SQL Server slide notes

The following sections contain the notes for the slides in the SQL Server security audit presentation.

Slide 5

It is important to understand:

1. SQL Server architecture
2. Data access model

This will help us to develop:

1. A thorough test plan
2. Analyze testing results data

Because we have a common ground and understanding of the technology:

1. We can perform consistent analysis
2. Business partners will understand better the scope of the audits

Slide 9

Each database is both a logical and physical container for securables (tables and other objects).

Slide 10

The scope of influence of a principal depends on the scope of the definition of the principal: Windows, server, database; and whether the principal is indivisible or a collection. A Windows Login is an example of an indivisible principal, and a Windows Group is an example of a principal that is a collection. Every principal has a security identifier (SID).

A “login” in SQL Server grants a principal entry at the SERVER level.

A “user” in SQL Server is granted login to a single database within the server.

https://msdn.microsoft.com/en-us/library/ms181127(v=sql.105).aspx

Slide 12

1. End point
    A. Point of entry into SQL Server
    B. Database object that defines way and means to connect over the network
    C. Each endpoint supports a specific type of communication
    D. System endpoints are set up in the master database during installation
        - One system end point set up for the following protocols
            - TCP/IP
            - Shared Memory
            - Named Pipe

        - VIA
    - PUBLIC is given CONNECT
    - “Dedicated Admin Connection” can only be used by members of the SYSADMIN server-level role
    - Cannot be dropped or disabled
    - Can be stopped or started
    - Settings stored in the registry

E. User-defined endpoints
- Traffic must be authorized before it can reach SQL Server
- Transport - HTTP or TCP
- Payload
    - TSQL - must use TCP
    - Service_Broker - must use TCP
    - Database Mirroring - must use TCP
    - SOAP - must use HTTP
- A login must have permission (CONNECT) to use an endpoint
    - By default, all members of the PUBLIC group have permission use the default TCP connection

https://msdn.microsoft.com/en-us/library/ms190401(v=sql.105).aspx

2. Endpoint catalog views - https://msdn.microsoft.com/en-us/library/ms180076(v=sql.105).aspx

3. Use the file db_endpoints.sql

https://www.simple-talk.com/sql/database-administration/sql-server-endpoints-soup-to-nuts/

Slide 13
https://msdn.microsoft.com/en-us/library/ms190401(v=sql.105).aspx

Slide 14
https://msdn.microsoft.com/en-us/library/ms190401(v=sql.105).aspx

Slide 15
https://msdn.microsoft.com/en-us/library/ms190401(v=sql.105).aspx

Slide 17
https://msdn.microsoft.com/en-us/library/ms130214(v=sql.105).aspx

Slide 21
https://technet.microsoft.com/en-us/library/ms179316(v=sql.105).aspx

SQL Server databases have three types of files:

- Primary data files

The primary data file is the starting point of the database and points to the other files in the database. Every database has one primary data file. The recommended file name extension for primary data files is .mdf.

- Secondary data files

Secondary data files make up all the data files, other than the primary data file. Some databases may not have any secondary data files, while others have several secondary data files. The recommended file name extension for secondary data files is .ndf.

- Log files

Log files hold all the log information that is used to recover the database and perform transaction management. There must be at least one log file for each database, although there can be more than one. The recommended file name extension for log files is .ldf.

SQL Server does not enforce the .mdf, .ndf, and .ldf file name extensions, but these extensions help you identify the different kinds of files and their use.

In SQL Server, the locations of all the files in a database are recorded in the primary file of the database and in the master database. The SQL Server Database Engine uses the file location information from the master database most of the time. However, the Database Engine uses the file location information from the primary file to initialize the file location entries in the master database in the following situations:

- When attaching a database using the CREATE DATABASE statement with either the FOR ATTACH or FOR ATTACH_REBUILD_LOG options.
- When restoring the master database.

Slide 22

The SQLOS was created to centralize common low-level tasks within the SQL Server process. Having a central location for these tasks means less duplication of code within the various components of the engine, but it also offers the flexibility to adjust SQL Server to new and advanced hardware architectures without impacting the other areas of SQL Server code.

The SQLOS behaves very much like an operating system. It abstracts the concept of memory management, I/O, scheduling etc. from the other components within the SQL engine. In this way, these components do not need to worry about managing things like NUMA and Resource Governor, they simply make resource allocation calls to the SQLOS via an API.

