GIAC
CERTIFICATIONS

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.

Interested in learning more?

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

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

Graham Thompson

© SANS Institute 2003, Author retains full rights.

Abstract:
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.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Assignment 1: Research in Audit, Measurement Practice, and Control 5
Company Overview 5
ACME Physical Network Layout 6
Identify the system to be audited 6
Evaluate risk to the system 7
Present state of SQL Server 2000 auditing 8
Assignment 2: Create an Audit Checklist 10
Check 1 - Service Pack and Hot Fix levels 10
Check 2 – Stored Procedures 11
Check 3 – Authentication Model 14
Check 4 – Audit Activity on server 16
Check 5 – Logon Auditing 18
Check 6 – SQL Service start-up accounts 19
Check 7 – Guest user access 21
Check 8 – Alerting 22
Check 9 – TCP/IP Port filtering 23
Check 10 – SQL Port 25
Check 11 –Password Strength 26
Check 12 – SQL ACLS 28
Check 13 – Excessive account permissions 29
Check 14 – File Sharing/NetBIOS settings 30
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 33
Check 19 – Network Protocol Libraries / On-The-Wire Encryption 34
Check 20– Backup/Restore Procedures 35
Check 21 – Physical Security of Server 36
Assignment 3: Conduct the audit 37
Audit 1 - Service Pack and Hot Fix levels 37
Audit 2 – Stored Procedures 38
Audit 3 – Authentication Model 44
Audit 4 – Audit Activity on server 47
Audit 5 – Logon Auditing 49
Audit 6 – SQL Service start-up accounts 52
Audit 7 – Guest user access 55
Audit 8 – Alerting 59
Audit 9 – TCP/IP Port filtering 61
Audit 10 – SQL Port 64
Residual Risk 66
Is the system auditable? 68
Assignment 4: Audit Report 70
Executive Summary 70
Audit Findings 70
Finding 1 – Missing patches on the server 70

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Risks 71
Finding 2 – Lack of detection mechanism 71
Risks 71
Finding 3 – Lack of notification system 71
Risks 72
Finding 4 – Stored Procedure vulnerabilities 72
Risks 73
Finding 5 – TCP/IP Port filtering 73
Risks 74
Finding 6 – SQL listening port 74
Risks 75
Audit Recommendations 75
Costs 77
Appendix A - References 79
Research references 79

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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

Company Overview

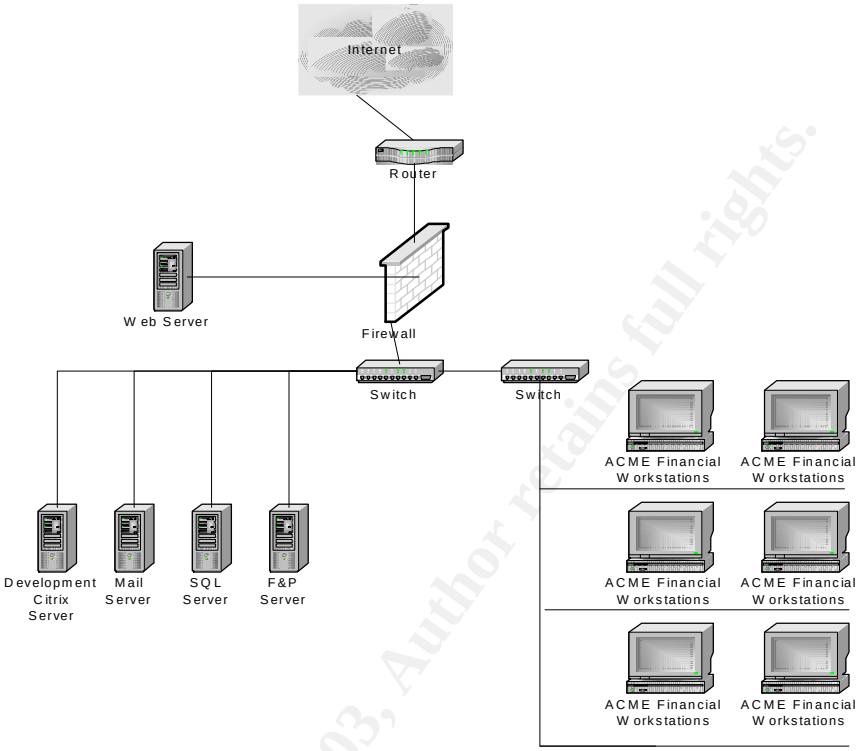
ACME Financial Inc is an independent financial services firm that primarily deals with insurance and investment needs of its clients. It does so by offering clients access to multiple mutual funds and insurance packages. The Company serves clients with high net worth. Due to a new Internet initiative 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.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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: http://www.microsoft.com/sql/techinfo/administration/2000/2000SecurityWP.doc

- SQLsecurity.com checklist was chosen due to its popularity and valuable information. The checklist can be found at: http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4.

- Luis Medina has created a good series of SQL security tips. The "Empirical hacker – Protect your database" series can be found at: http://searchnetworking.techtarget.com/tip/1,289483,sid7_gci845040,00.html

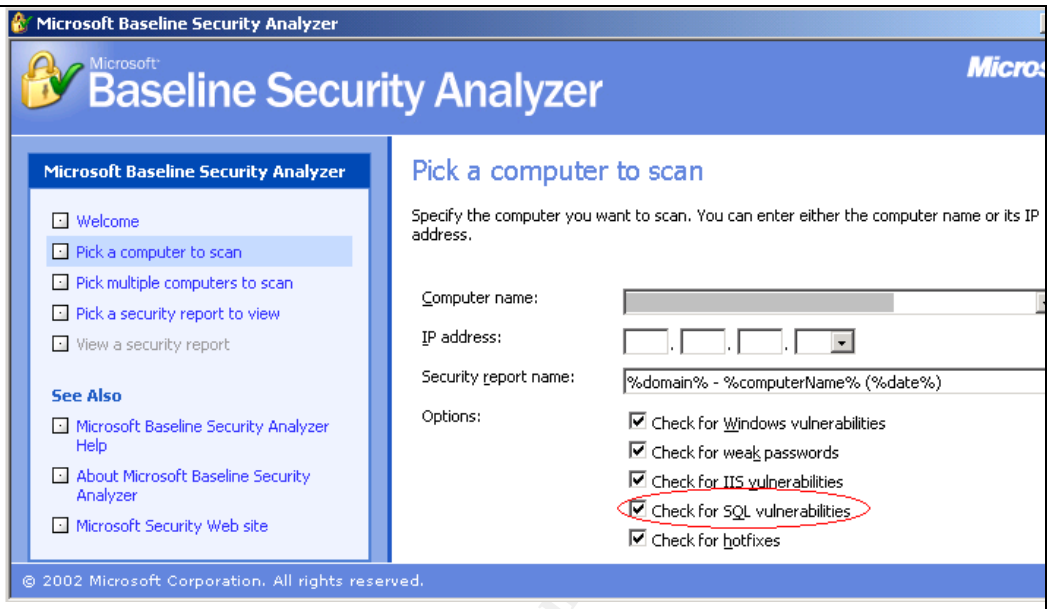
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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): http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/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	1) From the auditor's workstation with Internet access, obtain and run Microsoft Baseline Security Analyzer (MBSA). (Start|Programs|MBSA). 2) Select "scan a computer", enter the name or IP address of the server.

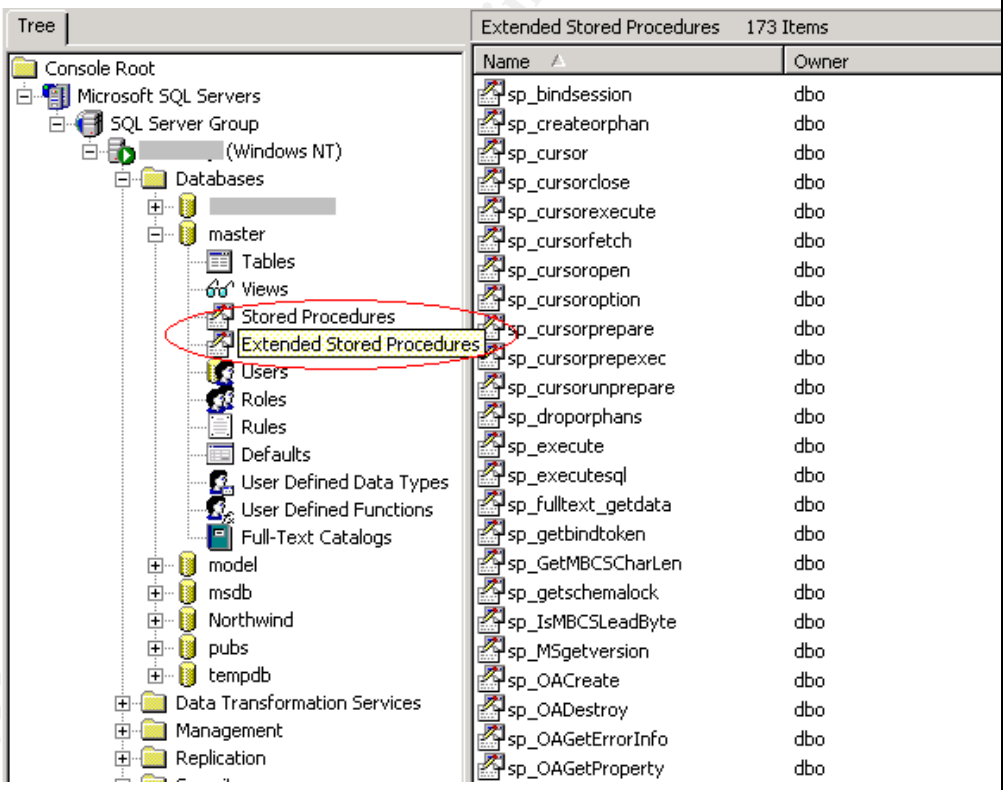
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	 3) Ensure that SQL component will be analyzed. Select start scan. 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 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
Test Results	
Auditor Notes / Test Results	

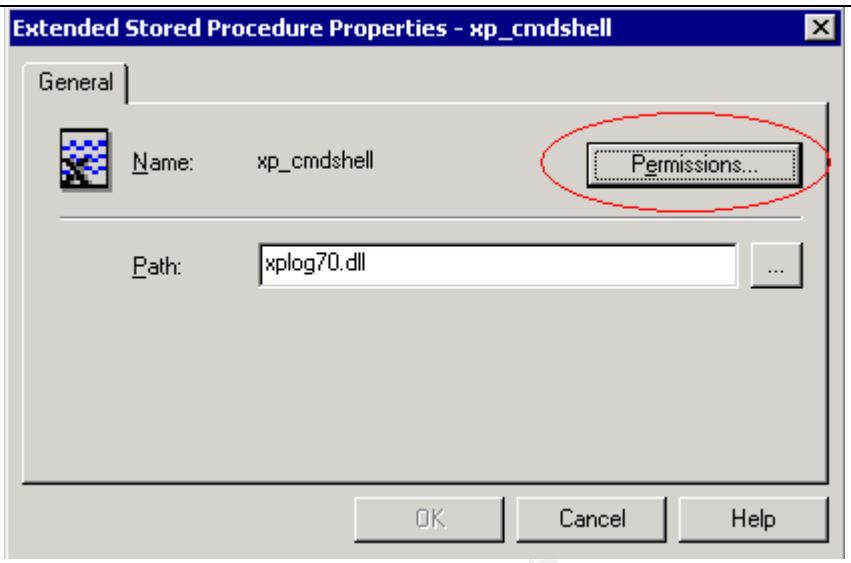
Check 2 – Stored Procedures

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 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

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

System Compliance/ Expected Results	Subjective. Stored procedures should be restricted from general usage where possible. Xp_cmdshell should be removed from the server unless it is required.
Test performed to ensure compliance	Check for existence of stored procedures and which permissions are assigned. To check the stored procedures: 1) Access the SQL Enterprise Manager (Start|Programs|MicrosoftSQLServer|EnterpriseManager) 2) Expand the SQLServerGroup and access the server. 3) Select the Databases tab, then access master database 4) Select "stored procedures" and "extended stored procedures" container.  5) Individually select all listed stored procedures found in the following table and check permissions by double-clicking name and selecting the permissions tab. Document all permissions and include in the report.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

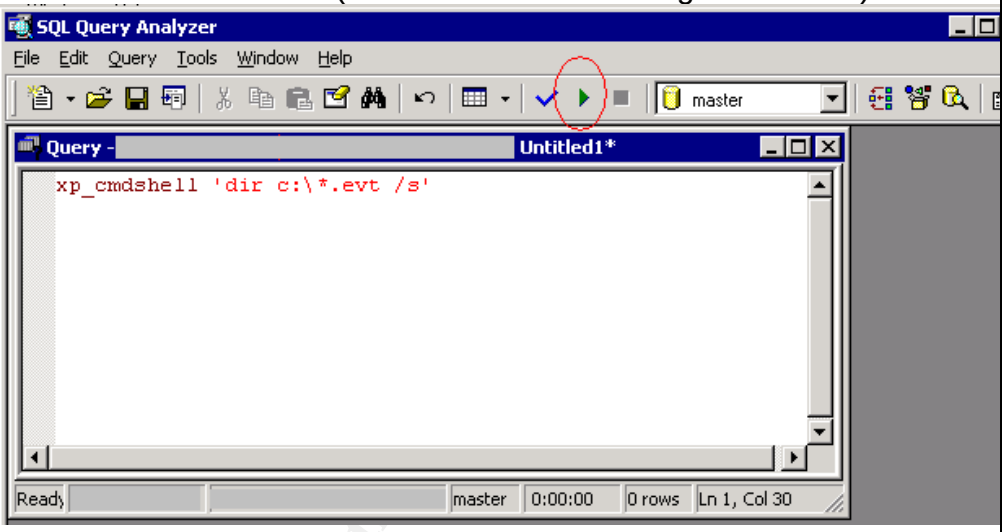


xp_fileexist
sp_sdidebug

xp_readerrorlog
xp_readmail

© SANS Institute 2003, Author retains

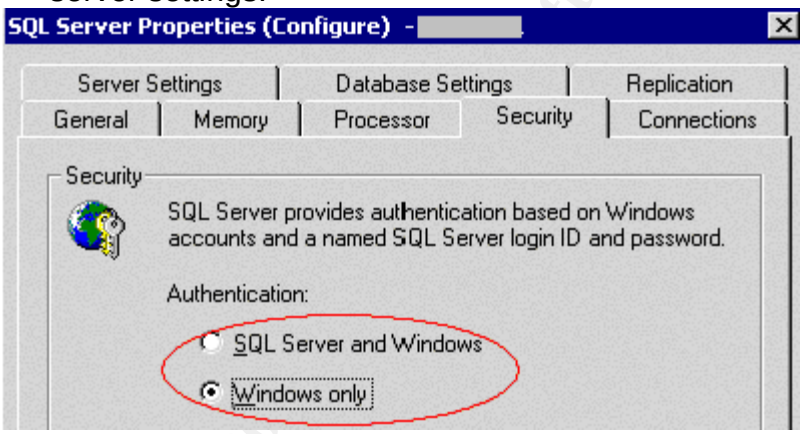
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	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).  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/2000/2000SecurityWP.doc
Control Objective	A single account database should be implemented for both the operating 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.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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	Check to ensure that only Windows authentication is used. 1) Access the enterprise manager (Start|Programs|MicrosoftSQLServer|EnterpriseManager) 2) Right click server name, select properties 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.  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)).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

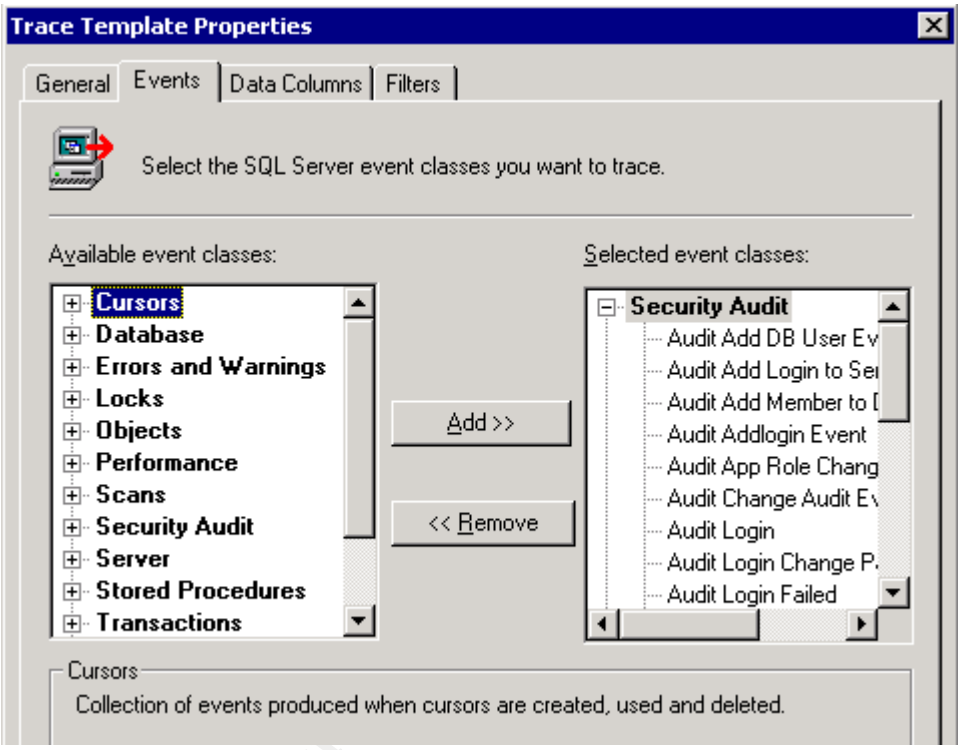
	  6) Document the results. Capture a screenshot and attach to the report.
Auditor Notes	

Check 4 – Audit Activity on server

Reference	SQL Server books online ("auditing SQL Server activity" as a search parameter).
Control Objective	Audit logs of all actions taken on SQL server must be kept.
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	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. 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

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

administrator. Once open, select “Events” tab.



