

# **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 SQL Server 2000 Server An Independent Auditors Perspective SANS GSNA V. 2.1 (Option 1)

Graham Thompson

for r This paper contains a checklist for securing Microsoft SQL Server 2000. The goal of this checklist is to give any IT generalist the information and test procedures required to harden SQL server security to meet industry good practices. In addition to the checklist, the paper analyzes the current state of SQL security, conducts a series of tests based on the checklist and reports the audit findings to ACME financial Management.

Assignment 1: Research in Audit, Measurement Practice, and Control Company Overview	
ACME Physical Network Layout	
Identify the system to be audited	
Evaluate risk to the system	
Present state of SQL Server 2000 auditing	
Assignment 2: Create an Audit Checklist	
Check 1 - Service Pack and Hot Fix levels	
Check 2 – Stored Procedures.	
Check 3 – Authentication Model	
Check 4 – Audit Activity on server	
Check 5 – Logon Auditing	
Check 6 – SQL Service start-up accounts	
Check 7 – Guest user access	
Check 8 – Alerting	
Check 9 – TCP/IP Port filtering	
Check 10 – SQL Port	
Check 11 –Password Strength	
Check 12 – SQL ACLS	
Check 13 – Excessive account permissions	29
Check 14 – File Sharing/NetBIOS settings	
Check 15 – Patch Policies and Procedures	. 31
Check 16 – Additional applications and services on server	. 31
Check 17 – Server Roles	. 32
Check 18 – SQL Database Encryption	
Check 19 – Network Protocol Libraries / On-The-Wire Encryption	. 34
Check 20– Backup/Restore Procedures	
Check 21 – Physical Security of Server	
Assignment 3: Conduct the audit	
Audit 1 - Service Pack and Hot Fix levels	
Audit 2 – Stored Procedures	
Audit 3 – Authentication Model	
Audit 4 – Audit Activity on server	
Audit 5 – Logon Auditing	
Audit 6 – SQL Service start-up accounts	
Audit 7 – Guest user access	
Audit 8 – Alerting	
Audit 9 – TCP/IP Port filtering	
Audit 10 – SQL Port	
Residual Risk	
Is the system auditable?	
Assignment 4: Audit Report	
Executive Summary	
Audit Findings	
Finding 1 – Missing patches on the server	

Risks	71
Finding 2 – Lack of detection mechanism	
Risks	
Finding 3 – Lack of notification system	71
Risks	
Finding 4 – Stored Procedure vulnerabilities	72
Risks	73
Finding 5 – TCP/IP Port filtering	73
Risks	
Finding 6 – SQL listening port	
Risks	75
Audit Recommendations	75
Costs	77
Appendix A - References	
Research references	

### Assignment 1: Research in Audit, Measurement Practice, and Control

#### **Company Overview**

ACME Financial Inc is an independent financial services firm that primarily deals with insurance and investment needs of its clients. It does so by offering clients access to multiple mutual funds and insurance packages. The Company serves clients with high net worth. Due to a new Internet initiative and resource constraints, the Company has decided to seek outside assistance with the analysis of the SQL server security.

The Company has one staff member that maintains its own internal switched network. The internal network consists of 5 servers and over 200 workstations running a mix of Windows 2000 and Windows NT 4 Workstation. ACME Financial has setup a web presence and maintains the servers on site. Their connection to the Internet is provided by a large ISP, which also offers minimal firewall services.

Recently, the Company decided to establish client access to their accounts from the Internet. This move was based on customer demand for access to their account information across the Internet. As the data held within the SQL Server will be exposed to the Internet, ACME executives have mandated that security of the internal network be investigated. Due to staffing and resource limitations, outside help was sought.

#### ACME Physical Network Layout



ACME Financial Network Diagram

#### Identify the system to be audited

The focus of this audit is the ACME Financial SQL Server 2000 standard edition (Service Pack 2) database server installed on top of Windows 2000 server (Service Pack 2). The server hardware is a Dell 2550 2U server with a single PIII 1Ghz processor and 1GB of RAM. The server's main duty, among other purposes, is to act as a central repository for confidential client and employee information. This server is accessed by all staff for daily functions such as the querying and updating of client information. The server also holds all employee related data such as payroll and other sensitive information.

There are two front-end access points to the SQL server. From the Internet, IIS is the front-end interface to client data. Internally, employees use Microsoft Access and periodically use IIS to gain access to information held in the database.

### Evaluate risk to the system

The SQL server was chosen as the lead candidate for a security audit due to the sensitivity of the data it holds, the amount of existing vulnerabilities associated with this product and the potential impact to business if the SQL server is compromised. Other servers in the environment will be audited in follow-up sessions.

The following table contains a high level overview of key risks associated with the SQL server, their possibility and their potential impact to the system. Please note that the auditor checklist will contain a detailed analysis of the tests required to ensure the reasonable assumption that these risks are covered.

Priority Ranking	Control Objective	Risk	Probability	Impact
Critical	System must have detection and response mechanism in place	Untraceable access to data stored in server	High. Vendor has included functionality, but is disabled by default.	Loss of detection and response capabilities
Critical	System data must be archived and restore procedures must be known by staff.	Loss of data due to inappropriate backup, restore and Disaster Recovery process and procedures in place.	Medium, depending on Company processes and procedures	Potential increased downtime, potential loss of availability.
Critical	Exposure to published vulnerabilities must be reduced.	Patch level maintenance process and procedures not established and are not followed	Medium. Depends on organization.	A lack of documentation of both management directives and procedures can lead to a lack of proper patch maintenance
High	Network controls should be in place to protect server data	Unauthorized outsider access to SQL Server	Medium. The server is filtered by a firewall. Compromise of the firewall would allow for direct access to the SQL server.	Theft of Corporate data Loss of credibility

High	Users must be given least privilege to data.	Inappropriate insider access to data	High. The SQL server is used by staff members on a daily basis.	Loss of confidentiality.
High	SQL files must not be accessed by unauthorized individuals.	Critical SQL files can be manipulated	Medium. The main directory that stores all SQL data is given permissions that restrict standard users from gaining access. Other directories may disclose sensitive information that can be used as a precursor to an attack	Loss of confidentiality, potential loss of availability and Integrity of data.
High	Audit logs of all actions taken on SQL server must be kept.	Account restrictions not established properly	Medium, depending on server configuration	Loss of confidentiality, possible loss of availability and integrity
Medium	Access to operating system level commands must be removed or restricted to privileged accounts.	Internal applications can be used to attack server	High. Stored procedures can be used to attack server and corporate network	Potential loss of all confidentiality Integrity and Availability of data stored on server.

### Table 1: System risks

Items outside of the above are considered out of scope for this particular audit. Although key aspects of the operating system are being investigated as a part of the SQL audit, this audit does not perform a complete Windows 2000 security audit. It does not analyze the configuration of the IIS server or it's connectivity to the SQL server. Potential SQL injection attacks due to improper code will not be investigated. Additionally, granular permissions on specific databases, tables, columns and views are excluded from this audit.

#### Present state of SQL Server 2000 auditing

Research was performed through the use of common Internet search engines such as Google, Yahoo and AltaVista. In addition to the generic search engines, the vendor web site was searched for further SQL security information, which uncovered a SQL security white paper as well as a C2 security document.

Information regarding some general security items for SQL server such as the outstanding patches that are available (located on the ICAT database) can be easily discovered. However, these patches only address public vulnerabilities and do not address zero-day or yet to be discovered attacks.

In the author's opinion, there are adequate resources to create and conduct a complete audit checklist for SQL Server 2000. An auditor can create a checklist through information available on the vendor website and the existing sqlsecurity.com checklist as a basis of a new checklist. Additionally, many vendors have applications that can be used to aid in the auditing of a SQL 2000 server.

A complete reference list of all resources used to research the product and its security can be found in Appendix A.

Of all research sites used, the following were leveraged heavily for their valuable information

- SQL 2000 Security white paper. The vendor has created a SQL 2000 Security white paper to document vendor recommended best practices and procedures. The white paper can be found at: <a href="http://www.microsoft.com/sql/techinfo/administration/2000/2000SecurityWP.doc">http://www.microsoft.com/sql/techinfo/administration/2000/2000SecurityWP.doc</a>
- SQLsecurity.com checklist was chosen due to its popularity and valuable information. The checklist can be found at: <u>http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4</u>.
- Luis Medina has created a good series of SQL security tips. The "Empirical hacker – Protect your database" series can be found at: <u>http://searchnetworking.techtarget.com/tip/1,289483,sid7\_gci845040,00.html</u>

### Assignment 2: Create an Audit Checklist

### Check 1 - Service Pack and Hot Fix levels

Reference	Search on ICAT Metabase for known SQL Server 2000 vulnerabilities: http://icat.nist.gov
	Microsoft Baseline Security Analyzer (MBSA) homepage (information and download link): <u>http://www.microsoft.com/technet/treeview/default.asp?url=/technet/secu</u> <u>rity/tools/Tools/MBSAhome.asp</u>
Control Objective	Exposure to published vulnerabilities must be reduced.
Risk	If not patched, the server is at an elevated risk level of attack against published vulnerabilities. Server can be exploited via scripts that exist to use vulnerabilities imposed through the lack of a proper patching.
Likelihood	High from external sources if server is accessible or if the firewall is compromised.
Consequence	Attacks can range from a denial of service (Availability) to information disclosure (Confidentiality) and manipulation of data (Integrity)
System Compliance/ Expected Results	The test results are objective. All relevant patches for the system must be installed. The MBSA must state there are no hotfixes missing on the server
Test performed to ensure compliance	<ol> <li>From the auditor's workstation with Internet access, obtain and run Microsoft Baseline Security Analyzer (MBSA). (Start Programs MBSA).</li> <li>Select "scan a computer", enter the name or IP address of the server.</li> </ol>
C	

Microsoft Baseline Security Analyzer       Pick a computer to scan         Welcome       Pick a computer to scan         Pick a computer to scan       Specify the computer you want to scan. You can enter either the computer name or address.		🚷 Microsoft Baseline Security Analyzer
<ul> <li>Welcome</li> <li>Pick a computer to scan</li> <li>Pick multiple computers to scan</li> </ul>		Baseline Security Analyzer
Image: Pick a security report to view       Computer name:         Image: View a security report       Image: Pick a security report         Image: View a security report       Image: Pick a security report         See Also       Security report name:         Image: Microsoft Baseline Security Analyzer       Security report name:         Help       Options:         Image: Pick a security Analyzer       Options:         Image: Pick a security Analyzer       Image: Pick a security report name:         Image: Pick a security Analyzer       Options:         Image: Pick a security Analyzer       Image: Pick a security report name:         Image: Pick a security Analyzer       Options:         Image: Pick a security Analyzer       Image: Pick a security report name:         Image: Pick a security Analyzer       Image: Pick a security report name:         Image: Pick a security Analyzer       Image: Pick a security report name:         Image: Pick a security Web site       Image: Pick a security report name:         Image: Pick a security Pick a security Pick a security Pick a security       Image: Pick a security Pick a security         Image: Pick a security Pick a security       Image: Pick a security         Image: Pick a security Pick a security       Image: Pick a security         Image: Pick a security Pick a security       Image: Pick a security		Welcome       Specify the computer you want to scan. You can enter either the computer name or its IP address.         Pick a computer to scan       Computer to scan         Pick accurity report to view       Computer name:         View a security report       IP address:         See Also       IP address:         Microsoft Baseline Security Analyzer       Security report name:         Help       Options:         About Microsoft Baseline Security Analyzer       Options:         Microsoft Security Web site       Check for Windows vulnerabilities
<ul> <li>4) The application will download the latest vulnerabilities from Microsoft. Accept the download of the xml file.</li> <li>5) The MBSA will now scan the server to determine any missing patches and other configuration information. Save the report as</li> </ul>	Auditor Notes	<ol> <li>3) Ensure that SQL component will be analyzed. Select start scan.</li> <li>4) The application will download the latest vulnerabilities from Microsoft. Accept the download of the xml file.</li> <li>5) The MBSA will now scan the server to determine any missing patches and other configuration information. Save the report as evidence. Affix screenshot of the SQL Server Hotfixes discovery</li> </ol>

### Check 2 – Stored Procedures

Reference	SQL Server Security Checklist (item 6):
	http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4
Control	Access to operating system level commands must be removed or
Objective	restricted to privileged accounts.
Risk	Stored procedures can be used as a means to attack corporate systems. An attacker who has access to certain stored procedures can use them to attack the underlying operating system (e.g. Attacker using xp_cmdshell to delete critical files or implement a Trojan on the server).
Likelihood	Medium. Stored procedure functionality ranges from simple data queries to enhanced shell access to the operating system and internal network at an O/S level.
Consequence	Use of a stored procedure such as xp_cmdshell can grant an attacker
-	complete control of the operating system

System Compliance/ Expected Results	Subjective. Stored procedures show where possible. Xp_cmdshell show it is required.		
Test performed to ensure compliance	<ul> <li>Check for existence of stored proce assigned. To check the stored proce</li> <li>1) Access the SQL Enterprise M (Start Programs MicrosoftSQ</li> <li>2) Expand the SQLServerGroup</li> <li>3) Select the Databases tab, the</li> <li>4) Select "stored procedures" and container.</li> </ul>	edures: /anager LServer EnterpriseMa o and access the serv en access master dat	anager) /er. abase
	Tree	Extended Stored Procedures 1	73 Items
		Name 🛆	Owner
	Console Root	sp_bindsession	dbo
	E G SQL Server Group	sp_createorphan	dbo
	(Windows NT)	sp_cursor	dbo
	🗇 🧰 Databases	sp_cursorclose	dbo
	主 🗋 👘 🛄	sp_cursorexecute	dbo
	🖻 🔋 master	sp_cursorfetch	dbo
	Tables	sp_cursoropen	dbo
	- 60' Views	sp_cursoroption	dbo
	Stored Procedures	sp_cursorprepare	dbo
	Extended Stored Procedures	sp_cursorprepexec	dbo
	22 Roles	Sp_cursorunprepare	dbo
	Rules	sp_droporphans	dbo
	Defaults	sp_execute	dbo
	🔤 🕵 User Defined Data Types	sp_executesql	dbo
	- 🕵 User Defined Functions	sp_fulltext_getdata	dbo
	Full-Text Catalogs	sp_getbindtoken	dbo
	庄 🕛 model	sp_GetMBCSCharLen	dbo
	🕀 🕕 📴 msdb	sp_getschemalock	dbo
	🕀 🛄 Northwind	sp_IsMBCSLeadByte	dbo
	🕀 🛄 🖽 🛄 pubs	sp_MSgetversion	dbo
	∠ <u>⊡</u> tempdb	sp_OACreate	dbo
	Data Transformation Services	sp_OADestroy	dbo
		sp_OAGetErrorInfo	dbo
G		sp_OAGetProperty	dbo
	<ol> <li>Individually select all listed st following table and check per and selecting the permissions include in the report.</li> </ol>	missions by double-c	licking name



	6) Stimulus/Response test: Open Query Analyzer (Start Programs MicrosoftSQLServer QueryAnalyzer). Logon when prompted. Type xp_cmdshell 'dir c:\*.evt /s' in query window. Select run (circled in red in following screenshot).
	🛒 SQL Query Analyzer
	Eile Edit Query Tools Window Help
	🖆 🕶 🖵 🗐   🙏 🖻 🛍 🖆 🚧   🗠   🎹 🗸   🗲 🔶   🕛 master 🔄 🛃 😤 🕰   👔
	Query - Untitled1*
	xp_cmdshell 'dir c:\*.evt /s'
	7) Document the findings and attach a screenshot to the report. This test will prove if xp_cmdshell is still present on the server.
Actual	
Results	
Auditor Notes	

### Check 3 – Authentication Model

Reference	Microsoft SQL 2000 Security White paper (page 15) http://www.microsoft.com/sql/techinfo/administration/2000/2000Security WP.doc
Control	A single account database should be implemented for both the operating
Objective	system and the SQL server.
Risk	Standard SQL authentication introduces a multitude of weaknesses (blank SA passwords, passwords left in install log files, password crackers, cleartext transmission, lack of built-in password restrictions and lockouts). This opens many opportunities for a savvy attacker to find a way into the server.
Likelihood	High. Many systems have the SQL authentication model in place for functionality or due to the lack of awareness.

Consequence	Potential loss of confidentiality if an attacker gains access to the server
	via one of the many vulnerabilities.
System Compliance/ Expected Test Results	Objective. Test must prove Windows authentication is in place.
	Check to ensure that only Windows outbantication is used
Test performed to ensure compliance	<ul> <li>Check to ensure that only Windows authentication is used.</li> <li>1) Access the enterprise manager (Start Programs MicrosoftSQLServer EnterpriseManager)</li> <li>2) Right click server name, select properties</li> <li>3) Open security tab. This will display the authentication mode in use (The following screenshot shows what screen should be seen). Document the setting and capture a screenshot of the server settings.</li> </ul>
	SQL Server Properties (Configure) – 🔀 🔀
	Server Settings       Database Settings       Replication         General       Memory       Processor       Security         Security       SQL Server provides authentication based on Windows accounts and a named SQL Server login ID and password.         Authentication:       SQL Server and Windows         ©       Windows only
	<ul> <li>Stimulus/Response test</li> <li>4) Open Query Analyzer (Start Programs MicrosoftSQLServer QueryAnalyzer).</li> <li>5) Enter SA account as username. Leave password as blank (the error returned will prove if SQL authentication is disabled (non trusted account) or a bad password was entered (incorrect password)).</li> </ul>
	password)).

