucial to take care of the root cause of the failure of the audited items to be able to prevent them from occurring again or from other risks evolving. After studying the reasons of the item failures it was noticed that the root cause could be the need of more security awareness and developing more skills in Windows 2003 Server administration.

In addition to the recommendation to solve the failure of each item here are some recommendations to solve the root causes of the problems.

Security Training and Awareness:

Security apathy and ignorance are the biggest threats to computer systems. [22.] The security of an organization depends on the detailed/well prepared security policy and technical solutions. But the best laid solutions and policies can and often do go astray because they are not effectively communicated to the people responsible for implementing them.

The best way to achieve a significant and lasting improvement in computer security is not by throwing more technical solutions at the problem -- it's by raising awareness and training and educating all computer users in the basics of computer security.

Windows 2003 Administration Skills

Microsoft Windows Server 2003 is rated as Microsoft's most scalable, reliable, and high-performing server operating system to date, built to handle the most complex business applications. It is designed to simplify managing mission-critical data with enhanced security technology and providing maximum server uptime for sophisticated business needs.

To be able to make the best out of this technology it's highly recommended to enhance administrator's skills and knowledge in Windows server 2003 through courses and practice.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Section E: Compensating Controls

Here is a list of some compensating controls that can help to increase the availability of the file server.

Security Policy Formulation and Implementation: A detailed well prepared security policy should be created and should include Anti-virus policy, file server access policy, file's sharing and permissions, backup and restoration policy. It is very important to communicate the policy to all involved stakeholders in order to make it effective.

Tested and certified configurations: Administrators of the system should use tested and certified configurations to avoid the failure of the operating system. Best practices recommended by vendor and other third parties can be of great help.

Limiting system modifications: The higher the number of modifications did to a stable system the higher the chances of system failure. It's highly recommended to limit the system modifications as much as possible.

Formal change and control processes: Administrators can help to prevent failure and loss of data through tight operational procedures including regular, complete backups and avoidance of unnecessary changes to systems, applications, and network configurations. [20.] Any and all changes must be well documented in order to be able to track any problems that rise in the future.

Disaster Recovery plan and drills: A disaster recovery plan should be kept in place and an incident response team should be allocated in order to be able to decrease the downtime incase of disaster. Disaster recovery drills should be conduct on scheduled bases to assure the appropriate response in disastrous situations.

Anti-virus solutions for clients: All file servers should have an updated anti-virus solution to avoid affecting or being affected by known malicious codes.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Section F: Overall Cost

After adding the cost of the security and the administration courses the overall cost of mitigating the risks found as a result of the audit would be as shown in the table 4.7.

Table 4.7: Item 1 risk mitigation cost

No	Description	RATE ($)		Qty	Cost ($)
		Setup	Per Day		
1	Security Awareness Course	7500	0	3 days	7500
2	Windows Server 2003 Administration Course	10000	0	4 days	10000
3	Internet access cost (already covered)	0	0	317KB	0
4	Installation and testing of patch file	0	250	2 hours	62
5	Hard Disk Configuration & Management	0	250	2 hours	62
6	Shadow Copies Configuration	0	250	1 hour	31
7	Configuring User Access to login hours	0	250	4 hours	125
8	Configuring User's Disk Space (Disk Quote management)	0	250	4 hours	125
9	Anti Virus Configuration	0	250	1 hour	31
				Total	**17936**

The server contains 1 GB of data stored on it, which includes data that can cause the loss of around 1 million US Dollars if exposed to competitors. Meanwhile, the cost of mitigating the found risks totals to 17,936 US Dollars.

This report was reviewed and approved by:

[Name]
[Date]
[Signature]

Director of Internal Audits

[Name]
[Date]
[Signature]

Manager/Supervisor

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Appendix A: Basic System Information

```
Host Name:                 SERV2003
OS Name:                   Microsoft(R) Windows(R) Server 2003,
Standard Edition
OS Version:                5.2.3790 Build 3790
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          [redacted]
Registered Organization:
Product ID:                69712-640-1444233-45750
Original Install Date:     [redacted]
System Up Time:
System Manufacturer:       Dell Computer Corporation
System Model:              PowerEdge 2500
System Type:               X86-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: x86 Family 6 Model 8 Stepping 6
GenuineIntel ~927 Mhz
                           [02]: x86 Family 6 Model 8 Stepping 6
GenuineIntel ~927 Mhz
BIOS Version:              DELL   - 1
Windows Directory:         [redacted]
System Directory:          [redacted]
Boot Device:               \Device\HarddiskVolume2
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (GMT+04:00) Abu Dhabi, Muscat
Total Physical Memory:     1,023 MB
Available Physical Memory: 655 MB
Page File: Max Size:       3,491 MB
Page File: Available:      2,880 MB
Page File: In Use:         611 MB
Page File Location(s):     D:\pagefile.sys
                           C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\SERV2003
Hotfix(s):                 23 Hotfix(s) Installed.
                           [01]: File 1
                           [02]: File 1
                           [03]: File 1
                           [04]: File 1
                           [05]: File 1
                           [06]: File 1
                           [07]: File 1
                           [08]: File 1
                           [09]: File 1
                           [10]: Q147222
                           [11]: Q828026 - Windows Media Player Hotfix
[See Q828026 for more information]
                           [12]: Q832483
                           [13]: Q828026
                           [14]: Q828026 - Update
                           [15]: KB819696 - Update
                           [16]: KB823182 - Update
                           [17]: KB823559 - Update
                           [18]: KB824105 - Update
                           [19]: KB824141 - Update
                           [20]: KB824146 - Update
```

© SANS Institute 2004, Author Retains Full Rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
                          [21]: KB825119 - Update
                          [22]: KB828035 - Update
                          [23]: KB832894 - Update
Network Card(s):          1 NIC(s) Installed.
                          [01]: Intel 8255x-based PCI Ethernet Adapter
(10/100)
                                Connection Name: Local Area Connection
                                DHCP Enabled:    No
                                IP address(es)
                                [redacted]
```

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Appendix B: Modern Language Association (MLA) – citation format

BOOKS

Format:

Author. *Title of Book.* City of Publication: Publisher, Year.

- Title from the title page, not the cover.
- Author's name written Last Name, First Name.

WEB SITE -- Professional or Personal

Format:

Creator's name (if given). *Web Page Title.* Institution or organization. Date of access <URL network address>.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.