



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 permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Auditing Systems, Applications, and the Cloud (Audit 507)"
at <http://www.giac.org/registration/gсна>



**Auditing a DELL Storage Area Network server:
An Auditor Perspective**

Patrick Boismenu

September 5th, 2003

GSNA Assignment Version 2.1

OPTION #1



ABSTRACT

This paper consists of an audit that was performed at a company that we will call GB Inc. It covers a particular server that uses the Storage Area Network technology and the accompanying risks and challenges.

At the end of this paper, you should be able to use the checklist provided to perform an audit on your own SAN and make accompanying recommendations to the proper authorities.

© SANS Institute 2003, Author retains full rights.



TABLE OF CONTENTS

ABSTRACT	2
Introduction	5
Assignment #1	5
Network Diagram	5
System to be audited	6
System Profile	6
Risk Evaluation	9
Current State of practice	11
Assignment #2	13
Storage Area Network Server Checklist	13
Checklist Item #1 – Physical Security	13
Checklist Item #2 – Server Vulnerability Testing	14
Checklist Item #3 – Virus Definitions and Software	14
Checklist Item #4 – Server Accessibility	15
Checklist Item #5 – Logging of System Events	16
Checklist Item #6 – Network Traffic	17
Checklist Item #7 – Hardware Support	18
Checklist Item #8 – Service packs and Hot Fixes	18
Checklist Item #9 – Running Services	19
Checklist Item #10 – Physical Hardware Inspection	20
Checklist Item #11 – Hardware Stability	20
Checklist Item #12 – Backup Procedures	21
Checklist Item #13 – Redundancy Verification	21
Checklist Item #14 – Power Outage Reaction	22
Checklist Item #15 – Disaster Recovery Planning Procedure	23
Checklist Item #16 – Server Password Policy	23
Checklist Item #17 – Remote Management Procedure	24
Checklist Item #18 – Centralized Consoles Configuration	25
Checklist Item #19 – System Configuration Modification	26
Checklist Item #20 – Administrator Accounts	26
Assignment #3	28
Conduct the Audit	28
Test Item #1 (Stimulus Response Test #1)	28
Results	30
Test Item #2	30
Results	31
Test Item #3 (Stimulus Response Test #2)	31
Results	33
Test Item #4 (Stimulus Response Test #3)	33



Results	35
Test Item #5	35
Results	37
Test Item #6	38
Results	38
Test Item #7 (Stimulus Response Test #4)	39
Results	40
Test Item #8	40
Results	41
Test Item #9 (Stimulus Response Test #5)	41
Results	42
Test Item #10	43
Results	44
Measure Residual Risk	45
Item #3	45
Item #4	45
Item #7	46
Is the system auditable?	46
Assignment #4	48
Executive Summary	48
Audit finding	49
Observation #1	49
Observation #2	50
Observation #3	51
Observation #4	52
Reference	53

© SANS Institute 2003. Author retains full rights.

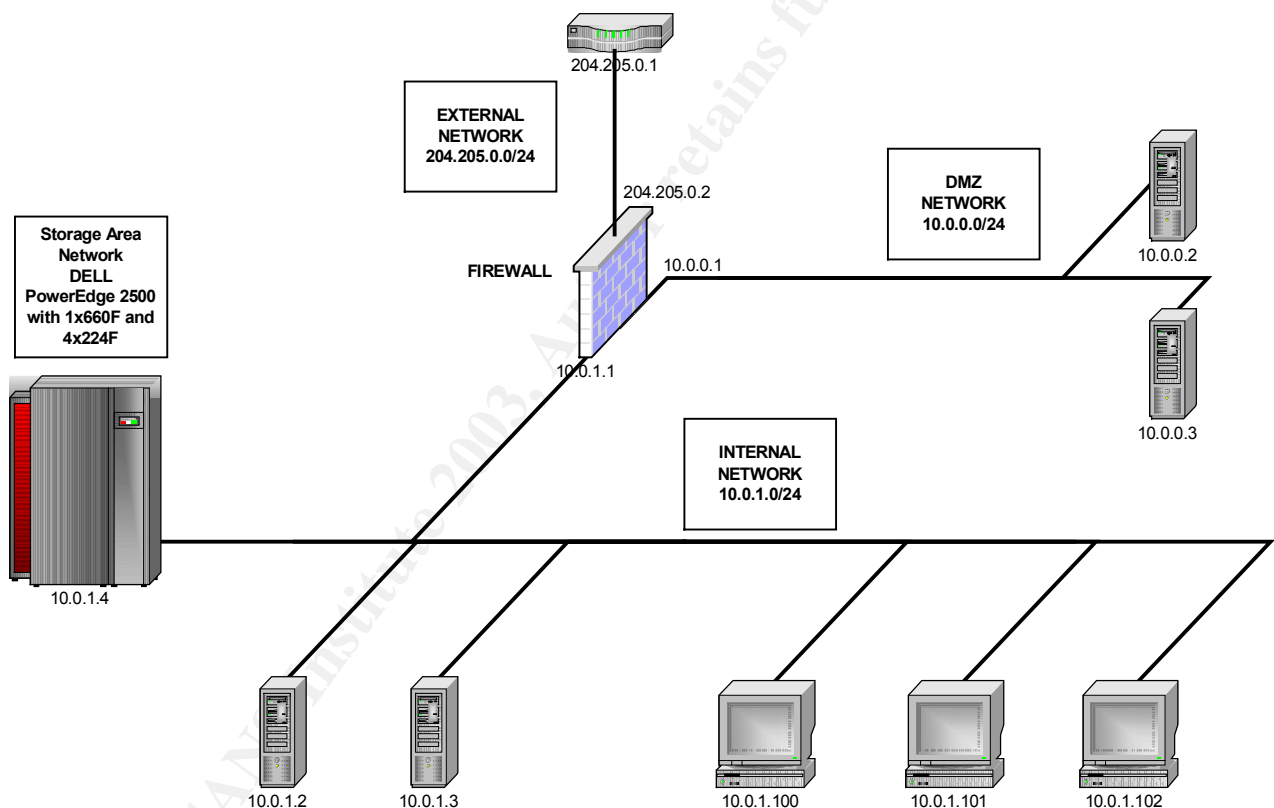


Introduction

GB Inc. is a mid-sized company that insures and secures ghost images of hard drives for redistribution in the event of a sinister. GB Inc. uses a SAN server to retain the large data that is brought to them by their customers. This data is accessible within the internal network shown below:

Assignment #1

Network Diagram



Network in question consists of a rather simple configuration. A firewall is used as a filter for the outside world and a DMZ network is also present. The SAN is located on the inside network. The scope of this audit will limit this report to the inside network and will not go beyond the internal firewall IP address. It is important to mention however that the external risk has not been defined. Until such a risk is reviewed, it should be considered a high risk and therefore taking the proper steps to insure the protection of the entire network should be implemented immediately.



System to be audited

System Profile

Intel® Pentium® III 1.4 GHz
133MHz front side bus
32KB Level 1 cache (16KB instruction cache and 16KB two-way write-back data cache)
512KB Level 2 cache
ServerWorks High End SL (HE-SL) Chipset
1GB 133MHz ECC SDRAM DIMM memory
Hard Drives: 3x18GB Fiber Channel SCSI hard drives
SCSI Controllers: Integrated Ultra-2/LVD SCSI Adaptec® AIC-7890 (primary)
Integrated Ultra/Narrow SCSI Adaptec AIC-7880 (secondary)

External Storage

- PowerVault 660F
 - 14x FiberChannel 10,000 revolutions per minute (rpm) hot-swappable Hard Drives of 73 Gig Capacity Each
 - Two hot-swappable loop resiliency circuit/SCSI enclosure services (LS)
 - Two redundant, hot-swappable power supply modules
 - Six LEDs on LS modules indicating shelf power, shelf fault, FC loop A and loop B status, and LS module fault
- 2x PowerVault 224F
 - 14x FiberChannel 10,000 revolutions per minute (rpm) hot-swappable Hard Drives of 73 Gig Capacity Each
 - Two redundant, hot-swappable power supply modules
 - Six LEDs on LS modules indicating shelf power, shelf fault, FC loop A and loop B status, and LS module fault

Backup

- Sony AIT 3 LIB-162
 - 4.16 TB Capacity (2.6:1 compression)
 - 16 slot internal carousel configuration with built-in barcode reader
 - Transfer rate of 224.6 GB per hour (2.6:1 compression) with AIT-3 drives



Communications

Onboard Intel PRO/10/100 Server Adapter
Intel PRO/100+ Server Adapter
Intel PRO/100+ Dual-Port Server Adapter
Intel PRO/100S Server Adapter (with IP SEC Encryption)
Intel PRO/1000 Gigabit Server Adapter
Alteon® ACEnic 10/100 Adapter (Cat-5 Copper Cabling)
Giganet cLAN1000 32/64-bit, 33MHz PCI-based Host Adapter®
3Com® EtherLink Server 10/100 PCI NIC (3C980C-TXM)