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 Failed
Login GDR
Logout
Object Derived Permission
Object GDR
Object Permission
Statement GDR
Statement Permission

Verify Trace Results

3) Select File|Open|TraceFile or TraceTable (depending on storage of traces given by administrator). Point to the location

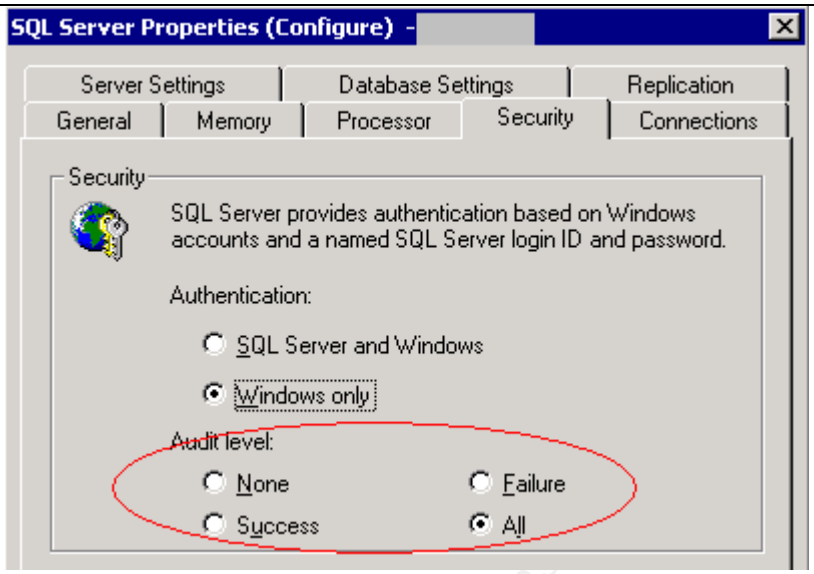
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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

Check 5 – Logon Auditing

Reference	Microsoft SQL 2000 Security White paper (page 54) http://www.microsoft.com/sql/techinfo/administration/2000/2000SecurityWP.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 Compliance/ Expected Test Results	Objective. Logging of failed SQL logins is turned on (the default setting is off.)
Test performed to ensure compliance	Ensure logon audit level for SQL server is set to all. 1) Access the enterprise manager (Start|Programs|MicrosoftSQLServer|EnterpriseManager) 2) Right click the server name, select properties 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.

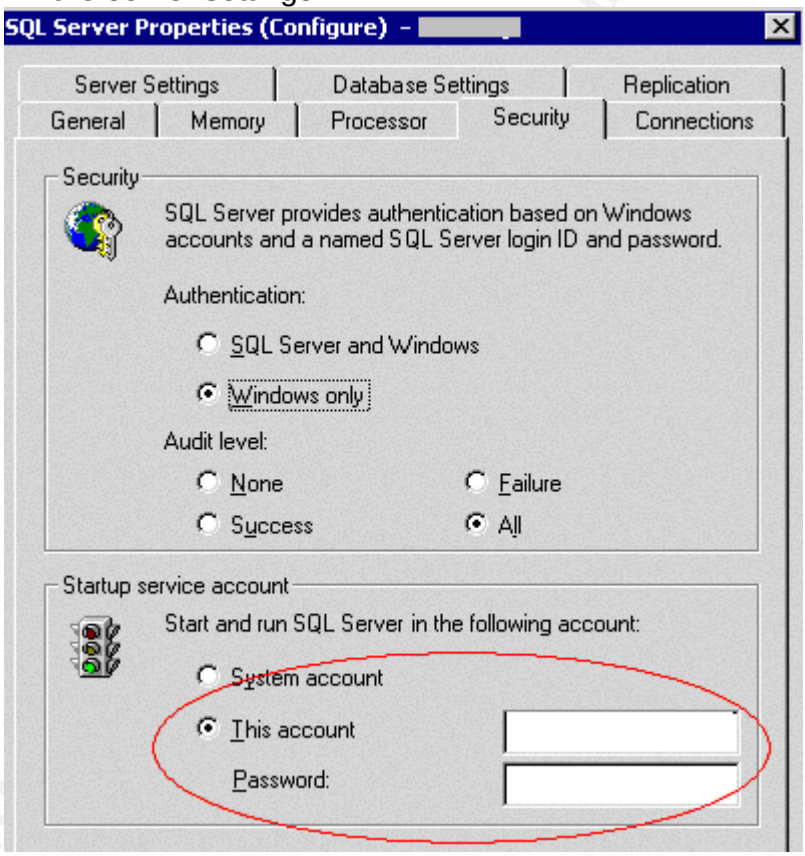
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	 Stimulus/Response Test: 4) Access Query Analyzer (Start|Programs|MicrosoftSQLServer|QueryAnalyzer) 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.
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/2000/2000SecurityWP.doc SQL Server Security Checklist (item 4): http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4
Control Objective	The SQL service must be assigned a user level start-up account
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

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	the server and network
System Compliance / Expected test results	Objective. MSSQLSERVER service must start as a user level account.
Test performed to ensure compliance	Check service startup account in enterprise manager. 1) Access the enterprise manager (Start|Programs|MicrosoftSQLServer|EnterpriseManager) 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.  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

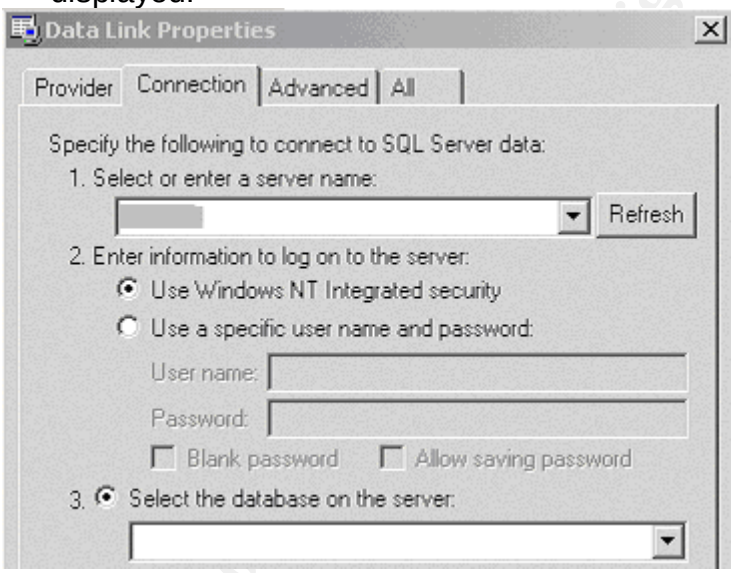
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	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/2000/2000SecurityWP.doc
Control Objective	Only authenticated accounts may access the SQL server.
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	Check permissions for the guest account on sensitive databases. 1) Access enterprise manager (Start|Programs|MicrosoftSQLServer|EnterpriseManager) 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. Check guest account at O/S level 4) Access Windows users and groups settings (Start|Programs|AdministrativeTools|ComputerManagement|LocalUsersAndGroups). 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.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	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). 7) Open Microsoft Access from the auditor workstation. Close any wizard that appears when opening the application. 8) Select the "new data access page". Choose design view. The "Data link properties" screen will open. 9) Enter the server name and select Windows Integrated Security. The following screenshot shows the screen that should be displayed.  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 Objective	An alerting mechanism must be established and notification 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.

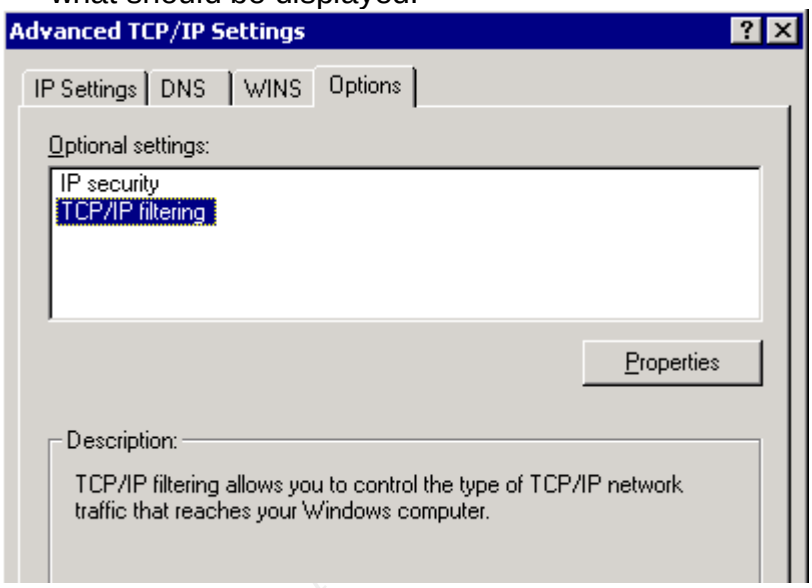
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Consequence	No response would be possible if alerting is not enabled.
System Compliance/ Expected Test Results	Objective. Alerts are configured and notification will be sent.
Test performed to ensure compliance	Access the server in SQL Enterprise Manager. Select Management | SQL Server Agent | Alerts. Check for the existence of an alert for severity 14 and that an operator is defined to receive a page or e-mail. 1) Access Enterprise Manager (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

Reference	Medina, Luis, Empirical Hacker – Protect your database series - part one, checklist item 7. http://searchnetworking.techtarget.com/tip/1,289483,sid7_gci845040,00.html
Control Objective	Network controls should be in place to protect the server data.
Risk	Malware can use high-level ports to communicate with an attacker and 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 Compliance / Expected test	Objective. All ports other than the required baseline ports are filtered at the O/S level.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

results	
Test performed to ensure compliance	Check TCP/IP filtering. 1) On the server desktop, right-click the “My Network Places” icon, 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.  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 report. 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.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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
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	1) Access Enterprise Manager (Start|Programs|MicrosoftSQLServer|EnterpriseManager) 2) Expand the server group, right click the servername and select properties. 3) Select the Network Configuration tab. Select the TCP/IP protocol option and select properties. 4) Document the port number and determine if the server is listed as 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) Obtain sqlping2 from www.sqlsecurity.com/scripts.asp. 7) Run SQLping2 against the server IP address. 8) Document the findings and attach a screenshot to the report.
Auditor Notes	

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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 Objective	All passwords must meet corporate minimum length requirements
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 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 authentication is used).
Consequence	Loss of all Confidentiality, Integrity and Availability through the guess of a simple administrative level password.
System Compliance:	Objective. Security policy states minimum password strength (6 characters and complex password requirements) must be followed to meet company security policy. This applies to both SQL and O/S level passwords. The system must reject weak passwords at an O/S level.
Test performed to ensure compliance	1) From the auditor's workstation with Internet access, obtain and run Microsoft Baseline Security Analyzer (MBSA). (Start|Programs|MBSA). 2) Select "scan a computer", enter the name or IP address of the server. 3) Ensure that SQL component will be analyzed. Select start scan. 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.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Domain Controller Test	SQL Server is not running on a domain controller. What was scanned
SQL Server Security Mode	SQL Server authentication mode is set to Windows Only. What was scanned
Registry Permissions	The Everyone group does not have more than Read access to the SQL Server registry keys. What was scanned
CmdExec role	CmdExec is restricted to sysadmin only. What was scanned
Folder Permissions	Permissions on the SQL Server installation folders are set properly. What was scanned
SQL Account Password Test	The check was skipped because SQL Server is operating in Windows Only authentication mode. What was scanned

Stimulus/Response Test:

1) Request that the administrator create a test account and supply you with the password.
2) Logon to the account and attempt to change password (Ctrl-Alt-Del, change password) to a null value. The system should reject this password. Document the test results and attach to the report.
3) Attempt to change password to "password". The system should reject this password. Document the test results and attach to the report.
4) Attempt to change password to "qwerty123!". The system should accept this password. Document the test results and attach to the report.

SQL password strength testing with a dictionary attack (use only for systems with SQL authentication implemented).