	Connect to SQL Server
	SQL Server:       Start SQL Server if it is stopped
	Connect using:       Windows authentication         SGL Server authentication       Login name:         Login name:       Bassword:         OK       Cancel         Help         6) Document the results. Capture a screenshot and attach to the report.
Auditor Notes	
Check 4 – Aud	lit Activity on server

Check 4 – Audit Activity on server

Reference	SQL Server books online ("auditing SQL Server activity" as a search
	parameter).
Control	Audit logs of all actions taken on SQL server must be kept.
Objective	
Risk	A lack of auditing will result in an inability to know when a breach has
	occurred. This will allow an attacker to access the system and perform
	malicious activities with little chance of being detected.
Likelihood	High. By default, auditing is not enabled in SQL server.
Consequence	If trace is not enabled, a log of activity will not be maintained.
System	Objective. Trace template created and logs exist to document activity
Compliance/	on the server
Expected Test	
Results	
Test performed	Request location of the trace template and template files or table from
to ensure	the administrator. Access SQL profiler. Open the trace template and
compliance	logs to ensure tracing is enabled and is monitoring activity on the
•	server.
	To access the required settings and files,
	Access trace template
	1) Open SQL profiler
	(Start Programs MicrosoftSQLServer Profiler).
	2) Select File Open TraceTemplate. Select template given by

administrator. Once open, select "Events" tab.
Trace Template Properties
General Events Data Columns Filters
Select the SQL Server event classes you want to trace.
A <u>v</u> ailable event classes: <u>S</u> elected event classes:
Image: Cursors       ▲         Image: Database       ▲         Image: Errors and Warnings       ▲         Image: Locks       ▲         Image: Dbjects       ▲         Image: Dbjects
Collection of events produced when cursors are created, used and deleted.
Items that must be enabled are as follows. Document any deviations Add DB User Event Add Login to Server Add Login to Server Role Add Member to DB Role Add Login App Role Change Password Change Audit Login Login Change Password Login GDR Logout Object Derived Permission Object GDR Object Permission Statement GDR Statement Permission
<ul> <li>Verify Trace Results</li> <li>3) Select File Open TraceFile or TraceTable (depending on storage of traces given by administrator). Point to the location</li> </ul>

	<ul> <li>of trace files or trace template.</li> <li>4) Open trace and check dates for latest activity (starttime column). Note if the trace activity is recent. Document the findings.</li> </ul>
Auditor Notes	

### Check 5 – Logon Auditing

Reference	Microsoft SQL 2000 Security White paper (page 54) http://www.microsoft.com/sql/techinfo/administration/2000/2000Security WP.doc
Control Objective	All system access must be logged.
Risk	A lack of tracing which accounts are failing logon attempts. If not established, an attacker can attempt a brute force attack on the server and no evidence of the attack will be available.
Likelihood	High. Auditing of server logon attempts is not enabled by default.
Consequence	If not configured, no failed logon detection is possible.
System	Objective. Logging of failed SQL logins is turned on (the default setting
Compliance/	is off.)
Expected	
Test Results	
Test	Ensure logon audit level for SQL server is set to all.
performed to	1) Access the enterprise manager
ensure	(Start Programs MicrosoftSQLServer EnterpriseManager)
compliance	2) Right click the server name, select properties
	<ol> <li>Open the security tab. This will display the audit level in place (The following screenshot shows what options should be selected). Document the settings and capture a screenshot of the server settings.</li> </ol>

	SQL Server Properties (Configure) -
	Server Settings Database Settings Replication
	General Memory Processor Security Connections
	General       Memory       Processor       Security       Connections         Security       SQL Server provides authentication based on Windows accounts and a named SQL Server login ID and password.       Authentication:       SQL Server and Windows       Windows only         Audit level:       None       Eailure       Laudit level:       Success       All         Stimulus/Response Test:       Access Query Analyzer (Start Programs MicrosoftSQLServer QueryAnalyzer)       Sterver with user account SA and a blank password.         A t the logon prompt, select SQL authentication. Attempt to logon to server with user account SA and a blank password.       At the logon prompt, select Windows authentication. Attempt to logon to server.         A Access the application log in Event Viewer (Start Programs AdministrativeTools EventViewer). Open log entries that show attempted logons (event 17055 shows all successful and failed logon attempts). Document findings and attach screenshots to report.
Auditor Notes	

### Check 6 – SQL Service start-up accounts

Reference	Microsoft SQL 2000 Security White paper (page 51) http://www.microsoft.com/sql/techinfo/administration/2000/2000Security WP.doc
	SQL Server Security Checklist (item 4): http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4
Control	The SQL service must be assigned a user level start-up account
Objective	
Risk	Excessive rights assigned to SQL service.
Likelihood	Medium. Depends on the server configuration
Consequence	These rights can be used by an attacker to increase their privilege on

	the server and network
System	Objective. MSSQLSERVER service must start as a user level account.
Compliance /	
Expected test	
results Test	Chack convice startup account in enterprise manager
performed to	Check service startup account in enterprise manager. 1) Access the enterprise manager
ensure	(Start Programs MicrosoftSQLServer EnterpriseManager)
compliance	2) Right click the server name, select properties.
	3) Open the security tab. This will display the startup account in
	place (The following screenshot shows what options should be
	selected). Document the settings and capture a screenshot of
	the server settings.
	SQL Server Properties (Configure) – 📉 🔀
	Server Settings Database Settings Replication
	General Memory Processor Security Connections
	- Security
	SQL Server provides authentication based on Windows
	accounts and a named SQL Server login ID and password.
	Authentication:
	C SQL Server and Windows
	Audit level:
	C None C Eailure
	Startup service account
	Start and run SQL Server in the following account:
	C System account
	This account
	Password:
C	4) Access Windows users and groups settings
	(Start Programs AdministrativeTools ComputerManagement
	LocalUsersAndGroups). Double-click the users tab. Double click
	the service account name. Check the group membership. Document and attach a screenshot to the report.
	5) Access Services window
	(Start Settings ControlPanel AdministrativeTools Services).
	Access MSSQLServer service by double-clicking the service.
	Access the logon tab. Confirm which account is being used to

	start the service. Document the account and attach a screenshot to the report.
Auditor Notes	

### Check 7 – Guest user access

Reference	SQL Server Security Checklist (item 8):
	http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4
	Microsoft SQL 2000 Security White paper (page 58)
	http://www.microsoft.com/sql/techinfo/administration/2000/2000Security
	WP.doc
Control	Only authenticated accounts may access the SQL server.
Objective	
Risk	Non-authenticated users have access to a database through the guest
	account. Potential disclosure of data is possible through guest access.
Likelihood	Medium. Depends on the server configuration.
Consequence	Disclosure of information is possible if the guest account has access.
System	Objective. The guest account is removed from all sensitive databases.
Compliance/	The guest account at the operating system level must be disabled.
Expected test	
results	
Test	Check permissions for the guest account on sensitive databases.
performed to	1) Access enterprise manager
ensure	(Start Programs MicrosoftSQLServer EnterpriseManager)
compliance	2) Expand the server group, open the target server then access the
•	databases tab. Expand the database in question. Select the
	users tab. All users allowed access are shown.
	3) Ensure the guest account is not listed and that only required
	groups/users are listed as having access to the database.
	Document the findings and attach a screenshot to the report.
G	Check guest account at O/S level
C	<ol> <li>Access Windows users and groups settings</li> </ol>
	(Start Programs AdministrativeTools ComputerManagement Loca
	IUsersAndGroups).
	5) Double-click users tab. Double click guest account. Ensure
	"account is disabled" box is checked. Document findings and
	attach a screenshot.
	Stimulus/Response test: Attempt to access the server with an
	account not listed as having access to ensure that access is denied.
L	

<ul> <li>6) Logon to the auditor workstation as a user that does not exist on the target server (this will force a guest connection when data access is performed).</li> <li>7) Open Microsoft Access from the auditor workstation. Close any wizard that appears when opening the application.</li> <li>8) Select the "new data access page". Choose design view. The "Data link properties" screen will open.</li> <li>9) Enter the server name and select Windows Integrated Security. The following screenshot shows the screen that should be displayed.</li> </ul>
Data Link Properties
Provider Connection Advanced All
Specify the following to connect to SQL Server data: 1. Select or enter a server name:
2. Enter information to log on to the server:
Use Windows NT Integrated security
Use a specific user name and password:
User name:
Password: Blank password Allow saving password
<ol> <li>Blank password 1 Allow saving password</li> <li>Select the database on the server:</li> </ol>
3. V <sup>o</sup> Select the database on the server.
10) Select the "select detenance on the conver" nulldown here
10) Select the "select database on the server" pulldown box. Access should be denied. Document the findings and attach a screenshot of any errors.
Auditor Notes

### Check 8 – Alerting

Reference	SQL Server Security Checklist (item 17):
	http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4
Control	An alerting mechanism must be established and notification established.
Objective	
Risk	A lack of alerting would prohibit response to malicious activity. This
	would allow an attacker ample opportunity to attack the server if no
	detection and response was possible.
Likelihood	High. Alerting is not configured by default.

Consequen	No response would be possible if alerting is not enabled.	
се		
System	Objective. Alerts are configured and notification will be sent.	
Compliance/		
Expected		
Test Results		
Test performed	Access the server in SQL Enterprise Manager. Select Management   SQL Server Agent   Alerts. Check for the existence of an alert for	
to ensure	severity 14 and that an operator is defined to receive a page or e-mail.	
compliance	1) Access Enterprise Manager	
compliance	(Start Programs MicrosoftSQLServer EnterpriseManager)	
	2) Expand the server group, open the server and access the	
	management tab. Select "SQL Server agent", then alerts.	
	3) Check for a listing with severity 14. Attach screenshot of alerts	
	screen.	
	4) Double click the severity 14 item. Click the "Response" tab. Note	
	all of the recipients of alerts. Attach a screenshot of the recipients	
	and the method of alerting.	
Auditor		
Notes		
Check 9 – TCP/IP Port filtering		

## Check 9 – TCP/IP Port filtering

Reference	Medina, Luis, Empirical Hacker – Protect your database series - part
	one, checklist item 7.
	http://searchnetworking.techtarget.com/tip/1,289483,sid7_gci845040,00.
	<u>html</u>
Control	Network controls should be in place to protect the server data.
Objective	
Risk	Malware can use high-level ports to communicate with an attacker and
C	allow access to server.
Likelihood	Medium. Previous examples of malware that allowed for remote control
	of the server included backorifice and netbus.
Consequence	If not restricted, any port can be used on the server. Malware would be
	able to report back to an attacker and open a connection through the
	corporate firewall.
System	Objective. All ports other than the required baseline ports are filtered at
Compliance /	the O/S level.
Expected test	
Expected test	

results	
Test	Check TCP/IP filtering.
performed to	
ensure	1) On the server desktop, right-click the "My Network Places" icon,
compliance	select properties. Right-Click "Local Area Connection", select
	properties. Double click Internet Protocol (TCP/IP). Select the
	advanced tab, then options. The following screen capture shows
	what should be displayed.
	Advanced TCP/IP Settings
	IP Settings DNS WINS Options
	Optional settings:
	IP security
	TCP/IP filtering
	Description
	Properties
	Description
	TCP/IP filtering allows you to control the type of TCP/IP network traffic that reaches your Windows computer.
	2) Select TCP/IP filtering, select properties. All filtered ports will be
	displayed at this point. Document and attach a screenshot to the
	report.
	Stimulus/Response Tests:
	3) From the auditor workstation on the LAN, run NMAP (windows
	executables available at http://sourceforge.net/projects/nmapwin.)
	Enter the IP address of the SQL server. Check the port range
	box and enter 1-65535. This will test which ports are accessible
	on the server. Ensure that all TCP and UDP ports are scanned
	(by repeating the test with UDP scan selected). Attach both
	screenshots (TCP and UDP scans) of discovered ports to the
G	report.
e	4) Execute fport (executables available at
	http://www.foundstone.com/knowledge/free_tools.html) on the
	server. Save the report and attach a screenshot to the report.

### Check 10 – SQL Port

Reference	Medina, Luis, Empirical Hacker – Protect your database series - part one,		
	checklist item 2.		
	http://searchnetworking.techtarget.com/tip/1,289483,sid7_gci845040,00.html		
	Partlow, Joe, Microsoft SQL Server 2000 Security Overview (page 6)		
	http://www.giac.org/practical/Joe_Partlow_GSEC.doc		
	nup.//www.glac.org/practical/Joe_Partiow_GSEC.doc		
Control	Network controls should be in place to protect the server data.		
Objective	e 🔊		
Risk	Attackers will portscan entire subnets on port 1433 (automated attacks), or		
	will use Sqlping2 (port 1434) to manually find SQL servers on the Internet.		
Likelihood	Depends on the firewall configuration.		
Consequence	A potential attacker would know of the existence of the SQL server. An		
Consequence			
	attacker can then use automated tools to attack server after initial the		
	reconnaissance.		
System	Objective. The port value should be changed from the default and the		
Compliance/	server port should be hidden. This will change both the listening port and		
Expected test	hide the actual SQL port in use from sqlping2.		
results			
Test	1) Access Enterprise Manager		
performed to	(Start Programs MicrosoftSQLServer EnterpriseManager)		
ensure	2) Expand the server group, right click the servername and select		
	, , ,		
compliance	properties.		
	<ol><li>Select the Network Configuration tab. Select the TCP/IP protocol</li></ol>		
	option and select properties.		
	<ol><li>Document the port number and determine if the server is listed as</li></ol>		
	hidden ("hide server" checkbox selected).		
	Stimulus/Response tests:		
	5) Run fport on the server to confirm which port the SQL Server is		
	listening to. Document findings and attach screenshot.		
6	6) Obtain sqlping2 from <u>www.sqlsecurity.com/scripts.asp</u> .		
e	7) Run SQLping2 against the server IP address.		
	<ol><li>B) Document the findings and attach a screenshot to the report.</li></ol>		
Auditor Notes			

### Check 11 – Password Strength

Reference	Cert Advisory # 635463: http://www.kb.cert.org/vuls/id/635463		
	SQL Server Security Checklist (item 3):		
	http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4		
Control	All passwords must meet corporate minimum length requirements		
Objective			
Risk	Simple and blank passwords can be easily guessed and/or be broken by		
	an attacker with a dictionary attack.		
Likelihood	Medium. SQL Server 2000 allows for a default password of <null> for</null>		
	the SA account. Factors such as personnel security training/awareness		
	and the initial compromise required to access the password hashes		
	mitigate the potential loss through weak passwords (if SQL		
Canadanuanaa	authentication is used).		
Consequence	Loss of all Confidentiality, Integrity and Availability through the guess of		
Sustam	a simple administrative level password.		
System	Objective. Security policy states minimum password strength (6		
Compliance:	characters and complex password requirements) must be followed to		
	meet company security policy. This applies to both SQL and O/S level		
Test	<ul> <li>passwords. The system must reject weak passwords at an O/S level.</li> <li>1) From the auditor's workstation with Internet access, obtain and</li> </ul>		
performed to			
ensure	run Microsoft Baseline Security Analyzer (MBSA). (Start Programs MBSA).		
compliance	<ol> <li>Select "scan a computer", enter the name or IP address of the</li> </ol>		
compliance	server.		
	<ol> <li>Ensure that SQL component will be analyzed. Select start scan.</li> </ol>		
	4) The application will download the latest vulnerabilities from		
	Microsoft. Accept the download of the xml file.		
	5) The MBSA will now scan the server to determine which		
	authentication mode the server is using and will determine if there		
	are any weak SQL passwords on the SQL server.		