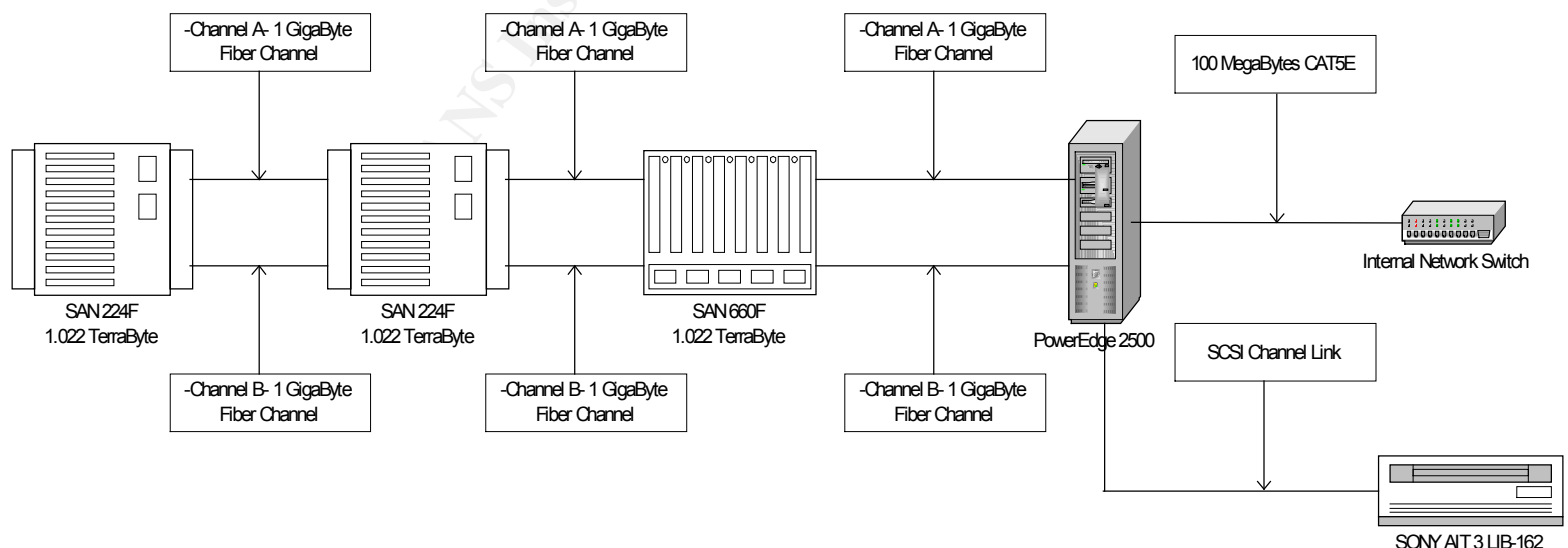
Operating system

Microsoft Windows 2000 Server

Physical Specifications

Mini-tower Chassis - 17.5" (h) x 10.5" (w) x 23.5" (d)
6U rack height
weight 55 lbs.
power - 330 Watts - 110/220 Volts

The audit consisted of a Windows 2000 Server that is configured physically as follow: (Logical Mapping)





The Dell PowerEdge 2500 server uses the following software for its configuration:

Windows 2000 server v5.00.2195 Service Pack 3

Backup Exec v8.6

Dell Open Manage Array Manager v3.3.0 (Build 515.1)

This audit covers the following area: physical security, local server security, privileges, backup, server configuration, its focus is to better evaluate the risks associated with hardware, software and procedures used within the Storage Arena Network server.

This scope does not include network configuration and ambient servers in same location of system audited.

© SANS Institute 2003, Author retains full rights.



Risk Evaluation

This system is a very important key to the organization's operations. Failure to secure this server correctly would result in elevated risks of consumer loss and eventually operational problems within the company itself. The database held by this system holds critical information and is required to have the utmost attention when it comes to security.

Here are the possible risk items and their associated consequences; items are prioritized in the probability field:

Risk Item	Probability	Consequence(s)
Outdated patches on server	High – Priority #1	Could be subject to vulnerabilities on the server.
Unnecessary Services running on server	High – Priority #2	Allows the attacker to infiltrate server through an exploitable service.
Running out of hot spares on the RAID-5	Med – Priority #3	In the event of a hard drive crash, complete data loss would be in effect if there are no hot spares available.
Attacker gains access to data server	High – Priority #4	Loss of data and troubles with active connections, data integrity would also be compromised.
Password Policy on system is poorly implemented or inexistent	High – Priority #5	Passwords can be easily guessed or brute forced by an attacker.
Insufficient logging of system events and alarms.	High – Priority #6	In the event of a system compromise, logs would not permit forensic recovery of the source of the attack.
Outdated virus protection	High – Priority #7	Integrity of data could be altered, virus infection could spread to internal network.



Risk Item	Probability	Consequence(s)
Two hard drives crash simultaneously	Low – Priority #8	Total loss of the data on the server, regardless of hot spares availability.
Eavesdropping network traffic emanating from server	High – Priority #9	Attacker could acquire confidential information and username/password.
Power outage for limited period of time	Low – Priority #10	Causes corrupted data and inaccessible resources for users.
Denial of Service (DOS) against server	Medium – Priority #11	The machine crashes and data is inaccessible.
Equipment is subject to theft or damage	Low – Priority #12	Expensive equipment and data lost would essentially halt the company until replacement.

The focus of this audit is to ascertain the level of security in which the server itself resides, the physical as well as the logical measures that were implemented to initiate its protection. The pieces of each area are key into evaluating the system as a whole and make the necessary recommendations on the findings.

Hackers and other malicious individuals may have a high level in interest in the data held by the SAN server at GB Inc. A particular attention should be posed concerning the security of this system.

An attacker for this system would be defined in the following categories:

INSIDER – INTERNAL EMPLOYEE

Someone who works for the organization and that has some type of grudge against the company or an individual within that organization.

OUTSIDER – EXTERNAL HACKER

Someone that seeks a personal profit or an elevated status within their community.

OUTSIDER – INDUSTRIAL ATTACKER

An external agency that hires individuals to perform attacks against their industrial competition.



Current State of practice.

There are a lot of organizations that define their own version of a good secure implementation of such a system, but very few go into the details of auditing the system itself. There is very little auditing information available on Storage Area Network's but most of the current state of practice has been found at the following location:

<http://www.snia.org/>
http://www.snia.org/apps/group_public/download.php/1618/Are_Storage_Networks_Secure.pdf
http://www.snia.org/apps/group_public/download.php/1626/Layered_Security_Architecture.pdf

It basically outlines the different challenges of today's technology and gives a heads up as to what to expect in terms of basic security from multiple SAN vendors.

@Stake also gives multiple presentations and documentations in regards to SAN/NAS security and best practices in effect.

http://www.storageworldconference.com/media/presentations/may6/panel2_atstake.ppt
http://www.snia.org/security_summit/tutorial_abstracts/

Of course there are many good sites that depict the necessary protection of a Windows 2000 server.

<http://www.sans.org/score/checklists/AuditingWindows2000.doc>
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/default.asp>

GSNA Certified Students and posted practicals.

<http://www.giac.org/GSNA.php>

The center for internet security is also a great site in order to grasp all necessary information for Windows 2000 practices.

<http://www.ietf.org/rfc/rfc2196.txt?number=2196>



SANS Publication Windows 2000 Security : Step by Step TRACK 5 depicts this method.

<http://www.sans.org/newengland03/track5.php>

Finally, using Internet search engines can easily identify many more links.

<http://www.google.com>

© SANS Institute 2003, Author retains full rights.



Assignment #2

Storage Area Network Server Checklist

Terms:

- This checklist has been designed to audit GB Inc.'s SAN server.
- Audit involves multiple layers of verification including physical and logical tests. Written permission was previously obtained by the President of this company and an outline of the tests to be performed was presented to him prior to his engagement.
- Auditors are using two laptops to perform the security auditing of the system. One will be used to perform the tests, the other will be used as a logging interface where all network data will be captured and used later as references.
- Finally, the auditor will perform certain function of this audit with the assistance of an authorized system administrator who has root privileges. This administrator will be responsible of typing all the commands and output the result to a separate logging file.

Checklist Item #1 – Physical Security

Reference	Information Technology Support Center http://www.itsc.state.md.us/info/InternetSecurity/BestPractices/PhysSecurity.htm
Control Objective	Server must be in a secure location.
Risk Probability Consequence	Theft of system or damage to system. Complete loss of data. An extensive financial impact on the business. Low Expensive equipment and data loss could cause disastrous problems to GB Inc.'s operational structure.
Compliance	Access to server is limited to authorized personnel.
Testing	<ul style="list-style-type: none">• Review list of personnel that has access to the room where server is located and compare it with the list of employees that is authorized to access this location.• Visit the location and observe day-to-day activities to see if people could gain access to room without proper authorization.• Review the magnetic card logs to insure that no one has attempted to gain access to the room without authorization.



	<ul style="list-style-type: none">• Within the server room, verify if server rack is properly secured and if the keys are properly stored away.
Objective/Subjective	Subjective – Mainly observations to get a feeling of how things work within the organization. While some tests may be objective, the entire process isn't.

Checklist Item #2 – Server Vulnerability Testing

Reference	Microsoft Best Practices http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/bpsp.asp
Control Objective	Server must be free of known vulnerabilities
Risk	Attacker gains access to server through an exploitable vulnerability. Data may be deleted or Stolen causing an important financial loss on the business.
Probability	High
Consequence	Attacker has control of the server and can alter/delete the data.
Compliance	Server is tested and patched accordingly.
Testing	<ul style="list-style-type: none">• Download a copy of a vulnerability scanner from a known reliable site. (NESSUS, ISS) http://www.nessus.org/download.html• Install the scanner on your system.• Connect to the network where the system to be audited is located.• Execute the vulnerability scanner against the system making sure logging is enabled for the scanning.• Review the report and analyze the results.
Objective/Subjective	Objective – The test results will show if a vulnerability has been identified or not. All that is left afterwards is to evaluate the level of risk of the identified vulnerability and act accordingly.