1) Obtain the SQLBF brute force/dictionary cracker for SQL server (http://www.cqure.net/tools.jsp?id=10).
2) Obtain a dictionary file if one is unavailable. A dictionary file can be obtained from ftp://ftp.ox.ac.uk/pub/wordlists/dictionaries/. Obtain the pocket-dict.gz dictionary. Expand with winzip and save to the same directory as the sqlbf application. Rename the file to pocket.dict.
3) Open the Query Analyzer (Start|Programs|MicrosoftSQLServer|QueryAnalyzer).
4) Issue the following command: "select name, password from master..sysxlogins". This will extract all accounts and passwords stored on the SQL server and display the hash values. Select all entries, copy with <ctrl-c> and save to a new text file called sqlhash.txt in the same directory as the sqlbf application. Modify the text file so that there is the name, followed by a comma, followed by the hash value of the user password. Ensure that only the users and hashes remain in the file, ensure the "null null"

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	values at the end of the file are removed. This file will be the target of our dictionary attack. 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.
Auditor Notes	

Check 12 – SQL ACLS

Reference	Microsoft SQL 2000 Security White paper (page 53) http://www.microsoft.com/sql/techinfo/administration/2000/2000SecurityWP.doc SQL Server Security Checklist (item 5): http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4
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	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. 1) Open a command prompt on the server (Start|Run|cmd). 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. 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. 4) Issue the command cacls "c:\program files\Microsoft SQL Server\mssql\binn*.*" /c. (replace path as required to point to location of

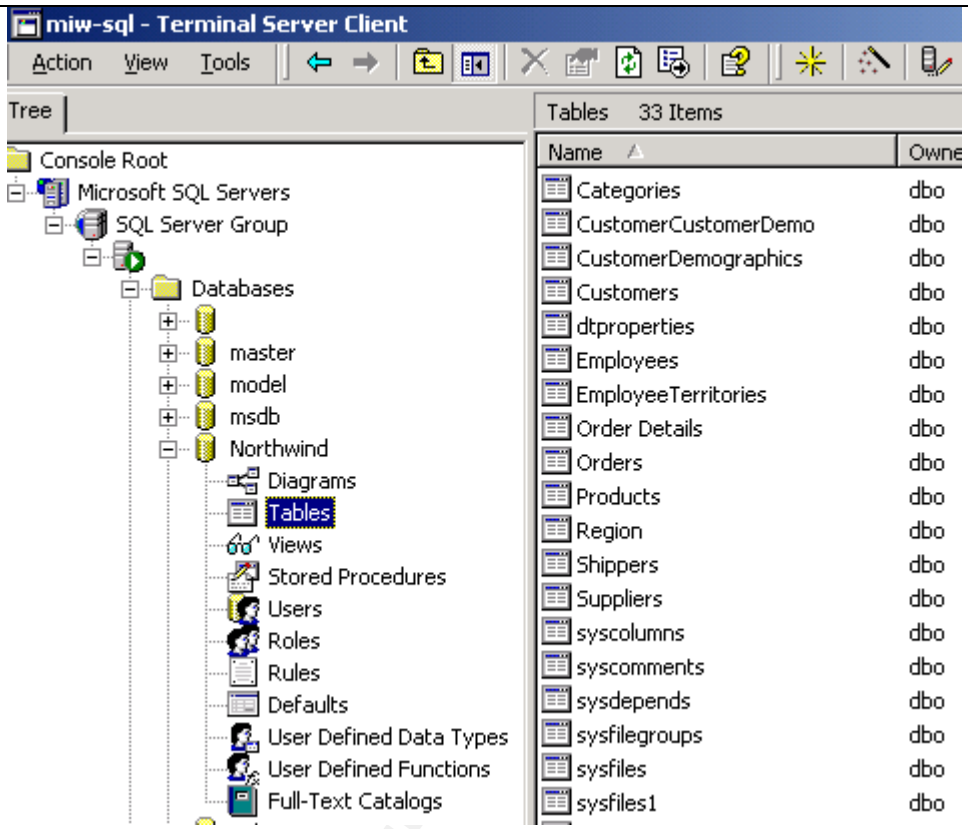
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	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 Objective	Users must be given least privilege to data.
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 Compliance/ Expected Test Results	Subjective. Least privilege assigned is to users. Only the owner of the system will be able to determine who should be given access and what level of access control is required.
Test performed to ensure compliance	Review the rights to all tables containing sensitive data in SQL. Check the rights to the views created. 1) Access Enterprise Manager (Start|Programs|MicrosoftSQLServer|EnterpriseManager) 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.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	 3) Check permissions on table to ensure that only authorized individuals have required access. Document the findings.
Auditor Notes	

Check 14 – File Sharing/NetBIOS settings

Reference	Medina, Luis, Empirical Hacker – Protect your database series - part one, checklist item 10. http://searchnetworking.techtarget.com/tip/1,289483,sid7_gci845040,00.html
Control Objective	Only SQL processes are allowed to run on the server.
Risk	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.)
Likelihood	Medium. Depends on server configuration.
Consequence	If not restricted, the additional functionality could open various vulnerabilities and slow access to the data.
System Compliance/	Subjective. No shares other than those required are established (Please note that some shares will be required for the system and some required

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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 – Patch Policies and Procedures

Reference	SANS Ottawa Conference, D Hoelzer.
Control Objective	Exposure to published vulnerabilities must be reduced.
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. http://searchnetworking.techtarget.com/tip/1,289483,sid7_gci845040,00.html
Control Objective	Only SQL processes are allowed to run on the server.
Risk	Applications can introduce vulnerabilities. Additional network ports may be

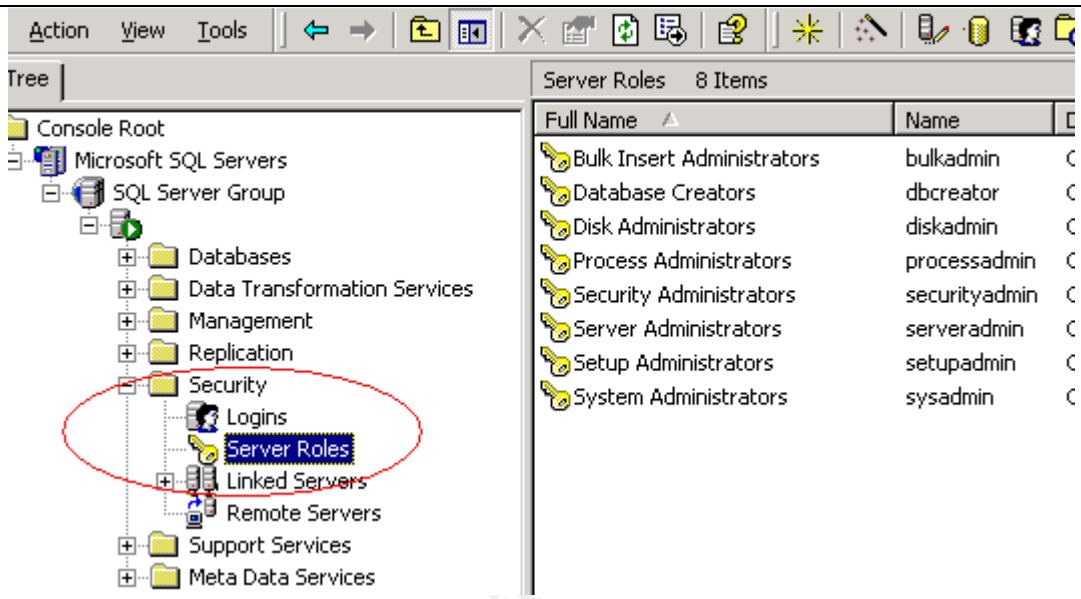
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	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 Compliance / Expected test results	Objective. Only SQL and its associated applications should exist on server.
Test performed to ensure compliance	1) Check Control Panel | Add/remove programs (Start|Settings|ControlPanel|Add/Remove Programs). Document applications found. 2) Run FPORT on the server to check for applications utilizing the network. Attach a screenshot to the report.
Auditor Notes	

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 Objective	Users must be given least privilege to the data.
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 Compliance/ Expected test results	Subjective. Only authorized accounts should be assigned to roles. Only the data owner can determine which accounts belong in a specific role.
Test performed to ensure compliance	1) Access SQL Enterprise Manager (Start|Programs|MicrosoftSQLServer|EnterpriseManager) 2) Select the server, choose security, then “server roles”.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	 3) Double-click the individual roles in the right pane and document the accounts listed as having membership. 4) Interview the data owner to ensure the proper accounts are assigned to the role membership.
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 Objective	SQL database files should be encrypted to limit exposure.
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 default.
Consequence	An attacker can copy database files and access data at their leisure.
System Compliance/ Expected test results	Objective. Encrypting File System (EFS) is enabled and the database files are encrypted.
Test performed to ensure compliance	Access the location of the mdf files. Right click the directory and select properties. In the folder properties window, select the advanced button. Ensure the "encrypt contents to secure data" checkbox is checked. Document the findings. Attach a screenshot to the report. The following screenshot

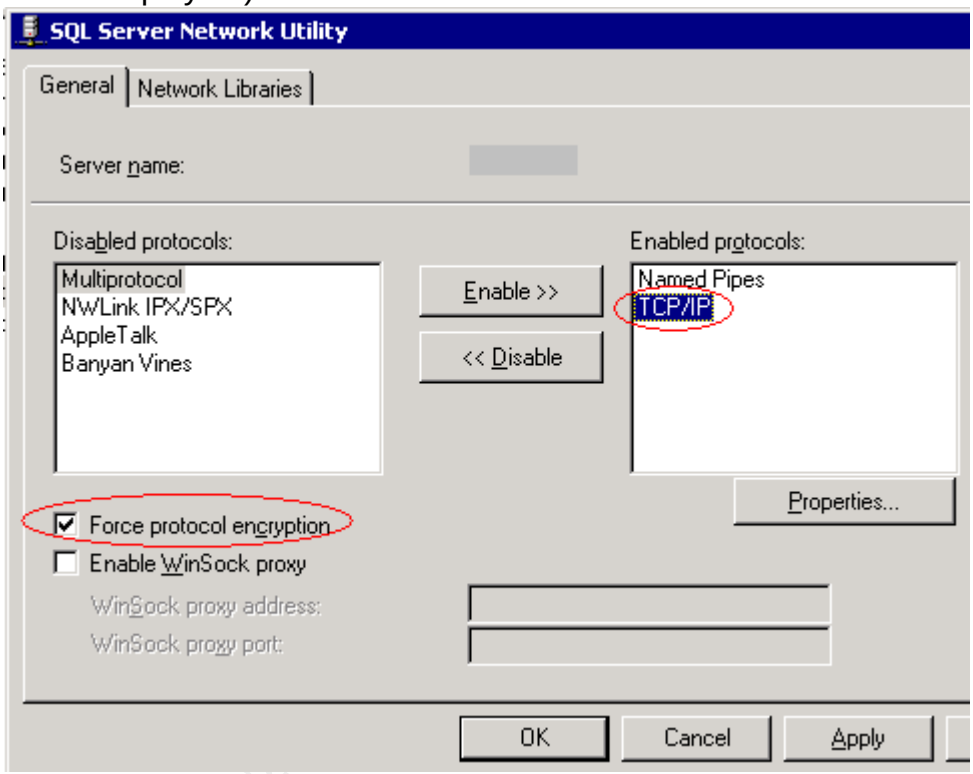
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	displays what should be seen.
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/2000/2000SecurityWP.doc
Control Objective	All data must be encrypted during transmission on network.
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 Compliance/ Expected test results	Objective. Test proves that network encryption is enforced.
Test performed to	1) Access the SQL Enterprise Manager

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

ensure compliance	(Start|Programs|MicrosoftSQLServer|EnterpriseManager) 2) Right click the server and select properties. Access the network configuration window at the bottom of the general tab. 3) Select TCP/IP. Ensure "Force Protocol Encryption" checkbox is established. (The following screenshot shows what should be displayed.)  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/2000/2000SecurityWP.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,

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	a longer time for recovery will be required to restore functionality.
System Compliance/ Expected test results	Subjective. Tapes and documentation exist. Administrative staff follow procedures. The administrator was able to find the procedural documentation and recent tapes. A test restoration was performed on 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	

Check 21 – Physical Security of Server

Reference	Microsoft SQL 2000 Security White paper (page 59) http://www.microsoft.com/sql/techinfo/administration/2000/2000SecurityWP.doc 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	

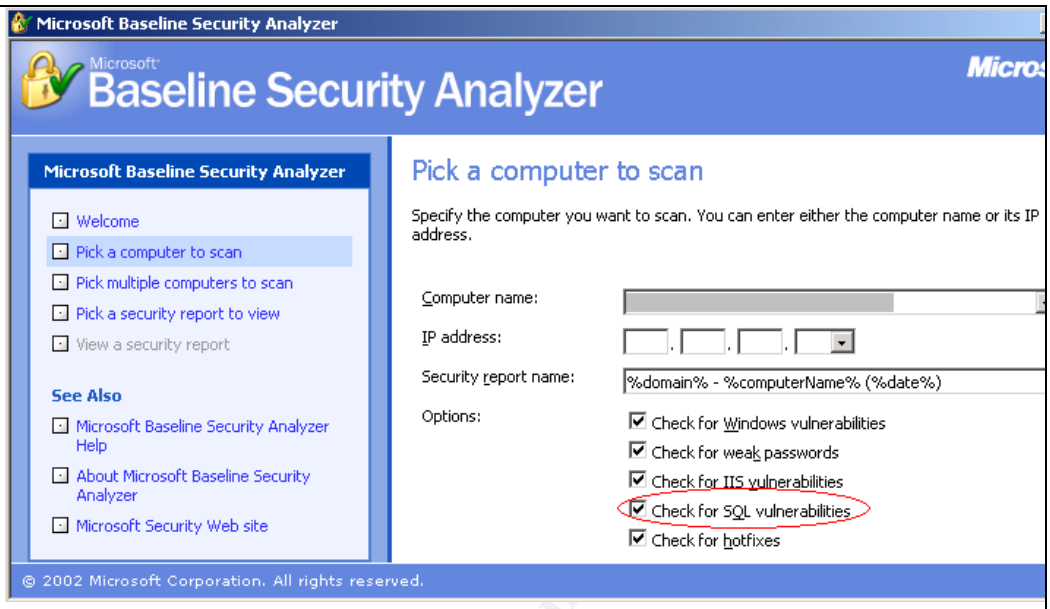
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

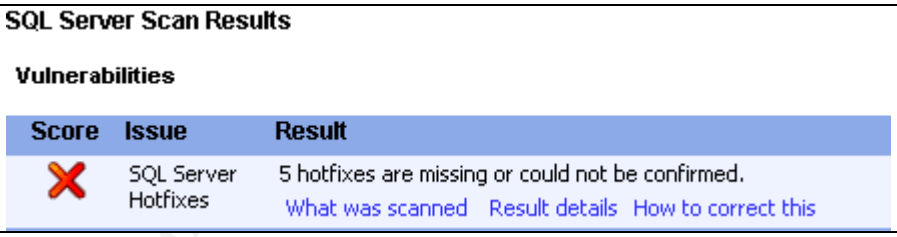
Assignment 3: Conduct the audit

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/security/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	Scan SQL Server from MBSA 1) From the auditor's workstation with Internet access, obtain and run Microsoft Baseline Security Analyzer (MBSA). (Start|Programs|MBSA). 2) Select "scan a computer", enter the name or IP address of the server.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

<table>
<tr><td></td><td>


3) Ensure that SQL component will be analyzed. Select start scan.
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 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
</td></tr>
<tr><td>Actual Results</td><td>


SQL Server Scan Results

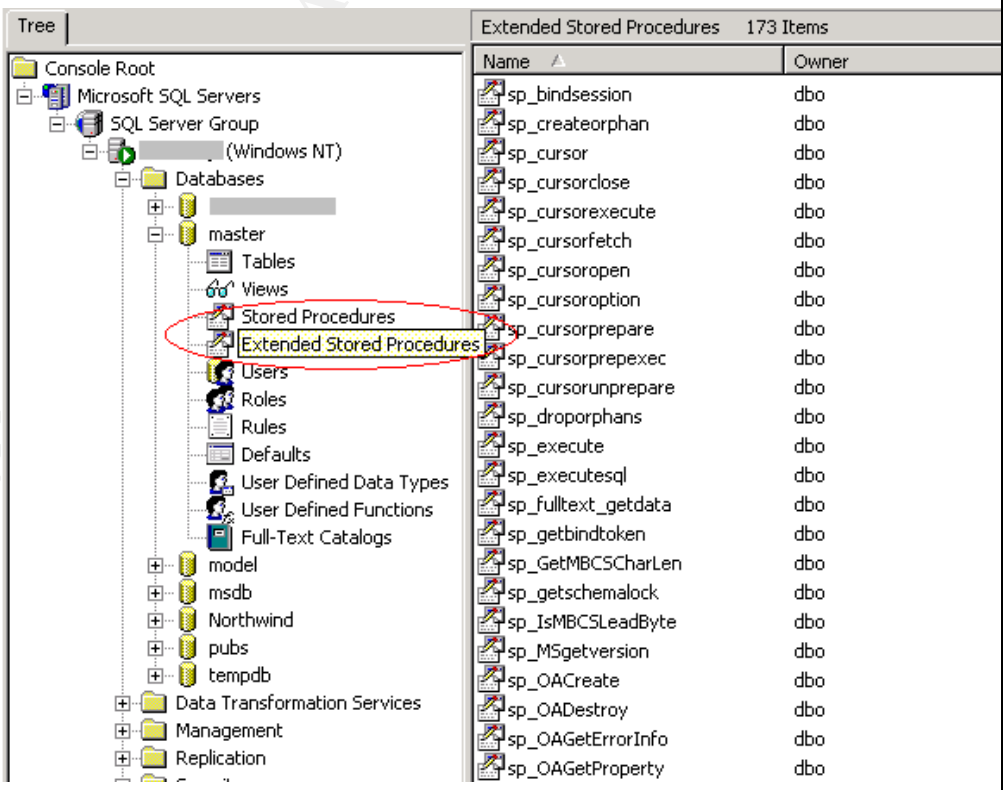
Vulnerabilities

Score	Issue	Result
✗	SQL Server Hotfixes	5 hotfixes are missing or could not be confirmed. What was scanned Result details How to correct this
</td></tr>
<tr><td>Auditor Notes / Test Results</td><td>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.</td></tr>
</table>