The SQL engine is still a process like any other process running on a Windows server. It does not have any special privileges or priority over other process. The SQLOS does not bypass Windows, it simply manages the resources within the SQL Server process space in a way that is efficient for SQL Server.

http://blogs.msdn.com/b/sqlosteam/archive/2010/06/23/sqlos-resources.aspx

Slide 27

Finding SQL Server instances across the network: https://www.mssqltips.com/sqlservertip/2013/find-sql-server-instances-across-your-network-using-windows-powershell/

http://www.powershellmagazine.com/2013/08/06/pstip-retrieve-all-sql-instance-names-on-local-and-remote-computers/

Slide 30

TCP/IP is a common protocol widely used over the Internet. It communicates across interconnected networks of computers that have diverse hardware architectures and various operating systems. TCP/IP includes standards for routing network traffic and offers advanced security features. It is the most popular protocol that is used in business today. Configuring your computer to use TCP/IP can be complex, but most networked computers are already correctly configured. To configure the TCP/IP settings that are not exposed in SQL Server Configuration Manager, see the Microsoft Windows documentation.

TCP/IP is a common protocol widely used over the Internet. It communicates across interconnected networks of computers that have diverse hardware architectures and various operating systems. TCP/IP includes standards for routing network traffic and offers advanced security features. It is the most popular protocol that is used in business today. Configuring your computer to use TCP/IP can be complex, but most networked computers are already correctly configured. To configure the TCP/IP settings that are not exposed in SQL Server Configuration Manager, see the Microsoft Windows documentation.

Named Pipes is a protocol developed for local area networks. A part of memory is used by one process to pass information to another process, so that the output of one is the input of the other. The second process can be local (on the same computer as the first) or remote (on a networked computer).

Shared memory has no configurable settings. Because clients using the shared memory protocol can only connect to a SQL Server instance running on the same computer, it is not useful for most database activity.

Virtual Interface Adapter (VIA) protocol works with VIA hardware.

https://technet.microsoft.com/en-us/library/ms187892(v=sql.105).aspx

Slide 31

General rule: Do not enable ports unless there is a need.

Slide 32

CIS 2.11

Do not use default ports.

Security by obfuscation. Port scanners can find and identify ports. Prevents scripts attacks (SQL Slammer).

Slide 33

How it works:

When an instance of SQL Server starts, if the TCP/IP or VIA protocols are enabled for SQL Server, the server is assigned a TCP/IP port. If the named pipes protocol is enabled, SQL Server listens on a specific named pipe. This port, or "pipe," is used by that specific instance to exchange data with client applications. During installation, TCP port 1433 and pipe \sql\query are assigned to the default instance, but those can be changed later by the server administrator using SQL Server Configuration Manager. Because only one instance of SQL Server can use a port or pipe, different port numbers and pipe names are assigned for named instances, including SQL Server Express. By default, when enabled, both named instances and SQL Server Express are configured to use dynamic ports, that is, an available port is assigned when SQL Server starts. If you want, a specific port can be assigned to an instance of SQL Server. When connecting, clients can specify a specific port; but if the port is dynamically assigned, the port number can change anytime SQL Server is restarted, so the correct port number is unknown to the client.
Upon startup, SQL Server Browser starts and claims UDP port 1434. SQL Server Browser reads the registry, identifies all instances of SQL Server on the computer, and notes the ports and named pipes that they use. When a server has two or more network cards, SQL Server Browser returns the first enabled port it encounters for SQL Server. SQL Server Browser support ipv6 and ipv4.
When SQL Server clients request SQL Server resources, the client network library sends a UDP message to the server using port 1434. SQL Server Browser responds with the TCP/IP port or named pipe of the requested instance. The network library on the client application then completes the connection by sending a request to the server using the port or named pipe of the desired instance.

https://technet.microsoft.com/en-us/library/ms181087(v=sql.105).aspx

Slide 34

Defaults are important in all systems. Some defaults might give access that may be beyond what may have been intended or specified.

Default components that are not used increases the vulnerability footprint of the database.

It is important to only install what is needed. Some organizations have a “standard installation” which may include features not needed by the application. In this case, look to mitigating controls to ensure these features are not used.

Slide 37

https://msdn.microsoft.com/en-us/library/cc281953.aspx

Slide 38

The Resource DB is a hidden database and is not seen in management studio.

Slide 39

1. master
   The master database contains all of the system level information for SQL Server – all of the logins, linked servers, endpoints, and other system-wide configuration settings. The master database is also where SQL Server stores information about the other databases on this instance and the location of their files.
2. model
   The model database is used as a template whenever a new user database is created. You can change most database properties, create users, stored procedures, tables, views, etc – whatever you do will be applied to any new databases.
3. msdb
   msdb is used by the SQL Server Agent, database mail, Service Broker, and other services.
4. Resource database
   The resource database is a hidden system database. This is where system objects are stored.
5. tempdb
   The workspace that SQL Server uses to store the intermediate results of query processing and sorting.

