

Global Information Assurance Certification Paper

Copyright SANS Institute Author Retains Full Rights

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

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

Graham Thompson

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

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

| 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 | |
| Research references | 79 |

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

Company Overview

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

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

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

ACME Physical Network Layout



ACME Financial Network Diagram

Identify the system to be audited

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

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

Evaluate risk to the system

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

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

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

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

Table 1: System risks

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

Present state of SQL Server 2000 auditing

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

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

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

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

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

- SQL 2000 Security white paper. The vendor has created a SQL 2000 Security white paper to document vendor recommended best practices and procedures. The white paper can be found at: 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: <u>http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4</u>.
- Luis Medina has created a good series of SQL security tips. The "Empirical hacker – Protect your database" series can be found at: <u>http://searchnetworking.techtarget.com/tip/1,289483,sid7_gci845040,00.html</u>

Assignment 2: Create an Audit Checklist

Check 1 - Service Pack and Hot Fix levels

| Reference | Search on ICAT Metabase for known SQL Server 2000 vulnerabilities: http://icat.nist.gov Microsoft Baseline Security Analyzer (MBSA) homepage (information |
|--------------|---|
| | and download link): |
| | http://www.microsoft.com/technet/treeview/default.asp?url=/technet/secu |
| | rity/tools/Tools/MBSAhome.asp |
| Control | Exposure to published vulnerabilities must be |
| Objective | 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 | The test results are objective. All relevant patches for the system must |
| Compliance/ | be installed. The MBSA must state there are no hotfixes missing on the |
| Expected | server |
| Results | JOU - |
| Test | 1) From the auditor's workstation with Internet access, obtain and |
| performed to | run Microsoft Baseline Security Analyzer (MBSA). |
| ensure | (Start Programs MBSA). |
| compliance | 2) Select "scan a computer", enter the name or IP address of the |
| | server. |
| | |

| | 🍪 Microsoft Baseline Security Analyzer | [|
|-------------------------------|--|----------|
| | Baseline Security Analyzer | cro |
| | Microsoft Baseline Security Analyzer Welcome Pick a computer to scan Pick a computer to scan Pick multiple computers to scan Pick a security report to view View a security report See Also Microsoft Baseline Security Analyzer Help About Microsoft Baseline Security Analyzer Microsoft Security Web site | · its IP |
| Test Results Auditor Notes | 2002 Microsoft Corporation. All rights reserved. 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 discover to actual results section of checklist | і. З |

Check 2 – Stored Procedures

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

| System Compliance/ Expected Results | Subjective. Stored procedures shou where possible. Xp_cmdshell shoul it is required. | Ild be restricted from g d be removed from the | jeneral usage e server unless |
|--|---|--|--|
| Test performed to ensure compliance | Check for existence of stored processigned. To check the stored processigned. To check the stored processigned. To check the stored processigned. 1) Access the SQL Enterprise M (Start Programs MicrosoftSQ 2) Expand the SQLServerGroup 3) Select the Databases tab, the 4) Select "stored procedures" are container. | dures and which perm edures: lanager LServer EnterpriseMan and access the serve an access master data nd "extended stored pr | issions are nager) er. base rocedures" |
| | Tree | Extended Stored Procedures 173 | Items |
| | Cancele Deet | Name A | Owner |
| | Consule Root | Sp. bindsession | dho |
| | E G SQL Server Group | sp_createorphan | dbo |
| | (Windows NT) | sp_cursor | dbo |
| | 🖻 📄 Databases | sp_cursorclose | dbo |
| | 🛨 🗋 👘 🕛 | sp_cursorexecute | dbo |
| | 🖻 🔋 master | sp_cursorfetch | dbo |
| | Tables | sp_cursoropen | dbo |
| | - Go' Views | sp_cursoroption | dbo |
| | Stored Procedures | sp_cursorprepare | dbo |
| | Extended Stored Procedur | es sp_cursorprepexec | dbo |
| | | sp_cursorunprepare | dbo |
| | | sp_droporphans | dbo |
| | Defaults | sp_execute | dbo |
| | Liser Defined Data Types | sp_executesql | dbo |
| | - Cost Defined Functions | sp_fulltext_getdata | dbo |
| | Full-Text Catalogs | sp_getbindtoken | dbo |
| | 🕀 🔋 model | sp_GetMBCSCharLen | dbo |
| | 😟 🔋 🗓 msdb | sp_getschemalock | dbo |
| | 庄 🛛 🚺 Northwind | sp_IsMBCSLeadByte | dbo |
| | 🕀 🕛 pubs | sp_MSgetversion | dbo |
| | 🔺 📑 🕛 tempdb | Sp_OACreate | dbo |
| | 📜 📋 Data Transformation Services | Sp_OADestroy | dbo |
| | 🕀 🛄 Management | sp_OAGetErrorInfo | dbo |
| | | sp_OAGetProperty | dbo |
| | | | |
| | Individually select all listed st following table and check per and selecting the permissions include in the report. | ored procedures found missions by double-cli s tab. Document all pe | d in the cking name ermissions and |



| | 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). |
|--------------------------|--|
| | |
| | Query - Untitled1* |
| | xp_cmdshell 'dlr C:*.evt /s' |
| | 7) Document the findings and attach a screenshot to the report. This test will prove if xp_cmdshell is still present on the server. |
| Actual | |
| Results Auditor Notes | |

Check 3 – Authentication Model

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

| Consequence | Potential loss of confidentiality if an attacker gains access to the server |
|---|---|
| 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. |
| | Server Settings Database Settings Replication General Memory Processor Security Security SQL Server provides authentication based on Windows accounts and a named SQL Server login ID and password. Authentication: SQL Server and Windows SQL Server and Windows Windows only Stimulus/Response test 4) 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)) |
| | SA |

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

Check 4 – Audit Activity on server

| Reference | SQL Server books online ("auditing SQL Server activity" as a search parameter). |
|---|--|
| Control 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. |
|--|
| Trace Template Properties |
| General Events Data Columns Filters |
| Select the SQL Server event classes you want to trace. |
| A <u>v</u> ailable event classes: <u>S</u> elected event classes: |
| Image: Cursors ▲ Image: Database ▲ Image |
| Collection of events produced when cursors are created, used and deleted. |
| Items that must be enabled are as follows. Document any deviations Add DB User Event Add Login to Server Add Login to Server Role Add Member to DB Role Add Login App Role Change Password Change Audit Login Login Change Password Login GDR Logout Object Derived Permission Object GDR Object Permission Statement GDR Statement Permission |
| 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. |
|---------------|---|
| | 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

| Deference | Microsoft SOL 2000 Security White paper (page 54) |
|--------------|---|
| Relefence | Wilcioson SQL 2000 Security while paper (page 54) |
| | http://www.microsoft.com/sql/techinfo/administration/2000/2000Security |
| | WP.doc |
| | |
| Control | All system access must be logged. |
| Objective | |
| Risk | A lack of tracing which accounts are failing logon attempts. If not |
| | established, an attacker can attempt a brute force attack on the server |
| | and no evidence of the attack will be available. |
| Likelihood | High. Auditing of server logon attempts is not enabled by default. |
| Consequence | If not configured, no failed logon detection is possible. |
| System | Objective. Logging of failed SQL logins is turned on (the default setting |
| Compliance/ | is off.) |
| Expected | Ϋ́Υ |
| Test Results | |
| Test | Ensure logon audit level for SQL server is set to all. |
| performed to | 1) Access the enterprise manager |
| ensure | (Start Programs MicrosoftSQLServer EnterpriseManager) |
| compliance | 2) Right click the server name, select properties |
| • | 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 |
| | Server settings. |
| <u> </u> | |
| | |
| | |
| | |

| | SQL Server Properties (Configure) - |
|---------------|--|
| | Server Settings Database Settings Replication |
| | General Memory Processor Security Connections |
| | Security SQL Server provides authentication based on Windows accounts and a named SQL Server login ID and password. Authentication: SQL Server and Windows SQL Server and Windows Mindows only Audit level: Solution Contemposities Con |
| | |
| | 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. |
| | 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) |
|-------------|--|
| C | http://www.microsoft.com/sql/techinfo/administration/2000/2000Security |
| | WP.doc |
| | |
| | SQL Server Security Checklist (item 4): |
| | |
| | http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4 |
| Control | The SQL service must be assigned a user level start-up account |
| Objective | |
| Risk | Excessive rights assigned to SQL service. |
| Likelihood | Medium. Depends on the server configuration |
| Consequence | These rights can be used by an attacker to increase their privilege on |