Audit 2 – Stored Procedures

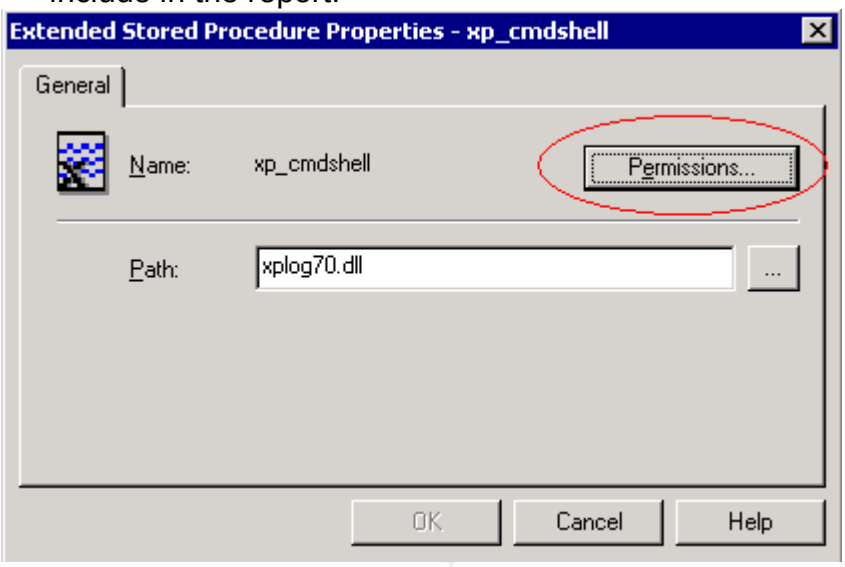
Reference	SQL Server Security Checklist (item 6): http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4
Control Objective	Access to operating system level commands must be removed or restricted to privileged accounts.
Risk	Stored procedures can be used as a means to attack corporate systems.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

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	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 should be restricted from general usage where possible. Xp_cmdshell should be removed from the server unless it is required.
Test performed to ensure compliance	Check for existence of stored procedures and which permissions are assigned. To check the stored procedures: 1) Access the SQL Enterprise Manager (Start|Programs|MicrosoftSQLServer|EnterpriseManager) 2) Expand the SQLServerGroup and access the server. 3) Select the Databases tab, then access master database 4) Select "stored procedures" and "extended stored procedures" container. 

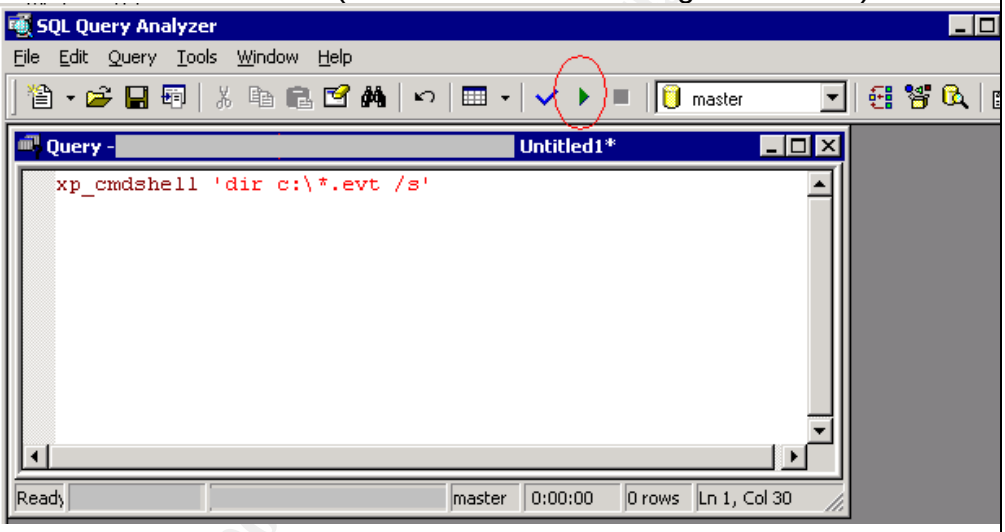
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

5) Individually select all listed stored procedures found in the following table and check permissions by double-clicking name and selecting the permissions tab. Document all permissions and include in the report.



xp_fileexist	xp_readerrorlog
sp_sdidebug	xp_readmail
xp_availablemedia	xp_revokelogin
xp_cmdshell	xp_runwebtask
xp_deletemail	xp_schedulersignal
xp_dirtree	xp_sendmail

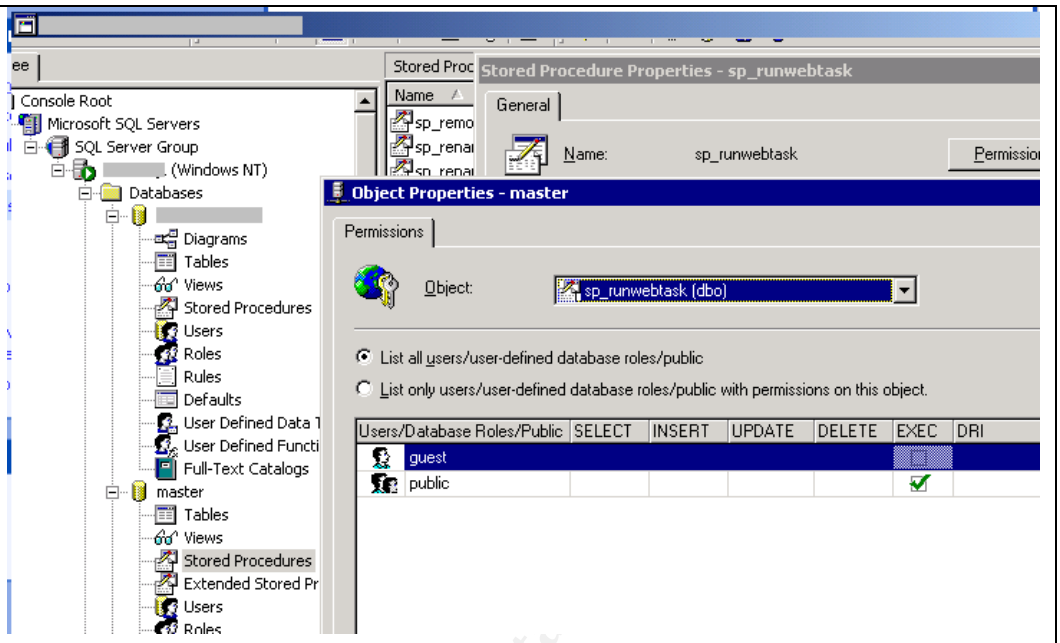
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	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).  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	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

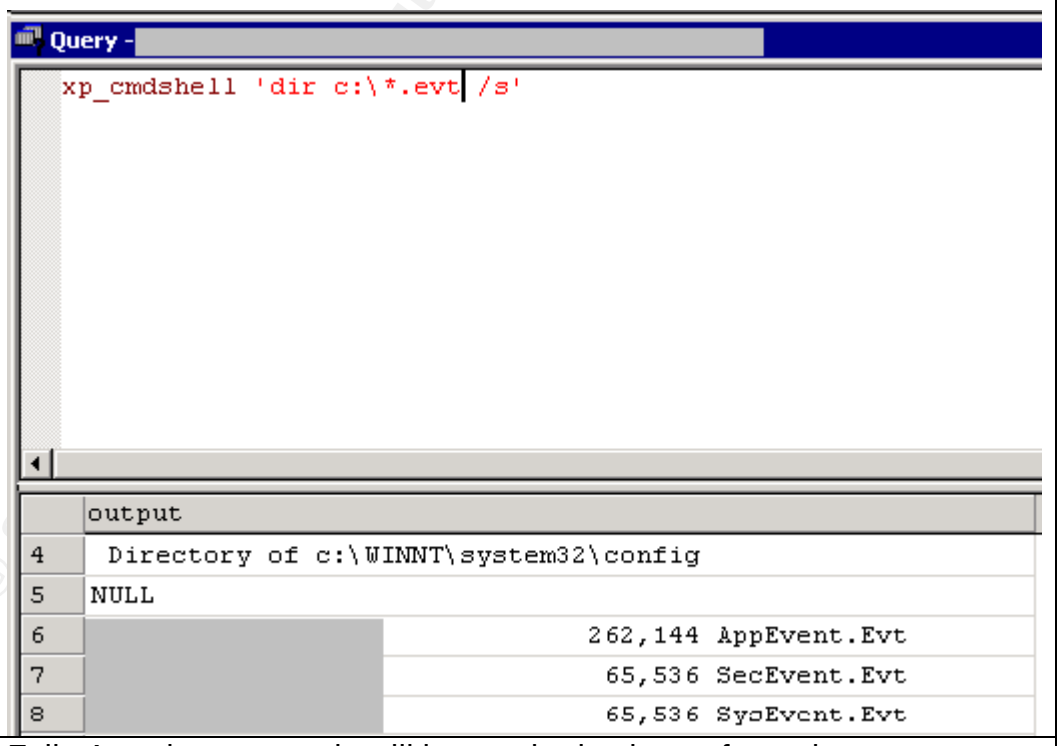
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	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.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



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.

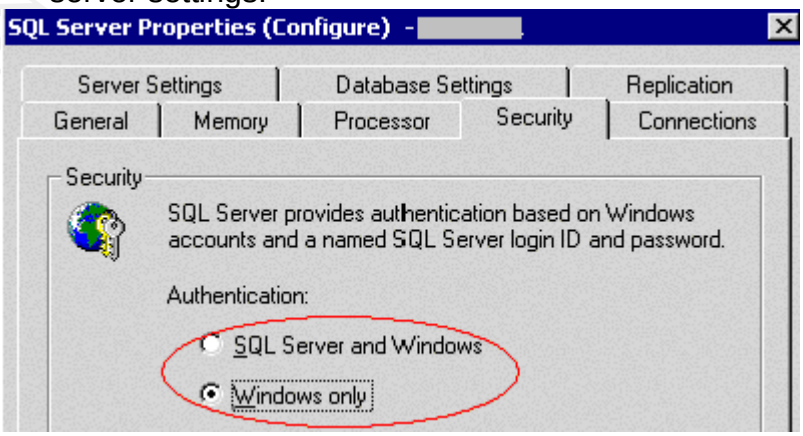


Auditor Notes / Test Results	Fail. Any changes made will be required to be performed on a test server to ensure functionality after changes have been implemented. An analysis should be performed for system stability in the event a procedure is dropped and the DLL removed; alternatively, tests should also be performed if permissions are removed from the public and guest

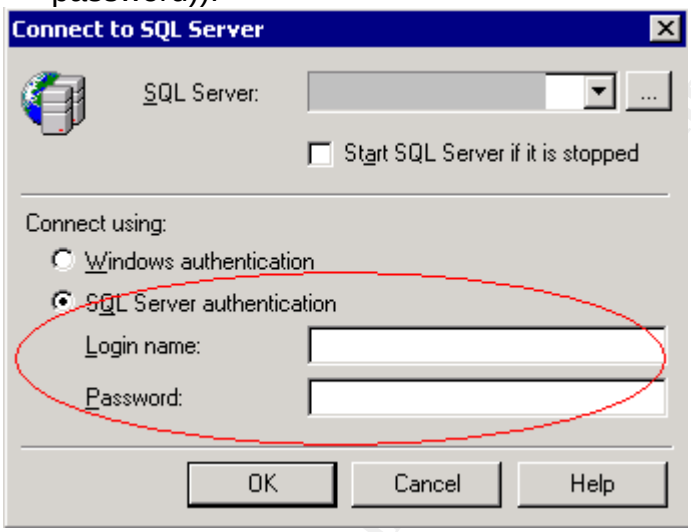
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	roles.

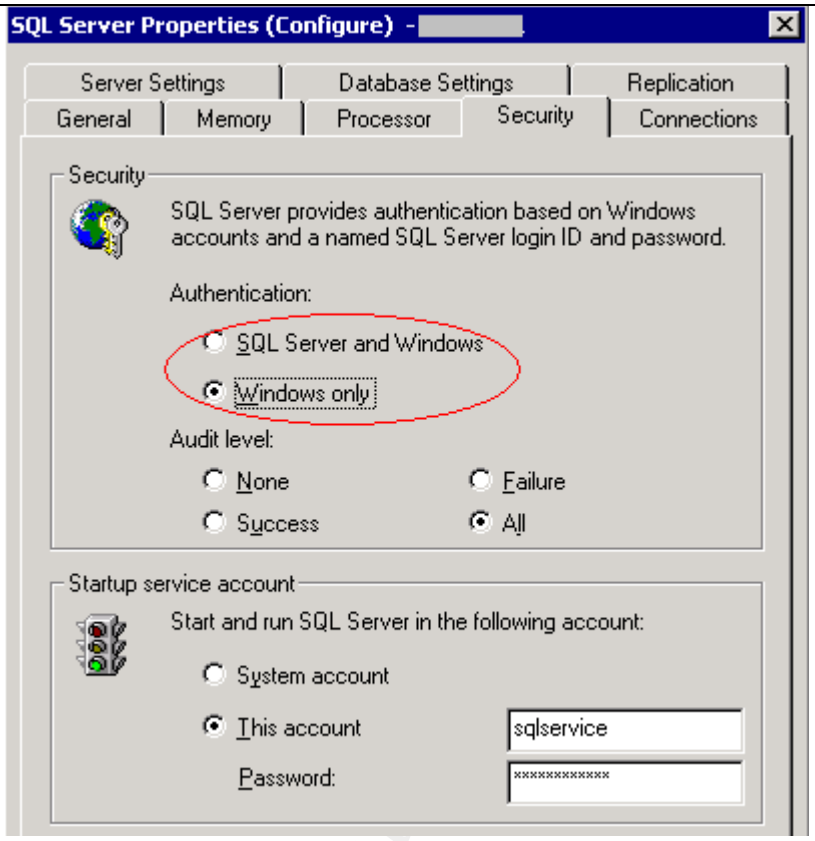
Audit 3 – Authentication Model

Reference	Microsoft SQL 2000 Security White paper (page 15) http://www.microsoft.com/sql/techinfo/administration/2000/2000SecurityWP.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	Check to ensure that only Windows authentication is used. 1) Access the enterprise manager (Start|Programs|MicrosoftSQLServer|EnterpriseManager) 2) Right click server name, select properties 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. 

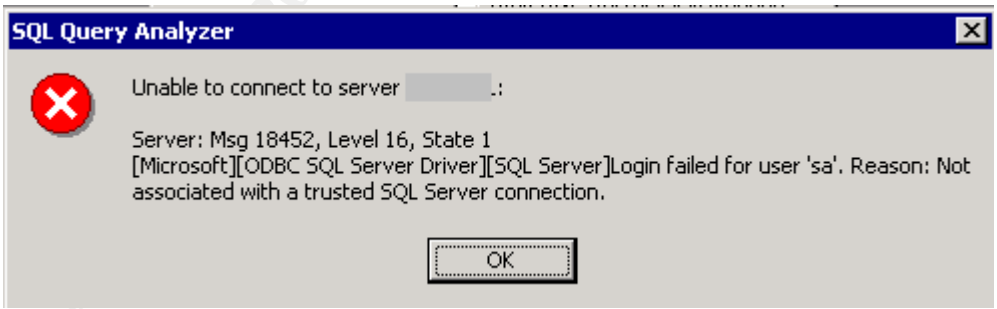
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	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)).  6) Document the results. Capture a screenshot and attach to the report.
Actual Results	Only Windows Authentication has been implemented on the server. The following screenshots confirm settings.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



To further test the authentication model, a logon to a query analyzer resulted in the following error message:



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 stating such is shown to the user.