Slide 40

The C:\ drive is the drive where the operating system is installed. No components of SQL Server (binaries, data, or log files) should be installed on the operating system partition.

This is found with the following commands:

1. C:\>set l findstr /C:"SystemDrive"

   Output:
   SystemDrive=C:

2. PS C:\> $env:systemdrive

   Output:
   C:

3. PS C:\> $env:systemroot

   Output:
   C:\Windows

https://msdn.microsoft.com/en-us/library/ms143547(v=sql.105).aspx

Slide 44

http://dennietidwell.com/Technical/VMware/Permissions%20Hierarchy%20(Database%20Engine)%20%5B2%5D.html

Posters: http://social.technet.microsoft.com/wiki/contents/articles/11842.sql-server-database-engine-permission-posters.aspx

Slide 45

Do not confuse SQL Server server-level roles with Windows server groups. They are distinct and different. This confusion can lead to incorrect root cause identification and issue remediation.

Slide 46

https://msdn.microsoft.com/en-us/library/ms188659(v=sql.120).aspx

Slide 53

Use the file high_risk_privileges.sql.

Slide 56

https://technet.microsoft.com/en-us/library/ms188371(v=sql.110).aspx

Slide 57

https://technet.microsoft.com/en-us/library/ms173724(v=sql.110).aspx

Slide 61

SQLRAP: http://www.microsoft.com/en-us/download/details.aspx?id=21738

Slide 63

https://msdn.microsoft.com/en-us/library/ms144284.aspx

Slide 64

Connections made through Windows authentication are called “trusted” connections.

Slide 65

Use the file sql_login_password_policy.sql.

https://msdn.microsoft.com/en-us/library/ms161962.aspx

Slide 66

User must change password: Third-party software developers should provide this feature if this option is used.

Slide 73

The version of SQL Server must be supported by the vendor. Support ensures the vendor is responding to security threats by developing patches for them as they are discovered.

CIS 1.1

SQL Server patches contain program updates that fix security and product functionality issues found in the software. These patches can be installed with a hotfix, which is a single patch, a cumulative update that is a small group of patches or a service pack, which is a large collection of patches.

The SQL Server version and patch levels should be the most recent compatible with the organizations' operational needs

Using the most recent SQL Server software, along with all applicable patches can help limit the possibilities for vulnerabilities in the software, the installation version and/or patches applied during setup should be established according to the needs of the organization.

Use the file version_sp.sql

Interpreting the version.

http://sqlserverbuilds.blogspot.com

Slide 75

Use the file list_databases.sql.

Slide 76

SQL Server should not be installed on the system drive because other components such as logging and backup locations will be installed where SQL Server is installed. If the system drive fills up, SQL Server will hang.

Use the file install_directory.sql

Slide 77

Find the system partition:

$env:systemdrive

Use the file list_data_log_files.sql.

Slide 78 & 79

Use the file lst_file_permissions.ps1

Slide 81

Validate all enabled protocols are needed and their use in the application.

Use the file list_protocols.sql.

By default, TCP is enabled for all versions.

Slide 82

How it works:

When an instance of SQL Server starts, if the TCP/IP or VIA protocols are enabled for SQL Server, the server is assigned a TCP/IP port. If the named pipes protocol is enabled, SQL Server listens on a specific named pipe. This port, or "pipe," is used by that specific instance to exchange data with client applications. During installation, TCP port 1433 and pipe \sql\query are assigned to the default instance, but those can be changed later by the server administrator using SQL Server Configuration Manager. Because only one instance of SQL Server can use a port or pipe, different port numbers and pipe names are assigned for named instances, including SQL Server Express. By default, when enabled, both named instances and SQL Server Express are configured to use dynamic ports, that is, an available port is assigned when SQL Server starts. If you want, a specific port can be assigned to an instance of SQL Server. When connecting, clients can specify a specific port; but if the port is dynamically assigned, the port number can change anytime SQL Server is restarted, so the correct port number is unknown to the client.
Upon startup, SQL Server Browser starts and claims UDP port 1434. SQL Server Browser reads the registry, identifies all instances of SQL Server on the computer, and notes the ports and named pipes that they use. When a server has two or more network cards, SQL Server Browser returns the first enabled port it encounters for SQL Server. SQL Server Browser support IPv6 and IPv4.