Checklist Item #3 – Virus Definitions and Software

Reference	Microsoft Best Practices https://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/virus/bp03026.asp
Control Objective	Protect server against virus infections.
Risk	Server is infected with a virus. Problems may vary, there is definitely a financial impact and a limitation in service



	availability.
Probability	High
Consequence	Data can be altered/deleted, it can create vulnerabilities or problems of any sorts.
Compliance	The server is running the current virus definitions from a license purchased software.
Testing	<ul style="list-style-type: none">• Verify that a proper virus program is installed. You can accomplish this by logging onto the system with the help of an administrator and asking him to display all the relevant information regarding the anti-virus software. (Name, version, signature update)• Verify the virus definitions last update and compare it with the current ones on the software's website making sure they are up to date.• Verify the virus definitions updating process and make sure it is compliant with the current network configuration insuring a proper level of protection for the server.
Objective/Subjective	Objective – This process is objective as you verify directly if the right software and definitions are installed. The only subjective twist to it would be with the updating process and the frequency of those updates.

Checklist Item #4 – Server Accessibility

Reference	Denial of Service (DOS) Protection Paper http://www.hp.com/rnd/support/manuals/pdf/release_06628_07110/Bk2_Apixon_DoS_Protection.pdf
Control Objective	To prevent a DOS attack to be effective against the server.
Risk	An attacker launches a denial of service attack against the server from an outside source. (External Network) Service offered to the public will be unavailable during that period causing monetary loss and the image of the business would be affected.
Probability	Med
Consequence	Users cannot access the data on the server.
Compliance	Proper filters should be integrated in the firewall to prevent this from occurring. No connections from server should leak to the internet and vice-versa. Preventing attackers from reaching the server internally.



	To ultimately protect against TCP Syn Attacks and Smurf Attacks.
Testing	<ul style="list-style-type: none">• Verify that the firewall does not allow outside connections to contact internal servers. To perform this, you must ask an administrator to log onto the firewall and display the firewall rules. Outside and Inside.• Verify the contents of the rules that were printed for your review.• Verify that the firewall prevents the server from connecting to an outside source. This can be viewed onto the inside firewall rules.• Verify the logs of the firewall with the help of an administrator to insure there is no abnormal traffic from or to the SAN server.
Objective/Subjective	Objective – This process is objective based on the fact that the verification will show if the firewall allows connections or not.

Checklist Item #5 – Logging of System Events

Reference	University of Wisconsin-Madison http://www.doit.wisc.edu/security/resources/bestpract/logging.asp
Control Objective	To insure the viability of an eventual forensic analysis of the system and to also identify alarms or security issues on the system.
Risk	System behaves erratically and no means of troubleshooting is available. Administrators would waste a great deal of time tracing back the problems.
Probability	High
Consequence	Problems to perform a proper forensic analysis of the system, inability to identify alarms or errors on a system.
Compliance	Have the correct logging level enabled in order to identify problems and solve them.
Testing	<ul style="list-style-type: none">• Verify the current logging level on the system as well as external logging.• Access the Event Viewer on the system with the help of an administrator and verify the properties System, Security and Application events. Take notes of the settings.



	<ul style="list-style-type: none">• Inquire if there are any other types of logging on the system and verify those as well.• Insure that the logs are saved in a safe location.• Inquire and verify external logging settings if it applies, Intrusion Detection Systems like SNORT.• Assess the required log size and compare it to the actual size defined.• Identify the wrapping options
Objective/Subjective	Subjective – You will verify if the current logging level is proper or not but you will also decide what is acceptable or not in terms of the log file size, location and other options. That is why I qualified it as subjective.

Checklist Item #6 – Network Traffic

Reference	Network Traffic Sniffing http://www.network-monitor.com/products/networkmonitor/docs42/network-monitor-toc.asp
Control Objective	To insure that no confidential data or abnormal traffic is leaking from the server.
Risk	Username and password are leaked from the server and confidential data is also available to capture off local network. Could cause an eventual intrusion and eventual financial losses.
Probability	Med
Consequence	Attacker could eavesdrop the network and gather multiple usernames and passwords as well as confidential data off the server and eventually use this information to further compromise the server or other activities.
Compliance	No network traffic is available for capture and no information is leaked off the server.
Testing	<ul style="list-style-type: none">• Hook up laptop #1 in a Hub between the local network switch and the server.• Run TCPDUMP on laptop #1.• Capture and analyze the results• Insure that no traffic containing vital information is leaking out of the server.• Insure that no abnormal traffic is directed at the server.• Hook up laptop #2 in the local network switch• Run TCPDUMP on laptop #2.• Capture and analyze the results.



	<ul style="list-style-type: none">• Verify the general traffic on the network and compare it with the results obtained with Laptop #1 to identify any abnormality.
Objective/Subjective	Objective – The logs will show clearly if data is leaking from the server and if that data is confidential or not.

Checklist Item #7 – Hardware Support

Reference	Personal Experience
Control Objective	To insure enough hot spares are available on the server.
Risk	RAID-5 configuration runs out of hot spares and a critical failure occurs. Causing big financial losses for rebuilding the system.
Probability	Low
Consequence	Total loss of data on the server.
Compliance	Server has sufficient hot spares for the RAID-5 Configuration and Hot spares are verified on a regular basis.
Testing	<ul style="list-style-type: none">• Verify within the DELL OPEN MANAGE ARRAY MANAGER how many hot spares are available. Select the Virtual Array and verify the number of Hot Spares assigned.• Compare the results with the total number of chassis included within the system.• Verify that there should be at least one Hard Disk in hot spare mode per chassis. If there is only one chassis. There has to be at least two hot spares to prevent data loss.
Objective/Subjective	Objective – Process is to verify if there are sufficient hot spares in case of a critical hard drive failure. Either, there are enough or not.

Checklist Item #8 – Service packs and Hot Fixes

Reference	Microsoft Technical Center http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/MBSAhome.asp
Control Objective	Insure that server is properly patched with current hotfixes.
Risk	An attacker could use any exploit that was not properly patched. Causing intrusion and eventual monetary losses.



Probability	High
Consequence	Attacker can gain access to system and alter/delete important data.
Compliance	All the current patches have been properly applied to the system.
Testing	<ul style="list-style-type: none">• Download latest copy of Baseline Security Analyzer from Microsoft's website.• Run the Baseline Security tool on the server with the assistance of an administrator.• Review the results and archive them on a floppy disk.
Objective/Subjective	Objective – Compare actual list of patches with the list of patches applied to server.

Checklist Item #9 – Running Services

Reference	University Information Technology Paper http://www.itso.iu.edu/howto/iis/
Control Objective	Insure that server isn't running services that are not required.
Risk	An attacker exploits a running service that has an exploit for it. Service was not required to be running.
Probability	High
Consequence	Attacker gains access to the system and can alter/delete data.
Compliance	Server is running only necessary services.
Testing	<ul style="list-style-type: none">• Download nmap from a known reliable site like http://www.insecure.org/nmap/• Use this copy of nmap and perform a port scan against the server.• Use command <code>nmap -sT -O -p 1-65535 -v</code>• Use command <code>nmap -sU -O -p 1-65535 -v</code>• Examine results and save a copy
Objective/Subjective	Subjective – This process includes an objective and subjective aspect to it, in the sense that it is objective to highlight certain services running against the normal security policy established. But it is subjective to evaluate the services identified and identifying them as unnecessary or not.



Checklist Item #10 – Physical Hardware Inspection

Reference	DELL Service Support http://www.dell.com/us/en/esg/topics/power_ps1q02-mclaugh.htm
Control Objective	Insure the hardware equipment is functioning properly with its embedded LED test lights.
Risk	A hardware device could fail. Causing replacement cost, and if not properly protected financial losses to fix situation that arose.
Probability	Low
Consequence	Data loss or server crash could occur.
Compliance	Material shows normal lighting for perfect condition.
Testing	<ul style="list-style-type: none">Physical inspection of the hardware by looking at lights and insuring cables are properly secured. Sometimes, amber lights may appear. Those lights are a premonition that something is wrong or may go wrong. It is important to visually explore this on a regular basis.Taking pictures to document testing.
Objective/Subjective	Objective – This process will show if hardware is functioning properly or not. A amber light does not necessarily means that the server is not functioning, it simply indicates a problem that need to be explored and resolved.

Checklist Item #11 – Hardware Stability

Reference	DELL Service Support http://www.dell.com/us/en/esg/topics/power_ps1q02-kammer.htm
Control Objective	Hard drives must be stable in order to insure data integrity.
Risk	Hard drive failure due to improper log screening. Financial losses could be substantial.
Probability	Med
Consequence	Complete data loss if no hot spares available or if two hard drives fail simultaneously.
Compliance	Insuring there are no errors in the Navisphere Array Manager Hard drive error control window.
Testing	<ul style="list-style-type: none">Open the Navisphere Array ManagerGo to individual hard drives and very that no errors



	are occurring in the log window. Data or transfer errors are uncommon but may occur from time to time. In these cases, the hard drive should be replaced without further delay. <ul style="list-style-type: none">• Note results and keep a copy for reference.
Objective/Subjective	Objective – This test will show if errors are occurring or not with the hard drives.

Checklist Item #12 – Backup Procedures

Reference	DELL Service Support http://www.dell.com/us/en/biz/topics/products_di1q03_pedge_di1q03-005.htm
Control Objective	Insure a proper backup procedure to prevent data loss and enable recovery operations.
Risk	Data loss occurs and no backup is available. Potentially a great deal of customers would leave the business and a major financial loss.
Probability	Med
Consequence	Data lost will be unrecoverable.
Compliance	Proper archiving should be in place and should adhere to company security policy. Successful recovery of test data.
Testing	<ul style="list-style-type: none">• Obtain a copy of the procedure if there are any.• Review the procedure with an administrator to insure your full understanding of it.• Load most recent backup tape in drive and browse content o verify their integrity.• Restore a test item using the backup software, with the help of the administrator.• Insure test was successful• Verify entire procedure and compare with company security policy to make sure they are both compliant with best practices.
Objective/Subjective	Subjective – File restore works or not and the review of guidelines and policy is subjective.