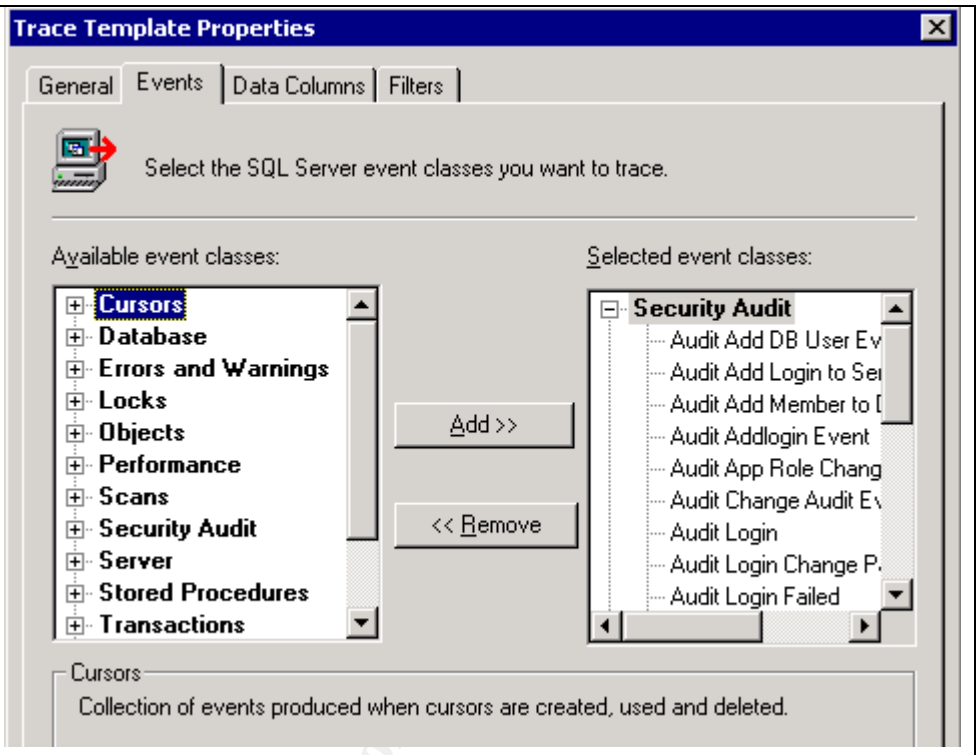
Auditor Notes / Test Results	Pass. The server has Windows Authentication established and stimulus/response tests have proven that an attempt to logon with a SQL account fails with an error stating that Windows Authentication is in place.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Audit 4 – Audit Activity on server

Reference	SQL Server books online ("auditing SQL Server activity" as a search parameter).
Control Objective	Audit logs of all actions taken on SQL server must be kept.
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	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. 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.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



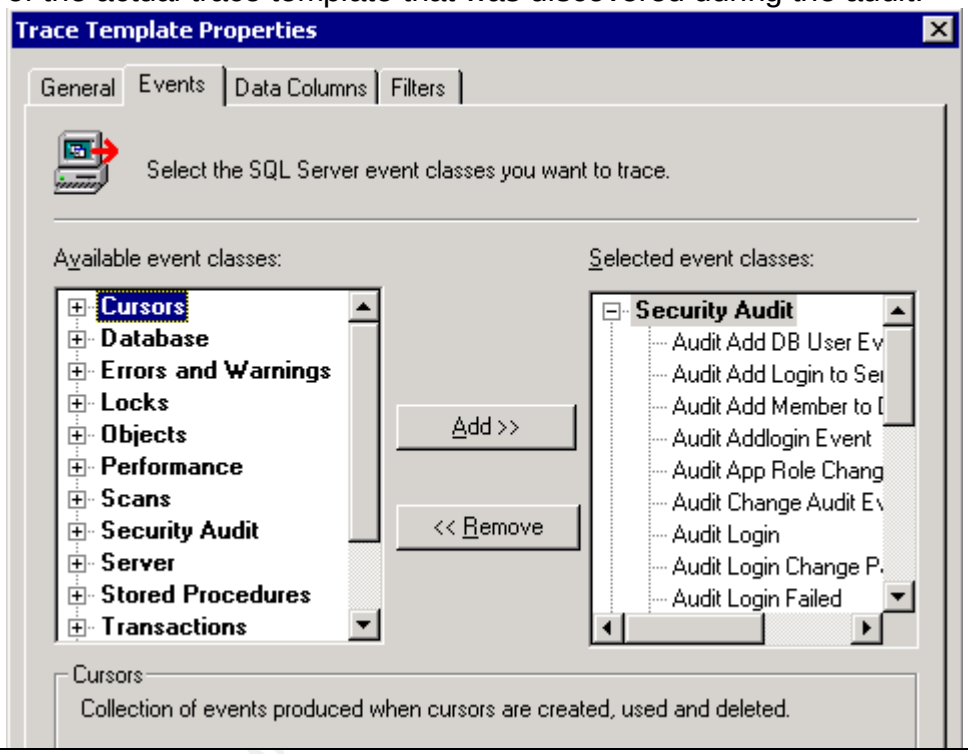
Items that must be enabled are as follows. Document any deviations

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 Failed
Login GDR
Logout
Object Derived Permission
Object GDR
Object Permission
Statement GDR
Statement Permission

Verify Trace Results

3) Select File|Open|TraceFile or TraceTable (depending on storage of traces given by administrator). Point to the location of trace files or trace template.
4) Open trace and check dates for latest activity (starttime

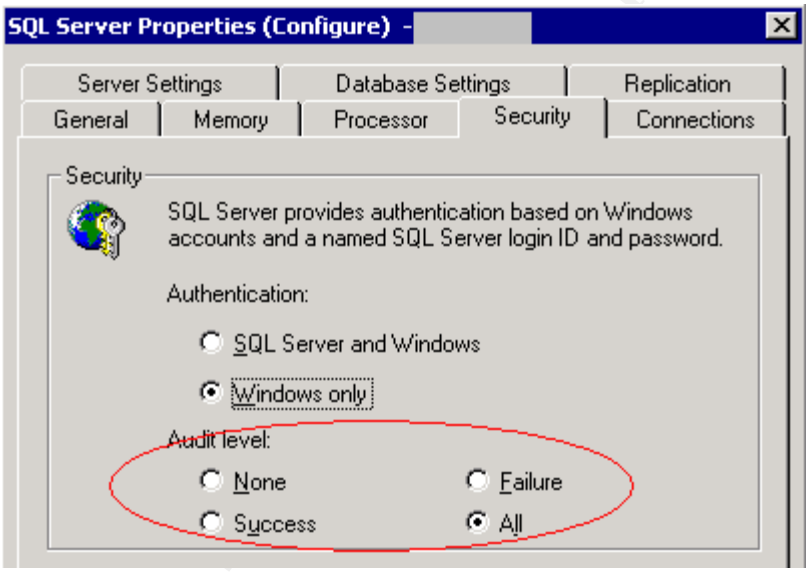
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	column). Note if the trace activity is recent. Document the findings.
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 screenshot of the actual trace template that was discovered during the audit. 
Auditor Notes / Test Results	Fail. Automated auditing of the server has not been established.

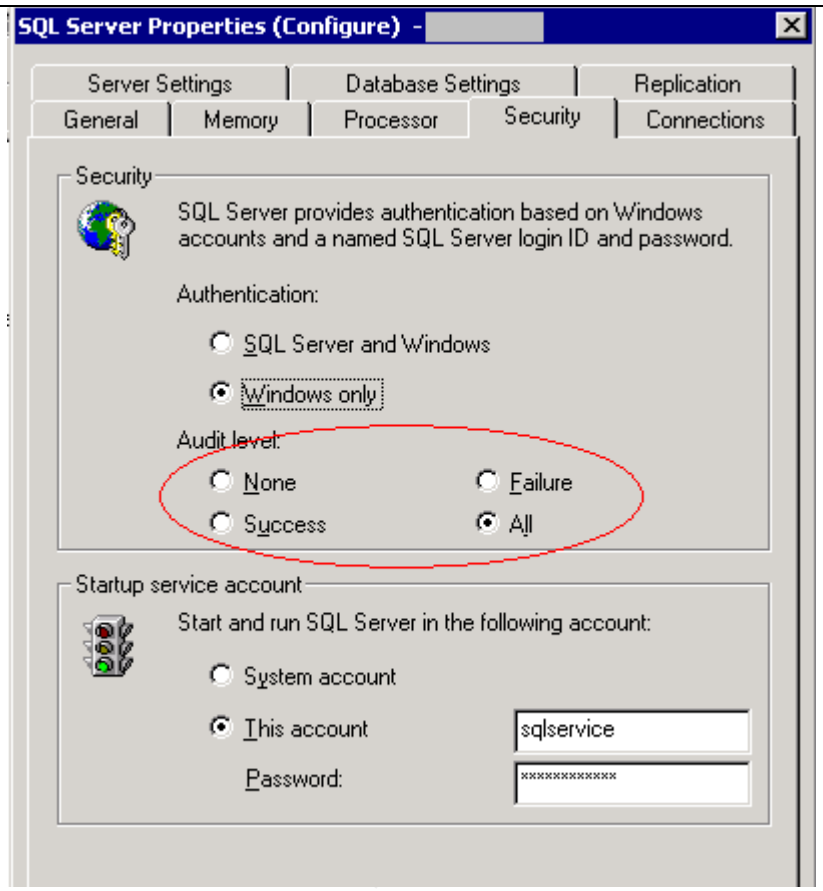
Audit 5 – Logon Auditing

Reference	Microsoft SQL 2000 Security White paper (page 54) http://www.microsoft.com/sql/techinfo/administration/2000/2000SecurityWP.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

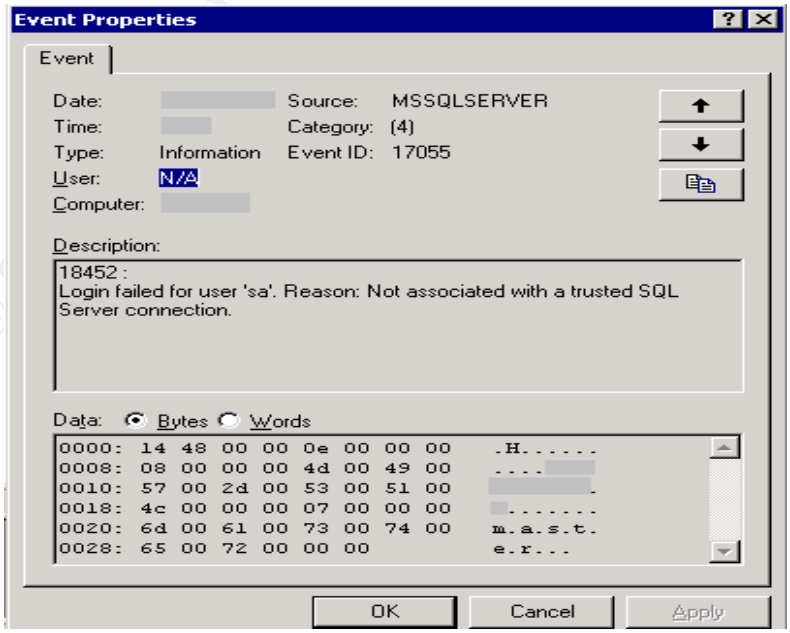
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Compliance/ Expected Test Results	is off.)
Test performed to ensure compliance	Ensure logon audit level for SQL server is set to all. 1) Access the enterprise manager (Start|Programs|MicrosoftSQLServer|EnterpriseManager) 2) Right click the server name, select properties 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.  Stimulus/Response Test: 4) Access Query Analyzer (Start|Programs|MicrosoftSQLServer|QueryAnalyzer) 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.

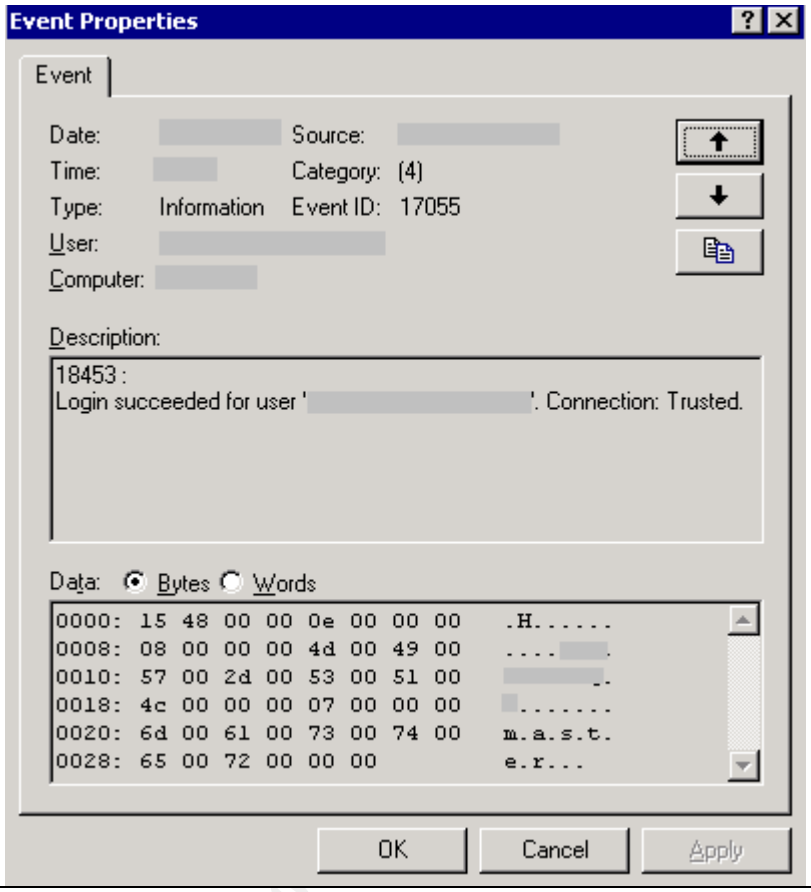
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



An invalid attempt to logon to query analyzer with a SQL account was performed and the following failure was noted in the server's application event log:



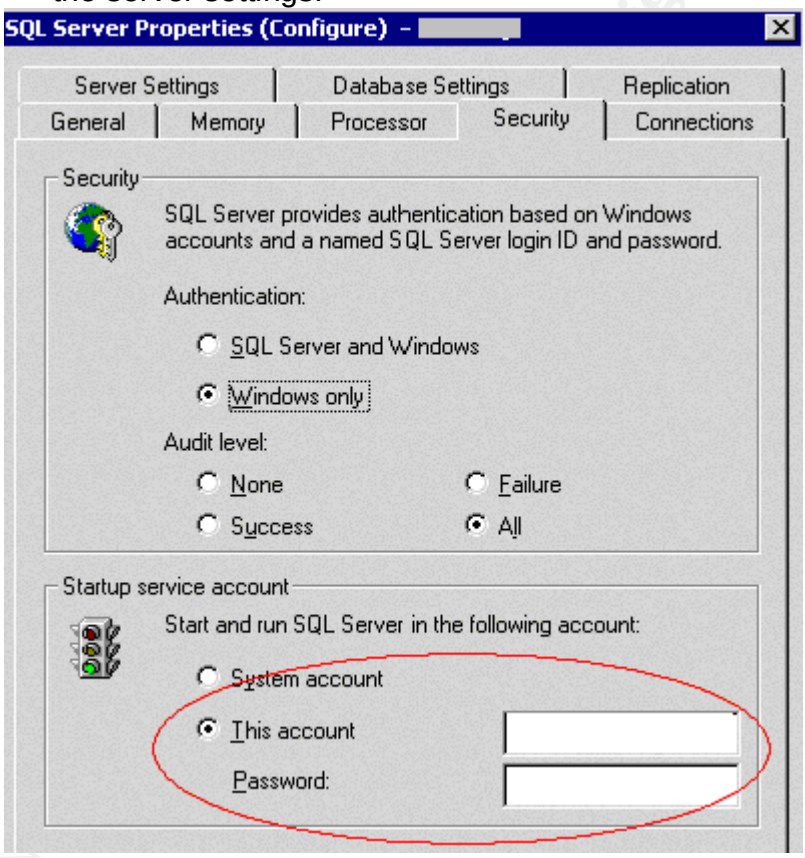
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	A valid access was noted as follows in the event log: 
Auditor Notes / Test Results	Pass. Auditing is established properly.