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

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

Check 7 – Guest user access

| Reference | SQL Server Security Checklist (item 8): http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4 |
|----------------------|---|
| | Microsoft SQL 2000 Security White paper (page 58) |
| | <u>WP.doc</u> |
| 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 | Objective. The guest account is removed from all sensitive databases. |
| Compliance/ | The guest account at the operating system level must be disabled. |
| Expected test | |
| results | |
| | Check permissions for the guest account on sensitive databases. |
| performed to | 1) Access enterprise manager (Start/Brograms/MicrosoftSQL Server/Enterprise/Manager) |
| ensure | (Start Programs with crossing a server the target convertible access the |
| compliance | 2) Expand the server group, open the target server then access 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. |
| C | Check guest account at O/S level |
| C | Access Windows users and groups settings |
| | (Start Programs AdministrativeTools ComputerManagement Loca IUsersAndGroups). |
| | 5) Double-click users tab. Double click guest account. Ensure |
| | "account is disabled" box is checked. Document findings and attach a screenshot. |
| | Stimulus/Response test: Attempt to access the server with an |
| | account not listed as having access to ensure that access is denied |
| | account net noted as having accoust to choure that accoust to defined. |

| 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. |
|--|
| 🗒 Data Link Properties 🔀 |
| Provider Connection Advanced All |
| Specify the following to connect to SQL Server data: 1. Select or enter a server name: |
| 2. Enter information to log on to the server: |
| Use Windows NT Integrated security |
| Use a specific user name and password. |
| |
| Password: |
| Diank password Milow saving password Select the database on the server |
| |
| 10) Select the "coloct database on the server" nulldown have |
| Access should be denied. Document the findings and attach a screenshot of any errors. |
| Auditor Notes |

Check 8 – Alerting

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

| Consequen | No response would be possible if alerting is not enabled. |
|---|---|
| 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 | |

Check 9 – TCP/IP Port filtering

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

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

Check 10 – SQL Port

| Reference | Medina, Luis, Empirical Hacker – Protect your database series - part one, checklist item 2. | | | |
|---------------|---|--|--|--|
| | http://searchnetworking.techtarget.com/tip/1,289483,sid7_gci845040,00.html | | | |
| | JĠ° | | | |
| | Partlow, Joe, Microsoft SQL Server 2000 Security Overview (page 6) | | | |
| | http://www.giac.org/practical/Joe_Partlow_GSEC.doc | | | |
| | | | | |
| 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 Salping2 (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 | Objective. The port value should be changed from the default and the | | | |
| Compliance/ | server port should be hidden. This will change both the listening port and | | | |
| Expected test | hide the actual SQL port in use from sqlping2. | | | |
| results | ý. | | | |
| Test | 1) Access Enterprise Manager | | | |
| performed to | (Start Programs MicrosoftSQLServer EnterpriseManager) | | | |
| ensure | 2) Expand the server group, right click the servername and select | | | |
| compliance | 3) Select the Network Configuration tab. Select the TCP/IP protocol | | | |
| | ontion and select properties | | | |
| | 4) Document the port number and determine if the server is listed as | | | |
| | hidden ("hide server" checkbox selected). | | | |
| | Stimulus/Beenenge tests: | | | |
| | 5) Pup faort on the server to confirm which part the SOL Server is | | | |
| | listening to Document findings and attach screenshot | | | |
| | 6) Obtain salping2 from www.salsecurity.com/scripts.asp. | | | |
| | 7) Run SQLping2 against the server IP address. | | | |
| | 8) Document the findings and attach a screenshot to the report. | | | |
| | | | | |
| Auditor Notes | | | | |

Check 11 – Password Strength

| Reference | Cert Advisory # 635463: http://www.kb.cert.org/vuls/id/635463 | | | |
|--------------|---|--|--|--|
| | SOL Server Security Checklist (item 3): | | | |
| | http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4 | | | |
| Control | All passwords must meet corporate minimum length requirements | | | |
| Objective | | | | |
| Risk | Simple and blank passwords can be easily guessed and/or be broken by an attacker with a dictionary attack. | | | |
| Likelihood | Medium. SQL Server 2000 allows for a default password of <null> for</null> | | | |
| | the SA account. Factors such as personnel security training/awareness | | | |
| | and the initial compromise required to access the password hashes | | | |
| | mitigate the potential loss through weak passwords (if SQL | | | |
| | authentication is used). | | | |
| Consequence | Loss of all Confidentiality, Integrity and Availability through the guess of | | | |
| | a simple administrative level password. | | | |
| System | Objective. Security policy states minimum password strength (6 | | | |
| Compliance: | characters and complex password requirements) must be followed to | | | |
| | meet company security policy. This applies to both SQL and O/S level | | | |
| | passwords. The system must reject weak passwords at an O/S level. | | | |
| Test | 1) From the auditor's workstation with Internet access, obtain and | | | |
| performed to | run Microsoft Baseline Security Analyzer (MBSA). | | | |
| ensure | (Start Programs MBSA). | | | |
| compliance | 2) Select "scan a computer", enter the name or IP address of the | | | |
| | Server. | | | |
| | a) Ensure that SQL component will be analyzed. Select start scan. 4) The application will deverted the latest vulnerabilities from | | | |
| | 4) The application will download the fatest vulnerabilities from Microsoft Account the download of the yml file | | | |
| | 5) The MRSA will now scan the converte determine which | | | |
| | authorization mode the server is using and will determine if there | | | |
| | are any weak SOL passwords on the SOL server | | | |
| l | | | | |

| √ | 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 |
| v | 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 |
| V | 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/Re | esponse Te | est: |
| 1) Requ you v | uest that the past th | e administrator create a test account and supply sword. |
| 2) Logo | n to the ac | count and attempt to change password (Ctrl-Alt- |
| _, _ege | change pa | ssword) to a null value. The system should reject |
| this r | assword | Document the test results and attach to the report |
| 3) Attor | not to char | becoment the test results and attach to the report. |
| 3) Aller | | iveral Degument the test results and attack to the |
| rejec | t this pass | word. Document the test results and attach to the |
| repo | rt. | |
| 4) Atter | npt to char | nge password to "qwerty123!". The system should |
| acce | pt this pase | sword. Document the test results and attach to |
| the r | eport. | |
| | | |
| SQL passw | ord strenat | h testing with a dictionary attack (use only for |
| systems wit | h SQL aut | hentication implemented). |
| 1) Ohta | in the SOI | BE brute force/dictionary cracker for SOL server |
| (http | | re net/tools isn2id=10) |
| $2) \bigcirc$ | in a distice | <u>renevicologic in unovailable</u> A distingent file ser |
| | | ary me if one is unavailable. A dictionary file can |
| be ol | stained froi | m <u>ttp://ttp.ox.ac.uk/pub/wordlists/dictionaries/</u> . |
| Obta | in the pock | et-dict.gz dictionary. Expand with winzip and |
| save | to the sam | ne directory as the sqlbf application. Rename the |
| file to | pocket.di | ct. |
| 3) Oper | the Quer | / Analyzer |
| (Stor | tlPrograms | MicrosoftSOI ServerlOuervAnalyzer) |
| | the fellow | ing commond, "coloct name recovered from |
| 4) ISSUE | | ing command: select name, password from |
| mast | ersysxlog | ins". This will extract all accounts and passwords |
| store | ed on the S | QL server and display the hash values. Select all |
| entrie | es, copy wi | th <ctrl-c> and save to a new text file called</ctrl-c> |
| salha | ash.txt in th | e same directory as the sulbf application. Modify |
| the t | ext file so t | hat there is the name followed by a comma |
| | | |
| 101101 | and by the | bach value of the user password. Ensure that |
| TOIIO | wed by the | hash value of the user password. Ensure that |

| | 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

| Check 12 – So Reference | QL ACLS Microsoft SQL 2000 Security White paper (page 53) http://www.microsoft.com/sql/techinfo/administration/2000/2000SecurityWP.doc SQL Server Security Checklist (item 5): |
|--|--|
| Control | http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4 Users must be given least privilege to data. |
| Objective Risk Likelihood | An attacker can obtain information through weak O/S Access Control. 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 System Compliance/ Expected test results | Elevation of privilege can occur resulting in loss of confidentiality. 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 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 *.*" /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 SQL Server *.*" /c. (replace path as required to point to location of the squere *.*" /c. (replace the path cacles *.*" /c. (replace the path cacles *.*" /c. (replace path as required to point to the report . Document any deviations. |