Checklist Item #13 – Redundancy Verification

Reference	DELL Service Support (SANS Technology) http://www.dell.com/us/en/esg/topics/power_ps4q00-berning.htm
Control Objective	Insure redundancy is active and functional.
Risk	No redundancy present and an hardware failure occurs.



	(Fan, power supply, cables) Could cause a big financial loss depending on the failed hardware.
Probability	Med
Consequence	Hardware failure with no redundancy leads to immediate data loss and communications dropout.
Compliance	Redundancy is correctly configured and fully functional.
Testing	<ul style="list-style-type: none"> • Access the Qlogic Card Configuration on the SAN Server with the help of an administrator. • Verify redundancy settings by accessing the Device and LUN configuration. • Ensure one card is set at Primary Path and second one is set as Failover path. • Verify they are both active and functional (you should see them in green) If they are not functional a red X would be over the icon that describes the card. • Take notes of your findings.
Objective/Subjective	Objective – Settings show whether or not redundancy is active.

Checklist Item #14 – Power Outage Reaction

Reference	Backup Professional http://www.emmanuel.com.sg/pages/powerfailure.htm
Control Objective	Ensure graceful shutdown of Storage Area Network upon power outage.
Risk	Data loss due to interrupted power. Financial cost involved to rebuild lost data.
Probability	Med
Consequence	Data is lost and communications are halted.
Compliance	Power Outage is detected early and graceful shutdown is initiated along with employee broadcast of service going down.
Testing	<ul style="list-style-type: none"> • Verify UPS installed and power level • Verify if Power Control software is installed • Verify its configuration against life expectancy of UPS during power outage. • Verify disaster recovery and planning policy. • Analyze the results
Objective/Subjective	Subjective – Settings will be configured as per the local company policy. Expectancy of uptime after a power outage should be enough for graceful shutdown with broadcasting.



Checklist Item #15 – Disaster Recovery Planning Procedure

Reference	Storage Info Website http://www.storagesearch.com/bakboneart.html
Control Objective	Have proper procedures in place in the case of a fire.
Risk	Fire burns through building and server room where system is located. Definite financial loss that would delay business for a long period of time.
Probability	Low
Consequence	Complete data loss.
Compliance	Backup plan should be in place and proper device should be installed (Halon Suppression Medium for Fire Sprinklers, ie: Inergen, CEA-410, FM-200)
Testing	<ul style="list-style-type: none">• Verify disaster recovery procedure• Verify external backup inventory location and procedure• Inspect and inquire about fire sprinkler device and chemical products used.• Verify if such procedure was already tested in the past and analyze the outcome of the test.
Objective/Subjective	Subjective – Fire sprinkler testing is objective as they are compliant or not with proper security procedures. Disaster recovery procedure and external backup procedures are subjective as they will vary depending on business cases.

Checklist Item #16 – Server Password Policy

Reference	GB Inc. Password Policy
Control Objective	Insure that passwords meet the company standards and are not easily compromised.
Risk	An attacker brute forces passwords on the server in a relatively short period of time. Confidentiality and Integrity of the data could no longer be insured.
Probability	High
Consequence	Attacker takes full control of system and uses the accounts maliciously.
Compliance	Passwords meet the company standards and are strong enough to sustain a reasonably long brute force attack.
Testing	<ul style="list-style-type: none">• Verify company password policy from textbook.• Try adding a user on the server with an easy



	<p>password to attack. (pass: internet)</p> <ul style="list-style-type: none">• Download L0phtcrack v4 from: http://www.atstake.com/research/lc/download.html• Install L0phtcrack v4 on laptop #1• Request an administrator to be present for this test as an administrator account is required to run a remote verification of passwords.• Insure your laptop is in the same network as the server to be audited. (This can be accomplished by simply plugging your laptop network cable into the local switch)• Direct the L0phtcrack application to the proper server when conducting your audit.• Use L0phtcrack to brute force passwords without showing resulted cracked password.• Save results in a file
Objective/Subjective	Objective – Server password policy either meets or not the company password policy. Accounts and passwords are also objective since they adhere or not to policy.

Checklist Item #17 – Remote Management Procedure

Reference	Personal Experience
Control Objective	Remote management is secure.
Risk	Remote management is exploitable and an attacker takes advantage of it. Data loss, integrity or confidentiality of the data is at risk in this situation.
Probability	Med
Consequence	Attacker has full control of server.
Compliance	Remote management is secure and is configured as per the company policy.
Testing	<ul style="list-style-type: none">• Verify if remote management is installed. This is accomplished by performing the following steps:<ul style="list-style-type: none">○ Verify the cables at the back of the server. Remote management is often performed via a serial or parallel link. Take note of your findings.○ Verify the ports opened on the server by using the command “netstat -na” and verify the origin of the ports that are reported by the command. (Log results in a file by adding “>> netstat_results.txt” to your command.



	<ul style="list-style-type: none"> ○ Inquire to an administrator if any remote management program is installed. ○ Manually verify amongst the installed applications on the server for traces of remote management program. (They will often load at startup on the machine, a good place to look is in the registry under the • Verify remote management program's settings. (If one is present) • Analyze the company policy on server remote management • Log the results of analysis
Objective/Subjective	Subjective – Depending on Remote management software and the company policy, we will be able to ascertain the situation on an individual basis and select the best avenue for GB Inc.

Checklist Item #18 – Centralized Consoles Configuration

Reference	Personal Experience
Control Objective	Insuring the KVM is inaccessible from an outside source.
Risk	Attacker gains KVM access and can attack server remotely. Causing severe financial loss if intruder is able to control server remotely this way.
Probability	Med
Consequence	Attacker can start attacking server and brute forcing accounts from a remote location.
Compliance	KVM is not IP Based or has Strong Password implementation.
Testing	<ul style="list-style-type: none"> • Physically identify the KVM Switch and researching the specifications of the hardware. • Verify if it has good password implementation according to Company Password Policy standard. (This method will depend on the hardware used by the company, most of them have simplistic menu system that can be used by anyone) • Log results
Objective/Subjective	Objective – It is or not IP Based and it does or not have a password protection on it.



Checklist Item #19 – System Configuration Modification

Reference	Personal Experience
Control Objective	Making sure changes brought to the server are according to local company guidelines.
Risk	Making modifications to server configuration without proper notification or approval. Could cause internal problems and eventual higher risk to the data stored within the server.
Probability	High
Consequence	Poorly tested changes may lead to erratic system behavior and may even affect other systems around it.
Compliance	All modifications are pre-approved and tested before any kind of implementation is performed.
Testing	<ul style="list-style-type: none">• Verify local company policy for modifications.• Verify recent system changes and inquire about pre-acceptance and testing of those changes. This is performed by questioning the administrators who have access to the system.• Verify the existence of an activity log and insured it was filed and correctly logged.
Objective/Subjective	Objective – Insuring that the areas of the policies were correctly implemented and followed is objective.

Checklist Item #20 – Administrator Accounts

Reference	Windows Scripting Solutions http://www.winscriptingsolutions.com/Articles/Index.cfm?ArticleID=25721
Control Objective	Insure every administrator has his own account.
Risk	Problems relating to repudiation of an incident. Risk is such that no management position will be able to identify who performed the wrongdoing and therefore no sanction could be issued. The problems created could vary from



	something benign to complete data loss.
Probability	Med
Consequence	Hard to account for the source of the problem when something occurs.
Compliance	Every administrator has his own account and password.
Testing	<ul style="list-style-type: none">• Ask an administrator to display list of users that are part of the administrative group and compare list with administrator's list indicated in the Server Security Account Policy. To accomplish this, you must go in the administrator group on the server and display the users that are part of that group. It will list all users who have been granted administrator access. If only the user administrator is displayed, then the only user able to perform administrative task is the administrator.• Log the results
Objective/Subjective	Objective – Administrators have an individual account or they share one or multiple accounts.

© SANS Institute 2003, Author retains full rights.