	Oom Conl	iain troller Test	SQL Server is not running on a domain controller. What was scanned
	SQL	Server urity Mode	SQL Server authentication mode is set to Windows Only. What was scanned
		istry nissions	The Everyone group does not have more than Read access to the SQL Server registry keys. What was scanned
	🖌 🗸 Cmd	Exec role	CmdExec is restricted to sysadmin only. What was scanned
	V Fold Pern	er nissions	Permissions on the SQL Server installation folders are set properly. What was scanned
		Account sword Test	The check was skipped because SQL Server is operating in Windows Only authentication mode.
			What was scanned
<b>.</b>		<del>.</del> .	
Stir	mulus/Respo		
	<i>'</i>		e administrator create a test account and supply
	you with	•	
	, .		count and attempt to change password (Ctrl-Alt-
		• •	ssword) to a null value. The system should reject
			Document the test results and attach to the repor
			nge password to "password". The system should
	-	is passv	word. Document the test results and attach to the
	report.		
	<i>,</i> .	his pass	nge password to "qwerty123!". The system should sword. Document the test results and attach to
	•	IT.	
	the repo	rt.	
SQ	the repo		h testing with a dictionary attack (use only for
	the repo	strengt	h testing with a dictionary attack (use only for nentication implemented).
	the repo L password stems with S	strengt QL autl	hentication implemented).
	the repo L password stems with S 1) Obtain tl	strengt QL autl he SQL	hentication implemented). BF brute force/dictionary cracker for SQL server
	the repo L password stems with S 1) Obtain th ( <u>http://w</u>	strengt QL autl he SQL <u>ww.cqu</u>	hentication implemented). BF brute force/dictionary cracker for SQL server re.net/tools.jsp?id=10).
	the repo L password stems with S 1) Obtain th ( <u>http://w</u> 2) Obtain a	strengt QL autl he SQL <u>ww.cqu</u> a diction	hentication implemented). BF brute force/dictionary cracker for SQL server re.net/tools.jsp?id=10). ary file if one is unavailable. A dictionary file can
	the repo L password stems with S 1) Obtain th ( <u>http://w</u> 2) Obtain a be obtain	strengt QL auti he SQL ww.cqu diction ned froi	hentication implemented). BF brute force/dictionary cracker for SQL server re.net/tools.jsp?id=10). ary file if one is unavailable. A dictionary file can m ftp://ftp.ox.ac.uk/pub/wordlists/dictionaries/.
	the repo to password stems with S 1) Obtain th ( <u>http://w</u> 2) Obtain a be obtain Obtain th	strengt QL auti he SQL ww.cqu a diction ned froi he pock	hentication implemented). BF brute force/dictionary cracker for SQL server re.net/tools.jsp?id=10). ary file if one is unavailable. A dictionary file can m ftp://ftp.ox.ac.uk/pub/wordlists/dictionaries/. ket-dict.gz dictionary. Expand with winzip and
	the report tems with S 1) Obtain the <u>tems</u> with S 2) Obtain a be obtain the obtain the save to the temport	strengt QL autl he SQL ww.cqu a diction ned from he pock the sam	hentication implemented). BF brute force/dictionary cracker for SQL server re.net/tools.jsp?id=10). hary file if one is unavailable. A dictionary file can m ftp://ftp.ox.ac.uk/pub/wordlists/dictionaries/. ket-dict.gz dictionary. Expand with winzip and he directory as the sqlbf application. Rename the
	the report tems with S 1) Obtain the <u>(http://wr</u> 2) Obtain a be obtain Obtain the save to the file to po	strengt QL auti he SQL ww.cqu a diction ned from he pock the sam ocket.dio	hentication implemented). BF brute force/dictionary cracker for SQL server re.net/tools.jsp?id=10). hary file if one is unavailable. A dictionary file can m ftp://ftp.ox.ac.uk/pub/wordlists/dictionaries/. ket-dict.gz dictionary. Expand with winzip and he directory as the sqlbf application. Rename the ct.
	the repo L password stems with S 1) Obtain th ( <u>http://w</u> 2) Obtain a be obtain Obtain th save to th file to po 3) Open the	strengt QL auti he SQL ww.cqu a diction ned from he pock the sam ocket.dic e Query	hentication implemented). BF brute force/dictionary cracker for SQL server re.net/tools.jsp?id=10). hary file if one is unavailable. A dictionary file can m ftp://ftp.ox.ac.uk/pub/wordlists/dictionaries/. ket-dict.gz dictionary. Expand with winzip and he directory as the sqlbf application. Rename the ct. y Analyzer
sys	the report tems with S 1) Obtain the (http://wr 2) Obtain a be obtain Obtain the save to the file to po 3) Open the (Start Pr	strengt QL auti he SQL ww.cqu a diction ned froi he pock the sam ocket.dio e Query rograms	hentication implemented). BF brute force/dictionary cracker for SQL server re.net/tools.jsp?id=10). hary file if one is unavailable. A dictionary file can m ftp://ftp.ox.ac.uk/pub/wordlists/dictionaries/. ket-dict.gz dictionary. Expand with winzip and he directory as the sqlbf application. Rename the ct. y Analyzer s MicrosoftSQLServer QueryAnalyzer).
sys	the report the report tems with S 1) Obtain the (http://ww 2) Obtain a be obtain Obtain the save to the file to poot 3) Open the (Start Pr 4) Issue the	strengt QL auti he SQL ww.cqu a diction ned from he pock the sam pocket.did e Query rograms e follow	hentication implemented). BF brute force/dictionary cracker for SQL server re.net/tools.jsp?id=10). hary file if one is unavailable. A dictionary file can m ftp://ftp.ox.ac.uk/pub/wordlists/dictionaries/. ket-dict.gz dictionary. Expand with winzip and he directory as the sqlbf application. Rename the ct. / Analyzer MicrosoftSQLServer QueryAnalyzer). ing command: "select name, password from
sys	the repo L password stems with S 1) Obtain th ( <u>http://w</u> 2) Obtain a be obtain Obtain th save to th file to po 3) Open the (Start Pr 4) Issue the master	strengt QL auti he SQL ww.cqu a diction ned from he pock the sam ocket.dic e Query rograms e follow sysxlog	hentication implemented). BF brute force/dictionary cracker for SQL server re.net/tools.jsp?id=10). hary file if one is unavailable. A dictionary file can m ftp://ftp.ox.ac.uk/pub/wordlists/dictionaries/. ket-dict.gz dictionary. Expand with winzip and he directory as the sqlbf application. Rename the ct. y Analyzer s MicrosoftSQLServer QueryAnalyzer). ing command: "select name, password from jins". This will extract all accounts and passwords
sys	the report L password stems with S 1) Obtain the (http://wr 2) Obtain a be obtain Obtain the save to the file to port 3) Open the (Start Pr 4) Issue the masters	strengt QL auth he SQL ww.cqu a diction ned from he pock the sam ocket.did e Query rograms e follow sysxlog n the S	hentication implemented). BF brute force/dictionary cracker for SQL server re.net/tools.jsp?id=10). hary file if one is unavailable. A dictionary file can m ftp://ftp.ox.ac.uk/pub/wordlists/dictionaries/. ket-dict.gz dictionary. Expand with winzip and he directory as the sqlbf application. Rename the ct. y Analyzer s MicrosoftSQLServer QueryAnalyzer). ing command: "select name, password from jins". This will extract all accounts and passwords QL server and display the hash values. Select all
sys	the report L password stems with S 1) Obtain the (http://wr 2) Obtain a be obtain Obtain the save to the file to po 3) Open the (Start Pr 4) Issue the masters stored o entries, o	strengt QL auti he SQL ww.cqu a diction ned from he pock the sam pocket.did e Query rograms e follow sysxlog n the S copy wi	hentication implemented). BF brute force/dictionary cracker for SQL server re.net/tools.jsp?id=10). ary file if one is unavailable. A dictionary file can m ftp://ftp.ox.ac.uk/pub/wordlists/dictionaries/. cet-dict.gz dictionary. Expand with winzip and he directory as the sqlbf application. Rename the ct. / Analyzer MicrosoftSQLServer QueryAnalyzer). ing command: "select name, password from jins". This will extract all accounts and passwords QL server and display the hash values. Select all th <ctrl-c> and save to a new text file called</ctrl-c>
sys	the report L password stems with S 1) Obtain the (http://ww 2) Obtain a be obtain Obtain the save to the file to po 3) Open the (Start Pr 4) Issue the master stored o entries, a sqlhash.	strengt QL auti he SQL ww.cqu a diction ned from he pock the sam ocket.did e Query rograms e follow sysxlog n the S copy wi txt in th	hentication implemented). BF brute force/dictionary cracker for SQL server re.net/tools.jsp?id=10). hary file if one is unavailable. A dictionary file can m ftp://ftp.ox.ac.uk/pub/wordlists/dictionaries/. ket-dict.gz dictionary. Expand with winzip and he directory as the sqlbf application. Rename the ct. / Analyzer S[MicrosoftSQLServer]QueryAnalyzer). ing command: "select name, password from jins". This will extract all accounts and passwords QL server and display the hash values. Select all th <ctrl-c> and save to a new text file called he same directory as the sqlbf application. Modify</ctrl-c>
sys	the report L password stems with S 1) Obtain the (http://wr 2) Obtain a be obtain Obtain the save to the file to po 3) Open the (Start Pr 4) Issue the master stored o entries, sqlhash. the text file	strengt QL auth he SQL ww.cqu a diction he pock the sam ocket.dic e Query ograms e follow sysxlog n the S copy wi txt in th file so th	hentication implemented). BF brute force/dictionary cracker for SQL server re.net/tools.jsp?id=10). hary file if one is unavailable. A dictionary file can m ftp://ftp.ox.ac.uk/pub/wordlists/dictionaries/. ket-dict.gz dictionary. Expand with winzip and he directory as the sqlbf application. Rename the ct. y Analyzer s MicrosoftSQLServer QueryAnalyzer). ing command: "select name, password from jins". This will extract all accounts and passwords QL server and display the hash values. Select all th <ctrl-c> and save to a new text file called he same directory as the sqlbf application. Modify hat there is the name, followed by a comma,</ctrl-c>
sys	the report L password stems with S 1) Obtain the (http://wr 2) Obtain a be obtain 0btain the save to the file to po 3) Open the (Start Pr 4) Issue the master stored o entries, of sqlhash. the text the followed	strengt QL auti he SQL ww.cqu a diction ned from he pock the sam ocket.did e Query rograms e follow sysxlog n the S copy wi txt in th file so th	hentication implemented). BF brute force/dictionary cracker for SQL server re.net/tools.jsp?id=10). hary file if one is unavailable. A dictionary file can m ftp://ftp.ox.ac.uk/pub/wordlists/dictionaries/. ket-dict.gz dictionary. Expand with winzip and he directory as the sqlbf application. Rename the ct. / Analyzer s[MicrosoftSQLServer]QueryAnalyzer). ing command: "select name, password from jins". This will extract all accounts and passwords QL server and display the hash values. Select all th <ctrl-c> and save to a new text file called he same directory as the sqlbf application. Modify</ctrl-c>

	<ul> <li>values at the end of the file are removed. This file will be the target of our dictionary attack.</li> <li>5) Open a command prompt (Start Run cmd). Change the working directory to the location of the sqlbf application. Issue the following command: sqlbf –u sqlhash.txt –d pocket.dict –r hashresults.txt. Document any found accounts and their passwords. Attach findings to the report.</li> </ul>
Auditor Notes	

### Check 12 – SQL ACLS

Auditor Notes	
Check 12 – SC	QL ACLS
Reference	Microsoft SQL 2000 Security White paper (page 53) <u>http://www.microsoft.com/sql/techinfo/administration/2000/2000SecurityWP.doc</u> SQL Server Security Checklist (item 5): <u>http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&amp;tabid=4</u>
Control Objective	Users must be given least privilege to data.
Risk	An attacker can obtain information through weak O/S Access Control.
Likelihood	High. Published vulnerabilities exist that disclose log files are stored with all users having access and can potentially contain system accounts and passwords if SQL authentication is used.
Consequence	Elevation of privilege can occur resulting in loss of confidentiality.
System Compliance/ Expected test results	Objective. Group and individual permissions should only allow administrators, system and SQL account access to the SQL files at an OS level.
Test performed to ensure compliance	<ul> <li>Access the security permissions for the SQL server directory under program files folder. Ensure that users do not have access to the directories unless it is required for functionality. Ensure the "everyone" account is removed from the ACL list. Document any deviations.</li> <li>1) Open a command prompt on the server (Start Run cmd).</li> <li>2) Issue the command cacls "c:\program files\Microsoft SQL Server\mssql\data\*.*" /c. (replace the path as required to point to the location of the database files). Redirect the output to a file and attach to the report. Document any deviations.</li> <li>3) Issue the command cacls "c:\program files\Microsoft SQL Server\ *.*" /c. (replace the path as required to point to the location of the SQL Server installation). Redirect the output to a file and attach to the report. Document any deviations.</li> <li>4) Issue the command cacls "c:\program files\Microsoft SQL Server\mssql\binn\*.*" /c. (replace path as required to point to location of the SQL Server installation).</li> </ul>

	database files). Redirect output to a diskette. Document any deviations.
Auditor Notes	

### Check 13 – Excessive account permissions

Reference	Microsoft SQL 2000 Security White paper (page 30)	
	http://www.microsoft.com/sql/techinfo/administration/2000/2000SecurityWP.doc	
Control	Users must be given least privilege to data.	
Objective		
Risk	Users may see information to which they are not privileged.	
Likelihood	Medium. Depends on the server security configuration.	
Consequence	Accidental or malicious activity on sensitive information can occur if the permissions exceed the required level.	
System	Subjective. Least privilege assigned is to users. Only the owner of the system	
Compliance/	will be able to determine who should be given access and what level of access	
Expected	control is required.	
Test Results		
Test	Review the rights to all tables containing sensitive data in SQL. Check the	
performed to	rights to the views created.	
ensure	<ol> <li>Access Enterprise Manager (Start Programs MicrosoftSQLServer EnterpriseManager)</li> </ol>	
compliance	2) Expand the server group, open the server then access the databases	
	tab. Select the database in question. Select the tables tab. All	
	available tables are shown.	
¢	Sharphille C	