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

Check 13 – Excessive account permissions

| Reference | Microsoft SQL 2000 Security White paper (page 30) |
|--------------|--|
| | http://www.microsoft.com/sql/techinfo/administration/2000/2000SecurityWP.doc |
| Control | Users must be given least privilege to data. |
| Objective | |
| Risk | Users may see information to which they are not privileged. |
| Likelihood | Medium. Depends on the server security configuration. |
| Consequence | Accidental or malicious activity on sensitive information can occur if the |
| | permissions exceed the required level. |
| System | Subjective. Least privilege assigned is to users. Only the owner of the system |
| Compliance/ | will be able to determine who should be given access and what level of access |
| Expected | control is required. |
| Test Results | |
| Test | Review the rights to all tables containing sensitive data in SQL. Check the |
| performed to | rights to the views created. |
| ensure | 1) Access Enterprise Manager |
| compliance | (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. |
| | |
| | |

| l | | | |
|---------------|------------------------------------|--|-----------------|
| | 🔚 miw-sql - Terminal Server Client | | |
| | Action View Tools 🗍 🖙 🔿 💽 🔝 | X 💣 🗹 🗟 😫] 🔆 🔅 | ► Q |
| | Tree | Tables 33 Items | |
| | Console Root | Name 🛆 | Owne |
| | A Microsoft SOL Servers | Categories | dbo |
| | 🗄 🖪 SOL Server Group | | dbo |
| | | CustomerDemographics | dbo |
| | 🗐 📃 Databases | Customers | dbo |
| | ÷ 🔋 | dtproperties | dbo |
| | 🕀 🔋 master | Employees | dbo |
| | 🕀 🕖 model | | dbo |
| | 🕀 🛄 msdb | The second secon | dbo |
| | 🖻 🔰 Northwind | T Orders | dbo |
| | art Diagrams | Products | dbo |
| | | 📰 Region | dbo |
| | | Shippers | dbo |
| | Users Roles Rules | E Suppliers | dbo |
| | | i syscolumns | dbo |
| | | syscomments | dbo |
| | | 📰 sysdepends | dbo |
| | 🖳 User Defined Data Types | sysfilegroups | dbo |
| | S. User Defined Functions | 📰 sysfiles | dbo |
| | 🔤 🖬 Full-Text Catalogs | 🗾 sysfiles1 | dbo |
| | 3) Check permissions on table to | ensure that only authoriz | zed individuals |
| | have required access Docum | nent the findings | |
| | | in ango. | |
| Auditor Notes | <u>s</u> | | |
| | | | |

Check 14 – File Sharing/NetBIOS settings

| Reference | Medina, Luis, Empirical Hacker – Protect your database series - part one, checklist item 10. <u>http://searchnetworking.techtarget.com/tip/1,289483,sid7_gci845040,00.html</u> |
|-----------------------|---|
| Control Objective | Only SQL processes are allowed to run on the server. |
| Risk | 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 |

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

Check 15 – Patch Policies and Procedures

| Reference | SANS Ottawa Conference, D Hoelzer. |
|---------------|--|
| Control | Exposure to published vulnerabilities must be reduced. |
| Objective | |
| 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 | Subjective. Ensure the policy and procedures for patch maintenance |
| Compliance: | exists. Check to see if the administrative staff follows the mandated |
| | procedures. |
| Test | Request the policy and procedures for patching of the servers. Review |
| performed to | the procedures to ensure that testing is being performed prior to |
| ensure | deployment. Ensure that all file changes introduced by the patching |
| compliance | 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 | Only SQL processes are allowed to run on the server. |
| Objective | |
| Risk | Applications can introduce vulnerabilities. Additional network ports may be |

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

Check 17 – Server Roles

| Reference | SQL Server Security Checklist (item 18): |
|---------------|--|
| | http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4 |
| | |
| | Microsoft SOL 2000 Security M/hite paper (page 16) |
| | Wilcrosoft SQL 2000 Security White paper (page 10) |
| | http://www.microsoft.com/sql/techinfo/administration/2000/2000SecurityWP.doc |
| | |
| Control | Users must be given least privilege to the data. |
| Objective | |
| Risk | Server roles can be used to elevate privilege. An attacker can embed their |
| T CION | own account in a role in order to alovate their privilage |
| | own account in a fole in order to elevate their privilege. |
| Likelihood | Medium. Roles should be reviewed to ensure that members are given |
| | appropriate privilege. |
| Consequence | Server roles contain many associated rights. Attacker can elevate privilege by |
| | adding account to server role. |
| System | Subjective. Only authorized accounts should be assigned to roles. Only the |
| Compliance/ | data owner can determine which accounts belong in a specific role. |
| Expected test | g |
| rogulto | |
| | |
| lest | 1) Access SQL Enterprise Manager |
| performed to | (Start Programs MicrosoftSQLServer EnterpriseManager) |
| ensure | 2) Select the server, choose security, then "server roles". |
| compliance | |
| | |
| | |

| | Action View Iools | × 💣 🖸 🗟 😫 🔸 🖄 | · 🕼 📵 💽 🕻 |
|---------------|---|---|--|
| | Tree | Server Roles 8 Items | |
| | Console Root | Full Name 🔺 | Name E |
| | Microsoft SQL Servers SQL Server Group Databases Data Transformation Services Management Replication Security Logins Server Roles | Bulk Insert Administrators Database Creators Disk Administrators Process Administrators Security Administrators Server Administrators Setup Administrators System Administrators | bulkadmin C dbcreator C diskadmin C processadmin C securityadmin C setupadmin C sysadmin C |
| | 3) Double-click the individual roles accounts listed as having member | in the right pane and docu ership. | ment the |
| | the role membership. | ire the proper accounts are | e assigned to |
| Auditor Notes | | | |

Check 18 – SQL Database Encryption

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

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

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

| Reference | SQL Server Security Checklist (item 2): <u>http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4</u> Microsoft SQL 2000 Security White paper (page 10) <u>http://www.microsoft.com/sql/techinfo/administration/2000/2000Security</u> <u>WP.doc</u> |
|---|--|
| 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 |

| 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.) SQL Server Network Utility |
|----------------------|--|
| | Server <u>n</u> ame: |
| | Disabled protocols: Enabled protocols: Multiprotocol Image: Constraint of the second |
| | Force protocol encryption |
| | Enable WinSock proxy WinSock proxy address: WinSock proxy port: |
| | OK Cancel Apply |
| | 4) Document the findings and attach a screenshot to the report. |
| Auditor Notes | |

Check 20– Backup/Restore Procedures

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

Check 21 – Physical Security of Server

| Reference | Microsoft SQL 2000 Security White paper (page 59) <u>http://www.microsoft.com/sql/techinfo/administration/2000/2000Security</u> <u>WP.doc</u> SQL Server Security Checklist (item 15): |
|---------------|---|
| | http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4 |
| | |
| Control | All servers must be placed in physically secured location. |
| Objective | |
| 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 | Objective. The server is in access-controlled environment. |
| Compliance: | |
| Test | Manually verify location of the server. If the server is in a separate |
| performed to | room, check for a lock on the door and determine who has access to |
| ensure | room. Document the findings in the report. |
| compliance | |
| Auditor Notes | |

Assignment 3: Conduct the audit

Audit 1 - Service Pack and Hot Fix levels

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

| | 🚷 Microsoft Baseline Security Analyzer | | |
|---------------------------------|---|--|--|
| | Microsoft Microsoft Microsoft Microsoft | | |
| Baseline Security Analyzer | | | |
| | Microsoft Baseline Security Analyzer Pick a computer to scan | | |
| | Welcome Specify the computer you want to scan. You can enter either the computer name or its IF address. Pick a computer to scan Specify the computer you want to scan. You can enter either the computer name or its IF Pick a computer to scan Computer name: | | |
| | Image: Provide a security report IP address: Image: Ima | | |
| | See Also Security report name: %domain% - %computerName% (%date%) Microsoft Baseline Security Analyzer Options: Check for Windows vulnerabilities Help Check for weak passwords Check for use passwords About Microsoft Baseline Security Analyzer Check for IIS yulnerabilities Microsoft Security Web site Check for SQL vulnerabilities | | |
| | Check for hotfixes | | |
| Actual | 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 SQL Server Scan Results | | |
| Results | Vulnerabilities | | |
| | Score Issue Result | | |
| | SQL Server 5 hotfixes are missing or could not be confirmed. Hotfixes What was scanned Result details How to correct this | | |
| Auditor Notes / Test Results | Fail. The MBSA has determined that 5 hotfixes are missing from the server. After discussions with the administrator, it was discovered the patches are currently under review and are slated for implementation within two weeks. | | |