Assignment #3

Conduct the Audit

Test Item #1 (Stimulus Response Test #1)

Checklist Item #2	Server Vulnerability Testing
Control Objective	Server must be free of known vulnerabilities
Risk	Attacker gains access to server through an exploitable vulnerability.
Probability	High
Compliance	Server is tested and patched accordingly.
Testing	<ul style="list-style-type: none">• Download a copy of a vulnerability scanner from a known reliable site. (NESSUS, ISS) http://www.nessus.org/download.html• Install the scanner on your system.• Connect to the network where the system to be audited is located.• Execute the vulnerability scanner against the system making sure logging is enabled for the scanning.• Review the report and analyze the results.
Actions	<ul style="list-style-type: none">• Installed a laptop on the local area network switch• NESSUS was pre-installed on laptop. With the following configuration:<ul style="list-style-type: none">◦ NESSUS v1.2.7◦ All Plug-Ins except DdoS.• Executed NESSUS on the audited system (For a full description on how to perform this exactly, please refer to this website http://www.nessus.org/demo/index.html) <p>**Please See Image of report on next page**</p>

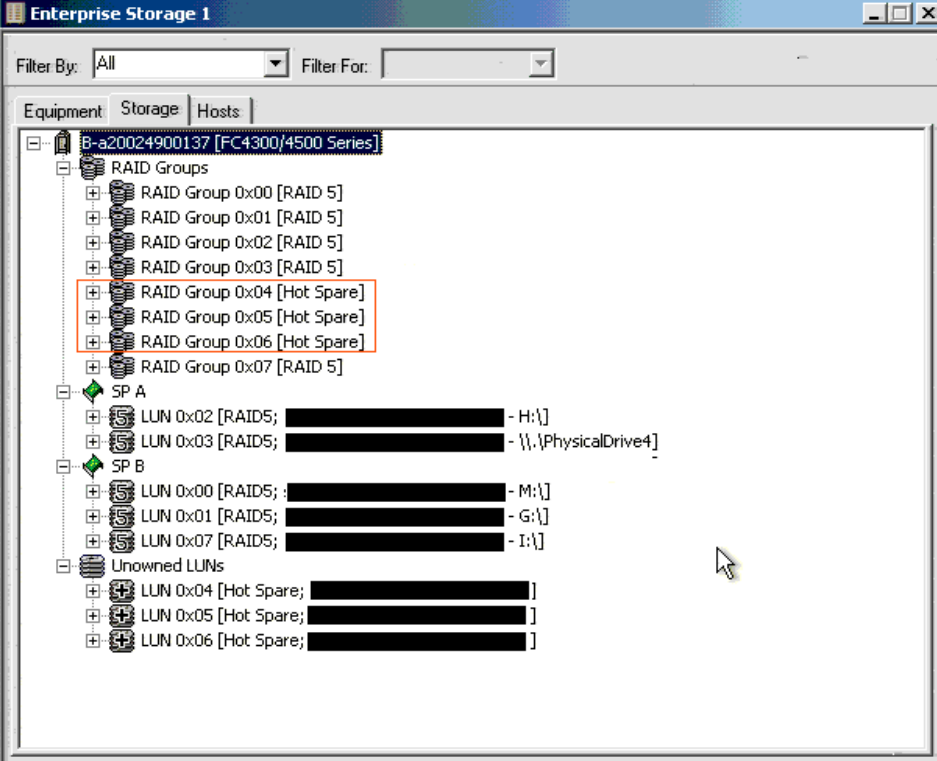


	<ul style="list-style-type: none">Image was truncated due to the fact that all 23 other warnings were of no consequence for this test to fail or succeed. It is clear that the full report will be presented to upper management when given. Exported results to an html file
Results	Fail

Test Item #2


Checklist Item #7	Hardware Support
Control Objective	To insure enough hot spares are available on the server.
Risk	RAID-5 configuration runs out of hot spares and a critical failure occurs.
Probability	Low
Compliance	Server has sufficient hot spares for the RAID-5 Configuration and Hot spares are verified on a regular basis.
Testing	<ul style="list-style-type: none">Verify within the DELL OPEN MANAGE ARRAY MANAGER how many hot spares are available. Select the Virtual Array and verify the number of Hot Spares assigned.Compare the results with the total number of chassis included within the system.Verify that there should be at least one Hard Disk in hot spare mode per chassis. If there is only one chassis. There has to be at least two hot spares to prevent data loss.
Actions	<ul style="list-style-type: none">Locally accessed the server with administrator at console.Ran DELL OPEN MANAGE ARRAY MANAGER and look if hot spares were configured for the system. <p>**Please see image on next page**</p>



	 <ul style="list-style-type: none"> • Hot Spares are present at a ratio of one per chassis • Its configured as per policy guidelines
Results	Pass

Test Item #3 (Stimulus Response Test #2)

Checklist Item #7	Hardware Support
Control Objective	To insure enough hot spares are available on the server.
Risk	RAID-5 configuration runs out of hot spares and a critical failure occurs. Causing big financial losses for rebuilding the system.
Probability	Low
Compliance	Server has sufficient hot spares for the RAID-5 Configuration and Hot spares are verified on a regular basis.
Testing	<ul style="list-style-type: none"> • Verify within the DELL OPEN MANAGE ARRAY MANAGER how many hot spares are available. Select the Virtual Array and verify the number of Hot Spares assigned. • Compare the results with the total number of chassis included within the system. • Verify that there should be at least one Hard Disk in hot spare mode per chassis. If there is only one chassis. There

	<p>has to be at least two hot spares to prevent data loss.</p> <ul style="list-style-type: none"> • Verify that this configuration works by pulling out a hard drive and verifying the system's reaction. Pulling out the corresponding logs for analysis.
Actions	<p>Having Hot Spares configured in a system is insufficient in itself, a test need to be conducted to confirm that the current configuration works correctly. It is important to note that this test should not be conducted on a production system; it should rather be performed on an empty strip where no vital data is located. Therefore, a complete data loss would have no effect on the company itself.</p> <ul style="list-style-type: none"> • Identify the correct strip to be tested. • Select a hard drive within that strip that is not one of the hot spares and pull it out.  <ul style="list-style-type: none"> • Once that is performed, insure the green light turned to amber (or red) and go look for the logs on the server with the help of the administrator. • These logs were taken from the DELL ARRAY MANAGER and can be exported to a text file. Here is the relevant log in this event, please note that this log is from newest event to oldest, so one must read it backwards. <p>Information 8/8/2003 2:26:00 PM Mylex 770 ctl: 0-0 Virtual Drive: 1 - Logical drive has been placed online. Information 8/8/2003 2:26:00 PM Mylex 700 ctl: 0-0 chn: 0, tgt: 49 (enclosure 4, slot 1) - A physical disk has been placed online.</p>



	<p>Information 8/8/2003 2:26:00 PM Mylex 706 ctl: 0-0 chn: 0, tgt: 49 (enclosure 4, slot 1) - Rebuild is over.</p> <p>Information 8/8/2003 2:07:36 PM Mylex 859 ctl: 0-0 - Controller entered normal cache mode.</p> <p>Warning 8/8/2003 2:07:25 PM Mylex 893 ctl: 0-0 - New configuration received.</p> <p>Information 8/8/2003 2:06:28 PM Mylex 712 ctl: 0-0 chn: 0, tgt: 49 (enclosure 4, slot 1) - A new physical disk has been found.</p> <p>Warning 8/8/2003 2:06:28 PM Mylex 858 ctl: 0-0 : param: 0x0000 - Controller entered conservative cache mode.</p> <p>Warning 8/8/2003 2:06:28 PM Mylex 750 ctl: 0-0 chn: 0, tgt: 49 (enclosure 4, slot 1) - Physical disk status changed to hot spare.</p> <p>Information 8/8/2003 2:05:16 PM Mylex 713 ctl: 0-1 chn: 0, tgt: 51 (enclosure 4, slot 1) - A physical disk has been removed.</p> <p>Information 8/8/2003 2:04:34 PM Mylex 713 ctl: 0-0 chn: 0, tgt: 51 (enclosure 4, slot 1) - A physical disk has been removed.</p> <p>Warning 8/8/2003 2:04:34 PM Mylex 891 ctl: 0-1 chn: 0, tgt: 51 (enclosure 4, slot 1) Key:02 ASC:04 ASCQ:02 - Request Sense</p> <p>Warning 8/8/2003 2:04:34 PM Mylex 891 ctl: 0-1 chn: 0, tgt: 51 (enclosure 4, slot 1) Key:02 ASC:04 ASCQ:02 - Request Sense</p> <ul style="list-style-type: none">• Hot spare picked up perfectly and rebuild was completed flawlessly. Test has passed.
Results	Pass

Test Item #4 (Stimulus Response Test #3)

Checklist Item #9	Running Services
Control Objective	Insure that server isn't running services that are not required.
Risk	An attacker exploits a running service that has an exploit for it. Service was not required to be running.
Probability	High
Compliance	Server is running only necessary services.
Testing	<ul style="list-style-type: none">• Download nmap from a known reliable site like




	<p>http://www.insecure.org/nmap/</p> <ul style="list-style-type: none">• Install your laptop on the local network switch.• Use this copy of nmap and perform a port scan against the server.• Use command <code>nmap -sT -O -p 1-65535 -v</code>• Use command <code>nmap -sU -O -p 1-65535 -v</code>• Examine results and save a copy																		
Actions	<ul style="list-style-type: none">• Installed a laptop in the local network switch• Launched nmap with the following command: <code>nmap -sT -O -p 1-65535 -v</code> <p>Starting nmap 3.30 (http://www.insecure.org/nmap/) at 2003-08-19 14:17 EDT Host xxx.xxxxxxxx.xxx (10.0.1.4) appears to be up ... good. Initiating Connect() Scan against xxx.xxxxxxxx.xxx (10.0.1.4) at 14:17 Adding open port 111/tcp Adding open port 135/tcp Adding open port 5800/tcp Adding open port 139/tcp Adding open port 5900/tcp The Connect() Scan took 4 seconds to scan 65535 ports. For OSScan assuming that port 111 is open and port 1 is closed and neither are firewalled Interesting ports on xxx.xxxxxxxx.xxx (10.0.1.4): (The 65523 ports scanned but not shown below are in state: closed)</p> <table><tr><th>Port</th><th>State</th><th>Service</th></tr><tr><td>111/tcp</td><td>open</td><td>sunrpc</td></tr><tr><td>135/tcp</td><td>open</td><td>loc-srv</td></tr><tr><td>139/tcp</td><td>open</td><td>netbios-ssn</td></tr><tr><td>5800/tcp</td><td>open</td><td>vnc-http</td></tr><tr><td>5900/tcp</td><td>open</td><td>vnc</td></tr></table> <p>Device type: general purpose Running: Microsoft Windows 95/98/ME NT/2K/XP OS details: Microsoft Windows Millennium Edition (Me), Win 2000 professional or Advanced Server, or WinXP TCP Sequence Prediction: Class=random positive increments Difficulty=7701 (Worthy challenge) IPID Sequence Generation: Incremental Nmap run completed -- 1 IP address (1 host up) scanned in 5.839 seconds</p> <ul style="list-style-type: none">• Launched nmap with the following command: <code>nmap -sU -O -p 1-65535 -v</code>	Port	State	Service	111/tcp	open	sunrpc	135/tcp	open	loc-srv	139/tcp	open	netbios-ssn	5800/tcp	open	vnc-http	5900/tcp	open	vnc
Port	State	Service																	
111/tcp	open	sunrpc																	
135/tcp	open	loc-srv																	
139/tcp	open	netbios-ssn																	
5800/tcp	open	vnc-http																	
5900/tcp	open	vnc																	