Imiw-sql - Terminal Server Client         Action View Tools         Console Root         Console Root         Console Root         SQL Servers         Cotagories         CustomerCustomerDemo         SQL Server Group         Databases         Image: CustomerCustomerDemographics         Microsoft SQL Servers         Databases         Image: CustomerCustomerDemographics         More CustomerDemographics         More Customer				
Tree       Tables       33 Items         Console Root       Name       Owne         Microsoft SQL Servers       Categories       dbo         SQL Server Group       CustomerCustomerDemo       dbo         Databases       CustomerCustomerDemo       dbo         master       Employees       dbo         model       Employees       dbo         model       Employees       dbo         Northwind       Order Details       dbo         Northwind       Orders       dbo         Stored Procedures       Supplers       dbo         Syscolumns       dbo       syscolumns         Rules       syscolumns       dbo         sysclepends       dbo       sysclepends         Order Patalls       dbo       sysclepends         Suber Defined Data Types       sbo       sysclepends         Sysclepends       dbo       sysclepends       dbo		🔚 miw-sql - Terminal Server Client		
Console Root       Name       Owne         Microsoft SQL Server Group       Categories       dbo         Databases       CustomerCustomerDemo       dbo         Databases       Customers       dbo         master       Employees       dbo         model       Employeeterritories       dbo         Northwind       Order Details       dbo         Diagrams       Products       dbo         Views       Stored Procedures       Suppliers       dbo         Syscelpends       dbo       syscelpends       dbo         Defaults       Syscelpends       dbo       systelpends       dbo         Systiles1       dbo       systiles1       dbo       systiles1		Action Yiew Iools 🗍 🖙 🔿 🔂 🚺	× 🖅 🖸 😼   😫  ] 🔆   🖄	• 🛛 🖳
Console Root       Categories       dbo         Sol, Server Group       CustomerCustomerDemo       dbo         Databases       CustomerPoemographics       dbo         Databases       CustomerS       dbo         Diagrams       dbo       Corder Details       dbo         Diagrams       Drodel       Products       dbo         Diagrams       Stored Procedures       Suppliers       dbo         Views       Stored Procedures       Suppliers       dbo         Rules       Syscolumns       dbo       systilegroups       dbo         Systilegroups       dbo       Systilegroups       dbo       systilegroups       dbo         Systilegroups       dbo       Systilegroups       dbo       systiles1       dbo         Systiles1       dbo       Systiles1       dbo       Systiles1       dbo		Tree	Tables 33 Items	
Microsoft SQL Servers <pre>             Categories</pre> dbo             CustomerCustomerDemo             dbo             CustomerS              dbo             SustomerDemographics              dbo             CustomerS              dbo             SustomerDemographics              dbo             SustomerDemographics              dbo             SustomerDemographics              dbo             SustomerDemographics              dbo             SustomerDemographics              dbo             SustomerDemographics              dbo		Console Root	Name 🛆	Owne
Sol. Server Group       CustomerCustomerDemo       dbo         Databases       CustomerCustomerDemographics       dbo         master       CustomerS       dbo         master       Employees       dbo         master       Employees       dbo         Model       Employees       dbo         Morthwind       Order Details       dbo         Diagrams       Products       dbo         Stored Procedures       Stopelers       dbo         Views       Stopelers       dbo         Stored Procedures       Syscolumns       dbo         Roles       Syscolumns       dbo         Syscolumns       dbo       Syscolumns         User Defined Data Types       Syscolumns       dbo         User Defined Functions       Sysfiles       dbo         Sysfiles       dbo       Sysfiles1       dbo         Sysfiles1       dbo       Sysfiles1       dbo			Categories	dbo
Image: CustomerDemographics       dbo         Image: CustomerDemographics       dbo         Image: CustomerS       dbo         Image: CustomerS       dbo         Image: CustomerDemographics       dbo         Image: CustomerDemographics       dbo         Image: CustomerS       dbo         Image: CustomerDemographics       dbo         Image: CustomerDemograp				dbo
Image: Customers       dbo         Image: Custalogs       gsystilegroups		ý j.		dbo
master       Employees       dbo         model       EmployeeTerritories       dbo         msdb       Order Details       dbo         Order Details       dbo         Diagrams       Products       dbo         Order S       dbo         Stored Procedures       Shippers       dbo         Northwind       Stored Procedures       Shippers       dbo         Stored Procedures       Shippers       dbo       dbo         Region       dbo       Suppliers       dbo         Rules       Syscolumns       dbo       syscolumns       dbo         User Defined Data Types       dbo       sysfilegroups       dbo         Sysfiles       dbo       sysfiles1       dbo         Stored Procedures       Sysfiles1       dbo       sysfiles1         Stored Procedures       Sysfiles2       dbo       sysfiles2         Stored Procedures       Sysfiles1       dbo       systiles1         Stored Procedur		🖃 🦲 Databases		dbo
Image: master model model       Employees       dbo         Image: model model model       Employee Territories       dbo         Image: model model model model model       Order Details       dbo         Image: model mod		庄 🚺		dbo
Image: Second state of the second s				dbo
Image: Stored Procedures       Image: Stored P				dbo
Diagrams       Orders       dbo         Tables       Products       dbo         Views       Stored Procedures       Shippers       dbo         Users       Suppliers       dbo         Rules       syscolumns       dbo         User Defaults       syscolumns       dbo         User Defined Data Types       dbo         Full-Text Catalogs       sysfiles       dbo         3) Check permissions on table to ensure that only authorized individuals have required access. Document the findings.			📰 Order Details	dbo
Image: Second Procedures       Image: Second P			📰 Orders	dbo
Wiews       Region       dbo         Stored Procedures       Shippers       dbo         Users       Suppliers       dbo         Rules       syscolumns       dbo         Defaults       syscolumns       dbo         User Defined Data Types       sysfilegroups       dbo         User Defined Functions       sysfiles       dbo         Full-Text Catalogs       sysfiles1       dbo         3) Check permissions on table to ensure that only authorized individuals have required access. Document the findings.       dbo			Products	dbo
Stored Procedures       Shippers       dbo         Users       Suppliers       dbo         Roles       syscolumns       dbo         Rules       syscolumns       dbo         User Defaults       syscolumns       dbo         User Defined Data Types       dbo       sysfilegroups       dbo         User Defined Functions       sysfiles       dbo       sysfiles1       dbo         3) Check permissions on table to ensure that only authorized individuals have required access. Document the findings.       dbo       stational systems			📰 Region	dbo
Users       Suppliers       dbo         Roles       syscolumns       dbo         Rules       syscolumns       dbo         Defaults       syscolumns       dbo         User Defined Data Types       dbo       sysfilegroups       dbo         User Defined Functions       sysfiles       dbo         Full-Text Catalogs       sysfiles1       dbo         3) Check permissions on table to ensure that only authorized individuals have required access. Document the findings.		Stored Procedures	📰 Shippers	dbo
Roles       Rules       dbo         Rules       Defaults       dbo         User Defined Data Types       dbo         User Defined Functions       sysfilegroups       dbo         Full-Text Catalogs       sysfiles1       dbo         3) Check permissions on table to ensure that only authorized individuals have required access. Document the findings.       dbo			📰 Suppliers	dbo
Rules       Defaults       dbo         User Defined Data Types       User Defined Functions       dbo         User Defined Functions       Full-Text Catalogs       dbo         Sysfiles       dbo         Sysfiles       dbo         Image: Sysfiles       dbo         Systit       dbo<			🗐 syscolumns	dbo
<ul> <li>Defaults</li> <li>User Defined Data Types</li> <li>User Defined Functions</li> <li>Full-Text Catalogs</li> <li>Check permissions on table to ensure that only authorized individuals have required access. Document the findings.</li> </ul>			i syscomments	dbo
<ul> <li>3) Check permissions on table to ensure that only authorized individuals have required access. Document the findings.</li> </ul>			📰 sysdepends	dbo
<ul> <li>Full-Text Catalogs</li> <li>Full-Text Catalogs</li> <li>Sysfiles1</li> <li>Gate of the sysfiles1</li> <li>Check permissions on table to ensure that only authorized individuals have required access. Document the findings.</li> </ul>		🔤 🅵 User Defined Data Types	📰 sysfilegroups	dbo
<ol> <li>Check permissions on table to ensure that only authorized individuals have required access. Document the findings.</li> </ol>		- 🕵 User Defined Functions	📰 sysfiles	dbo
have required access. Document the findings.		Full-Text Catalogs	📰 sysfiles1	dbo
have required access. Document the findings.		3) Check permissions on table to	ensure that only authoriz	ed individuals
			•	
		601		
Auditor Notes	Auditor Notes			

### Check 14 – File Sharing/NetBIOS settings

Medina, Luis, Empirical Hacker – Protect your database series - part one, checklist item 10.
http://searchnetworking.techtarget.com/tip/1,289483,sid7_gci845040,00.html
Only SQL processes are allowed to run on the server.
Additional usage of the server would reduce the performance of the server.
This would impact availability of the server and introduce potential
vulnerabilities (such as vulnerabilities introduced by applications.)
Medium. Depends on server configuration.
If not restricted, the additional functionality could open various vulnerabilities
and slow access to the data.
Subjective. No shares other than those required are established (Please
note that some shares will be required for the system and some required

Expected test results	applications (e.g. Arcserve) to function properly).
Test performed to ensure compliance	Access a command prompt (Start Run cmd) and type net share. The resulting output will display all shares on the server. Redirect the output to a file and attach a screenshot to the report.
Auditor Notes	
Check 15 – Pa	atch Policies and Procedures

### Check 15 – Patch Policies and Procedures

Reference	SANS Ottawa Conference, D Hoelzer.
Control	Exposure to published vulnerabilities must be reduced.
Objective	<u> </u>
Risk	A lack of procedures and process can result in unpatched server.
Likelihood	Medium. Depends on the organization.
Consequence	If policies, guidelines and procedures do not exist, the server is at a high risk level due to a non-structured patch cycle.
System Compliance:	Subjective. Ensure the policy and procedures for patch maintenance exists. Check to see if the administrative staff follows the mandated procedures.
Test performed to ensure compliance	Request the policy and procedures for patching of the servers. Review the procedures to ensure that testing is being performed prior to deployment. Ensure that all file changes introduced by the patching process are documented and that a general timeline between the release of a patch and its implementation is dictated in the management policy.
Auditor Notes	

### Check 16 – Additional applications and services on server

Reference	Medina, Luis, Empirical Hacker – Protect your database series - part one, checklist item 6. <u>http://searchnetworking.techtarget.com/tip/1,289483,sid7_gci845040,00.html</u>
Control Objective	Only SQL processes are allowed to run on the server.
Risk	Applications can introduce vulnerabilities. Additional network ports may be

	T
	opened and introduce additional points of access for an attacker.
Likelihood	Medium. Depends on the server configuration.
Consequence	Additional applications and services can introduce additional security holes
	that may be used by an attacker to gain privileges.
System	Objective. Only SQL and its associated applications should exist on server.
Compliance /	
Expected test	
results	
Test	<ol> <li>Check Control Panel   Add/remove programs</li> </ol>
performed to	(Start Settings ControlPanel Add/Remove Programs). Document
ensure	applications found.
compliance	<ol><li>Run FPORT on the server to check for applications utilizing the</li></ol>
	network. Attach a screenshot to the report.
Auditor Notes	
Check 17 – Server Roles	

### Check 17 – Server Roles

Reference	SQL Server Security Checklist (item 18):
	http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4
	Microsoft SQL 2000 Security White paper (page 16)
	http://www.microsoft.com/sql/techinfo/administration/2000/2000SecurityWP.doc
Control	Users must be given least privilege to the data.
Objective	
Risk	Server roles can be used to elevate privilege. An attacker can embed their
	own account in a role in order to elevate their privilege.
Likelihood	Medium. Roles should be reviewed to ensure that members are given
	appropriate privilege.
Consequence	Server roles contain many associated rights. Attacker can elevate privilege by
	adding account to server role.
System	Subjective. Only authorized accounts should be assigned to roles. Only the
Compliance/	data owner can determine which accounts belong in a specific role.
Expected test	
results	
Test	1) Access SQL Enterprise Manager
performed to	(Start Programs MicrosoftSQLServer EnterpriseManager)
ensure	<ol><li>Select the server, choose security, then "server roles".</li></ol>
compliance	

	Action View Tools	× 🖅 🗗 🖪   😫  ] 米   🏠	💊 🗐 🚺 🗐
	Tree	Server Roles 8 Items	
	Console Root	Full Name 🔺	Name E
	Microsoft SQL Servers  SQL Server Group  SQL Server Group  Databases  Data Transformation Services  Management  Replication  Security  Logins  Linked Servers  Remote Servers  Remote Servers	Bulk Insert Administrators         Database Creators         Disk Administrators         Process Administrators         Security Administrators         Server Administrators         Setup Administrators         Setup Administrators         Setup Administrators         System Administrators	bulkadmin C dbcreator C diskadmin C processadmin C securityadmin C serveradmin C setupadmin C sysadmin C
	<ul> <li>Support Services</li> <li>Meta Data Services</li> <li>3) Double-click the individual roles i accounts listed as having member</li> <li>4) Interview the data owner to ensu the role membership.</li> </ul>	ership.	
Auditor Notes			

Check 18 – SQL Database Encryption

Reference	Microsoft SQL 2000 Security White paper (page 11)
	http://www.microsoft.com/sql/techinfo/administration/2000/2000SecurityWP.doc
Control	SQL database files should be encrypted to limit exposure.
Objective	
Risk	Databases stored in clear-text can be copied or opened by unauthorized
	individuals.
Likelihood	Medium. On-disk encryption is rarely implemented, however, due to the default
	permissions, regular users do not have access to the database directory by
G	default.
Consequence	An attacker can copy database files and access data at their leisure.
System	Objective. Encrypting File System (EFS) is enabled and the database files are
Compliance/	encrypted.
Expected test	
results	
Test	Access the location of the mdf files. Right click the directory and select
performed to	properties. In the folder properties window, select the advanced button.
ensure	Ensure the "encrypt contents to secure data" checkbox is checked. Document
compliance	the findings. Attach a screenshot to the report. The following screenshot

	displays what should be seen.
	Advanced Attributes       ? ×         Image: Choose the settings you want for this folder       When you apply these changes you will be asked if you want the changes to affect all subfolders and files as well.         Archive and Index attributes       ·         Image: Folder is ready for archiving       ·         Image: For fast searching, allow Indexing Service to index this folder         Compress or Encrypt attributes         Image: Compress contents to save disk space         Image: Compress to secure data         OK       Cancel
Auditor Notes	

# Check 19 – Network Protocol Libraries / On-The-Wire Encryption

Reference	SQL Server Security Checklist (item 2):
	http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4
	Microsoft SQL 2000 Security White paper (page 10)
	http://www.microsoft.com/sql/techinfo/administration/2000/2000Security
	WP.doc
Control	All data must be encrypted during transmission on network.
Objective	
Risk	An attacker can view passwords and sensitive data in clear-text.
Likelihood	Low. Due to the network using switches rather than hubs, there is a
	greater difficulty in "sniffing" the traffic between other clients and the
	SQL server.
Consequence	Sensitive information and SQL passwords can be stolen if information is
-	transmitted in a clear-text format.
System	Objective. Test proves that network encryption is enforced.
Compliance/	
Expected test	
results	
Test	
performed to	1) Access the SQL Enterprise Manager

ensure compliance	<ul> <li>(Start Programs MicrosoftSQLServer EnterpriseManager)</li> <li>2) Right click the server and select properties. Access the network configuration window at the bottom of the general tab.</li> <li>3) Select TCP/IP. Ensure "Force Protocol Encryption" checkbox is established. (The following screenshot shows what should be displayed.)</li> <li>SQL Server Network Utility</li> <li>General Network Libraries</li> </ul>
	Server <u>n</u> ame:
	Disabled protocols:     Enabled protocols:       Multiprotocol     Image: Constraint of the second
	Force protocol encryption
	Enable WinSock proxy     WinSock proxy address:     WinSock proxy port:
	OK Cancel Apply
	4) Document the findings and attach a screenshot to the report.
Auditor Notes	

### Check 20– Backup/Restore Procedures

Reference	Microsoft SQL 2000 Security White paper (page 56) http://www.microsoft.com/sql/techinfo/administration/2000/2000Security WP.doc		
Control Objective	System data must be archived and restore procedures must be known by staff.		
Risk	Loss of availability and integrity of data for a prolonged period of time. System recovery would be impossible if tapes are unavailable or unreadable.		
Likelihood	Medium, depending on organization.		
Consequence	If proper backup and restore procedures do not exist or are not followed,		
	a longer time for recovery will be required to restore functionality.		
--	--	--	--
System	Subjective. Tapes and documentation exist. Administrative staff follow		
Compliance/	procedures. The administrator was able to find the procedural		
Expected test	documentation and recent tapes. A test restoration was performed on		
results	the server. A tape rotation is in place that will allow for off-site storage of		
	archived data.		
Test performed to ensure compliance	Complete stimulus/response testing is not possible as performing a test restore on live server may adversely impact server availability. Document where tapes are being stored. Determine the last time a test recovery was performed. Verify that the recovery procedure documentation exists. Determine if the tape rotation is in use by verifying labels on tapes to ensure a rotation is established. Determine if the tapes are held off-site.		
Auditor Notes	e S		
Check 21 – Physical Security of Server			

# Check 21 – Physical Security of Server

Reference	Microsoft SQL 2000 Security White paper (page 59) http://www.microsoft.com/sgl/techinfo/administration/2000/2000Security
	<u>WP.doc</u>
	SQL Server Security Checklist (item 15):
	http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4
Control Objective	All servers must be placed in physically secured location.
Risk	Ease of attack if physical access to the server is gained. Accidental loss of availability through unintentional or intentional physical damage. Elevated risk of theft.
Likelihood	Intentional attack is low. Only employees have access to the corporate premises. Loss of availability is ranked as medium to high if the server is located in an unsecured location.
Consequence	Potential loss of availability and confidentiality.
System Compliance:	Objective. The server is in access-controlled environment.
Test performed to ensure compliance	Manually verify location of the server. If the server is in a separate room, check for a lock on the door and determine who has access to room. Document the findings in the report.
Auditor Notes	

# Assignment 3: Conduct the audit

#### Audit 1 - Service Pack and Hot Fix levels

Reference	Search on ICAT Metabase for known SQL Server 2000 vulnerabilities: http://icat.nist.gov
	Microsoft Baseline Security Analyzer (MBSA) homepage (information and download link):
	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/secu rity/tools/Tools/MBSAhome.asp
Control Objective	Exposure to published vulnerabilities must be reduced.
Risk	If not patched, the server is at an elevated risk level of attack against published vulnerabilities. Server can be exploited via scripts that exist to use vulnerabilities imposed through the lack of a proper patching.
Likelihood	High from external sources if server is accessible or if the firewall is compromised.
Consequence	Attacks can range from a denial of service (Availability) to information disclosure (Confidentiality) and manipulation of data (Integrity)
System Compliance/ Expected Results	The test results are objective. All relevant patches for the system must be installed. The MBSA must state there are no hotfixes missing on the server
Test performed to ensure compliance	<ul> <li>Scan SQL Server from MBSA</li> <li>1) From the auditor's workstation with Internet access, obtain and run Microsoft Baseline Security Analyzer (MBSA). (Start Programs MBSA).</li> <li>2) Select "scan a computer", enter the name or IP address of the server.</li> </ul>

	🚱 Microsoft Baseline Security Analyzer
	Microsoft Baseline Security Analyzer
	Microsoft Baseline Security Analyzer         Welcome         Pick a computer to scan         Pick a computer to scan         Pick a security report to view         View a security report         Welcome         Microsoft Baseline Security Analyzer         Microsoft Baseline Security web site
Actual Results	<ul> <li>© 2002 Microsoft Corporation. All rights reserved.</li> <li>3) Ensure that SQL component will be analyzed. Select start scan.</li> <li>4) The application will download the latest vulnerabilities from Microsoft. Accept the download of the xml file.</li> <li>5) The MBSA will now scan the server to determine any missing patches and other configuration information. Save the report as evidence. Affix screenshot of the SQL Server Hotfixes discovery to actual results section of checklist</li> <li>SQL Server Scan Results</li> </ul>
	Score Issue Result
	SQL Server Hotfixes         5 hotfixes are missing or could not be confirmed.           What was scanned         Result details           Hours         What was scanned
Auditor Notes / Test Results	Fail. The MBSA has determined that 5 hotfixes are missing from the server. After discussions with the administrator, it was discovered the patches are currently under review and are slated for implementation within two weeks.