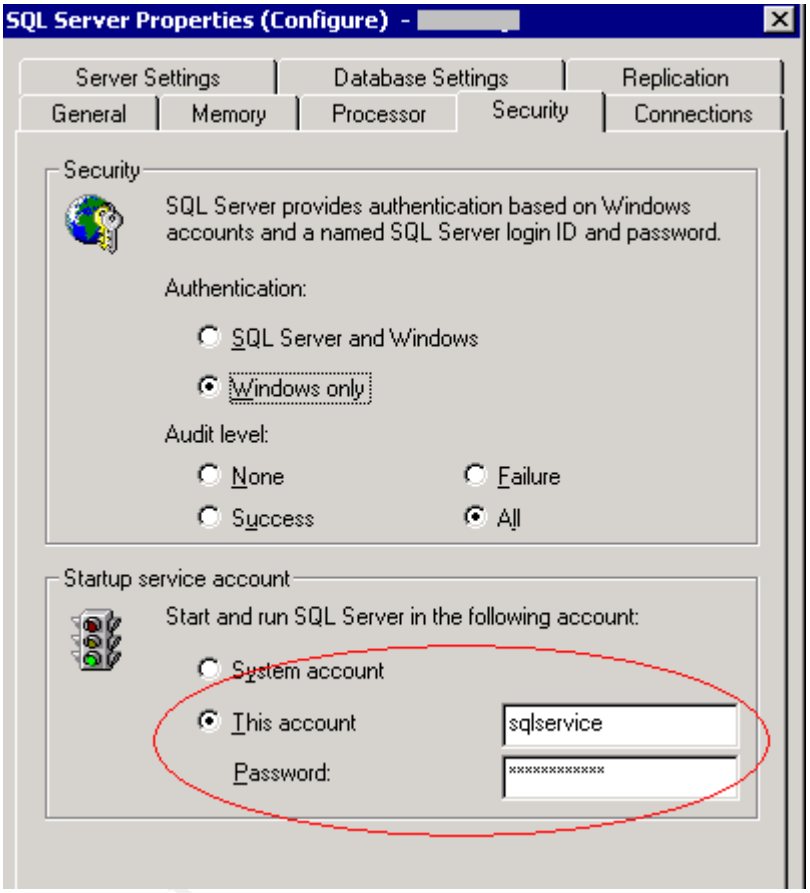
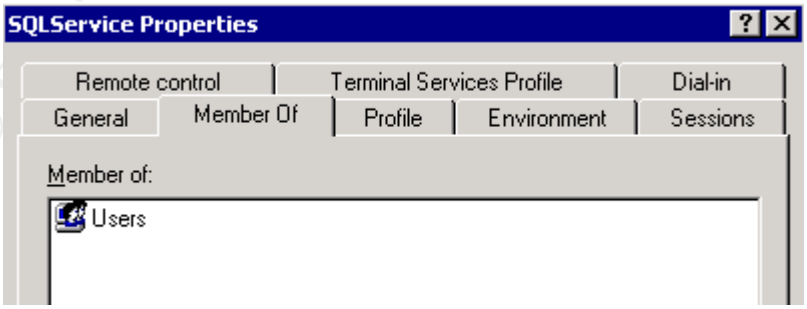
Audit 6 – SQL Service start-up accounts

Reference	Microsoft SQL 2000 Security White paper (page 51) http://www.microsoft.com/sql/techinfo/administration/2000/2000SecurityWP.doc SQL Server Security Checklist (item 4): http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4
Control Objective	The SQL service must be assigned a user level start-up account
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.

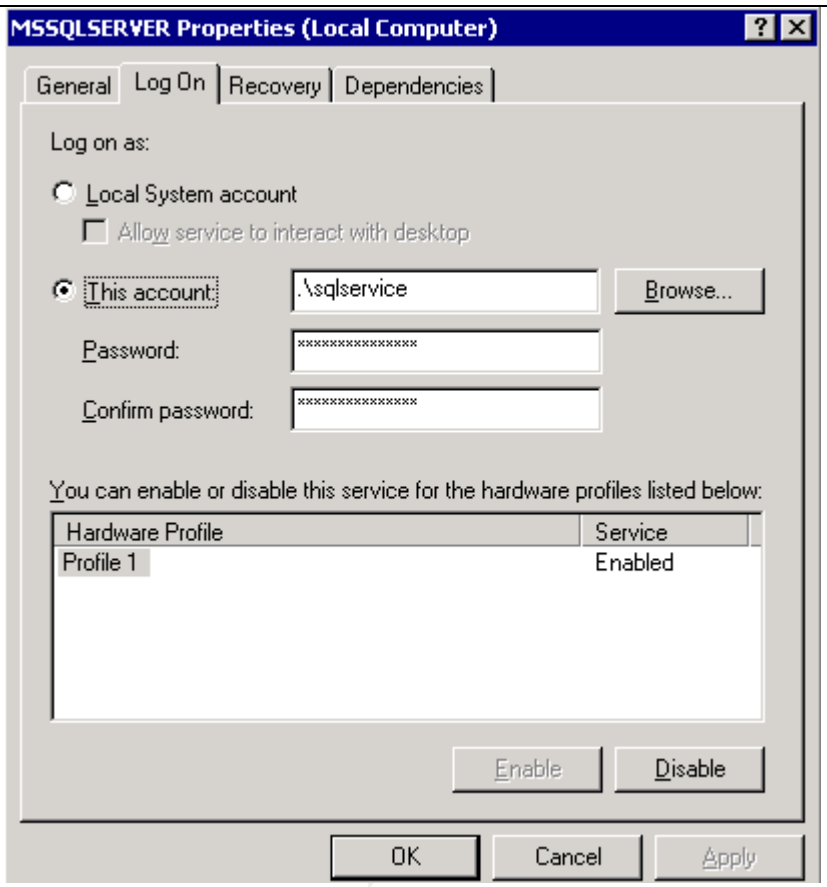
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Compliance/ Expected test results	
Test performed to ensure compliance	Check service startup account in enterprise manager. 1) Access the enterprise manager (Start|Programs|MicrosoftSQLServer|EnterpriseManager) 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.  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.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Actual Results	The server is established as having a standard user account being used to run under.  The following screenshot proves the account is a member of the local users account.  Verification was performed by accessing the properties for the SQL services in the system's control panel. The following was discovered

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	 As the screenshot shows, the SQL service is starting under the sqlservice user account.
Auditor Notes / Test Results	Pass. The server is configured to start with the context of a standard user.

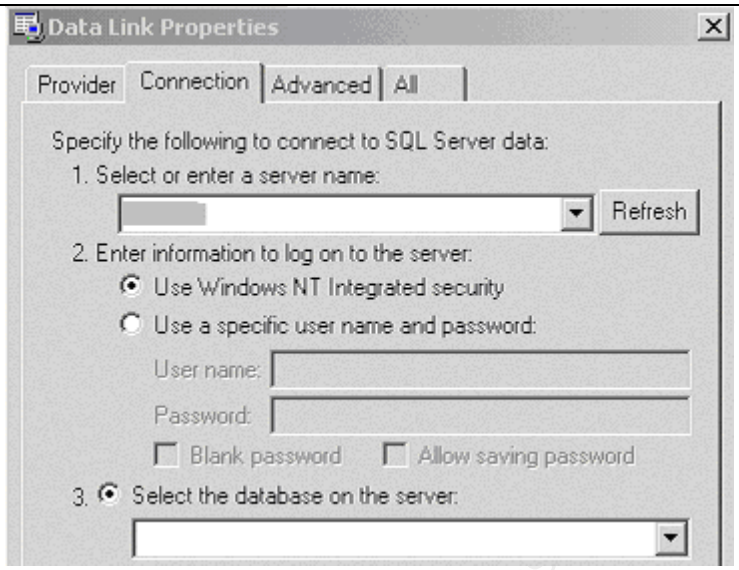
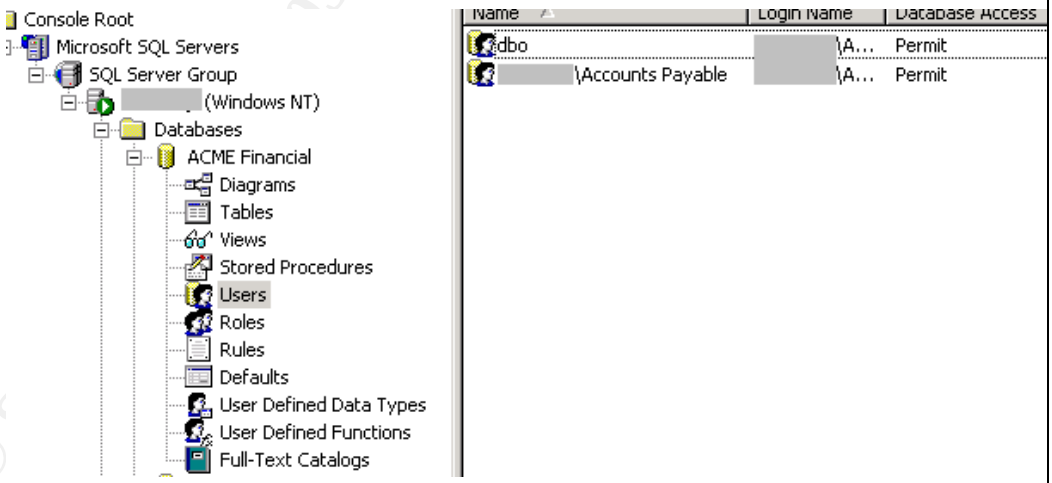
Audit 7 – Guest user access

Reference	SQL Server Security Checklist (item 8): 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/2000/2000SecurityWP.doc
Control Objective	Only authenticated accounts may access the SQL server.
Risk	Non-authenticated users have access to a database through the guest

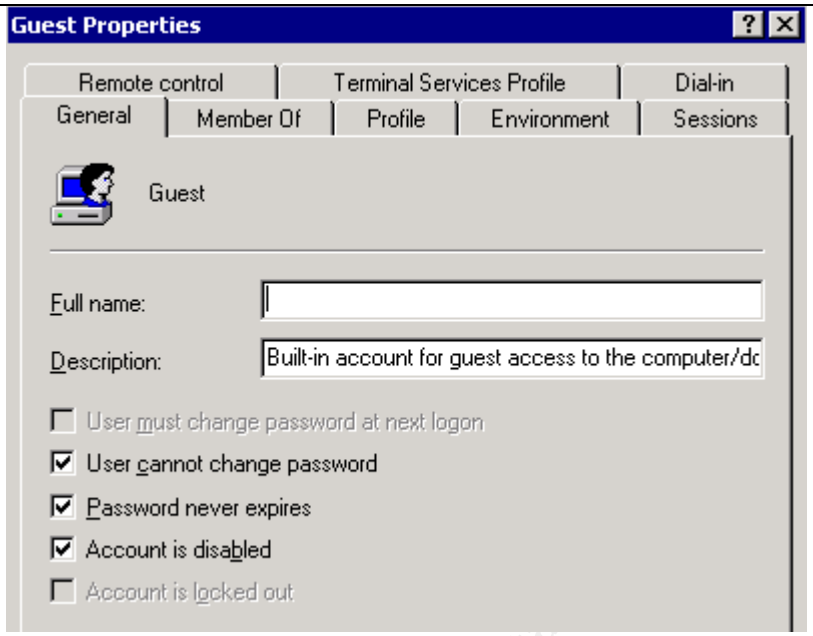
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	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	Check permissions for the guest account on sensitive databases. 1) Access enterprise manager (Start|Programs|MicrosoftSQLServer|EnterpriseManager) 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. Check guest account at O/S level 4) Access Windows users and groups settings (Start|Programs|AdministrativeTools|ComputerManagement|LocalUsersAndGroups). 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. 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). 7) Open Microsoft Access from the auditor workstation. Close any wizard that appears when opening the application. 8) Select the "new data access page". Choose design view. The "Data link properties" screen will open. 9) Enter the server name and select Windows Integrated Security. The following screenshot shows the screen that should be displayed.

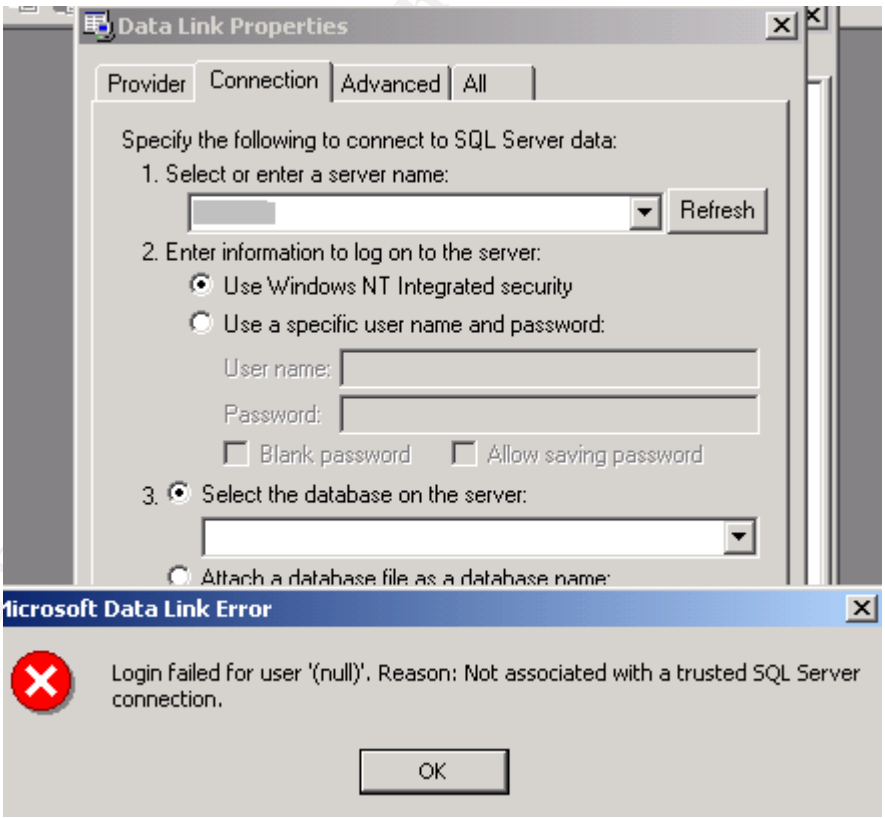
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	 10) Select the "select database on the server" pulldown box. Access should be denied. Document the findings and attach a screenshot of any errors.
Actual Results	The following screen shows that guest access is restricted from the Company database.  The Guest account has been disabled at the O/S level.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



Stimulus/Response test: The following shows the results of an access test using an account called "sqltest"