Audit 2 – Stored Procedures

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

| | to attack the underlying operating system (e.g. Attacker using xp_cmdshell to delete critical files or 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. | | |
| | | | |
| | Tree | Extended Stored Procedures 17 | 3 Items |
| | Console Root | | Owner |
| | Microsoft SQL Servers | sp_bindsession | dbo |
| | | | |
| | - (Mindowis NT) | sp_createorphan | dbo dbo |
| | (Windows NT) | sp_creaceorphan sp_cursor | dbo dbo |
| | | sp_createorphan sp_cursor sp_cursorclose | dbo dbo dbo dbo |
| | □···□ Databases □···□ master | sp_createorphan sp_cursor sp_cursorclose sp_cursorexecute | dbo dbo dbo dbo dbo |
| | (Windows NT) Databases 0 master 1 master 1 master 1 master | sp_cursorexecute sp_cursorexecute sp_cursorexecute sp_cursorexecute | dbo dbo dbo dbo dbo dbo |
| | (Windows NT) □ ·· □ Databases □ ·· □ master □ ·· □ Tables ···································· | sp_cursorexecute sp_cursorexecute sp_cursorexecute sp_cursorexecute sp_cursorexecute sp_cursoropen sp_cursoropen | dbo dbo dbo dbo dbo dbo dbo |
| | (Windows NT) □ → □ Databases □ → □ master □ → □ Tables → ♂ Views Stored Procedures | sp_cursoreateorphan sp_cursor sp_cursoreateorphan sp_cursoreateorphan sp_cursoreateorphan sp_cursoropen sp_cursoropen sp_cursoroption | dbo dbo dbo dbo dbo dbo dbo |
| | (Windows NT) Control Databases | sp_cursoreateorphan sp_cursor sp_cursorexecute sp_cursoretech sp_cursoropen sp_cursoropen sp_cursoroption sp_cursoroption sp_cursorprepare sp_cursorprepare | dbo dbo dbo dbo dbo dbo dbo dbo |
| | (Windows NT) Current Control (Windo | sp_createorphan sp_cursor sp_cursorclose sp_cursorexecute sp_cursorfetch sp_cursoropen sp_cursoroption sp_cursoroption sp_cursorprepare sp_cursorprepare sp_cursorprepare | dbo dbo dbo dbo dbo dbo dbo dbo dbo |
| | (Windows NT) Databases Tables | sp_cursoropan sp_cursorexecute sp_cursorexecute sp_cursoropan sp_cursoropan sp_cursoropan sp_cursoropan sp_cursoropan sp_cursorprepare sp_cursorprepare sp_cursoruprepare sp_cursoruprepare sp_cursoruprepare sp_cursoruprepare | dbo dbo dbo dbo dbo dbo dbo dbo dbo dbo |
| | (Windows NT) Databases Tables Control Views Stored Procedures Extended Stored Procedure Rules Defaults | sp_createorphan sp_cursor sp_cursorclose sp_cursorexecute sp_cursorpetch sp_cursoropen sp_cursoropen sp_cursorprepare sp_cursorprepare sp_cursorprepare sp_cursorprepare sp_cursorprepare sp_cursorprepare sp_cursorprepare sp_cursorprepare sp_cursorprepare sp_cursorprepare | dbo dbo dbo dbo dbo dbo dbo dbo dbo dbo |
| | (Windows NT) Control Databases | sp_createorphan sp_cursor sp_cursorclose sp_cursorexecute sp_cursorptech sp_cursoropen sp_cursoroption sp_cursorprepare sp_cursorprepare sp_cursoruprepare sp_cursoruprepare sp_cursoruprepare sp_droporphans sp_execute sp_executesql | dbo dbo dbo dbo dbo dbo dbo dbo dbo dbo |
| | (Windows NT) Control Databases | sp_createorphan sp_cursor sp_cursorclose sp_cursorexecute sp_cursorpetch sp_cursoropen sp_cursoroption sp_cursorprepare sp_cursorprepare sp_cursorunprepare sp_cursorunprepare sp_droporphans sp_execute sp_execute sp_executesql sp_fulltext_getdata | dbo dbo dbo dbo dbo dbo dbo dbo dbo dbo |
| | (Windows NT) Control Databases | sp_createorphan sp_cursor sp_cursorclose sp_cursorexecute sp_cursorpen sp_cursoropen sp_cursorprepare sp_cursorprepare sp_cursorprepare sp_cursorphans sp_execute sp_executesql sp_etbindtoken | dbo dbo dbo dbo dbo dbo dbo dbo dbo dbo |
| | (Windows NT) Databases Tables Gof Views Stored Procedures Extended Stored Procedures Rules Defaults User Defined Data Types User Defined Functions Full-Text Catalogs Total Stored Procedures Rules Defaults Stored Procedures Rules Mules Stored Procedures Rules Mule | sp_cursor sp_cursor sp_cursor sp_cursorexecute sp_cursorexecute sp_cursorpen sp_cursoropen sp_cursorprepare sp_cursorprepare sp_cursorprepare sp_cursorprepare sp_cursoruprepare sp_cursoruprepare sp_droporphans sp_execute sp_execute sp_execute sp_executesql sp_fulltext_getdata sp_getbindtoken sp_GetMBCSCharLen | dbo dbo dbo dbo dbo dbo dbo dbo dbo dbo |
| | (Windows NT) Constraints Cons | sp_cursor sp_cursor sp_cursor sp_cursorexecute sp_cursorexecute sp_cursoretech sp_cursoropen sp_cursoropen sp_cursorprepare sp_cursorprepare sp_cursorunprepare sp_cursorunprepare sp_droporphans sp_execute sp_executesql sp_executesql sp_executesql sp_getbindtoken sp_getbindtoken sp_getschemalock | dbo dbo dbo dbo dbo dbo dbo dbo dbo dbo |
| | (Windows NT) Control Databases | sp_cursor sp_cursor sp_cursor sp_cursorexecute sp_cursorexecute sp_cursoretech sp_cursoropen sp_cursoropen sp_cursorprepare sp_cursorprepare sp_cursorunprepare sp_droporphans sp_execute sp_execute sp_execute sp_executesd sp_sp_tilltext_getdata sp_getbindtoken sp_GetMBCSCharLen sp_getschemalock sp_ISMBCSLeadByte | dbo dbo dbo dbo dbo dbo dbo dbo dbo dbo |
| | (Windows NT) Databases Databases Tables Tables Control Views Stored Procedures Extended Stored Procedures Extended Stored Procedures Rules Rules Users User Defined Data Types User Defined Data Types User Defined Functions Full-Text Catalogs model mode | sp_cursor sp_cursor sp_cursor sp_cursorexecute sp_cursorexecute sp_cursoretech sp_cursoropen sp_cursoropen sp_cursorprepare sp_cursorprepare sp_cursorunprepare sp_cursorunprepare sp_droporphans sp_execute sp_execute sp_execute sp_execute sp_fulltext_getdata sp_getbindtoken sp_GetMBCSCharLen sp_getschemalock sp_IsMBCSLeadByte sp_MSgetversion | dbo dbo dbo dbo dbo dbo dbo dbo dbo dbo |
| | (Windows NI) Databases Tables Tables Tables Tables Stored Procedures Extended Stored Procedure Extended Stored Procedure Users Rules Rules User Defined Data Types User Defined Functions Full-Text Catalogs Tothwind Tables Defaults User Defined Functions Full-Text Catalogs Tothwind Data Transformation Services | sp_cursor sp_cursor sp_cursor sp_cursorexecute sp_cursorexecute sp_cursoretech sp_cursoropen sp_cursoropen sp_cursorprepare sp_cursorunprepare sp_cursorunprepare sp_cursorunprepare sp_droporphans sp_execute sp_execute sp_execute sp_executesql sp_fulltext_getdata sp_getbindtoken sp_getbindtoken sp_getschemalock sp_lstMBCSLeadByte sp_MSgetversion sp_OACreate | dbo dbo dbo dbo dbo dbo dbo dbo dbo dbo |
| | (Windows NI) Databases Tables Tables Tables Tables Tables Tables Tables Tables Stored Procedures Extended Stored Procedure Rules Defaults User Defined Data Types User Defined Data Types User Defined Functions Full-Text Catalogs Torel Northwind Data Transformation Services Tables | sp_cursor sp_cursor sp_cursor sp_cursorexecute sp_cursorexecute sp_cursoretech sp_cursoropen sp_cursoropen sp_cursorprepare sp_cursorunprepare sp_cursorunprepare sp_droporphans sp_execute sp_execute sp_execute sp_fulltext_getdata sp_getbindtoken sp_getbindtoken sp_getschemalock sp_GetMBCSCharLen sp_getschemalock sp_ISMBCSLeadByte sp_OACreate sp_OADestroy | dbo dbo dbo dbo dbo dbo dbo dbo dbo dbo |
| | (Windows NI) Databases Table | sp_cursor sp_cursor sp_cursorexecute sp_cursorexecute sp_cursorpen sp_cursorpen sp_cursorprepare sp_otherecursor sp_OACreate sp_OACreate sp_OACreate | dbo dbo dbo dbo dbo dbo dbo dbo dbo dbo |
| | (Windows NI) Databases Tables Tables Grave Views Stored Procedures Extended Stored Procedures Extended Stored Procedures Extended Stored Procedures Extended Stored Procedures User Defaults User Defined Data Types User Defined Functions Full-Text Catalogs Total model Total model Data Transformation Services Total Transformation Services Total Transformation Services Total Transformation Services | sp_createorphan sp_cursor sp_cursorexecute sp_cursorexecute sp_cursorphan sp_cursorphan sp_cursorphan sp_cursorphan sp_cursorphane sp_execute sp_executes sp_executes sp_executes sp_executes sp_executes sp_executes sp_oethmode sp_oethmode sp_OACreate sp_OAGetErrorInfo sp_OAGetProperty | dbo dbo dbo dbo dbo dbo dbo dbo dbo dbo |