# Audit 2 – Stored Procedures

Reference	SQL Server Security Checklist (item 6): http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4
Control Objective	Access to operating system level commands must be removed or restricted to privileged accounts.
Risk	Stored procedures can be used as a means to attack corporate systems. An attacker who has access to certain stored procedures can use them

	to attack the underlying operating system (e.g. Attacker using			
	xp_cmdshell to delete critical files or			
Likelihood	Medium. Stored procedure function	ality ranges from s	imple data queries	
	to enhanced shell access to the ope	rating system and	internal network at	
	an O/S level.	0,		
Consequence	Use of a stored procedure such as xp_cmdshell can grant an attacker			
Concequence	complete control of the operating sy			
System			m ganaral usaga	
	Subjective. Stored procedures should be restricted from general usage			
Compliance/	where possible. Xp_cmdshell should be removed from the server unless			
Expected	it is required.			
Results				
Test	Check for existence of stored proce	dures and which pe	ermissions are	
performed to	assigned. To check the stored proc			
ensure	1) Access the SQL Enterprise M			
	(Start Programs MicrosoftSQ		Managor)	
compliance		· · ·	<b>U</b> ,	
	2) Expand the SQLServerGroup			
	3) Select the Databases tab, the			
1	<ol><li>Select "stored procedures" ar</li></ol>	nd "extended store	d procedures"	
	container.			
	Tree	Extended Stored Procedures	173 Items	
	Tree Console Root	Extended Stored Procedures	173 Items Owner	
	Console Root	Name A	Owner dbo	
	Console Root Microsoft SQL Servers Group	Name △ Sp_bindsession Sp_createorphan	Owner dbo dbo	
	Console Root Microsoft SQL Servers SQL Server Group Constant SQL Server Group Constant SQL Server Group	Name A	Owner dbo dbo dbo	
	Console Root Microsoft SQL Servers Group	Name A Sp_bindsession Sp_createorphan Sp_cursor Sp_cursor Sp_cursorclose	Owner dbo dbo dbo dbo dbo	
	Console Root Microsoft SQL Servers SQL Server Group (Windows NT) The Databases	Name A Sp_bindsession Sp_createorphan Sp_cursor Sp_cursor Sp_cursorclose Sp_cursorexecute	Owner dbo dbo dbo	
	Console Root Microsoft SQL Servers SQL Server Group (Windows NT) Constant SQL Windows NT) Constant SQL Microsoft SQL (Windows NT) Constant SQL Microsoft SQL (Windows NT) Constant SQL Microsoft SQL Microsoft SQL (Windows NT) Constant SQL Microsoft SQL Microsoft SQL (Windows NT) Constant SQL Microsoft SQL Micros	Name A Sp_bindsession Sp_createorphan Sp_cursor Sp_cursor Sp_cursorclose	Owner dbo dbo dbo dbo dbo dbo	
	Console Root Microsoft SQL Servers SQL Server Group (Windows NT) Console Root SQL Server Group (Windows NT) Console Root SQL Server Group (Windows NT) Console Root SQL Server Group (Windows NT) Console Root SQL Server Group (Windows NT) Console Root (Windows NT) (Windows NT) (	Name Sp_bindsession Sp_createorphan Sp_cursor Sp_cursorclose Sp_cursorexecute Sp_cursorexecute Sp_cursorfetch	Owner dbo dbo dbo dbo dbo dbo	
	Console Root Microsoft SQL Servers SQL Server Group (Windows NT) Databases master Tables 	Name Sp_bindsession Sp_createorphan Sp_cursor Sp_cursorclose Sp_cursorexecute Sp_cursoretech Sp_cursoropen Sp_cursoropen Sp_cursoroption	Owner dbo dbo dbo dbo dbo dbo dbo	
	Console Root Microsoft SQL Servers SQL Server Group (Windows NT) Console Root SQL Server Group (Windows NT) Console Root SQL Server Group (Windows NT) Console Root SQL Server Group (Windows NT) Console Root SQL Server Group (Windows NT) Console Root (Windows NT) (Windows NT) (	Name Sp_bindsession Sp_createorphan Sp_cursor Sp_cursorclose Sp_cursorexecute Sp_cursoretch Sp_cursorpen Sp_cursoropen Sp_cursoroption Sp_cursorprepare Sp_cursorp	Owner dbo dbo dbo dbo dbo dbo dbo dbo dbo dbo	
	Console Root Microsoft SQL Servers SQL Server Group (Windows NT) Databases	Name       A         Image: Sp_bindsession       Sp_createorphan         Image: Sp_cursor       Sp_cursor	Owner dbo dbo dbo dbo dbo dbo dbo dbo dbo dbo	
	Console Root Microsoft SQL Servers SQL Server Group (Windows NT) Databases Tables - 0 Stored Procedures Extended Stored Procedur Rules Rules	Name N	Owner dbo dbo dbo dbo dbo dbo dbo dbo dbo dbo	
	Console Root Microsoft SQL Servers SQL Server Group (Windows NT) Databases Tables - Tables - Tables - Tables - Console Root - Consol	Name A Sp_bindsession Sp_createorphan Sp_cursor Sp_cursorexecute Sp_cursorexecute Sp_cursoropen Sp_cursoropen Sp_cursoroption Sp_cursorprepare Sp_cursoruprepare Sp_cursoruprepare Sp_cursoruprepare Sp_cursoruprepare Sp_cursoruprepare Sp_cursoruprepare Sp_cursoruprepare Sp_cursoruprepare Sp_cursoruprepare Sp_cursoruprepare Sp_cursoruprepare Sp_cursoruprepare Sp_cursoruprepare Sp_cursoruprepare Sp_cursoruprepare	Owner dbo dbo dbo dbo dbo dbo dbo dbo dbo dbo	
	Console Root Microsoft SQL Servers SQL Server Group (Windows NT) Databases Tables - Tables - Tables - Tables - Console Root Windows NT) - Tables - Console Root -	Name N	Owner dbo dbo dbo dbo dbo dbo dbo dbo dbo dbo	
	Console Root Microsoft SQL Servers SQL Server Group (Windows NT) Databases Tables - Tables - Tables - Tables - Console Root - Consol	Name       A         Image: Sp_bindsession       Sp_createorphan         Image: Sp_cursor       Sp_cursor	Owner dbo dbo dbo dbo dbo dbo dbo dbo dbo dbo	
	Console Root Microsoft SQL Servers SQL Server Group (Windows NT) Databases Tables 	Name Name Sp_bindsession Sp_createorphan Sp_cursor Sp_cursorexecute Sp_cursorexecute Sp_cursorpen Sp_cursorpen Sp_cursorprepare Sp_cursorpre	Owner dbo dbo dbo dbo dbo dbo dbo dbo dbo dbo	
	Console Root Microsoft SQL Servers SQL Server Group (Windows NT) Databases Tables Gar Views Stored Procedures Extended Stored Procedur Rules Defaults User Defined Data Types User Defined Data Types Suser Defined Functions Full-Text Catalogs model Tables Tables Tables Tables Stored Procedures Tables Tables Stored Procedures Tables Stored Procedures Tables Tables Stored Procedures Tables Stored Procedures Microsoft Stored Procedures Tables Stored Procedures Tables Stored Procedures Tables Stored Procedures Tables Stored Procedures Tables Stored Procedures Tables Stored Procedures Tables Stored Procedures Stored Procedures St	Name       A         Image: Sp_bindsession       Sp_createorphan         Image: Sp_cursor       Sp_cursor         Image: Sp_cursor       Sp_cursorexecute         Image: Sp_cursorexecute       Sp_cursorexecute         Image: Sp_cursorexecute       Sp_cursoropen         Image: Sp_cursoropen       Sp_cursoropen         Image: Sp_cursorprepare       Sp_cursorprepare         Image: Sp_cursorunprepare       Sp_cursorunprepare         Image: Sp_execute       Sp_executesql         Image: Sp_getbindtoken       Sp_getbindtoken         Image: Sp_getschemalock       Sp_getschemalock	Owner       dbo	
	Console Root Microsoft SQL Servers SQL Server Group (Windows NT) Databases Database	Name       A         Image: Sp_bindsession       Sp_createorphan         Image: Sp_cursor       Sp_cursor         Image: Sp_cursor       Sp_cursorexecute         Image: Sp_cursorexecute       Sp_sp_cutexecute         Image: Sp_sp_sp_sp_sp_sp_sp_sp_sp_sp_sp_sp_sp_sp	Owner dbo dbo dbo dbo dbo dbo dbo dbo dbo dbo	
	Console Root Microsoft SQL Servers SQL Server Group (Windows NT) Databases Tables Grave Stored Procedures Extended Stored Procedures Rules Defaults User Defined Data Types Stored Functions Full-Text Catalogs model Stored Procedures Northwind pubs	Name       A         Sp_bindsession       sp_createorphan         sp_cursor       sp_cursor         sp_cursor       sp_cursorexecute         sp_cursorexecute       sp_cursorexecute         sp_cursoropen       sp_cursoropen         sp_cursorprepare       sp_cursorprepare         sp_cursorprepare       sp_cursorunprepare         sp_cursorunprepare       sp_droporphans         sp_cursorunprepare       sp_dexecute         sp_cursorunprepare       sp_dexecute         sp_cursorunprepare       sp_dexecute         sp_cursorunprepare       sp_dexecute         sp_cursorunprepare       sp_dexecute         sp_cursorunprepare       sp_dexecute         sp_dexecute       sp_dexecute         sp_dexecute       sp_sp_dexecute         sp_fulltext_getdata       sp_sp_detindtoken         sp_getschemalock       sp_jestschemalock         sp_jsymbol       sp_MSgetversion	Owner       dbo	
	Console Root Microsoft SQL Servers SQL Server Group (Windows NT) Databases Database	Name       A         Sp_bindsession       Sp_createorphan         Sp_cursor       Sp_cursor         Sp_cursor       Sp_cursorexecute         Sp_cursorexecute       Sp_cursorexecute         Sp_cursoropen       Sp_cursoropen         Sp_cursorprepare       Sp_cursoruprepare         Sp_cursorprepare       Sp_cursoruprepare         Sp_cursoruprepare       Sp_cursoruprepare         Sp_cursoruprepare       Sp_droporphans         Sp_sp_execute       Sp_execute         Sp_fulltext_getdata       Sp_GetMBCSCharLen         Sp_getschemalock       Sp_JSMBCSLeadByte         Sp_OACreate       Sp_OACreate	Owner       dbo       dbo	
	Console Root Microsoft SQL Servers SQL Server Group (Windows NT) Databases Tables Gar Views Stored Procedures Extended Stored Procedures Rules Defaults User Defined Data Types Susr Defined Functions Full-Text Catalogs Tothwind Dubs Let Dubs Let Dubs	Name Name Sp_bindsession Sp_createorphan Sp_cursor Sp_cursor Sp_cursorexecute Sp_cursorpece Sp_cursorpen Sp_cursorpepare Sp_cursorprepare Sp	Owner       dbo       dbo	
	Console Root Microsoft SQL Servers SQL Server Group (Windows NT) Databases Tables Gar Views Stored Procedures Extended Stored Procedure Rules Defaults User Defined Data Types Susr Defined Functions Full-Text Catalogs Tothwind Dubs Tothwind Dubs Tempdb Data Transformation Services	Name       A         Sp_bindsession       Sp_createorphan         Sp_cursor       Sp_cursor         Sp_cursor       Sp_cursorexecute         Sp_cursorexecute       Sp_cursorexecute         Sp_cursoropen       Sp_cursoropen         Sp_cursorprepare       Sp_cursoruprepare         Sp_cursorprepare       Sp_cursoruprepare         Sp_cursoruprepare       Sp_cursoruprepare         Sp_cursoruprepare       Sp_droporphans         Sp_sp_execute       Sp_execute         Sp_fulltext_getdata       Sp_GetMBCSCharLen         Sp_getschemalock       Sp_JSMBCSLeadByte         Sp_OACreate       Sp_OACreate	Owner       dbo       dbo	
	Console Root Microsoft SQL Servers SQL Server Group (Windows NT) Databases Tables Grave Views Stored Procedures Extended Stored Procedures Rules Defaults User Defined Data Types Suser Defined Data Types Suser Defined Functions Full-Text Catalogs Tothwind Data Transformation Services Management	Name       A         Image: Sp_bindsession       Sp_createorphan         Image: Sp_cursor       Sp_cursor         Image: Sp_cursor       Sp_cursor         Image: Sp_cursor       Sp_cursorexecute         Image: Sp_cursorexecute       Sp_cursorexecute         Image: Sp_cexecute       Sp_sp_cexecute         Image: Sp_execute       Sp_sp_execute         Image: Sp_execute       Sp_sp_execute         Image: Sp_execute       Sp_sp_execute         Image: Sp_execute       Sp_sp_execute         Image: Sp_getschemalock       Sp_sp_execute         Image: Sp_OACreate       Sp_OACreate         Image: Sp_OACetErrorInfo       Sp_OACeterrorInfo	Owner       dbo       dbo	
	Console Root Microsoft SQL Servers SQL Server Group (Windows NT) Databases Tables Grave Views Stored Procedures Extended Stored Procedures Rules Defaults User Defined Data Types Suser Defined Data Types Suser Defined Functions Full-Text Catalogs Tothwind Data Transformation Services Management	Name       A         Image: Sp_bindsession       Sp_createorphan         Image: Sp_cursor       Sp_cursor         Image: Sp_cursor       Sp_cursor         Image: Sp_cursor       Sp_cursorexecute         Image: Sp_cursorexecute       Sp_cursorexecute         Image: Sp_cexecute       Sp_sp_cexecute         Image: Sp_execute       Sp_sp_execute         Image: Sp_execute       Sp_sp_execute         Image: Sp_execute       Sp_sp_execute         Image: Sp_execute       Sp_sp_execute         Image: Sp_getschemalock       Sp_sp_execute         Image: Sp_OACreate       Sp_OACreate         Image: Sp_OACetErrorInfo       Sp_OACeterrorInfo	Owner       dbo       dbo	

	tended Stored Pro General   Name: <u>P</u> ath:	xp_cmdshell	- xp_cmdshell	
-	Laur	OK	Cancel Help	
sp_s xp_a xp_c xp_d	leexist didebug vailablemedia mdshell eletemail irtree		xp_readerrorlog xp_readmail xp_revokelogin xp_runwebtask xp_schedulersignal xp_sendmail	
xp_d				

	Sp_OADestroy Sp_OASetProperty SP_OAStop, Xp_ regaddmultistring
	6) Stimulus/Response test: Open Query Analyzer (Start Programs MicrosoftSQLServer QueryAnalyzer). Logon when prompted. Type xp_cmdshell 'dir c:\*.evt /s' in query window. Select run (circled in red in following screenshot).          Image: Sol Query Analyzer         Image: Sol Query Indox Help         Image: Sol Query Indox Help <t< th=""></t<>
	<ul> <li>7) Document the findings and attach a screenshot to the report. This test will prove if xp_cmdshell is still present on the server.</li> </ul>
Actual Results	All of the stored procedure permissions on the server are at a default value. Public (e.g. everyone) has access to many of the stored procedures. Permissions: xp_cmdshell: Guest and public: None listed xp_fileexist: Guest: None Public: Checked sp_sdidebug: Guest and public: None listed
	xp_availablemedia Guest and public: None listed xp_deletemail Guest and public: None listed xp_dirtree Guest: None Public: Checked xp_dropwebtask Guest and public: None listed xp_dsninfo Guest and public: None listed xp_enumdsn Guest and public: None listed xp_enumerrorlogs Guest and public: None listed xp_enumgroups Guest and public: None listed

xp\_eventlog Guest and public: None listed xp\_fixeddrives Guest: None Public: Checked xp getfiledetails Guest: None Public: Checked xp\_getnetname Guest: None Public: Checked xp grantlogin Guest: None Public: Checked xp\_logevent Guest and public: None listed xp\_loginconfig Guest and public: None listed xp\_logininfo Guest and public: None listed xp\_makewebtask Guest and public: None listed xp\_msver Guest: None Public: Checked Sp OACreate Guest and public: None listed sp\_OAGetErrorInfo Guest and public: None listed Sp OAGetProperty Guest and public: None listed Sp\_OAMethod Guest and public: None listed Sp OADestroy Guest and public: None listed Sp OASetProperty Guest and public: None listed SP OAStop, Guest and public: None listed Xp regaddmultistring Guest and public: None listed xp\_readerrorlog Guest and public: None listed xp readmail Guest and public: None listed xp revokelogin Guest: None Public: Checked xp\_runwebtask Guest and public: None listed xp sendmail Guest and public: None listed xp servicecontrol Guest and public: None listed xp sprintf Guest: None Public: Checked xp sscanf Guest: None Public: Checked xp startmail Guest and public: None listed xp stopmail Guest and public: None listed xp\_subdirs Guest and public: None listed xp unc to drive Guest: None Public: Checked Xp\_regdeletekey Guest and public: None listed Xp\_regdeletevalue Guest and public: None listed Xp regenumvalues Guest and public: None listed Xp regread Guest: None Public: Checked Xp\_regremovemultistring Guest and public: None listed Xp regwrite Guest and public: None listed The following is a screenshot of the findings for the sp runwebtask stored procedure. For brevity purposes, the remaining screenshots have been omitted from this document.

	ee Stored Proc Stored Procedure Properties - sp_runwebtask
	Console Root
	Microsoft SQL Servers
	B E (Windows NT)
	Diperties - master
	Permissions Permissions
	) Tables God Views Object: Sp_runwebtask (dbo)
	Stored Procedures
	Roles 💿 List all users/user-defined database roles/public
	Rules     List only users/user-defined database roles/public with permissions on this object.
	User Defined Data 1 Users/Database Roles/Public SELECT INSERT UPDATE DELETE EXEC DRI
	Full-Text Catalogs
	Tables
	Gor' Views
	Extended Stored Pr
	Users
	In order to ensure that xp_cmdshell is still installed on the server, the
	query analyzer was opened and a test of the stored procedure was
	performed.
	🗰 Query -
	xp cmdshell 'dir c:\*.evt /s'
	•
	output
G	4 Directory of c:\WINNT\system32\config
	5 NULL
	6 262,144 AppEvent.Evt
	7 65,536 SecEvent.Evt
	8 65,536 SydEvent.Evt
Auditor Notes	Fail. Any changes made will be required to be performed on a test
/ Test Results	server to ensure functionality after changes have been implemented. An
	analysis should be performed for system stability in the event a
	procedure is dropped and the DLL removed; alternatively, tests should

roles.