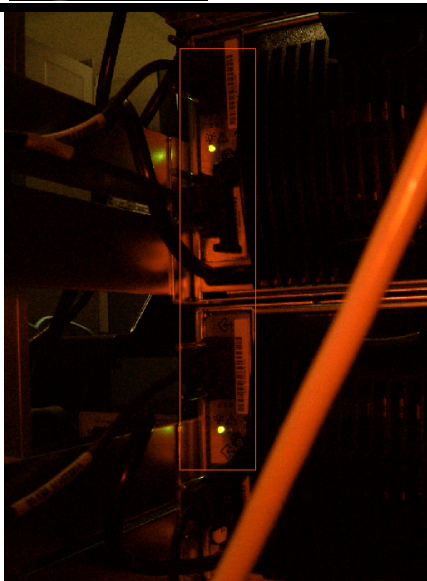
	<p>Starting nmap 3.30 (http://www.insecure.org/nmap/) at 2003-08-19 14:17 EDT</p> <p>Host xxx.xxxxxxxx.xxx (10.0.1.4) appears to be up ... good.</p> <p>Initiating UDP Scan against xxx.xxxxxxxx.xxx (10.0.1.4) at 14:17</p> <p>The UDP Scan took 12 seconds to scan 65535 ports.</p> <p>Adding open port 137/udp</p> <p>Adding open port 135/udp</p> <p>Adding open port 500/udp</p> <p>Adding open port 111/udp</p> <p>Adding open port 138/udp</p> <p>Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port</p> <p>Interesting ports on xxx.xxxxxxxx.xxx (10.0.1.4):</p> <p>(The 65524 ports scanned but not shown below are in state: closed)</p> <table><tr><th>Port</th><th>State</th><th>Service</th></tr><tr><td>111/udp</td><td>open</td><td>sunrpc</td></tr><tr><td>135/udp</td><td>open</td><td>loc-srv</td></tr><tr><td>137/udp</td><td>open</td><td>netbios-ns</td></tr><tr><td>138/udp</td><td>open</td><td>netbios-dgm</td></tr><tr><td>500/udp</td><td>open</td><td>isakmp</td></tr></table> <p>Too many fingerprints match this host to give specific OS details</p> <p>TCP/IP fingerprint:</p> <p>(None)</p> <p>Nmap run completed -- 1 IP address (1 host up) scanned in 16.472 seconds</p> <ul style="list-style-type: none">Results were logged in two separate text files names scantcp.txt for first command and scanudp.txt for second command.	Port	State	Service	111/udp	open	sunrpc	135/udp	open	loc-srv	137/udp	open	netbios-ns	138/udp	open	netbios-dgm	500/udp	open	isakmp
Port	State	Service																	
111/udp	open	sunrpc																	
135/udp	open	loc-srv																	
137/udp	open	netbios-ns																	
138/udp	open	netbios-dgm																	
500/udp	open	isakmp																	
Results	Fail																		

Test Item #5

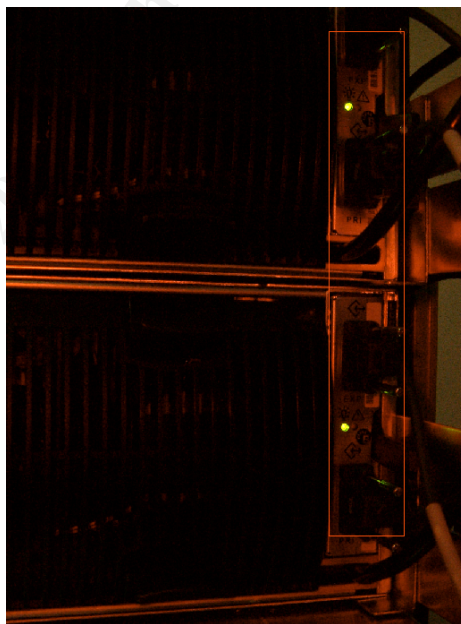
Checklist Item #10	Physical Hardware Inspection
Control Objective	Insure the hardware equipment is functioning properly with its embedded LED test lights.
Risk	A hardware device could fail.
Probability	Low

Compliance	Material shows normal lighting for perfect condition.
Testing	<ul style="list-style-type: none"> Physical inspection of the hardware by looking at lights and insuring cables are properly secured. Sometimes, amber lights may appear. Those lights are a premonition that something is wrong or may go wrong. It is important to visually explore this on a regular basis. Taking pictures to document testing.
Actions	<ul style="list-style-type: none"> Physically inspected the hardware and took several pictures that show the LEDs status on the SAN server.  <ul style="list-style-type: none"> Those LEDs are for the Hard drives BAYs in front of the chassis.

© SANS



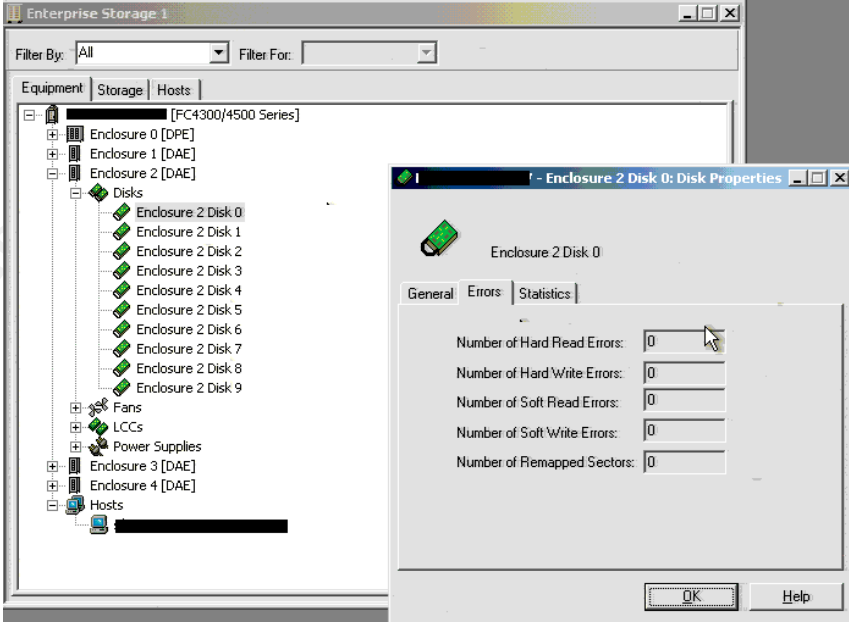
- Those LEDs are for cables connections on the left side of the system.



- Those LEDs are for cables connections on the right side of the system.
- Documented the test

Results	Pass
----------------	------

Test Item #6

Checklist Item #11	Hardware Stability
Control Objective	Hard drives must be stable in order to insure data integrity.
Risk	Hard drive failure due to improper log screening.
Probability	Med
Compliance	Insuring there are no errors in the Navisphere Array Manager Hard drive error control window.
Testing	<ul style="list-style-type: none"> • Open the Navisphere Array Manager • Go to individual hard drives and very that no errors are occurring in the log window. Data or transfer errors are uncommon but may occur from time to time. In these cases, the hard drive should be replaced without further delay. • Note results and keep a copy for reference.
Actions	<ul style="list-style-type: none"> • Went with administrator on the system. • Entered the Navisphere Array Manager • Selected all Hard drives individually from all chassis • Took a Screen capture of error logging for every hard drive (Here is a sample of an image, they were all similar)  <ul style="list-style-type: none"> • Saved the results
Results	Pass

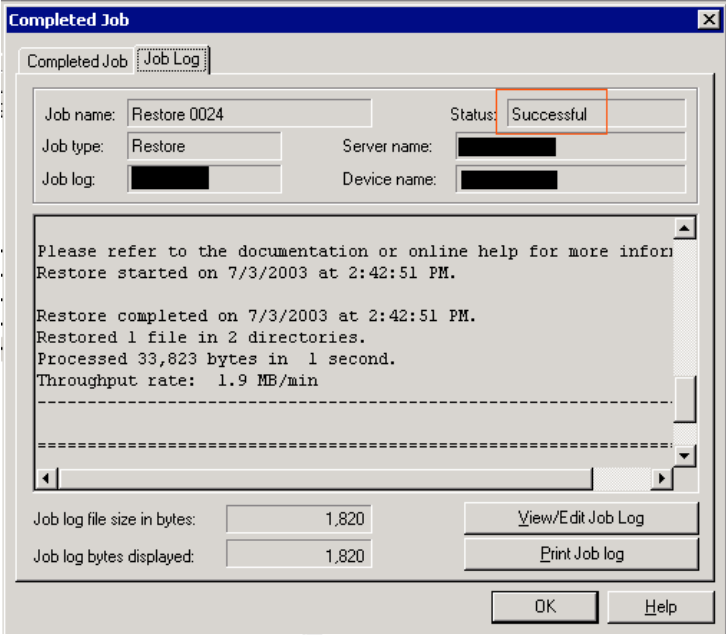


Test Item #7 (Stimulus Response Test #4)

Checklist Item #12	Backup Procedures
Control Objective	Insure a proper backup procedure to prevent data loss and enable recovery operations.
Risk	Data loss occurs and no backup is available.
Probability	Med
Compliance	Proper archiving should be in place and should adhere to company security policy. Successful recovery of test data.
Testing	<ul style="list-style-type: none">• Obtain a copy of the procedure if there are any.• Review the procedure with an administrator to insure your full understanding of it.• Load most recent backup tape in drive and browse content to verify their integrity.• Restore a test item using the backup software, with the help of the administrator.• Insure test was successful• Verify entire procedure and compare with company security policy to make sure they are both compliant with best practices.
Actions	<ul style="list-style-type: none">• Reviewed the procedure on policy for backups• Loaded most recent tape with administrator and browsed the content, verified if procedure used to backup was according to policy.• Restored an item off the tape (item selected at random). This was performed using BackupEXEC v8.6.