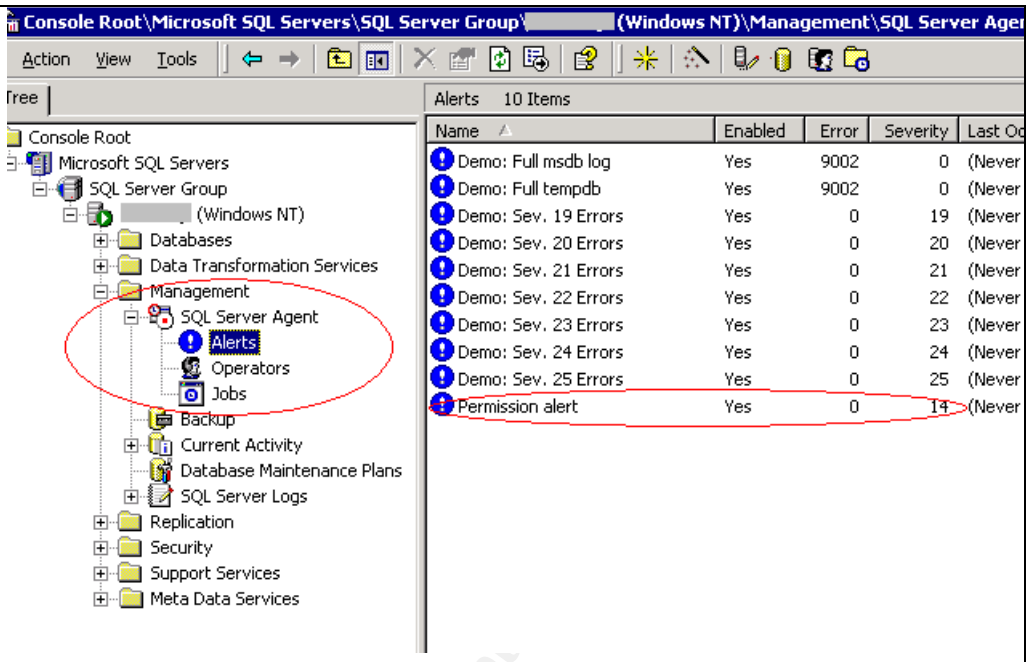
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

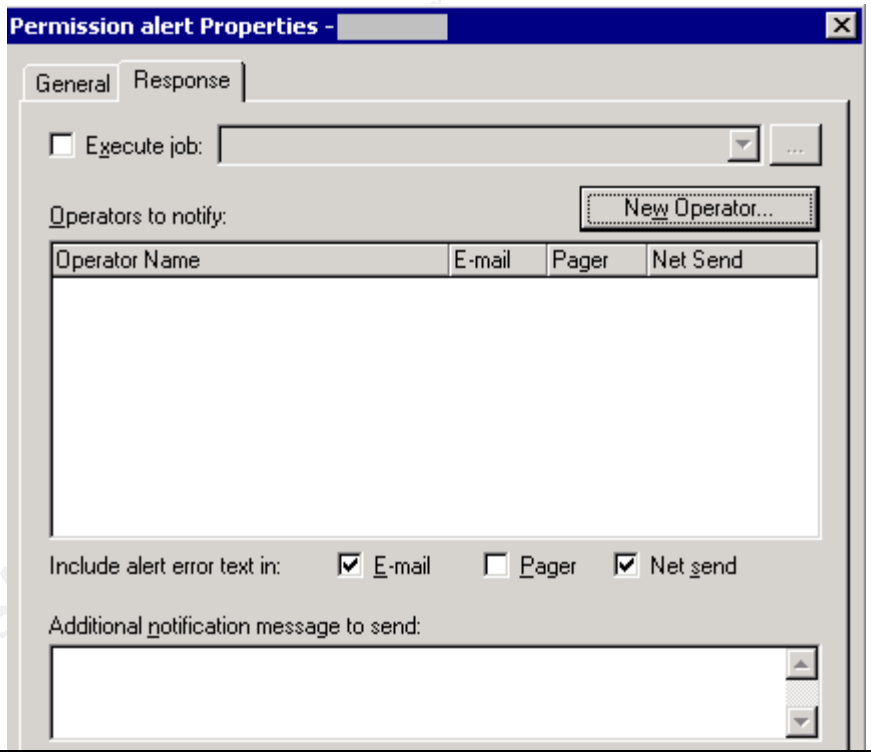
Auditor Notes / Test Results	Pass. Guest account is removed from corporate databases and the guest account has been disabled at the operating system level.

Audit 8 – Alerting

Reference	SQL Server Security Checklist (item 17): http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4
Control Objective	An alerting mechanism must be established and notification 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 Compliance/ Expected Test Results	Objective. Alerts are configured and notification will be sent.
Test performed to ensure compliance	Access the server in SQL Enterprise Manager. Select Management | SQL Server Agent | Alerts. Check for the existence of an alert for severity 14 and that an operator is defined to receive a page or e-mail. 1) Access Enterprise Manager (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.
Actual Results	Alerting has been established for the server; however, there is no notification established, nor are there any operators established.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

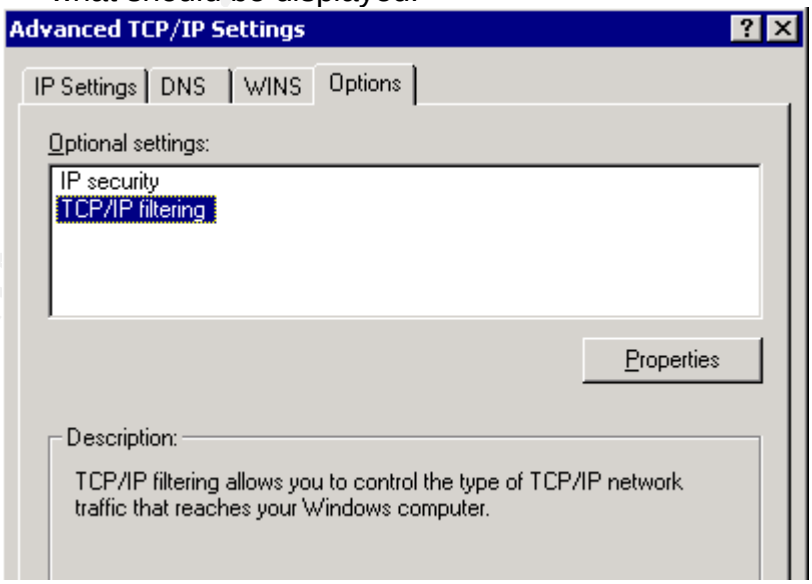




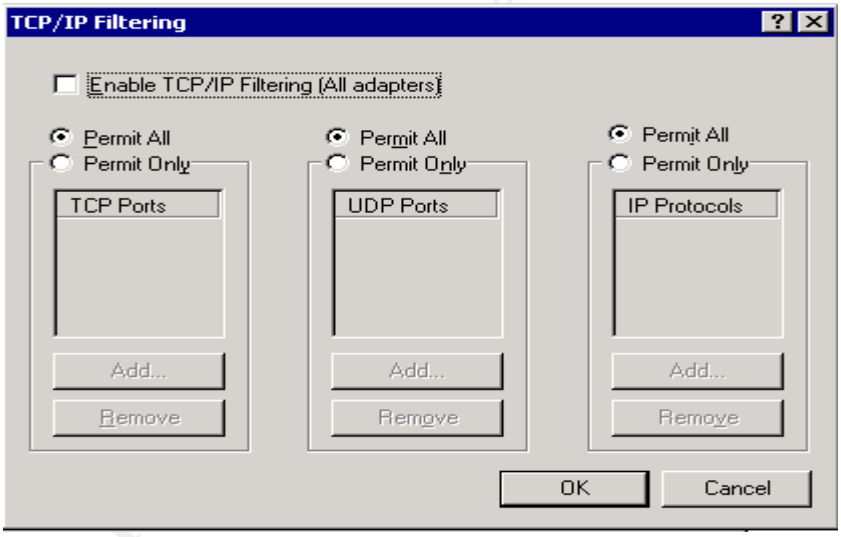
Auditor Notes / Test Results	Fail. As a result of the issues identified in the test results, there would be no alerts sent in case of a permission denial.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Audit 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.html
Control Objective	Network controls should be in place to protect the server data.
Risk	Malware can use high-level ports to communicate with an attacker and 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 Compliance / Expected test results	Objective. All ports other than the required baseline ports are filtered at the O/S level.
Test performed to ensure compliance	Check TCP/IP filtering. 1) On the server desktop, right-click the "My Network Places" icon, 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.  2) Select TCP/IP filtering, select properties. All filtered ports will be displayed at this point. Document and attach a screenshot to the

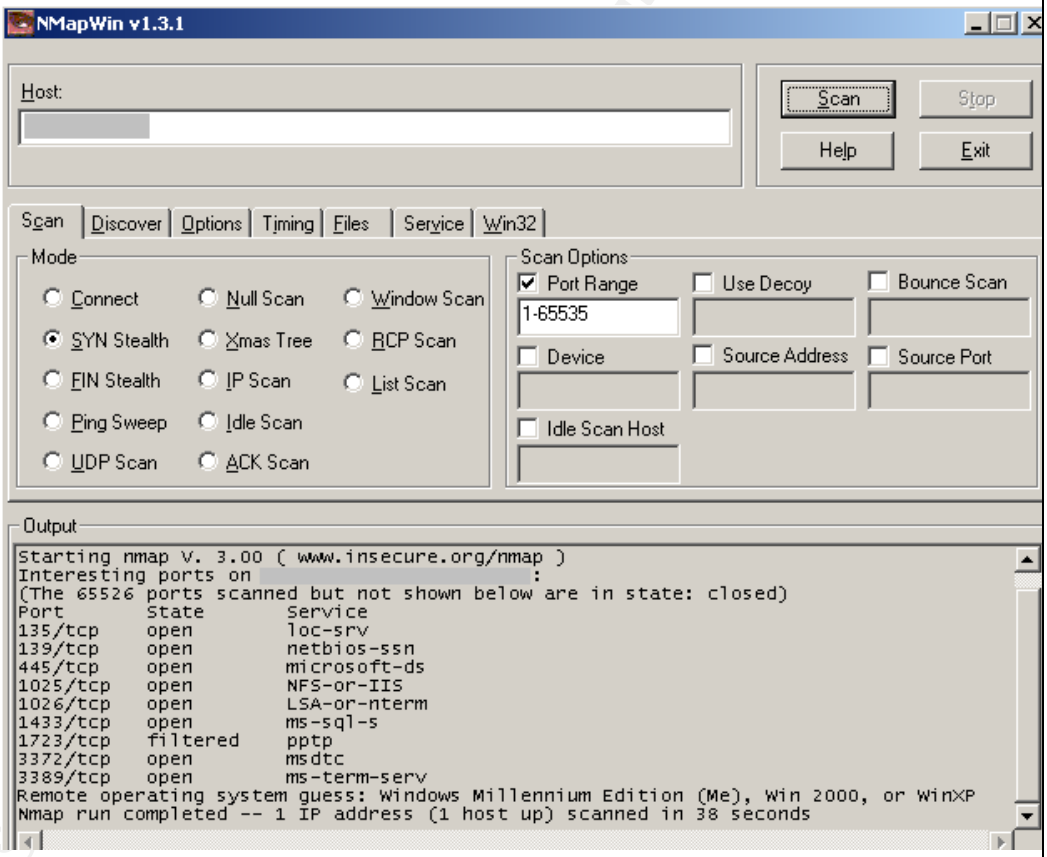
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	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 report. 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.
Actual test results	As shown in the following screenshots, port filtering is not enabled on the server.  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.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

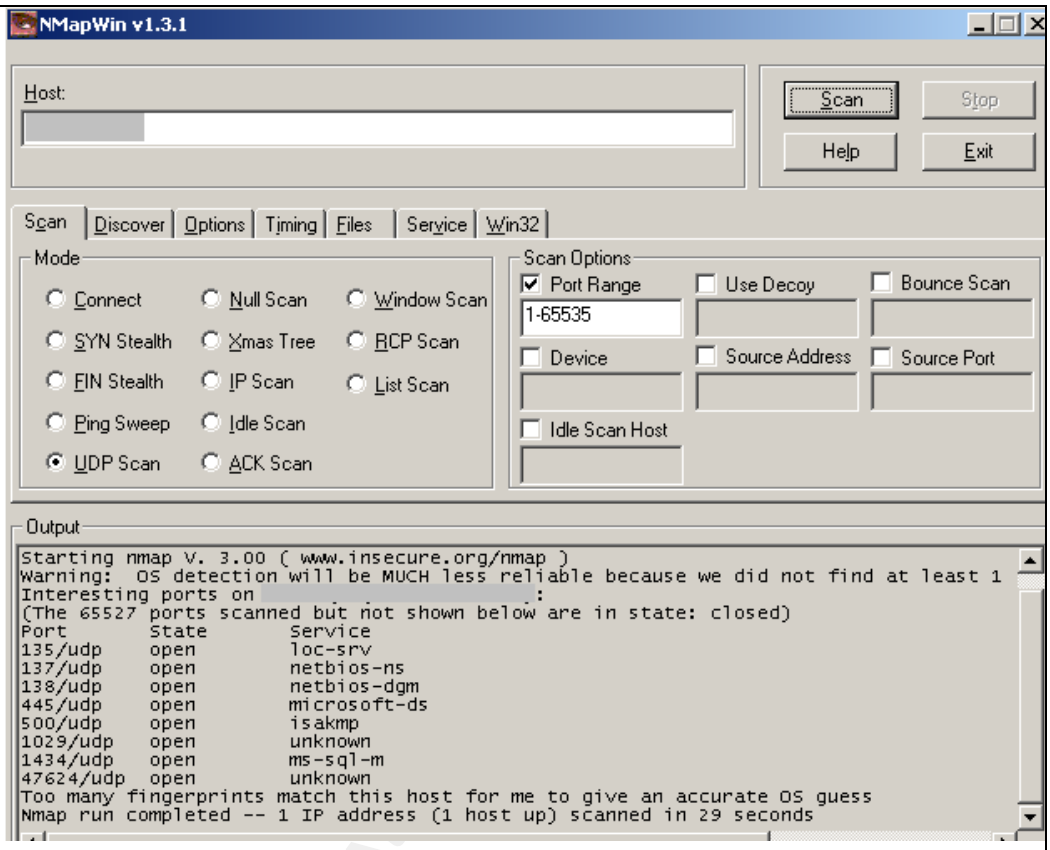
```
FPort v1.33 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid   Process          Port  Proto Path
500   svchost     ->   135   TCP   C:\WINNT\system32\svchost.exe
8     System      ->   139   TCP
8     System      ->   445   TCP
560   msdtc       ->   1025  TCP   C:\WINNT\System32\msdtc.exe
812   MSTask      ->   1026  TCP   C:\WINNT\system32\MSTask.exe
8     System      ->   1031  TCP
768   sqlservr    ->   1433  TCP   C:\PROGRA~1\MICROS~3\MSSQL\binn\sql
e
560   msdtc       ->   3372  TCP   C:\WINNT\System32\msdtc.exe
384   termsrv     ->   3389  TCP   C:\WINNT\System32\termsrv.exe

500   svchost     ->   135   UDP   C:\WINNT\system32\svchost.exe
8     System      ->   137   UDP
8     System      ->   138   UDP
8     System      ->   445   UDP
264   lsass       ->   500   UDP   C:\WINNT\system32\lsass.exe
252   services    ->   1028  UDP   C:\WINNT\system32\services.exe
768   sqlservr    ->   1434  UDP   C:\PROGRA~1\MICROS~3\MSSQL\binn\sql
e
```