#### Audit 3 – Authentication Model

Reference	Microsoft SQL 2000 Security White paper (page 15) http://www.microsoft.com/sql/techinfo/administration/2000/2000Security WP.doc	
Control Objective	A single account database should be implemented for both operating system and SQL server.	
Risk	Standard SQL authentication introduces a multitude of weaknesses (blank SA passwords, passwords left in install log files, password crackers, cleartext transmission, lack of built-in password restrictions and lockouts). This opens many opportunities for a savvy attacker to find a way into the server.	
Likelihood	High. Many systems have the SQL authentication model in place for functionality or due to the lack of awareness.	
Consequence	Potential loss of confidentiality if an attacker gains access to the server via one of the many vulnerabilities.	
System Compliance/ Expected Test Results	Objective. Test must prove Windows authentication is in place.	
Test performed to ensure compliance	<ul> <li>Check to ensure that only Windows authentication is used.</li> <li>1) Access the enterprise manager (Start Programs MicrosoftSQLServer EnterpriseManager)</li> <li>2) Right click server name, select properties</li> <li>3) Open security tab. This will display the authentication mode in use (The following screenshot shows what screen should be seen). Document the setting and capture a screenshot of the server settings.</li> </ul>	
	Server Settings       Database Settings       Replication         General       Memory       Processor       Security         Security       SQL Server provides authentication based on Windows accounts and a named SQL Server login ID and password.         Authentication:       SQL Server and Windows         Image: SQL Server and Windows       Image: SQL Server and Windows	

	Stimulus/Response test
	4) Open Query Analyzer
	(Start Programs MicrosoftSQLServer QueryAnalyzer).
	5) Enter SA account as username. Leave password as blank (the
	error returned will prove if SQL authentication is disabled (non
	trusted account) or a bad password was entered (incorrect
	password)).
	Connect to SQL Server
	SQL Server:
	☐ Start SQL Server if it is stopped
	Connect using:
	C <u>Windows authentication</u>
	© S@L Server authentication
	Login name:
	Password:
	OK Cancel Help
	6) Document the results. Capture a screenshot and attach to the
	report.
Actual	Only Windows Authentication has been implemented on the server. The
Results	following screenshots confirm settings.

	SQL Server Properties (Configure) -
	Server Settings Database Settings Replication
	General Memory Processor Security Connections
	Security
	SQL Server provides authentication based on Windows accounts and a named SQL Server login ID and password.
	Authentication:
	© SQL Server and Windows © Windows only
	Audit level:
	C None C Failure
	C Success C All
	Startup service account
	Start and run SQL Server in the following account:
	System account
	Ihis account     Inis account
	Password:
	To further test the authentication model, a logon to a query analyzer
	resulted in the following error message:
	SQL Query Analyzer 🛛 🔀
	Unable to connect to server .:
	Server: Msg 18452, Level 16, State 1 [Microsoft][ODBC SQL Server Driver][SQL Server]Login failed for user 'sa'. Reason: Not associated with a trusted SQL Server connection.
C	The above shows that SQL logins are not allowed on the server. When SQL logins are allowed but an incorrect password is given, an error
Auditor Notes	stating such is shown to the user. Pass. The server has Windows Authentication established and
/ Test Results	stimulus/response tests have proven that an attempt to logon with a SQL
	account fails with an error stating that Windows Authentication is in place.

#### Audit 4 – Audit Activity on server

Reference	SQL Server books online ("auditing SQL Server activity" as a search parameter).
Control	Audit logs of all actions taken on SQL server must be kept.
Objective	
Risk	A lack of auditing will result in an inability to know when a breach has occurred. This will allow an attacker to access the system and perform malicious activities with little chance of being detected.
Likelihood	High. By default, auditing is not enabled in SQL server.
Consequence	If trace is not enabled, a log of activity will not be maintained.
System Compliance/ Expected Test Results	Objective. Trace template created and logs exist to document activity on the server
Test performed to ensure compliance	<ul> <li>Request location of the trace template and template files or table from the administrator. Access SQL profiler. Open the trace template and logs to ensure tracing is enabled and is monitoring activity on the server.</li> <li>To access the required settings and files, Access trace template</li> <li>1) Open SQL profiler <ul> <li>(Start Programs MicrosoftSQLServer Profiler).</li> </ul> </li> <li>2) Select File Open TraceTemplate. Select template given by administrator. Once open, select "Events" tab.</li> </ul>

	Trace Template Properties		×
	General Events Data Columns	Filters	
	Select the SQL Server a	event classes you want to trace.	
	A <u>v</u> ailable event classes:	<u>S</u> elected even	it classes:
	<ul> <li>Cursors</li> <li>Database</li> <li>Errors and Warnings</li> <li>Locks</li> <li>Objects</li> <li>Performance</li> <li>Scans</li> <li>Security Audit</li> <li>Stored Procedures</li> <li>Transactions</li> </ul>	Add >> Audit Audit Audit Audit Audit Audit Audit Audit Audit Audit	Add DB User Ev Add Login to Ser Add Member to [ Addlogin Event App Role Chang Change Audit Ev
	Cursors Collection of events produced a	when cursors are created, used and d	leleted.
lt	ems that must be enabled a	re as follows. Document	any deviations
	Add DB User Event Add Login to Server Add Login to Server Role Add Member to DB Role Add Login App Role Change Password Change Audit Add Login Change Add Log		
	<ul> <li>Verify Trace Results</li> <li>3) Select File Open Trace storage of traces given of trace files or trace te</li> <li>4) Open trace and check</li> </ul>	n by administrator). Point emplate.	to the location

Actual Results	Proper trace templates were found to exist on the server in a trace template file named acmetemplate.trc. However, no trace files or trace tables were found to exist on the server. The following is a screenshor of the actual trace template that was discovered during the audit. Trace Template Properties General Events Data Columns Filters Select the SQL Server event classes you want to trace.
	Available event classes:       Selected event classes:                • Database             • Database             • Locks             • Objects             • Performance             • Scans             • Security Audit             • Security Audit             • Server             • Stored Procedures             • Transactions             • Cursors             Collection of events produced when cursors are created, used and deleted.              • Security and teleted.
	Fail. Automated auditing of the server has not been established.

# Audit 5 – Logon Auditing

Reference	Microsoft SQL 2000 Security White paper (page 54) http://www.microsoft.com/sql/techinfo/administration/2000/2000Security WP.doc
Control	All system access must be logged.
Objective	
Risk	A lack of tracing which accounts are failing logon attempts. If not established, an attacker can attempt a brute force attack on the server and no evidence of the attack will be available.
Likelihood	High. Auditing of server logon attempts is not enabled by default.
Consequence	If not configured, no failed logon detection is possible.
System	Objective. Logging of failed SQL logins is turned on (the default setting

Compliance/	is off.)
Expected	
Test Results	
Test performed to ensure compliance	<ul> <li>Ensure logon audit level for SQL server is set to all.</li> <li>1) Access the enterprise manager (Start Programs MicrosoftSQLServer EnterpriseManager)</li> <li>2) Right click the server name, select properties</li> <li>3) Open the security tab. This will display the audit level in place (The following screenshot shows what options should be selected). Document the settings and capture a screenshot of the server settings.</li> </ul>
	SQL Server Properties (Configure) -
	Server Settings       Database Settings       Replication         General       Memory       Processor       Security       Connections         Security       SQL Server provides authentication based on Windows accounts and a named SQL Server login ID and password.       Authentication:       SQL Server and Windows         Windows only       Windows only       Windows only       Windows only         Audit Tevel:       Success       Authentication:       Stimulus/Response Test:         4)       Access Query Analyzer (Start Programs MicrosoftSQLServer QueryAnalyzer)       Stimulus/Response Test:         5)       At the logon prompt, select SQL authentication. Attempt to logon to server with user account SA and a blank password.         6)       At the logon prompt, select Windows authentication. Attempt to logon to server.         7)       Access the application log in Event Viewer (Start Programs AdministrativeTools EventViewer). Open log entries that show attempted logons (event 17055 shows all successful and failed logon attempts). Document findings and attach screenshots to report.
Actual Results	Auditing has been established on the server to audit all logon attempts (both success and failure). The following screen shows logon auditing is enabled.

		onfigure) -			×
	Settings	Database S		Replication	
General	Memory	Processor	Security	Connections	4
Security	SQL Server	provides authenti id a named SQL (			
	Authenticatio	on:			
		Server and Wind	ows		
		lows only			
	Audit level				
			○ <u>F</u> ailure		
	O Succ	ess	• Aļ		
Startup	service accoun				
386	Start and run	n SQL Server in th	ne following acc	ount:	
3 <u>6</u> 7	O Syste	em account			
	⊙ <u>T</u> his a	account	sqlservic	e	
	Pass	word:	******	(X	
	T_200.				
	<u>-</u>		,		
		- <u></u>			
	attempt to	) logon to qu		zer with a So	
performed	attempt to	) logon to qu		zer with a So ted in the so	
	attempt to	) logon to qu			
performed event log: Event Prope	attempt to and the fo	) logon to qu			erve
event log:	attempt to and the fo	) logon to qu ollowing fail	ure was no	oted in the so	erve
performed event log: Event Prope	attempt to and the fo	) logon to qu ollowing fail		oted in the so	erve
Event Proper Event Proper Event Date: Time: Type: User: Computer: Description	attempt to and the fo	) logon to qu ollowing fail Source: MSSQ Category: (4)	ure was no	oted in the se	erve
Event log: Event Proper Event Date: Time: Type: User: Computer: Descriptior 18452 :	attempt to and the fo	) logon to qu ollowing fail Source: MSSQ Category: (4)	LSERVER	eted in the second control of the second con	erve
Event log: Event log: Event log: Event log: Date: Time: Type: User: Computer: Description 18452 : Login faile Server co	attempt to and the fo	logon to qu ollowing fail Source: MSSQ Category: (4) Event ID: 17055	LSERVER	eted in the second control of the second con	erve
Event log: Event Proper Event Date: Time: Type: User: Computer: Description 18452 : Login faile Server co	attempt to and the for ties	b logon to qu bllowing fail Source: MSSQ Category: (4) Event ID: 17055 Reason: Not assoc	LSERVER	eted in the second control of the second con	erve
Event log: Event log: Event log: Event log: Date: Time: Type: User: Computer: Description 18452 : Login faile Server co Data: Coon: 1 0000: 1 0000: 1 0000: 5	attempt to and the for ties	b logon to qu bllowing fail Source: MSSQ Category: (4) Event ID: 17055 Reason: Not associ ds 0e 00 00 00 4a 00 49 00 4a 00 49 00	LSERVER	eted in the set ? >	erve
Derformed event log: Event Proper Event Date: Time: Type: User: Computer: Description 18452 : Login faile Server co	attempt to and the fo	Iogon to quot           Source:         MSSQ           Category:         (4)           Event ID:         17055           Reason:         Not assoc           0=         00         00           44         00         49         00           53         00         51         00           73         00         74         00	LSERVER	eted in the set ? > ted SQL	erve
Derformed event log: Event Proper Event Date: Time: Type: User: Computer: Description 18452 : Login faile Server co	attempt to and the for ties	Iogon to quot           Source:         MSSQ           Category:         (4)           Event ID:         17055           Reason:         Not assoc           0=         00         00           44         00         49         00           53         00         51         00           73         00         74         00	LSERVER	eted in the set ? >	erve

A va	alid access was noted as follows in the event log:
Ever	nt Properties ? X
Ev	/ent
	Date: Source:
1	Fime: Category: (4)
1	Гуре: Information Event ID: 17055
<u>l</u>	Lser:
<u>(</u>	Computer:
	Description:
	18453 :
	Login succeeded for user ' '. Connection: Trusted.
, , , , , , , , , , , , , , , , , , ,	
[	Da <u>t</u> a: 💿 <u>B</u> ytes 🔿 <u>W</u> ords
	0000: 15 48 00 00 0e 00 00 00 .H
	0008: 08 00 00 00 4d 00 49 00 0010: 57 00 2d 00 53 00 51 00
	0018: 4c 00 00 00 07 00 00 00 🔍
	0020: 6d 00 61 00 73 00 74 00 m.a.s.t. 0028: 65 00 72 00 00 00 e.r
	0028: 65 00 72 00 00 00 e.r
	OK Conset
	OK Cancel Apply
	s. Auditing is established properly.
/ Test Results	

# Audit 6 – SQL Service start-up accounts

Reference	Microsoft SQL 2000 Security White paper (page 51) <u>http://www.microsoft.com/sql/techinfo/administration/2000/2000Security</u> <u>WP.doc</u> SQL Server Security Checklist (item 4): <u>http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&amp;tabid=4</u>
Control	The SQL service must be assigned a user level start-up account
Objective	
Risk	Excessive rights assigned to SQL service.
Likelihood	Medium. Depends on the server configuration
Consequence	These rights can be used by an attacker to increase their privilege on
	the server and network
System	Objective. MSSQLSERVER service must start as a user level account.

Compliance/ Expected test	
results Test performed to ensure compliance	<ul> <li>Check service startup account in enterprise manager.</li> <li>1) Access the enterprise manager (Start Programs MicrosoftSQLServer EnterpriseManager)</li> <li>2) Right click the server name, select properties.</li> <li>3) Open the security tab. This will display the startup account in place (The following screenshot shows what options should be selected). Document the settings and capture a screenshot of the server settings.</li> </ul>
	Server Settings       Database Settings       Replication         General       Memory       Processor       Security       Connections         Security       SQL Server provides authentication based on Windows accounts and a named SQL Server login ID and password.       Authentication:       SQL Server and Windows         SQL Server and Windows       SQL Server and Windows       Equip SQL Server and Windows       Equip SQL Server and Windows         Windows only       Audit level:       Equip Square       Equip Square
	Success       All         Startup service account       Start and run SQL Server in the following account:         System account       System account         Ihis account       Password:
	<ul> <li>4) Access Windows users and groups settings (Start Programs AdministrativeTools ComputerManagement  LocalUsersAndGroups). Double-click the users tab. Double click the service account name. Check the group membership. Document and attach a screenshot to the report.</li> <li>5) Access Services window (Start Settings ControlPanel AdministrativeTools Services). Access MSSQLServer service by double-clicking the service. Access the logon tab. Confirm which account is being used to start the service. Document the account and attach a screenshot to the report.</li> </ul>



MSSQLSERVER Properties (Local Computer)
General Log On Recovery Dependencies
Log on as:         Local System account         Allow service to interact with desktop         This account:       .\sqlservice         Password:       ************************************
You can enable or disable this service for the hardware profiles listed below:          Hardware Profile       Service         Profile 1       Enabled
OK Cancel Apply As the screenshot shows, the SQL service is starting under the
sqlservice user account.
Pass. The server is configured to start with the context of a standard user.