© SANS Institute

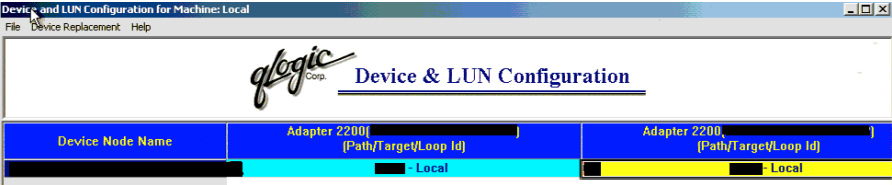


	 <ul style="list-style-type: none"> • Saved the results • Verified the integrity of the file (in this case was a text file and file was correct after reading it).
Results	Pass

Test Item #8

Checklist Item #13	Hardware Support
Control Objective	Insure redundancy is active and functional.
Risk	No redundancy present and an hardware failure occurs. (Fan, power supply, cables)
Probability	Med
Compliance	Redundancy is correctly configures and fully functional.
Testing	<ul style="list-style-type: none"> • Access the Qlogic Card Configuration on the SAN Server with the help of an administrator. • Verify redundancy settings by accessing the Device and LUN configuration. • Insure one card is set at Primary Path and second one is set as Failover path. • Verify they are both active and functional (you should see them in green) If they are not functional a red X would be over the icon that describes the card.



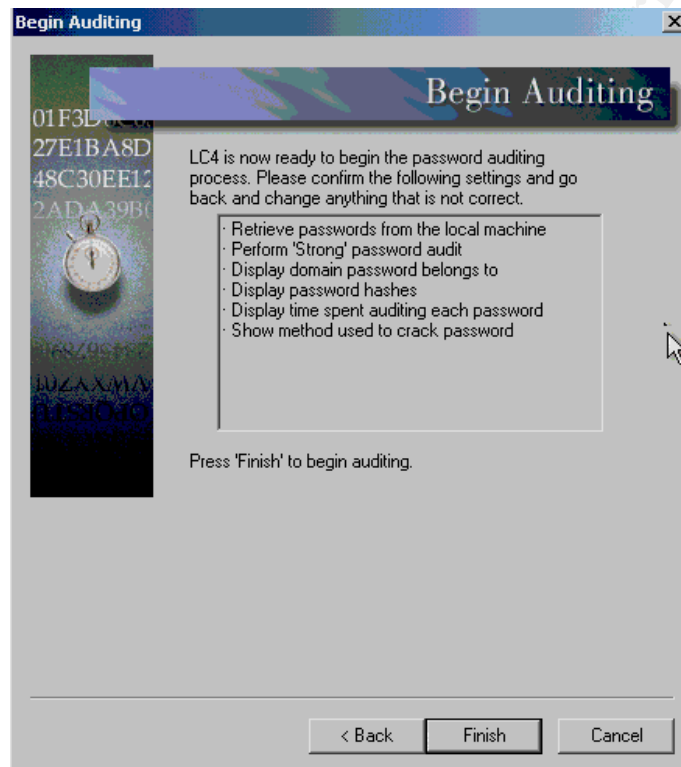
Actions	<ul style="list-style-type: none"> • Take notes of you findings. • Accessed the Array Manager with administrator • Verified the redundancy settings • Took a screenshot of them  <ul style="list-style-type: none"> • Redundancy settings are correct. Blue on left means its set for primary node and yellow on the right means its set for fail-over node.
Results	Pass

Test Item #9 (Stimulus Response Test #5)

Checklist Item #16	Server Password Policy
Control Objective	Insure that passwords meet the company standards and are not easily compromised.
Risk	An attacker brute forces passwords on the server is a relatively short period of time.
Probability	High
Compliance	Passwords meet the company standards and are strong enough to sustain a reasonably long brute force attack.
Testing	<ul style="list-style-type: none"> • Verify company password policy from textbook. • Try adding a user on the server with an easy password to attack. (pass: internet) • Download L0phtcrack v4 from: http://www.atstake.com/research/lc/download.html • Install Lophtcrack v4 on laptop #1 • Request an administrator to be present for this test as an administrator account is required to run a remote verification of passwords. • Insure your laptop is in the same network as the server to be audited. (This can be accomplished by simply plugging your laptop network cable into the local switch) • Direct the L0phtcrack application to the proper server when conducting your audit. • Use Lophtcrack to brute force passwords without showing resulted cracked password. • Save results in a file
Actions	<ul style="list-style-type: none"> • Verified the password policy



- Was not able to add a new user with an easy to guess password. The policy would not allow a password like "internet". It had to be at least 8 characters and have at least 1 numerical and 1 alphabetical and also one special character.
- Installed Lophtrcrack v4 on a laptop
- Requested help of administrator to audit accounts from external source of server (Admin account needed)
- Executed LC4 with the following settings



- Executed the Audit and got the results

Domain	User Name	LM Hash	NTLM Hash	Challenge	Audit Time	Method
		0740B0DD...B80F1DC8B26A88	246F96D8CE1C4453...	8C62F		
		AAD3B435B51404EEAA...	31D6CF...	73C59D7E0C089C0		
		E143...	79373B68558DEA9CCB...	8E409		
		90D24E8916428...	B63A...	7D38B03173F2991267		
		0740B0DD...	246F96D8CE1C4453FA00...	62F		
		C7ACE96BE21F3948...	E0872C...	1D24CDEE53FC010		

- Audit was performed and no passwords were cracked. Run time was 18 hours and 43 minutes.
- Saved results in file

Results

Pass

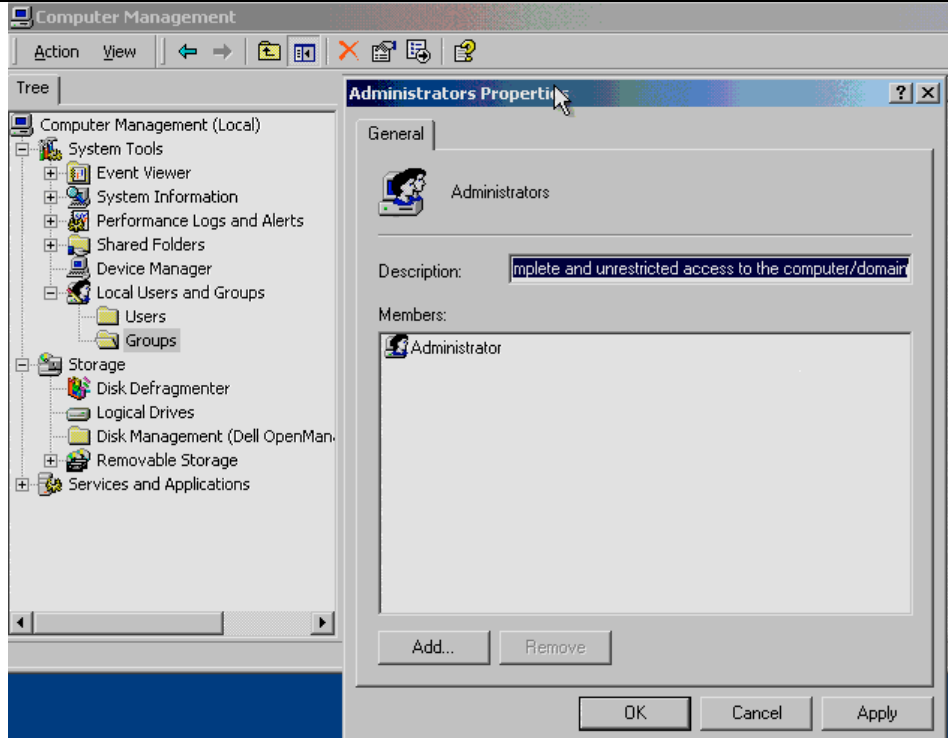


Test Item #10

Checklist Item #20	Administrator Accounts
Control Objective	Insure every administrator has his own account.
Risk	Problems relating to repudiation of an incident.
Probability	Med
Compliance	Every administrator has his own account and password.
Testing	<ul style="list-style-type: none">• Ask an administrator to display list of users and compare list with administrator's list indicated in the Server Security Account Policy. To accomplish this, you must go in the administrator group on the server and display the users that are part of that group. It will list all users who have been granted administrator access. If only the user administrator is displayed, then the only user able to perform administrative task is the administrator.• Log the results
Actions	<ul style="list-style-type: none">• Asked an administrator to display the user that are part of the administrator group.• Took a screen capture of the information

© SANS Institute



	<div data-bbox="448 243 1391 976"></div> <ul style="list-style-type: none">• Compared the result with the administrators that have access to the server and found it to be inaccurate. There were three (3) administrators using the same account on this server. Therefore this test has failed.• Saved the image and logged the results
Results	Fail

© SANS Institute



Measure Residual Risk

There is no such thing as a risk free environment, therefore you must weigh the risks identified and define if they require immediate fixing.