| Ex | General Control Pro | xp_cmdshell | - xp_cmdshell | |
|---|---|-------------|--|--|
| - | Laur | OK | Cancel Help | |
| xp_fi sp_s xp_a xp_c xp_d xp_d | leexist didebug vailablemedia mdshell eletemail irtree | | xp_readerrorlog xp_readmail xp_revokelogin xp_runwebtask xp_schedulersignal xp_sendmail | |
| | | | | |

| | 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). SQL Query Analyzer Image: Control of the |
| | 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_eventlog Guest and public: None listed xp_fixeddrives Guest: None Public: Checked xp getfiledetails Guest: None Public: Checked xp_getnetname Guest: None Public: Checked xp grantlogin Guest: None Public: Checked xp_logevent Guest and public: None listed xp_loginconfig Guest and public: None listed xp_logininfo Guest and public: None listed xp_makewebtask Guest and public: None listed xp_msver Guest: None Public: Checked Sp OACreate Guest and public: None listed sp_OAGetErrorInfo Guest and public: None listed Sp OAGetProperty Guest and public: None listed Sp_OAMethod Guest and public: None listed Sp OADestroy Guest and public: None listed Sp OASetProperty Guest and public: None listed SP OAStop, Guest and public: None listed Xp regaddmultistring Guest and public: None listed xp_readerrorlog Guest and public: None listed xp readmail Guest and public: None listed xp revokelogin Guest: None Public: Checked xp_runwebtask Guest and public: None listed xp sendmail Guest and public: None listed xp servicecontrol Guest and public: None listed xp sprintf Guest: None Public: Checked xp sscanf Guest: None Public: Checked xp startmail Guest and public: None listed xp stopmail Guest and public: None listed xp_subdirs Guest and public: None listed xp unc to drive Guest: None Public: Checked Xp_regdeletekey Guest and public: None listed Xp_regdeletevalue Guest and public: None listed Xp regenumvalues Guest and public: None listed Xp regread Guest: None Public: Checked Xp_regremovemultistring Guest and public: None listed Xp regwrite Guest and public: None listed The following is a screenshot of the findings for the sp runwebtask stored procedure. For brevity purposes, the remaining screenshots have been omitted from this document.

| | ee Stored Proc Stored Procedure Dispersition, consumptional |
|-------------------------------|--|
| | Console Root |
| | Microsoft SQL Servers |
| | Bermission |
| | Databases |
| | Permissions |
| |) |
| | Stored Procedures |
| | Roles C List all users/user-defined database roles/public |
| | C List only users/user-defined database roles/public with permissions on this object. |
| | User Defined Data 1 Users/Database Roles/Public SELECT INSERT UPDATE DELETE EXEC DRI Section 2010 - |
| | Full-Text Catalogs |
| | Tables |
| | |
| | Extended Stored Pr |
| | Users |
| | |
| | In order to ensure that xp_cmdshell is still installed on the server, the |
| | query analyzer was opened and a test of the stored procedure was |
| | performed. |
| | |
| | 👜 Query - |
| xp cmdshell 'dir c:*.evt /s' | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | • |
| | output |
| | 4 Directory of c.\WINNT\eyetem32\config |
| | E MULT |
| | |
| | b 262,144 AppEvent.Evt |
| | 7 65,536 SecEvent.Evt |
| | 8 65,536 SypEvent.Evt |
| Auditor Notes | Fail. Any changes made will be required to be performed on a test |
| / Test Results | server to ensure functionality after changes have been implemented. An |
| | analysis should be performed for system stability in the event a |
| | procedure is dropped and the DLL removed; alternatively, tests should |
| | also be performed if permissions are removed from the public and guest |

roles.

Audit 3 – Authentication Model

| Reference | Microsoft SQL 2000 Security White paper (page 15) | | |
|--------------|---|--|--|
| | http://www.microsoft.com/sql/techinfo/administration/2000/2000Security | | |
| | WP.doc | | |
| Control | A single account database should be implemented for both operating | | |
| Objective | 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 | Objective. Test must prove Windows authentication is in place. | | |
| Compliance/ | ∇ | | |
| Expected | | | |
| Test Results | | | |
| Test | Check to ensure that only Windows authentication is used. | | |
| performed to | Access the enterprise manager | | |
| ensure | (Start Programs MicrosoftSQLServer EnterpriseManager) | | |
| compliance | Right click server name, select properties | | |
| | 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. | | |
| | SQL Server Properties (Configure) - 🔀 | | |
| | Server Settings Database Settings Benlication | | |
| C | General Memory Processor Security Connections | | |
| e | | | |
| | Security | | |
| | SQL Server provides authentication based on Windows | | |
| | | | |
| | Authentication: | | |
| | SQL Server and Windows | | |
| | | | |
| | | | |
| | | | |

| | Stimulus/Response test | |
|---------|--|--|
| | 4) Open Query Analyzer (Stort/Drograma/MicrosoftSOL Convert/Oversides/uper) | |
| | (Start Programs MicrosoftSQLServer QueryAnalyzer). | |
| | 5) Enter SA account as username. Leave password as blank (the | |
| | error returned will prove if SQL authentication is disabled (non | |
| | trusted account) or a bad password was entered (incorrect | |
| | password)). | |
| | Connect to SQL Server | |
| | <u>SQL Server:</u> | |
| | □ St <u>a</u> rt SQL Server if it is stopped | |
| | Connect using: | |
| | O <u>w</u> indows authentication | |
| | (• Stor Server authentication | |
| | Login name: | |
| | Password: | |
| | | |
| | OK Cancel Help | |
| | 6) Decument the regults Centure a screenshot and attach to the | |
| | o) Document the results. Capture a screenshot and attach to the | |
| | Teport. | |
| Actual | Only Windows Authentication has been implemented on the server. The | |
| Results | following screenshots confirm settings | |
| Results | Tonowing serven shots commin settings. | |
| | | |
| | | |
| | O Share Institute | |
| | | |