# Audit 7 – Guest user access

Reference	SQL Server Security Checklist (item 8):
	<u>http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&amp;tabid=4</u>
	Microsoft SQL 2000 Security White paper (page 58)
	http://www.microsoft.com/sql/techinfo/administration/2000/2000Security
	WP.doc
Control	Only authenticated accounts may access the SQL server.
Objective	
Risk	Non-authenticated users have access to a database through the guest

	account. Potential disclosure of data is possible through guest access.
Likelihood	Medium. Depends on the server configuration.
Consequence	Disclosure of information is possible if the guest account has access.
System Compliance/ Expected test results	Objective. The guest account is removed from all sensitive databases. The guest account at the operating system level must be disabled.
Test performed to ensure compliance	<ul> <li>Check permissions for the guest account on sensitive databases.</li> <li>1) Access enterprise manager (Start Programs MicrosoftSQLServer EnterpriseManager)</li> <li>2) Expand the server group, open the target server then access the databases tab. Expand the database in question. Select the users tab. All users allowed access are shown.</li> <li>3) Ensure the guest account is not listed and that only required groups/users are listed as having access to the database. Document the findings and attach a screenshot to the report.</li> <li>Check guest account at O/S level</li> <li>4) Access Windows users and groups settings (Start Programs AdministrativeTools ComputerManagement Loca IUsersAndGroups).</li> <li>5) Double-click users tab. Double click guest account. Ensure "account is disabled" box is checked. Document findings and attach a screenshot.</li> <li>Stimulus/Response test: Attempt to access the server with an account not listed as having access to ensure that access is denied.</li> <li>6) Logon to the auditor workstation as a user that does not exist on the target server (this will force a guest connection when data access is performed).</li> <li>7) Open Microsoft Access from the auditor workstation. Close any wizard that appears when opening the application.</li> <li>8) Select the "new data access page". Choose design view. The "Data link properties" screen will open.</li> </ul>
	<ol> <li>Enter the server name and select Windows Integrated Security. The following screenshot shows the screen that should be displayed.</li> </ol>

	🗐 Data Link Properties 🛛 🔀
	Provider Connection Advanced All
	Specify the following to connect to SQL Server data: 1. Select or enter a server name:
	▼ Refresh
	2. Enter information to log on to the server:     • Use Windows NT Integrated security
	C Use a specific user name and password:
	User name:
	Password:
	Blank password Allow saving password
	3.      Select the database on the server:
	<ol> <li>Select the "select database on the server" pulldown box.</li> <li>Access should be denied. Document the findings and attach a</li> </ol>
	screenshot of any errors.
Actual	The following approach above that guest appears is restricted from the
Results	The following screen shows that guest access is restricted from the Company database.
	Console Root  Mame A Login Name Database Access  Mame A Login Name Database Access  Mame A Login Name Database Access  A Permit
	SQL Server Group       Image: Constant of the server of the
	The Guest account has been disabled at the O/S level.
L	

Guest Properties ? X
Remote control Terminal Services Profile Dial-in
General Member Of Profile Environment Sessions
Guest
Euli name:
Description: Built-in account for guest access to the computer/do
User <u>m</u> ust change password at next logon
<ul> <li>User cannot change password</li> <li>Password never expires</li> </ul>
Account is disabled
Account is locked out
Stimulus/Response test: The following shows the results of an access test using an account called "sqltest"
Data Link Properties
Provider Connection Advanced All
Specify the following to connect to SQL Server data: 1. Select or enter a server name:
<ul> <li>2. Enter information to log on to the server:</li> <li>O Use Windows NT Integrated security</li> </ul>
C Use a specific user name and password:
User name:
Password:
<ul> <li>Blank password Allow saving password</li> <li>Select the database on the server:</li> </ul>
O Attach a database file as a database name:
Login failed for user '(null)'. Reason: Not associated with a trusted SQL Server connection.
ОК

Auditor Notes	Pass. Guest account is removed from corporate databases and the
/ Test Results	guest account has been disabled at the operating system level.

## Audit 8 – Alerting

Reference	SQL Server Security Checklist (item 17):
	http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4
Control	An alerting mechanism must be established and notification
Objective	established.
Risk	A lack of alerting would prohibit response to malicious activity. This
	would allow an attacker ample opportunity to attack the server if no
	detection and response was possible.
Likelihood	High. Alerting is not configured by default.
Consequence	No response would be possible if alerting is not enabled.
System	Objective. Alerts are configured and notification will be sent.
Compliance/	
Expected Test	Ô'
Results	
Test	Access the server in SQL Enterprise Manager. Select Management
performed to	SQL Server Agent   Alerts. Check for the existence of an alert for
ensure	severity 14 and that an operator is defined to receive a page or e-mail.
compliance	<ol> <li>Access Enterprise Manager (Start Programs MicrosoftSQLServer EnterpriseManager)</li> </ol>
	2) Expand the server group, open the server and access the
	management tab. Select "SQL Server agent", then alerts.
	3) Check for a listing with severity 14. Attach screenshot of alerts
	screen.
	<ol> <li>Double click the severity 14 item. Click the "Response" tab.</li> </ol>
	Note all of the recipients of alerts. Attach a screenshot of the
	recipients and the method of alerting.
Actual Results	Alerting has been established for the server; however, there is no
0	notification established, nor are there any operators established.

	n Console Root\Microsoft SQL Servers\SQL Se	erver Group\ <b>erver</b> (Windo	ows NT)\Manag	jement\S	iQL Serv	er Ager
	Action View Iools	X 🖅 🖸 🗟   😫   🔸	8 🛛 🖗 🔒	💽 🔂		
	Tree	Alerts 10 Items				
	Console Root	Name 🛆	Enabled	Error	Severity	Last Oc
	🗄 🍘 Microsoft SQL Servers	Demo: Full msdb log	Yes	9002	0	(Never
	🖻 🐨 🕣 SQL Server Group	Demo: Full tempdb Demo: Sev. 19 Errors	Yes Yes	9002 0	0 19	(Never (Never
	Databases	Demo: Sev. 20 Errors	Yes	0	20	(Never
	🗄 🚞 Data Transformation Services	Demo: Sev. 21 Errors	Yes	0	21	(Never
	🖨 🔁 Management 🚊 😨 SQL Server Agent	Demo: Sev. 22 Errors	Yes	0	22	(Never
		Demo: Sev. 23 Errors Demo: Sev. 24 Errors	Yes Yes	0 0	23	(Never (Never
	Operators	Demo: Sev. 25 Errors	Yes	0	24 25	(Never (Never
	jobs Backup	Permission alert	Yes	0		>(Never
	⊡ ∰ Current Activity					
	🙀 Database Maintenance Plans					
	😟 🔁 SQL Server Logs					
	⊡-( Replication ⊕( Security					
	u Support Services					
	🗄 🛅 Meta Data Services					
	Permission alert Properties -			×		
	General Response			- 1		
	Execute job:		▼	11		
	Operators to notify:	New	Operator			
	Operator Name	E-mail Pager Ne	et Send			
	Include alert error text in: 🔽 E-ma	ail 🔲 <u>P</u> ager 🔽 Ne	t <u>s</u> end			
2	_					
	Additional notification message to send	:				
			<b>T</b>			
Auditor Notes						
	Fail. As a result of the issues	s identified in the te	est results	s, ther	e wou	ula

#### Audit 9 – TCP/IP Port filtering

Reference	Medine Luie Empirical Hacker Protect your detabase series part					
Reference	Medina, Luis, Empirical Hacker – Protect your database series - part one, checklist item 7.					
	http://searchnetworking.techtarget.com/tip/1,289483,sid7_gci845040,00.					
Control	html					
· -	Network controls should be in place to protect the server data.					
Objective	Malwara can use high lovel parts to communicate with an attacker and					
Risk	Malware can use high-level ports to communicate with an attacker and					
Likalihaad	allow access to server.					
Likelihood	Medium. Previous examples of malware that allowed for remote control					
0	of the server included backorifice and netbus.					
Consequence	If not restricted, any port can be used on the server. Malware would be					
	able to report back to an attacker and open a connection through the					
	corporate firewall.					
System	Objective. All ports other than the required baseline ports are filtered at					
Compliance /	the O/S level.					
Expected test						
results	<u> </u>					
Test	Check TCP/IP filtering.					
performed to						
ensure	1) On the server desktop, right-click the "My Network Places" icon,					
compliance	select properties. Right-Click "Local Area Connection", select					
	properties. Double click Internet Protocol (TCP/IP). Select the					
	advanced tab, then options. The following screen capture shows					
	what should be displayed.					
	Advanced TCP/IP Settings					
	IP Settings DNS WINS Options					
	in Seconds   DNS   Wints Operation					
	Optional settings:					
	IP security					
	TCP/IP filtering					
C	<u>Properties</u>					
6						
	Description:					
	TCP/IP filtering allows you to control the type of TCP/IP network					
	traffic that reaches your Windows computer.					
	2) Select TCP/IP filtering, select properties. All filtered ports will be					
	displayed at this point. Document and attach a screenshot to the					
	מוסףומצטע מג נחוס פטחונ. בטטטווופווג מווע מונמטון מ סטופפרוסווטג נט נוופ					

	report.			
	<ul> <li>Stimulus/Response Tests:</li> <li>3) From the auditor workstation on the LAN, run NMAP (windows executables available at <u>http://sourceforge.net/projects/nmapwin.</u>) Enter the IP address of the SQL server. Check the port range box and enter 1-65535. This will test which ports are accessible on the server. Ensure that all TCP and UDP ports are scanned (by repeating the test with UDP scan selected). Attach both screenshots (TCP and UDP scans) of discovered ports to the report.</li> <li>4) Execute fport (executables available at <u>http://www.foundstone.com/knowledge/free_tools.html</u>) on the server. Save the report and attach a screenshot to the report.</li> </ul>			
Actual test	As shown in the following screenshots, port filtering is not enabled on			
results	the server. TCP/IP Filtering			
	Enable TCP/IP Filtering (All adapters)			
	Permit All     Permit All     Permit All     Permit Only     Permit Only			
	TCP Ports     UDP Ports     IP Protocols			
	Add     Add       Bemove     Bemove			
	OK Cancel			
	FPORT scan results. Fport shows that terminal services have been enabled on the server. It has been determined that management of the server is performed remotely through terminal services.			



	NMapWin v1.3.1
	Host: Help Exit
	Sgan       Discover       Options       Timing       Files       Service       Win32         Mode       Scan       Options       Scan       Scan       Options         O       Connect       Null Scan       Window Scan       Port Range       Use Decoy       Bounce Scan         O       SYN Stealth       Xmas Tree       BCP Scan       Device       Source Address       Source Port         O       Eins Stealth       Ip Scan       List Scan       Idle Scan Host       Idle Scan Host
	Output Starting nmap V. 3.00 ( www.insecure.org/nmap ) warning: OS detection will be MUCH less reliable because we did not find at least 1 Interesting ports on : (The 65527 ports scanned but not shown below are in state: closed) Port State Service 135/udp open netbios-ns 138/udp open netbios-dgm 445/udp open microsoft-ds 500/udp open isakmp 1029/udp open unknown 1434/udp open ms-sql-m 44624/udp open unknown 1434/udp open unknown 1434/udp open 1 IP address (1 host up) scanned in 29 seconds
Auditor Notes	Fail. No ports are restricted on the server. Additionally, terminal services are installed and listening on the server. Server should be investigated to determine what application is listening on UDP port 47624. Research has shown this port to be associated with a game server. Fport does not list any service listening on this port.
Audit 10 – SQ	L Port

Reference	Medina, Luis, Empirical Hacker – Protect your database series - part one, checklist item 2. <u>http://searchnetworking.techtarget.com/tip/1,289483,sid7_gci845040,00.</u> <u>html</u> Partlow, Joe, Microsoft SQL Server 2000 Security Overview (page 6) <u>http://www.giac.org/practical/Joe_Partlow_GSEC.doc</u>
Control Objective	Network controls should be in place to protect the server data.
Risk	Attackers will portscan entire subnets on port 1433 (automated attacks), or will use Sqlping2 (port 1434) to manually find SQL servers on the

	Internet.				
Likelihood	Depends on the firewall configuration.				
Consequence	A potential attacker would know of the existence of the SQL server. An attacker can then use automated tools to attack server after initial the reconnaissance.				
System Compliance/ Expected test results	Objective. The port value should be changed from the default and the server port should be hidden. This will change both the listening port and hide the actual SQL port in use from sqlping2.				
Test performed to ensure compliance	<ol> <li>Access Enterprise Manager (Start Programs MicrosoftSQLServer EnterpriseManager)</li> <li>Expand the server group, right click the servername and select properties.</li> <li>Select the Network Configuration tab. Select the TCP/IP protocol option and select properties.</li> <li>Document the port number and determine if the server is listed as hidden ("hide server" checkbox selected).</li> <li>Stimulus/Response tests:</li> <li>Run fport on the server to confirm which port the SQL Server is listening to. Document findings and attach screenshot.</li> <li>Obtain sqlping2 from www.sqlsecurity.com/scripts.asp.</li> <li>Run SQLping2 against the server IP address.</li> <li>Document the findings and attach a screenshot to the report.</li> </ol>				
Actual test results	The SQL listening port is at its default value of TCP 1433 and the "hide server" checkbox is not selected.  SQL Server Network Utility  General Network Libraries  Server name:  Disabled protocols:  Multiprotocol  NWLink IPX/SPX AppleT alk Banyan Vines  Force protoco  Force protoco  Force protoco  C - TCP/IP  Network Protocol Default Value Setup  Default port:  Hide server				

Fport	screenshot s	hows th	at all po	orts are at their de	fault values.	
	VINNT\System32\cm					_ [
http:	//www.foundstor	ne.com				
Pid 500 8 8 556 808 8 1220	Process svchost System System msdtc MSTask System acleanwy	Por → 135 → 139 → 445 → 102 → 102 → 103 → 143	TCP TCP TCP 5 TCP 6 TCP 6 TCP 0 TCP	Path C:\WINNT\system32\ C:\WINNT\System32\ C:\WINNT\system32\ C:\PROGRA~1\MICROS	\msdtc.exe \MSTask.exe	og]oonun /
e 556 384	sqlservr msdtc termsrv	-> 337 -> 338	2 TCP	C:\WINNT\System32\ C:\WINNT\System32\	msdtc.exe	sqiservr.e
500 8 8 8	svchost System System System	-> 135 -> 137 -> 138 -> 445	UDP UDP	C:\WINNT\system32\	\svchost.exe	
264 252 1220	lsass services sqlservr	-> 500 -> 102	UDP	C:\WINNT\system32\ C:\WINNT\system32\ C:\PROGRA~1\MICROS	services.exe	sqlservr.e
± <sup>™</sup> squ	Ping2 confirms Ping2 by Chip Andrews			ver is listening to T	FCP port 1433	3.
	ttings <u>U</u> tility <u>H</u> elp		Live IP Add	dresses File:		
	IP Range From Live Address File					
_ Scan R			User List: -			
	Address:		Password L	ist —		
<u></u>	Begin Scan	Cancel				
	:Found:	Name		Clustered? No	? Version 8.00.194	TCP Por 1433
5						
or Notes Fail.	•	port is a	t defau	It value of 1433 a	nd server is n	ot
	711.					

#### **Residual Risk**

Most steps have been taken to prevent an attack from occurring. Thought and effort have been employed to restrict many of the inherent preventative weaknesses with the product. On the whole, the majority of control objectives have been met during this audit. Exceptions to this statement are as follows:

Exposure	Published vulnerabilities in SQL Server 2000
Control in place	Patch implementation
Residual Risk	Time between patch release and implementation. Patches only address published vulnerabilities, not "zero-day" or future vulnerabilities.
Recommendation	Automated system for patch implementation. Software Update Services (SUS) is supplied by Microsoft to automate patch deployment. Defense in depth approach to securing the server mitigates the risk of zero-day exploits.
Estimated cost of recommendation	\$1500 in labour charges (assumption 5 days effort @ \$300/day), software free of charge. The implementation of SUS will reduce the administrative overhead associated with patch maintenance and should be justifiable as the reduction of effort required to manually maintain patches will outweigh the effort required to implement the service.

Exposure	Stored procedures can be used by an attacker to gain access to the underlying operating system	
Control in place	Removal of stored procedures and/or permission hardening of stored procedures.	
Residual Risk	Some stored procedures may be required for functionality.	
Recommendation	Perform a full audit of the underlying operating system and implement suggested controls.	
Estimated cost of recommendation	Acquire audit checklist for Windows 2000 and conduct audit. The costs associated with this endeavor are estimated to be 2 days of effort for a cost of \$600 (if performed internally). The audit and subsequent implementation efforts will further harden the operating system and implement defense in depth. This should be viewed as justifiable as the potential monetary damage is well in excess of the estimated costs.	

Exposure	Physical theft of server components or hardware failure	
Control in place	Server located in locked room	
Residual Risk	Server remains as a single point of failure. Physical barriers may be	
	circumvented.	
Recommendation	Acquire hot-spare server to reduce the downtime associated with	
	loss or failure of hardware components	
Estimated cost of	Purchase of identical server platform. Time required to install	
recommendation	software components and data migration procedures or	

implementation of a replication mechanism. Estimated cost of implementation is \$5000 for the server platform and another 2 weeks of labour, estimated at \$3000. Based on the assumed value of the data stored on the server, this implementation of a hot spare
is justifiable.