NMAP TCP Results



NMAP UDP Results

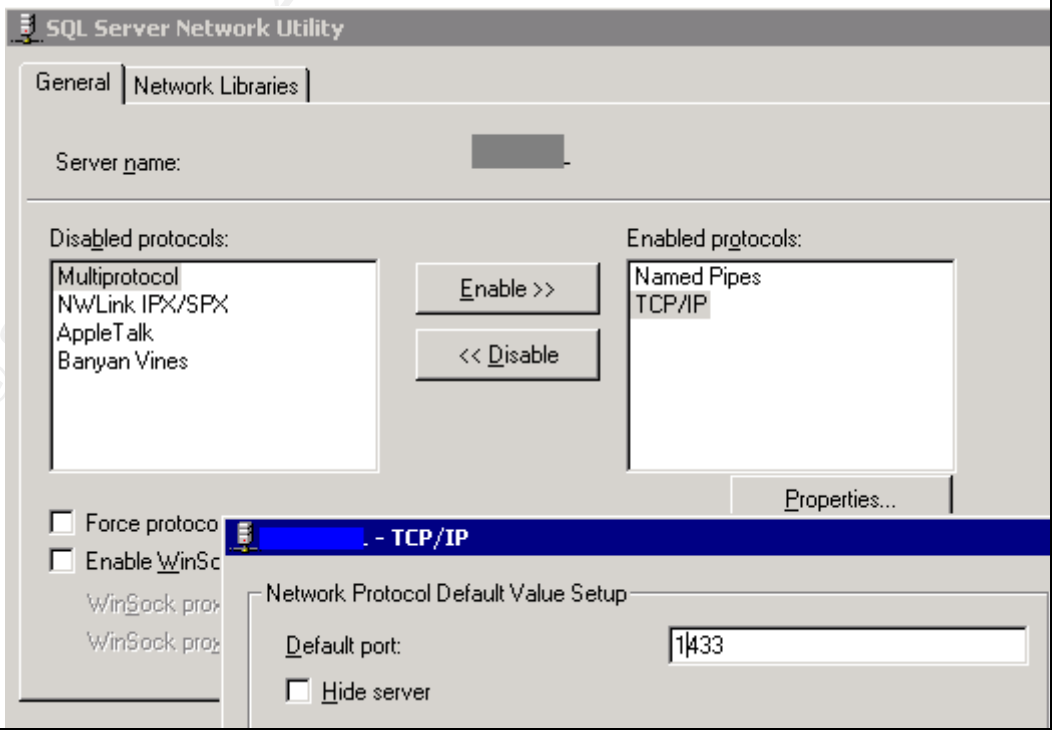
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	
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 – 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
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

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

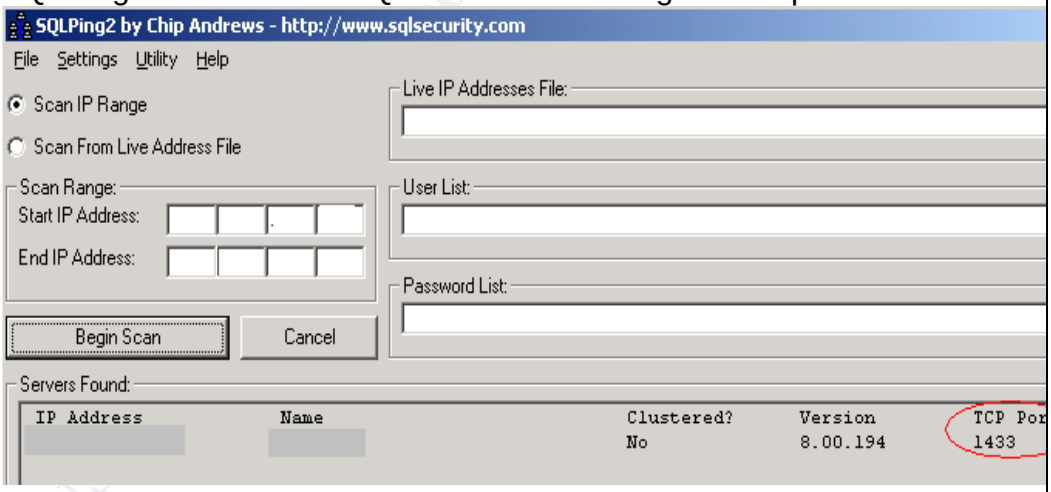
	Internet.
Likelihood	Depends on the firewall configuration.
Consequence	A potential attacker would know of the existence of the SQL server. An attacker can then use automated tools to attack server after initial the reconnaissance.
System Compliance/ Expected test results	Objective. The port value should 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	1) Access Enterprise Manager (Start|Programs|MicrosoftSQLServer|EnterpriseManager) 2) Expand the server group, right click the servername and select properties. 3) Select the Network Configuration tab. Select the TCP/IP protocol option and select properties. 4) Document the port number and determine if the server is listed as 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) Obtain sqlping2 from www.sqlsecurity.com/scripts.asp. 7) Run SQLping2 against the server IP address. 8) Document the findings and attach a screenshot to the report.
Actual test results	The SQL listening port is at its default value of TCP 1433 and the "hide server" checkbox is not selected. 

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Fport screenshot shows that all ports are at their default values.

```
C:\WINNT\System32\cmd.exe
http://www.foundstone.com

Pid   Process          Port  Proto Path
500   svchost      -> 135   TCP   C:\WINNT\system32\svchost.exe
8     System       -> 139   TCP
8     System       -> 445   TCP
556   msdtc        -> 1025  TCP   C:\WINNT\System32\msdtc.exe
808   MSTask       -> 1026  TCP   C:\WINNT\system32\MSTask.exe
8     System       -> 1030  TCP
1220  sqlservr     -> 1433  TCP   C:\PROGRA~1\MICROS~3\MSSQL\binn\sqlservr.e
e
556   msdtc        -> 3372  TCP   C:\WINNT\System32\msdtc.exe
384   termsrv      -> 3389  TCP   C:\WINNT\System32\termsrv.exe

500   svchost      -> 135   UDP   C:\WINNT\system32\svchost.exe
8     System       -> 137   UDP
8     System       -> 138   UDP
8     System       -> 445   UDP
264   lsass        -> 500   UDP   C:\WINNT\system32\lsass.exe
252   services     -> 1029  UDP   C:\WINNT\system32\services.exe
1220  sqlservr     -> 1434  UDP   C:\PROGRA~1\MICROS~3\MSSQL\binn\sqlservr.e
e

C:\tools>
```

SQLPing2 confirms that SQL Server is listening to TCP port 1433.



Auditor Notes	Fail. The listening port is at default value of 1433 and server is not hidden.

Residual Risk

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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 recommendation	Purchase of identical server platform. Time required to install software components and data migration procedures or

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

	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 recommendation	Hiring of additional resource who will be able to share the workload. 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 http://www.nextgenss.com/software/ngssquirrel.html for more information regarding this product and to download a (crippled and time bombed) trial copy of the software.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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

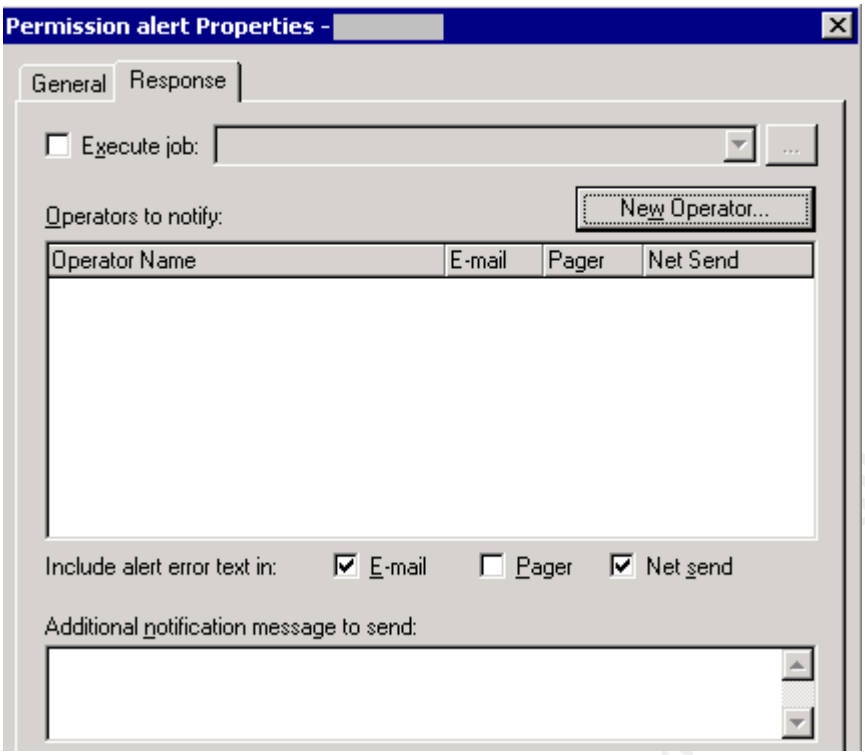
With the exception of logon auditing, there are no logs or trace tables that contain information regarding the transactions on the database. The items to trace have been established, however, no activity logs were found during the audit, which confirms that logging had not been established. The implementation 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.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



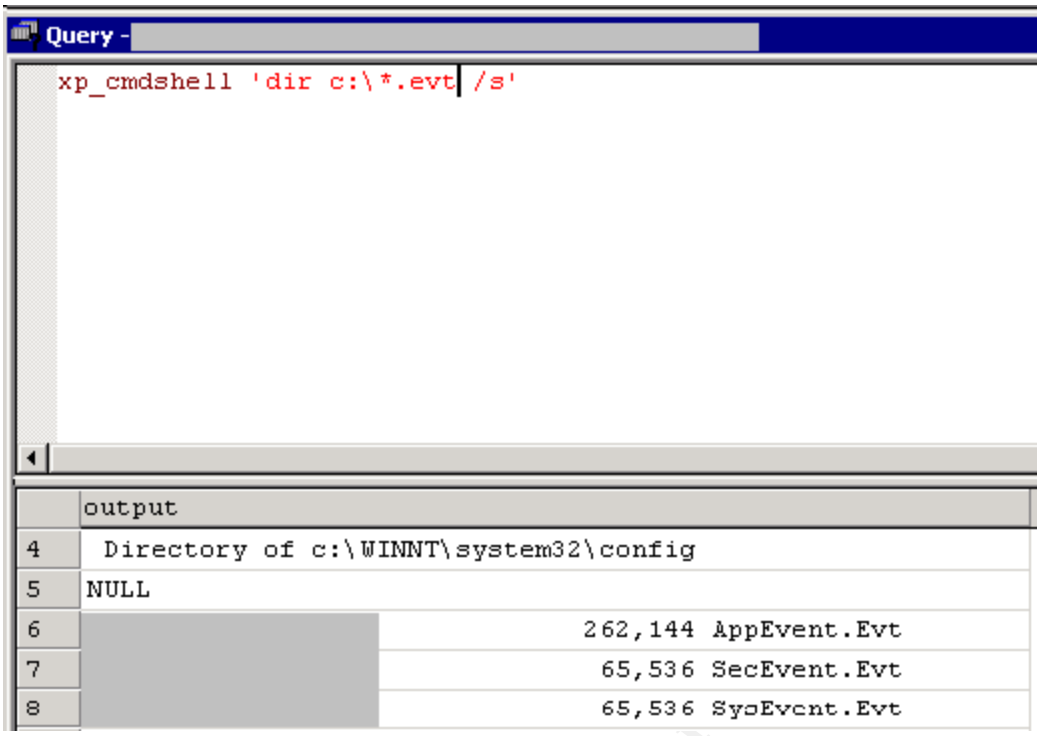
Risks

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:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



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.

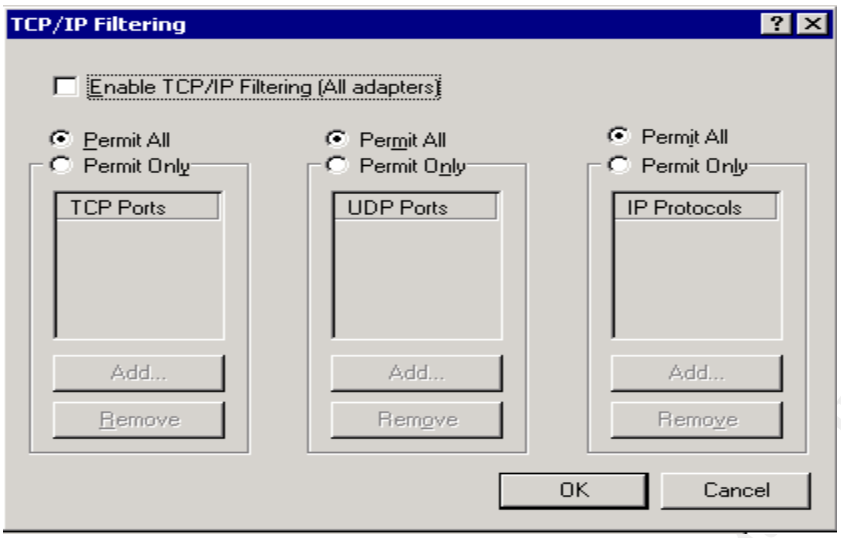
The likelihood of an attacker using these procedures to mount an attack on the server is low. However, they should be removed to mitigate the potential risk of exploitation.

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

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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



Risks

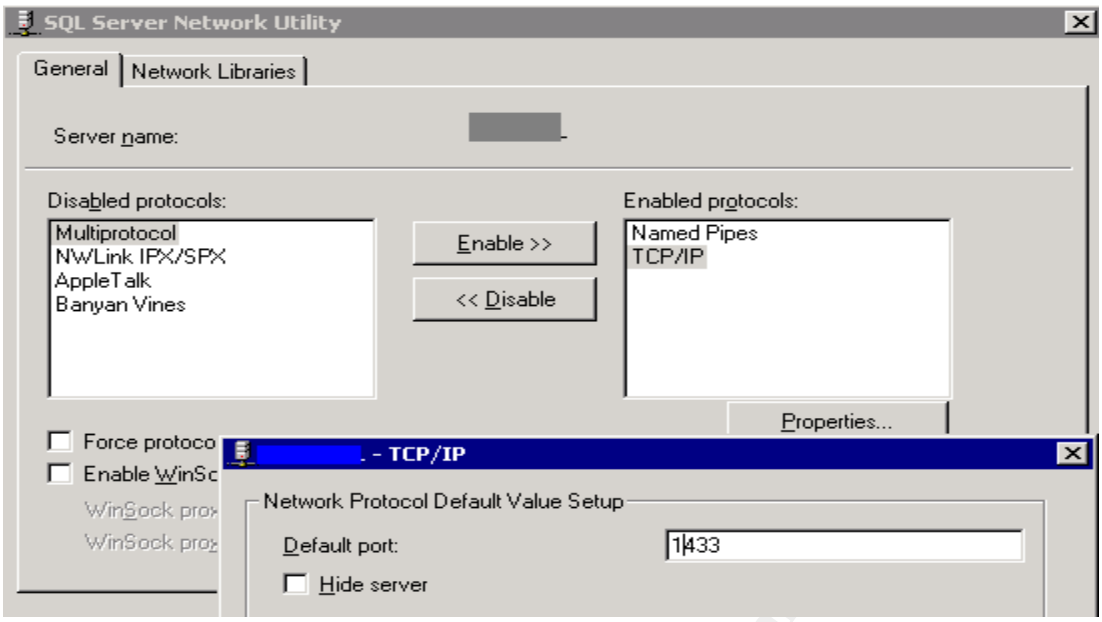
Vulnerabilities associated with malware are remote administration (e.g. Backorifice and netbus) and other Trojan applications. By having all ports open, an attacker can implement an application that will listen to the network for commands. Such applications can be used to gain complete access to the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

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



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.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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 ($3000USD @ 1.57 exchange rate)	$ 4710
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.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

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
http://icat.nist.gov/

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

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

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
http://searchsecurity.techtarget.com/bestWebLinks/0,289521,sid14_tax281918,00.html

Out-of-the-Box NT Security Checklist
http://www.windowsitlibrary.com/Content/121/18/3.html

SANS. Security Consensus Operational Readiness Evaluation
http://www.sans.org/SCORE/**checklist**s/

Overview of SQL Server security model and security best practices
http://vyaskn.tripod.com/sql_server_security_best_practices.htm

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

Microsoft. Commerce Server 2002: Using SQL Authentication
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/csvr2002/htm/cs_se_securityconcepts_sfxq.asp

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

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/sql/maintain/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
http://support.microsoft.com/default.aspx?scid=KB;en-us;80397&

Spenik, Mark Sledge, Orryn. An Overview of SQL Server's Security Model
http://www.developer.com/tech/article.php/10923_721441_1

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

Talmage, Ron**.** Auditing in SQL Server 2000
http://www.itworld.com/nl/db_mgr/04162001/

Utility Download Sources

Fport: http://www.foundstone.com/knowledge/free_tools.html

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

SQLPING2: www.sqlsecurity.com/scripts.asp

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

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.