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

Audit 4 – Audit Activity on server

| Reference | SQL Server books online ("auditing SQL Server activity" as a search parameter). |
|---|--|
| Control 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. |
| | |

| | Trace Template Properties | × |
|----|---|--|
| | General Events Data Columns Fil | ters |
| | Select the SQL Server even | it classes you want to trace. |
| | A <u>v</u> ailable event classes: | Selected event classes: |
| | Cursors Database Errors and Warnings Locks Objects Performance Scans Security Audit Server Stored Procedures Transactions | Add >> Add Add DB User Ev Addit Add Login to Sei Addit Add Member to I Addit Add Member to I Addit Add Degin Event Audit App Role Chang Audit Login Audit Login Audit Login Change P. Audit Login Failed |
| | Cursors Collection of events produced when | n cursors are created, used and deleted. |
| li | tems that must be enabled are | as follows. Document any deviations |
| | Add DB User Event Add Login to Server Add Login to Server Role Add Member to DB Role Add Login App Role Change Password Change Audit Login Login Change Password Login GDR Login GDR Logout Dbject Derived Permission Dbject Permission Statement GDR Statement Permission | |
| | Verify Trace Results 3) Select File Open TraceFil storage of traces given by of trace files or trace temp 4) Open trace and check da | le or TraceTable (depending on y administrator). Point to the location plate. tes for latest activity (starttime |

| | 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. Trace Template Properties General Events Data Columns Filters Select the SQL Server event classes you want to trace. |
| | Available event classes: Selected event classes: • Database • Audit Add DB User Ev • Dbjects • Audit Add Login to Se • Objects • Audit Addlogin Event • Scans • Audit Addlogin Event • Scans • Audit Addlogin Event • Stored Procedures • Audit Login • Transactions • Audit Login Failed • Cursors • Cursors Collection of events produced when cursors are created, used and deleted. |
| Auditor Notes / Test Results | Fail. Automated auditing of the server has not been established. |
| Audit 5 Lago | Auditing |

Audit 5 – Logon Auditing

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

| Compliance/ Expected | is off.) |
|--|--|
| Test Results | |
| 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. |
| | SQL Server Properties (Configure) - |
| | Server Settings Database Settings Replication General Memory Processor Security Connections Security SQL Server provides authentication based on Windows accounts and a named SQL Server login ID and password. Authentication: SQL Server and Windows SQL Server and Windows SQL Server and Windows Eailure Eailure None Eailure Success All |
| | 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 |
| | 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. |

| | | oningure) - | | | <u> </u> |
|--|---|--|--|---|---------------|
| Server | Settings | , Database S | ettings | Replication | Į |
| General | Memory | Processor | Security | Connections | |
| Security | SQL Server (| provides authenti | cation based or |) Windows | |
| | accounts an | d a named SQL 9 | erverlogin ID a | and password. | |
| | Authenticatio | on: Server and Windo | ows | | |
| | • Wind | ows only | | | |
| | Audit level: | | | | |
| | O None | | C <u>F</u> ailure | \mathbf{D} | |
| | O Succe | ess | • Al | | |
| - Startup | service account | t | | | |
| 198 | Start and run | n SQL Server in th | e following acc | ount: | |
| 300 | O System | m account | | | |
| | ⊙ <u>T</u> his a | account | sqlservic | e | |
| | <u>P</u> assv | word: | ******** | (X | |
| | | | | | |
| | | | | | |
| | | | | | |
| | ottomat ta | lagan ta gi | | ar with a SC | |
| An invalid | attempt to and the fo | logon to qu | iery analyz ure was no | zer with a SC | QL a |
| An invalid performed event log: | attempt to and the fo | logon to qu bllowing failu | iery analyz ure was no | zer with a SC oted in the se | QL a erve |
| An invalid performed event log: | attempt to and the fo | logon to qu blowing failu | iery analyz ure was no | zer with a SC oted in the se | QL a erve |
| An invalid performed event log: | attempt to and the fo | logon to qu blowing failu | iery analyz ure was no | zer with a SC oted in the se | QL a erve |
| An invalid performed event log: Event Prope Event Date: | attempt to and the fo | logon to qu blowing failu | iery analyz ure was no | zer with a So oted in the se ? × | QL a ervei |
| An invalid performed event log: Event Prope Event Date: Time: Tune: | attempt to and the fo | logon to qu bllowing failu Source: MSSQI Category: (4) Swent ID: 17055 | iery analyz ure was no | zer with a SC oted in the se ? × | QL a ervei |
| An invalid performed event log: Event Prope Event Date: Time: Type: User: Computer: | attempt to and the fo rties | logon to qu blowing failu Source: MSSQI Category: (4) Event ID: 17055 | iery analyz ure was no | zer with a SC oted in the se ? × | QL a ervei |
| An invalid performed event log: Event Prope Event Date: Time: Type: User: Computer: | attempt to and the fo | logon to qu bllowing failu Source: MSSQI Category: (4) Event ID: 17055 | iery analyz ure was no | zer with a SC oted in the se ? × | QL a ervei |
| An invalid performed event log: Event Prope Event Date: Time: Type: User: Computer: Description 18452: Login faile Server co | attempt to and the fo rties | logon to qu bllowing failu Source: MSSQI Category: (4) Event ID: 17055 | iery analyz ure was no _SERVER | zer with a SQ oted in the se ? × | QL a ervei |
| An invalid performed event log: Event log: Date: Time: Type: User: Computer: Description 18452 : Login faile Server co | attempt to and the fo rties | logon to qu bllowing failu Source: MSSQI Category: (4) Event ID: 17055 | Lery analyz Liery was no -SERVER | zer with a SC oted in the se ? × | QL a ervei |
| An invalid performed event log: Event log: Date: Time: Type: User: Computer: Description 18452 : Login faile Server co | attempt to and the for rties | logon to qu ollowing failu Source: MSSQI Category: (4) Event ID: 17055 Reason: Not assoc | Jery analyz Line was not SERVER | zer with a SQ oted in the se ? × | QL a ervei |
| An invalid performed event log: Event Prope Event Date: Type: User: Computer: Description 18452 : Login faile Server co | attempt to and the for rties | logon to qu blowing failu Source: MSSQI Category: (4) Event ID: 17055 Reason: Not assoc | SERVER | zer with a SO oted in the se ? × • • • • • • • | QL a ervei |
| An invalid performed event log: Event Prope Event Date: Time: Type: User: Computer: Description 18452: Login faile Server co | attempt to and the for rties Information Information <t< td=""><td>Iogon to quotical Source: MSSQI Source: MSSQI Category: (4) Event ID: 17055 Reason: Not association 0 00 00 44 00 49 05 00 00 07 00 74</td><td>SERVER</td><td>zer with a SC oted in the se ? × </td><td>QL a ervei</td></t<> | Iogon to quotical Source: MSSQI Source: MSSQI Category: (4) Event ID: 17055 Reason: Not association 0 00 00 44 00 49 05 00 00 07 00 74 | SERVER | zer with a SC oted in the se ? × | QL a ervei |
| An invalid performed event log: Event Prope Event Date: Type: User: Description 18452 : Login faile Server co | attempt to and the for rties Information Information Mathematical attempt to and the for Information Information Mathematical attempt to attempt to Information Bytes Work 4 48 00 00 attempt to | Ogon to que blowing fails Source: MSSQI Category: (4) Event ID: 17055 Reason: Not assoc ds 0 0= 00 00 44 00 49 00 53 00 51 00 07 00 00 74 00 | SERVER | zer with a SQ oted in the se ? | QL a ervei |

| A valid access was noted as follows in the event log: | |
|---|--|
| | |
| Event Properties ? X | |
| Event | |
| Date: Source: | |
| Time: Category: (4) | |
| Type: Information Event ID: 17055 | |
| User: | |
| Computer: | |
| Description: | |
| 18453 : | |
| Login succeeded for user ''. Connection: Trusted. | |
| | |
| | |
| | |
| Da <u>t</u> a: 💽 <u>By</u> tes C <u>W</u> ords | |
| 0000: 15 48 00 00 0e 00 00 00 .H | |
| | |
| 0018: 4c 00 00 07 00 00 00 | |
| 0020: 6d 00 61 00 73 00 74 00 m.a.s.t. | |
| 10028: 65 00 72 00 00 00 e.r | |
| | |
| OK Cancel Apply | |
| Auditor Notes Pass. Auditing is established properly. | |
| / Test Results | |