Exposure	Notification to unauthorized access (response mechanism)		
Control in place	Alerts created to notify administrator		
Residual Risk	Single individual tasked with maintaining 24x7 support of server.		
Recommendation Add extra administrator to segregate duties and share workload			
Estimated cost of Hiring of additional resource who will be able to share the wor			
recommendation	The estimated cost of this recommendation is \$50,000/year. Due to		
	the workload of the present administrator and the lack of		
	segregation of duties controls, this step is justifiable.		

#### Is the system auditable?

The Microsoft SQL Server 2000 system is auditable, but requires configuration to enable auditing. For example, by default, audit logs are not kept. Due to the lack of a log system, it was not possible to determine if the system has already had malicious activity performed on the data, or if individuals have been accessing sensitive data to which they should not have access. All of the other goals of the audit were successfully completed, as the required components were available to the auditor for analysis.

Many of the other controls in the system allow for complete auditing. The system does create event entries into the generic system event viewer. Additionally, the SQL Server does populate the performance monitor application with SQL-specific counters. These counters can be used to trigger alerts based on thresholds being met and can be used for both auditing and performance tuning purposes.

The use of third party tools can assist with auditing of the system. For instance, one application, NGSSquirrel, can be used to greatly enhance the auditing and testing of SQL server. Use of this application could not be included in this paper due to the fact that it is not freeware and must be licensed at a cost (price varies depending on license purchased). To learn more about NGSSquirrel and its increased auditing capabilities, go to <a href="http://www.nextgenss.com/software/ngssquirrel.html">http://www.nextgenss.com/software/ngssquirrel.html</a> for more information regarding this product and to download a (crippled and time bombed) trial copy of the software.

#### Assignment 4: Audit Report

#### **Executive Summary**

The purpose of the audit was to determine if the SQL server met a baseline of security with protection, detection and response mechanisms being implemented. The audit of the server examined the policies and procedures of the Company and compared them against industry best practices.

The scope of this project was to determine if confidentiality, integrity and availability of server data could be reasonably expected with a Time Based Security approach. This includes analysis of preventative measures, as well as detection and reaction capabilities to unauthorized access to the server.

The analysis of the SQL server has shown that while attention has been given to preventative security, some areas of the server have vulnerabilities that could be used by a threat agent to gain access to the server. For the most part (with exceptions noted following this summary), prevention mechanisms have been implemented on the server. Patches are applied on a frequent basis and the latest patches were being investigated. Accounts are restricted and authentication mechanisms are in place to limit exposure. Detection of any mischievous actions taken on the server could not be determined due to a lack of an audit trail. Response is also hindered through a lack of detection capability.

It is highly recommended that while maintaining a vigilant watch on the preventative side of security, detection and response mechanisms should be put in place for this server.

#### Audit Findings

The following risks were discovered during the audit of the SQL server.

#### Finding 1 – Missing patches on the server

Priority: Critical Reference: Audit Item #1, page 38

Patches were found to be missing on the server. Patch maintenance is critical for this server as all known exploits are controlled through the implementation of patches. This lack of patching, although scheduled, is an indicator of the inability of one person to

manage all facets of the corporate IT structure. This root cause is believed to be the reason these patches have not been implemented.

#### SQL Server Scan Results

Vulnerabilities				
Score	Issue	Result		
×	SQL Server Hotfixes	5 hotfixes are missing or could not be confirmed. What was scanned Result details How to correct this		

#### **Risks**

Attackers can create a script that exploits a published vulnerability. The script can then be executed in an automated fashion by entities known as "script kiddies". These individuals need not know of the system or its' inner workings to successfully attack a server. Once an attack is successful, all confidentiality of data would be lost.

#### Finding 2 – Lack of detection mechanism

Priority: Critical Reference: Audits #4 and #5, pages 48-53

With the exception of logon auditing, there are no logs or trace tables that contain information regarding the transactions on the database. The items to trace have been established, however, no activity logs were found during the audit, which confirms that logging had not been established. The implementation of a process whereby logs are checked on a weekly basis will serve to address detection of malicious activity.

#### Risks

Without a detailed log of activities performed, it is impossible to determine what transactions have occurred on the database. While there is no detection, there is also no possibility of a timely reaction. This would allow an attacker to gain access to the server undetected and manipulate data as (s)he desires with little possibility of being caught.

#### Finding 3 – Lack of notification system

Priority: High

#### Reference: Audit #8, page 60

Notification functionality is included in the software to notify an administrator (operator) in the event of a security breach. At the present time, the items that should trigger a notification alert are established, however, there are no operators listed as recipients of an alert, nor does an infrastructure exist to facilitate such notifications. The lack of recipients is shown in the following screenshot. Establishment of a notification system and pager rotation will address this shortcoming.

Permission alert Properties	5 -				×	
General Response						
Execute job:				T	] [	
Operators to notify:				Ne <u>w</u> Operato	r	
Operator Name		E-mail	Pager	Net Send		
I Include alert error text in:	☑ <u>E</u> -mail	□ <u>P</u> ag	ger [	✓ Net send		
Additional notification messa	ige to send:					
					Ŧ	
						I

#### Risks

The lack of a notification system would imply that there is no reaction capability in the event of an attack. An intruder would have ample time to perform their attack and cover their tracks. The likelihood of discovering an intruder accessing the server is highly improbable with no notification established.

#### Finding 4 – Stored Procedure vulnerabilities

#### Priority: Medium

#### Reference: Audit Item #2, page 39

Stored Procedures are included by the vendor to facilitate administration of the SQL server. Stored procedure functionality can range from simplification of routine administrative tasks up to the ability to run operating system command through the SQL server (xp\_cmdshell). The stored procedures on the system are the default system procedures and the permissions assigned to the procedures are also at their default values. Once the initial changes are implemented, a process should be created to allow for a periodic review of stored procedures available in the system.

The following is a screenshot of the functionality that an attacker can gain through the use of the xp\_cmdshell. In this example, the attacker can get a listing of all event logs on the server to perform initial reconnaissance prior to hiding any activities (s)he performs:

🚔 Query -							
xp_cmdshell 'dir c:\*.evt /s'							
	······································						
<b>I I</b>							
	output						
	-						
4	Directory of c:\WINNT\system32\config						
5	NULL						
6		262,144	AppEvent.Evt				
7		65,536	SecEvent.Evt				
8		65,536	SysEvent.Evt				

#### Risks

An attacker can use these stored procedures to stage an attack of the server operating system for the purposes of gaining access to databases files, or to install malware on the server such as Trojan software.

It is recommended that all stored procedures mentioned in the audit checklist be analyzed for their usefulness to the company. These procedures can be removed, or have their permissions changed so only the required users have access. In some cases (xp\_cmdshell, and various registry manipulation procedures) their removal is recommended.

The likelihood of an attacker using these procedures to mount an attack on the server is low. However, they should be removed to mitigate the potential risk of exploitation.

#### Finding 5 – TCP/IP Port filtering

Priority: Medium Reference: Audit Item #9, page 62

In much the same manner as a firewall, server-based port filtering allows for a limitation to be placed on the ports that an application can use to listen to the network. By enabling port filtering, you limit the potential for a port to be activated by malware to listen for instructions on the network. No port filtering has been established on the

server. Port filtering can be used to limit applications from gaining access to the network.



#### Risks

Vulnerabilities associated with malware are remote administration (e.g. Backorifice and netbus) and other Trojan applications. By having all ports open, an attacker can implement an application that will listen to the network for commands. Such applications can be used to gain complete access to the server.

It is recommended that port filtering be implemented on the server to limit the exposure related to network aware malware.

#### Finding 6 – SQL listening port

Priority: High Reference: Audit Item #10, page 65

The vendor has added the capability to change the default port that SQL uses to listen to the network. In addition to being able to change the port, the capability to hide the port being listened to has also been implemented. This functionality serves to hide the server from automated tools that scan entire subnets to find SQL servers on the Internet. The server is listening to the default port of 1433 and it is not hidden. A process should be implemented that calls for a periodic scan of the network from the Internet. This will detect any deviations in the future and will help secure the network from intruders.

🚦 SQL Server Network U	tility		×
General Network Librarie	s		
Server <u>n</u> ame:			
Disa <u>b</u> led protocols:		Enabled protocols:	
Multiprotocol NWLink IPX/SPX AppleTalk Banyan Vines	<u>E</u> nable >> << <u>D</u> isable		
		<u>P</u> roperties	
Force protoco     Enable WinSc	TCP/IP		×
	stwork Protocol Default Valu	ue Setup	
	Default port:	1 433	
I	Hide server		

### Risks

Attackers will use automated tools to discover SQL servers in a subnet. By having the server listening to the default port of 1433, discovery of the SQL server would be possible if the rule-set on the firewall does not block port 1433 or if the firewall is compromised. Once the discovery is made, an attacker would use other applications to attempt compromise of the server.

#### Audit Recommendations

As stated in the overview, it is highly recommended the detection and response capabilities for this server be improved. Implementation of detection and response mechanisms will satisfy all Time Based Security requirements. Additionally, it is recommended that all stored procedures be analyzed for potential misuse. Their removal or hardening of their permissions should be reviewed and implemented in a timely manner.

1) Response capabilities are impacted by a lack of a notification system: Implement a notification process and a pager rotation for on-call staff members. This will greatly reduce the time required to respond to a security breach. The likelihood of requiring a notification of an attempted attack in progress is high, and the consequence of not having this system in place is a complete breakdown of response capabilities. The costs for the implementation are relatively low (estimated 5 days effort), since the technical requirements to implement the solution are provided by the vendor. During testing of the solution, it may be determined that additional hardware/software must be purchased (e.g. pager capabilities) depending on the functionality required.

- 2) Detection capabilities are impacted by a lack of auditing: Implement auditing of transactions within the database and develop a script that will analyze the log files for suspicious text strings as part of a detection process. Without the logging of activity, it is impossible to determine who performed an improper action and if their intent was malicious or accidental. As with the notification, the likelihood of requiring a detection mechanism for actions taken within the database is high. The cost of implementing this solution is estimated to be 5 days of effort. Depending on the amount of log data generated and the archiving period required, a separate log server may be required due to the amount of log entries, but at the present time, data can be stored on the existing server.
- 3) Limit potential impact of stored procedures: Review all stored procedures listed in the audit checklist. Removal or hardening of permissions is highly recommended to remove the possibility of them being used as a vehicle to stage an attack on the server or the computing infrastructure. The likelihood of an attack using one of the existing stored procedures is low, however, as is the case with xp\_cmdshell, their potential for damage is severe. Complete control of the server and the entire network can be gained. Additionally, several SQL vulnerabilities that focus on system stored procedures have been recently released. The cost of implementing this solution is estimated at 5 days of effort. Once the initial changes are implemented, a process should be created to allow for a periodic review of stored procedures available in the system.
- 4) Increase administrative security awareness: Staff should attend formal security training to increase their awareness of all aspects of security, not just the preventative side of security. Vendor neutral training will give the administrator a greater understanding of defense in depth security and how to properly maintain security in the organization. The cost of this initiative is estimated to be \$3000 USD.
- 5) Enable port filtering on the server. Many Trojan applications written are network aware and will listen to the network via a port in order to communicate with the attacker. By enabling port filtering, an attacker may be thwarted in their attempts to collect data from the system. The costs related with this initiative are estimated to be 1 hour, which includes connectivity testing. Through the implementation of both port filtering on the server and the creation of a network scanning procedure, future risks regarding listening ports on the network would be mitigated.
- 6) Software Update Services. Software Update Services (SUS) is available from Microsoft at no cost and is a means to automate existing patch processes for all servers in the enterprise. The effort for this implementation is estimated at 5 days. Presently, the probability of a published vulnerability being exploited on the server is low, due to the inability of clients to access the server from

the Internet. Implementation of this system will address the root cause of the failure itself, which is believed to be the lack of personnel available to address patch management.

#### Costs

The majority of costs are associated with the time required to configure, test and implement the recommendations. No software or hardware purchases are required for the recommendations. Because all changes should be made in a lab environment, all of the recommendations will take time to implement due to the doubling of effort to make the changes on the production server.

Approximate costing guideline for recommendations

Initial Stored Procedure review and implementation	
(5 days @ \$300/day):	\$ 1500
Initial enforcement of auditing and log storage 🔜	
(5 days @ \$300/day):	\$ 1500
Initial creation and implement notification process	
(5 days effort @ \$300/day):	\$ 1500
Security Training	\$ 4710
(\$3000USD @ 1.57 exchange rate)	
Software Update Services (Windows Update) implementation	\$ 1500
Approximate totals for implementation of recommendations	\$10710 CDN

Please note that costs listed are for the initial implementation of the systems. Ongoing costs are estimated as follows:

Ongoing effort for Stored Procedures @ 2days/year (½ day per quarter) \$600/Yr. Ongoing effort for log reviews @ 26 days/year (½ day per week) \$7800/Yr. Notification system. Varies, depending on alerts generated. Unknown. Software Update Services. Varies, depending on updates. Unknown.

#### **Compensating Controls**

With the exception of the security training, all of the recommendations made within this report are both necessary and low cost measures that can be performed by the system administrator.

The lack of segregation of duties (due to company having one administrator) can be compensated by the implementation of periodic reviews of changes made by the administrator.

Short of implementing a notification system, a process could be created whereby the administrator of the system views the logs every morning for suspicious activity. Although response would remain hindered, there would be a detection mechanism put in place. This process would also assist with log storage. If the logs were reviewed every morning, there would be a lesser demand for log storage space.

Stored procedures could have a blanket permission set established and have the required functionality restored as required by adding permissions as needed. This would alleviate the time requirement for hardening or removing stored procedures.

Timely patching could alleviate the requirement for the implementation of SUS. This would require the implementation of a process for patch maintenance and complete participation of the administrator to perform these patches in a timely manner.

The Company may opt to send the administrator to SANS online training instead of attending the SANS conference. This decision would save approximately \$700 USD.

#### **Appendix A - References**

#### **Research references**

Microsoft SQL Server 2000 Security White Paper http://www.microsoft.com/sql/techinfo/administration/2000/2000SecurityWP.doc

National Institute of Standards and Technology (NIST). The ICAT metabase <u>http://icat.nist.gov/</u>

SANS Top 20 Lists http://www.sans.org/top20

Microsoft. Microsoft Baseline Security Analyzer Homepage <u>http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/</u> <u>MBSAhome.asp</u>

SQL Security Checklist http://www.sqlsecurity.com/checklist.asp

Malone, Ted. "Hacking SQL Server" http://www.eknowlogist.com/presentations/Archive/0802SQLAgent.ppt

Medina, Luis. Empirical Hacker series <u>http://searchsecurity.techtarget.com/bestWebLinks/0,289521,sid14\_tax281918,00.html</u>

Out-of-the-Box NT Security Checklist <a href="http://www.windowsitlibrary.com/Content/121/18/3.html">http://www.windowsitlibrary.com/Content/121/18/3.html</a>

SANS. Security Consensus Operational Readiness Evaluation <a href="http://www.sans.org/SCORE/checklists/">http://www.sans.org/SCORE/checklists/</a>

Overview of SQL Server security model and security best practices <u>http://vyaskn.tripod.com/sql\_server\_security\_best\_practices.htm</u>

Partlow, Joe. Microsoft SQL Server 2000 Security Overview http://www.giac.org/practical/Joe\_Partlow\_GSEC.doc

Microsoft. Commerce Server 2002: Using SQL Authentication <u>http://msdn.microsoft.com/library/default.asp?url=/library/en-us/csvr2002/htm/cs\_se\_securityconcepts\_sfxq.asp</u>

Microsoft. SQL Server 2000 C2 Administrator's and User's Security Guide

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/sql/mai ntain/security/sqlc2.asp

Microsoft SQL Server Books online: http://www.microsoft.com/sql/techinfo/productdoc/2000/books.asp

Microsoft. INF: Implementing Password Expiration of SQL Server Login IDs <u>http://support.microsoft.com/default.aspx?scid=KB;en-us;80397&</u>

Spenik, Mark Sledge, Orryn. An Overview of SQL Server's Security Model <a href="http://www.developer.com/tech/article.php/10923\_721441\_1">http://www.developer.com/tech/article.php/10923\_721441\_1</a>

Microsoft. FIX: Service Pack Installation May Save Standard Security Password in File <u>http://support.microsoft.com/default.aspx?scid=KB;en-us;q263968</u>

Talmage, Ron. Auditing in SQL Server 2000 <a href="http://www.itworld.com/nl/db\_mgr/04162001/">http://www.itworld.com/nl/db\_mgr/04162001/</a>

Utility Download Sources

Fport: http://www.foundstone.com/knowledge/free\_tools.html

NMAP: http://sourceforge.net/projects/nmapwin

SQLPING2: <a href="http://www.sqlsecurity.com/scripts.asp">www.sqlsecurity.com/scripts.asp</a>

Microsoft Baseline Security Analyzer:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/ MBSAhome.asp