Below you can find the different items of note that were identified during the audit.

Item #3

Residual Risk	Even if a system is protected behind a firewall does not mean that it will not be the subject of an attack. The importance of patching the servers is of the utmost priority.
Threat	Any attacker being from the inside of the network or the outside would have an easy time to defeat the security features of an unpatched server.
Recommendation	Make sure that the fixes are applied to the server and that the proper service pack is also installed. The Windows Update site is an excellent one and can be easily used at any time.
Potential Cost	No cost, just making sure someone verifies the latest patches on a regular basis.

Item #4

Residual Risk	Identifying the necessary services on a system is not necessarily an easy task, however it must be done properly. Different services were identified and some of them may pose a threat to the system if they are not configured properly. And if the services are not used, they should be entirely removed from the system so it elevates the security one more notch. A constant verification of the server is required in order to prevent these services from being installed, sometimes unintentionally.
Threat	More services running = Less security on the server. If there are services that do not need to be there, they could be attacked and eventually exploited. There is



	no reasons why you would keep unused services on a server with that much important data on it.
Recommendation	Identify your required services and adjust them within the server. Make sure you make a proper verification that it is not used before removing them.
Potential Cost	No cost, just shutdown the services not needed.

Item #7

Residual Risk	Hot Spares play a very important role in the SAN technology. If they are to fail and/or not operate properly, they could cause a tremendous amount of problems for the company.
Threat	A failure of a hard drive is not uncommon. In certain situations it may be acceptable or even feasible that such failure occurs. In this technology, a company cannot afford such a risk. All data could be lost as a result.
Recommendation	Making sure there are more than one hot spare per chassis. Therefore reducing the risk by adding additional security measures that would prevent this situation. The cost of one additional hard disk can go a long way when you think about the amount of money that would be lost if this risk would become a reality.
Potential Cost	Business could be closing down. Enormous cost.

As you can see, with close to no cost to perform these modifications, they should be applied and verified. There is no way to quantify the amount of problems that could arise from a failure to do so. In terms of cost, we could easily be talking in the hundreds of thousands of dollars. Therefore, changes must be applied after proper review of the necessary modifications.

Is the system auditable?

The objectives included within this audit were relating to physical security, local server security, privileges, backup, server configuration, its focus is to better evaluate the risks associated with hardware, software and procedures used within the Storage Arena Network server.

If the checklist is followed and proper hardware tests are performed, there should be no doubt that this technology, which is the Storage Area Network technology, is totally auditable.



The most important factor is definitely the hardware in which the server all depends on. Audits should focus on that part of the SAN in order to really circumvent any risks that might endanger the data that resides on the system.

There are however certain aspects that may be taken in consideration when performing an audit of such a system. Here they are:

Do not make any modifications on a production system.

- Often these systems contain a large amount of data that is require by a company to operate normally. A loss of this data, even temporary could be disastrous.
- In the event you are required to perform such a modification. Make sure you have received prior **written** authorization and that you have performed a test on a virtual network.

Do not attempt to verify settings on a system without being helped by an administrator. You may know how to perform these tasks easily, but it all comes down to liability in terms of an error. Also, who knows the system better than the administrator himself.

© SANS Institute 2003, Author retains full rights.



Assignment #4

Executive Summary

The purpose of this audit was to assess the different risks involved around a certain technology that GB Inc. carries. That technology is the Storage Area Network, which is mainly used to store large quantities of data on a centralized server. The accompanying Windows 2000 server was also reviewed along with the different policies and procedures that apply.

The policies were well written and clear to the auditor, it enabled an easier process to test the system thoroughly. The cooperation of the employees for the auditor were also remarkable and always followed policies when it came to apply security measures.

Unfortunately, several items were identified during the audit process and they are worth mentioning since they involve a certain level of risk that varies from Low to High.

The risks are depicted in the following pages along with the associating recommendations and what should be performed in order to allow an environment with limited risks.

It is important to mention as well that there is no such thing as a risk free environment. It's all a matter of evaluating where you can sustain a little risk and where you can definitely not. The SAN server within GB Inc. is a major key to its functionality. In the event of a problem with it, the costs incurred may be very high. Therefore, a good review of those recommendations may help the company to defeat certain risks and minimize others in order to achieve a better security overall.

© SANS Institute 2003, Author retains full rights.



Audit finding

Observation #1

Checklist Item #1 – Vulnerability Tests

Background and Risk	A test was performed in order to identify certain vulnerabilities within the server audited. Several problems were identified but most of them are minor and can be avoided with a simple configuration twist. Although one of the problems identified was a high-risk item in the sense that it requires an immediate patching to solve a major exploitable attack. It is basically oriented at an attacker who could use this attack to penetrate the system and eventually control it totally, which would lead to data integrity problems, theft of information and even data loss. This problem is called the "NULL Session Exploit" and fortunately is easy to fix.
Recommendation	Any administrator could simply modify the system's configuration to fix this type of exploit. A proper verification of all the items identified should also be taken in mind and applied. Therefore it would minimize the risks of a compromise and protect the server against those vulnerabilities.
Cost	The only costs incurred may be associated with assigning an administrator to perform those duties and the drive space required to store the necessary patches. Less than 1000\$.
Compensating Controls	The recommendation could be applied immediately without alternative temporary measures. It would take longer to install a form of protection against this type of attack then it would take to actually patch it correctly, therefore, no compensating control is recommended.



Observation #2

Checklist Item #3 – Service Packs and Hotfixes

Background and Risk	A comparative analysis was performed on your system in order to identify if the server was patched with the current hotfixes that the associated applications company had released (In this case, Microsoft). The test determined that the system was not patched correctly and was missing several security fixes that protect against different system compromise situations. Even if a system is protected behind a firewall does not mean that it will not be the subject of an attack. The importance of patching the servers is of the utmost priority.
Recommendation	Making sure that the fixes are applied to the server and that the proper service pack is also installed. Any administrator can easily perform these functions and there is much information on the internet that relates to these types of updates. The most important thing to implement however is not only the patching of the servers themselves, but the follow-up that the administrators have to do it about it. Basically, patches are sometimes released on a daily basis and its very important to verify the update site several times a week in order to insure an up-to-date patched server.
Cost	Like in the previous recommendation the only costs incurred may be associated with assigning an administrator to perform those duties and the drive space required to store the necessary patches. Less than 1000\$.
Compensating Controls	The recommendation could be applied immediately, however, in the event this is a problem. A temporary firewall could be brought up between the server and the network that would give the administrators enough time to perform all the necessary patches on the system. It would elevate the level of protection of the server while it is being patched. All this without the need to bring it down for an extensive period of time.



Observation #3

Checklist Item #4 – Running Services

Background and Risk	The purpose of a server is to offer services to the users that connect to it. It is a normal process that involves many aspects to it. There is also a factor that is often overlooked; unnecessary services are left on the server even do they are not used. This enables a risk in the fact that attackers could exploit those services that were not even used anyway.
Recommendation	It is important to identify the services needed for a server and closing all the others. This is primarily done by identifying the purpose of the server itself. Once that is well established, you can select the necessary services offered and configure your server accordingly. Working the other way around might be problematic and you might forget a service that would not be used in the context that you would want it to be used.
Cost	The only cost here is the amendment of your System Policy to include necessary services for the different servers and the time it will take for an administrator to perform the changes. Less than 2500\$.
Compensating Controls	An administrator should go through the server services and shutdown the ones that definitely has nothing to do with the services required. This would alleviate the problems that could be encountered until a proper solution is put in place.



Observation #4

Checklist Item #10 – Administrator Accounts

Background and Risk	This is a problem that is very common upon many companies. It was written correctly in your password policy, the problem was simply that it was not applied correctly. The problem relates to the fact that administrators should all have their individual accounts. Problems associated with sharing accounts pertains to a lack of personal accountability should a problem occur. Also, there is no way to account for changes and who performed them, other than the activity logbook that I located within the server room. In the case of your company, your policy clearly states “ Every Administrator is assigned a username and a password for every server they are assigned to administer.” Unfortunately, it was never applied on the system we audited.
Recommendation	Identifying the administrators of the server in question and creating an account with a password on an individual basis is all that is needed for this item. It will prevent headaches in the future should an incident occur after a server modification based on the fact that you will be able to identify the person who perform those modifications and question them in order to reconstruct the error and fix it in the future. Some individuals may not want to go forward when a problem arises if the accounts are shared, because they know it is much more difficult to trace it back to them.
Cost	Like in the previous recommendation the only costs incurred is associated with assigning an administrator to perform those. Less than 1000\$.
Compensating Controls	A log book could be used by administrators when a change is made and who has performed such modification. This log could be compared with who was present in the server room when the change that caused an error was applied. (from the door card reader).



Reference

- Storage Network Industry Association Website <http://www.snia.org/>
- GSNA Certified Students and posted practical <http://www.giac.org/GSNA.php>
- SANS Track-7 Courseware, Various, 2003
- @Stake Website and documentation on LC4 <http://www.atstake.com/>
- Microsoft TechNet Educational Center <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/default.asp>
- SANS Website on Checklist Auditing <http://www.sans.org/score/checklists/AuditingWindows2000.doc>
- <http://www.cisecurity.org/>
- Internet Search Engines <http://www.google.com>

© SANS Institute 2003. All rights reserved. Author retains full rights.