Audit 6 – SQL Service start-up accounts

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

| Compliance/ Expected test | |
|--|--|
| 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. |
| | Server Settings Database Settings Replication General Memory Processor Security Security SQL Server provides authentication based on Windows accounts and a named SQL Server login ID and password. Authentication: SQL Server and Windows © SQL Server and Windows @ Mone C Eailure O None C to the security |
| | Startup service account Start and run SQL Server in the following account: System account Ihis account Password: |
| | 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. |



| | MSSQLSERVER Properties (Local Computer) |
|---------------------------------|--|
| | General Log On Recovery Dependencies |
| | Log on as: |
| | You can enable or disable this service for the hardware profiles listed below: Hardware Profile Service Profile 1 Enabled |
| | OK Cancel Apply As the screenshot shows, the SQL service is starting under the |
| | sqlservice user account. |
| 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): <u>http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4</u> Microsoft SQL 2000 Security White paper (page 58) <u>http://www.microsoft.com/sql/techinfo/administration/2000/2000Security</u> <u>WP.doc</u> |
|----------------------|--|
| 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 | Objective. The guest account is removed from all sensitive databases. |
| Compliance/ | The guest account at the operating system level must be disabled. |
| Expected test | |
| results | |
| Test | Check permissions for the guest account on sensitive databases. |
| performed to | 1) Access enterprise manager |
| ensure | (Start Programs MicrosoftSQLServer EnterpriseManager) |
| compliance | 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. |
| | 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 Administrative I ools ComputerManagement Loca |
| | IUsersAndGroups). |
| | 5) Double-click users tab. Double click guest account. Ensure |
| | "account is disabled" box is checked. Document findings and |
| | attach a screenshot. |
| | Stimulus/Personance test: Attempt to access the conver with an |
| | Sumulus/Response lesi. Allempt to access the server with an |
| | account not instea as naving access to ensure that access is defied. |
| | 6) Logon to the auditor workstation as a user that does not exist on |
| | the target server (this will force a quest 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. |
| C | |

| | 🗐 Data Link Properties 🛛 🔀 |
|---------|---|
| | Provider Connection Advanced All |
| | Specify the following to connect to SQL Server data: 1. Select or enter a server name: |
| | ▼ Refresh |
| | 2. Enter information to log on to the server: |
| | O Use a specific user name and password: |
| | User name: |
| | Password: |
| | Blank password Allow saving password |
| | 3. Select the database on the server: |
| | |
| | Select the "select database on the server" pulldown box. Access should be denied. Document the findings and attach a |
| | screenshot of any errors. |
| | |
| | ST . |
| Actual | The following screen shows that quest access is restricted from the |
| Results | Company database. |
| | |
| | |
| | Image: Solution of the soluti |
| | SQL Server Group Image: Constraint of the server of the |
| | Tables |
| | |
| | |
| | Full-Text Catalogs |
| | |
| | The Guest account has been disabled at the Ω/S level |
| | The edget account has been disabled at the 0/0 level. |

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

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

Audit 8 – Alerting

| Reference | SQL Server Security Checklist (item 17): | | | | |
|----------------|--|--|--|--|--|
| | http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4 | | | | |
| Control | An alerting mechanism must be established and notification | | | | |
| Objective | established. | | | | |
| Risk | A lack of alerting would prohibit response to malicious activity. This | | | | |
| | would allow an attacker ample opportunity to attack the server if no | | | | |
| | detection and response was possible. | | | | |
| Likelihood | High. Alerting is not configured by default. | | | | |
| Consequence | No response would be possible if alerting is not enabled. | | | | |
| System | Objective. Alerts are configured and notification will be sent. | | | | |
| Compliance/ | | | | | |
| Expected Test | | | | | |
| Results | | | | | |
| Test | Access the server in SQL Enterprise Manager. Select Management | | | | |
| performed to | SQL Server Agent Alerts. Check for the existence of an alert for | | | | |
| ensure | severity 14 and that an operator is defined to receive a page or e-mail. | | | | |
| compliance | 1) Access Enterprise Manager | | | | |
| | (Start Programs MicrosoftSQLServer EnterpriseManager) | | | | |
| | 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. | | | | |
| | 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 | | | | |
| \bigcirc | notification established, nor are there any operators established. | | | | |
| | | | | | |
| | | | | | |

| | n Console Root\Microsoft SQL Servers\SQL Servers | erver Group\(Wind | ows NT)\Manageme | nt\SQL Server Ager |
|----------------|--|--------------------------|------------------|----------------------------|
| | Action View Iools | X 🖅 🕼 🗟 🛿 🔆 | \land 🕼 🕕 💽 🕻 | 6 |
| | [ree | Alerts 10 Items | | |
| | Console Root | Name 🔺 | Enabled Erro | r Severity Last Oc |
| | 🗄 🗐 Microsoft SQL Servers | Demo: Full msdb log | Yes 900 | 2 0 (Never |
| | 🖃 👘 SQL Server Group | Demo: Full tempdb | Yes 900 | 2 0 (Never |
| | (Windows NI) | Demo: Sev. 19 Errors | Yes | 0 19 (Never |
| | ⊡ Data Transformation Services | Demo: Sev. 20 Errors | res Ves | 0 20 (Never 0 21 (Never |
| | - Management | Demo: Sev. 22 Errors | Yes | 0 22 (Never |
| | 🖻 🔁 SQL Server Agent | Demo: Sev. 23 Errors | Yes | 0 23 (Never |
| | (Alerts) | Demo: Sev. 24 Errors | Yes | 0 24 (Never |
| | | Demo: Sev. 25 Errors | Yes | 025 (Never |
| | | OPERMISSION alert | Yes | 0 <u>14</u> >(Never |
| | 🕀 🛅 Current Activity | | | |
| | Database Maintenance Plans | | | |
| | E I SQL Server Logs | | | |
| | Ender Security | | | |
| | 🕀 🧰 Support Services | | | |
| | 🕀 💼 Meta Data Services | | | |
| | | | | |
| | | | | |
| | | | | |
| | | 2 Y | | |
| | Permission alert Properties - | | × | J |
| | General Response | | | |
| | | | | |
| | Execute job: | | ▼ | |
| | | ····· | | |
| | Operators to notify: | <u>New</u> | Operator | |
| | Operator Name | E-mail Pager N | et Send | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | 1 | | | |
| | Include alert error text in: 🔽 E-ma | ail 🔽 <u>P</u> ager 🔽 No | et <u>s</u> end | |
| à | | | | |
| | Additional notification message to send | : | | |
| | | | A | |
| | | | | |
| | | | v | |
| Auditor Notes | Fail. As a result of the issue | s identified in the t | est results, th | nere would |
| / Toet Roculto | he no alerte sont in caso of a | normission donio | | |
| | שב הט מובונס סבווג ווו נמסב טו מ | permission defila | 1. | |

Audit 9 – TCP/IP Port filtering

| Reference | Medina, Luis, Empirical Hacker – Protect your database series - part | | | | |
|---------------|---|--|--|--|--|
| | one, checklist item 7. | | | | |
| | html | | | | |
| Control | Network controls should be in place to protect the server data. | | | | |
| Objective | <u>Ś</u> | | | | |
| Risk | Malware can use high-level ports to communicate with an attacker and | | | | |
| Likelihood | Medium Previous examples of malware that allowed for remote control | | | | |
| Lincoliniood | 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 | | | | |
| Sustam | Corporate firewall. | | | | |
| Compliance / | the O/S level | | | | |
| Expected test | | | | | |
| results | | | | | |
| Test | Check TCP/IP filtering. | | | | |
| performed to | | | | | |
| ensure | 1) On the server desktop, right-click the "My Network Places" icon, | | | | |
| compliance | properties Double click Internet Protocol (TCP/IP) Select the | | | | |
| | advanced tab, then options. The following screen capture shows | | | | |
| | what should be displayed. | | | | |
| | Advanced TCP/IP Settings | | | | |
| | IP Settings DNS WINS Options | | | | |
| | Optional settings: | | | | |
| | IP security | | | | |
| | TCP/IP filtering | | | | |
| | | | | | |
| | | | | | |
| C | Properties | | | | |
| | | | | | |
| | Description: | | | | |
| | TCP/IP filtering allows you to control the type of TCP/IP network | | | | |
| | traine that reaches your windows computer. | | | | |
| | | | | | |
| | 2) Select TCP/IP filtering, select properties. All filtered ports will be | | | | |
| | displayed at this point. Document and attach a screenshot to the | | | | |

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



| | NMapWin v1.3.1 | | | | | |
|---------------|--|--|--|--|--|--|
| | Host: | | | | | |
| | | | | | | |
| | Sgan Discover Options Timing Files Service Win32 | | | | | |
| | Mode Scan Options ✓ Port Range Use Decoy ■ Bounce Scan | | | | | |
| | © SYN Stealth O Xmas Tree O BCP Scan | | | | | |
| | C EIN Stealth C IP Scan C List Scan | | | | | |
| | <u>Ping Sweep</u> O <u>I</u> dle Scan □ Idle Scan Host UDB Scan | | | | | |
| | | | | | | |
| | Output Starting nmap V. 3.00 (www.insecure.org/nmap) | | | | | |
| | Interesting ports on | | | | | |
| | Port State Service 135/udp open loc-srv 137/udp open netbios-ns | | | | | |
| | 138/udp open netbios-dgm 445/udp open microsoft-ds 500/udp open isakmp | | | | | |
| | 1029/udp open unknown 1434/udp open ms-sql-m 47624/udp open unknown | | | | | |
| | Nmap run completed 1 IP address (1 host up) scanned in 29 seconds | | | | | |
| | | | | | | |
| Auditor Notes | Fail. No ports are restricted on the server. Additionally, terminal | | | | | |
| | investigated to determine what application is listening on UDP port | | | | | |
| | 47624. Research has shown this port to be associated with a game | | | | | |
| | server. Fport does not list any service listening on this port. | | | | | |
| | | | | | | |
| Audit 10 – SQ | L Port | | | | | |
| | | | | | | |
| | | | | | | |

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

| | Internet. | | | | |
|---|--|--|--|--|--|
| Likelihood | Depends on the firewall configuration. | | | | |
| Consequence | A potential attacker would know of the existence of the SQL server. An attacker can then use automated tools to attack server after initial the reconnaissance. | | | | |
| System Compliance/ Expected test results | Objective. The port value should be changed from the default and the server port should be hidden. This will change both the listening port and hide the actual SQL port in use from sqlping2. | | | | |
| Test performed to ensure compliance | Access Enterprise Manager (Start Programs MicrosoftSQLServer EnterpriseManager) Expand the server group, right click the servername and select properties. Select the Network Configuration tab. Select the TCP/IP protocol option and select properties. Document the port number and determine if the server is listed as hidden ("hide server" checkbox selected). Stimulus/Response tests: Run fport on the server to confirm which port the SQL Server is listening to. Document findings and attach screenshot. Obtain sqlping2 from www.sqlsecurity.com/scripts.asp. Run SQLping2 against the server IP address. 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. Server Network Utility General Network Libraries Server name: | | | | |
| | Disabled protocols: Enabled protocols: Multiprotocol Enable >> NWLink IPX/SPX AppleT alk Banyan Vines << Disable | | | | |
| | Force protoco | | | | |

| Fport | screenshot s | hows tha | t all po | orts are at their de | fault values. | |
|--|---|--|--|--|---|------------|
| | /INNT\System32\cm | d.exe | | | | |
| http: | //www.foundston | ie.com | | | | |
| Pid 500 8 8 556 808 8 8 1220 | Process svchost System System msdtc MSTask System | Port -> 135 -> 139 -> 445 -> 1025 -> 1026 -> 1030 -> 1030 | Proto TCP TCP TCP TCP TCP TCP TCP | Path C:\WINNT\system32\ C:\WINNT\System32\ C:\WINNT\system32\ | svchost.exe msdtc.exe MSTask.exe | og]oonun , |
| e 556 384 | msdtc termsrv | -> 3372 -> 3389 | TCP TCP | C:\WINNT\System32\ C:\WINNT\System32\ | msdtc.exe termsrv.exe | sqiservr.t |
| 500 8 8 8 | svchost System System Sustem | -> 135 -> 137 -> 138 -> 445 | UDP UDP UDP UDP | C:\WINNT\system32\ | svchost.exe | |
| 264 252 1220 | lsass services sqlservr | -> 500 -> 1029 -> 1434 | UDP UDP UDP | C:\WINNT\system32\ C:\WINNT\system32\ C:\PROGRA~1\MICROS | lsass.exe services.exe ~3\MSSQL\binn\ | sqlservr.e |
| | Ping2 confirms | s that SQ - http://www.s | L Serv | ver is listening to T | CP port 1433 | 3. |
| | ICH Ings Ochicy Melp | ſ | - Live IP Add | dresses File: | | |
| G Scan | From Live Address File | | | | | |
| , ⊂ Scan ⊢Scan R | ange: | | – User List: – | | | |
| Start IP. | Address: | | | | | |
| End IP A | Address: | | - Password L | ist: | | |
| | Begin Scan | Cancel | 1 | | | |
| | Found: | None | | Clustere 12 | Uarciar | TCD Dev |
| | duress | Mame | | No | version 8.00.194 | 1433 |
| S | | | | | | |
| otes Fail. | The listening | port is at | defau | It value of 1433 a | nd server is n | ot |
| Inidde | n. | | | | | |

Residual Risk

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

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

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

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

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

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

Is the system auditable?

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

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

The use of third party tools can assist with auditing of the system. For instance, one application, NGSSquirrel, can be used to greatly enhance the auditing and testing of SQL server. Use of this application could not be included in this paper due to the fact that it is not freeware and must be licensed at a cost (price varies depending on license purchased). To learn more about NGSSquirrel and its increased auditing capabilities, go to 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.

Assignment 4: Audit Report

Executive Summary

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

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

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

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

Audit Findings

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

Finding 1 – Missing patches on the server

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

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

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

SQL Server Scan Results

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

Risks

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

Finding 2 – Lack of detection mechanism

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

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

Risks

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

Finding 3 – Lack of notification system

Priority: High

Reference: Audit #8, page 60

Notification functionality is included in the software to notify an administrator (operator) in the event of a security breach. At the present time, the items that should trigger a notification alert are established, however, there are no operators listed as recipients of an alert, nor does an infrastructure exist to facilitate such notifications. The lack of recipients is shown in the following screenshot. Establishment of a notification system and pager rotation will address this shortcoming.
| Permission alert Properties | 5 - | | | | × | |
|-----------------------------------|------------------|---------------|-------|---------------------|-----|---|
| General Response | | | | | | |
| Execute job: | | | | T |] [| |
| Operators to notify: | | | | Ne <u>w</u> Operato | r | |
| Operator Name | | E-mail | Pager | Net Send | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| I Include alert error text in: | ☑ <u>E</u> -mail | □ <u>P</u> ag | ger [| ✓ Net send | | |
| Additional notification messa | ige to send: | | | | | |
| | | | | | | |
| | | | | | Ŧ | |
| | | | | | | I |

Risks

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

Finding 4 – Stored Procedure vulnerabilities

Priority: Medium

Reference: Audit Item #2, page 39

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

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

| ······ | | | | | | | |
|---|----------|--|--|--|--|--|--|
| xp cmdshell 'dir c:*.evt /s' | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| output | | | | | | | |
| 4 Directory of c:\WINNT\system32\config | | | | | | | |
| 5 NULL | | | | | | | |
| 6 262,144 AppE | vent.Evt | | | | | | |
| 7 65,536 SecE | vent.Evt | | | | | | |
| 8 65,536 SyoE | vent.Evt | | | | | | |

Risks

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

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

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

Finding 5 – TCP/IP Port filtering

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

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

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



Risks

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

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

Finding 6 – SQL listening port

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

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

| 🚦 SQL Server Network Uti | ility | | × |
|--|---|-----------------------|---|
| General Network Libraries | 1 | | |
| Server <u>n</u> ame: | | | |
| Disa <u>b</u> led protocols: | | Enabled protocols: | |
| Multiprotocol NWLink IPX/SPX AppleTalk Banyan Vines | <u>E</u> nable >> << <u>D</u> isable | Named Pipes TCP/IP | |
| | | Properties | |
| Force protoco | TCP/IP | | × |
| WinSock prox CNet | work Protocol Default Value Se | etup | |
| WinSock pro <u>s</u> | efault port: | 1 433 | |
| F | <u>H</u> ide server | | |

Risks

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

Audit Recommendations

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

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

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

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

Costs

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

Approximate costing guideline for recommendations

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

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

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

Compensating Controls

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

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

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

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

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

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

Appendix A - References

Research references

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

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

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

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

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

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

Medina, Luis. Empirical Hacker series <u>http://searchsecurity.techtarget.com/bestWebLinks/0,289521,sid14_tax281918,00.html</u>

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

SANS. Security Consensus Operational Readiness Evaluation http://www.sans.org/SCORE/checklists/

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

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

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

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

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

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

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

Spenik, Mark Sledge, Orryn. An Overview of SQL Server's Security Model 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