When SQL Server clients request SQL Server resources, the client network library sends a UDP message to the server using port 1434. SQL Server Browser responds with the TCP/IP port or named pipe of the requested instance. The network library on the client application then completes the connection by sending a request to the server using the port or named pipe of the desired instance.

https://technet.microsoft.com/en-us/library/ms181087(v=sql.105).aspx

Slide 85

https://msdn.microsoft.com/en-us/library/ms188659.aspx

Slide 86

Server-level roles are used for overall management of the server. The scope is server wide, meaning holders of these roles have power over all databases in the instance.

Use the file list_acct_server_level_roles.sql.

Slide 88

Database-level roles are “sweeping” in nature (not fine-grained). Care must be taken when reviewing at this level of access.

Use the file list_acct_database_level_roles.sql.

Slide 91
Use the file list_administrators.ps1

Slide 92
Use the file service_accounts.ps1

Slide 93
Use the file check_expiration_admin.sql.

https://technet.microsoft.com/en-us/library/ms188304(v=sql.105).aspx

Slide 94
Use the file builtin_users.sql

Slide 95
Use the file builtin_admins.sql

Slide 97
Use the file configuration.sql

Ad hoc distributed queries: https://msdn.microsoft.com/en-us/library/ms187569(v=sql.110).aspx
Ole Automation Procedures: https://msdn.microsoft.com/en-us/library/ms191188(v=sql.105).aspx
Remote access: https://msdn.microsoft.com/en-us/library/ms191464(v=sql.110).aspx
Remote admin connections: https://msdn.microsoft.com/en-us/library/ms190468(v=sql.110).aspx
Scan for startup procs: https://msdn.microsoft.com/en-us/library/ms187889(v=sql.110).aspx
cross db ownership chaining: https://msdn.microsoft.com/en-us/library/ms188694(v=sql.110).aspx
show advanced options: https://msdn.microsoft.com/en-us/library/ms188265(v=sql.110).aspx
c2 audit mode: https://msdn.microsoft.com/en-us/library/ms187634(v=sql.110).aspx
remote login timeout (s): https://msdn.microsoft.com/en-us/library/ms175136(v=sql.110).aspx
clr enabled: https://msdn.microsoft.com/en-us/library/ms175193(v=sql.110).aspx
default trace enabled: https://msdn.microsoft.com/en-us/library/ms175513(v=sql.110).aspx
user instance timeout:
filestream access level: https://msdn.microsoft.com/en-us/library/cc645956(v=sql.110).aspx
Database Mail XPs: https://msdn.microsoft.com/en-us/library/ms191189(v=sql.110).aspx
SMO and DMO XPs: https://msdn.microsoft.com/en-us/library/ms190461(v=sql.110).aspx
xp_cmdshell: https://msdn.microsoft.com/en-us/library/ms190693(v=sql.110).aspx
contained database authentication: https://msdn.microsoft.com/en-us/library/ff929237(v=sql.110).aspx (security considerations: https://msdn.microsoft.com/en-us/library/ff929055(v=sql.110).aspx)

Slide 98
Use the file list_clr.sql

Slide 99
Use the file list_startup_rocs.sql

Slide 101
Use the file trustworthy.sql

Slide 102
https://msdn.microsoft.com/en-us/library/ms187611(v=sql.105).aspx

The default permissions that are granted to system objects at the time of setup are carefully evaluated against possible threats and need not be altered as part of hardening the SQL Server installation. Any changes to the permissions on the system objects could limit or break the functionality and could potentially leave your SQL Server installation in an unsupported state.

A compensating control is to enable audit for use of these stored procedures and monitor the audit logs.

Slide 103
Use the file public_access_stored_rocs.sql

Slide 108
Use the file cfg_mgmt.sql

Slide 110 & 111
https://msdn.microsoft.com/en-us/library/ms188796.aspx
https://msdn.microsoft.com/en-us/library/ms188396(v=sql.110).aspx

Slide 113
https://technet.microsoft.com/en-us/library/ms188304(v=sql.105).aspx

Slide 114 & 115
Server-level roles are used for overall management of the server. The scope is server wide, meaning holders of these roles have power over all databases in the instance.

Use the file list_acct_server_level_roles.sql.

Slide 116
Database-level roles are “sweeping” in nature (not fine-grained). Care must be taken when looking at this level of access.

Slide 122
https://technet.microsoft.com/en-us/library/dd283095(v=sql.100).aspx

Slide 127
Use the file all_db_all_public.sql.

Slide 128
Use the file list_protocols1.sql

Slide 129
One-way hashing: https://en.wikipedia.org/wiki/Cryptographic_hash_function#Password_verification

Slide 132
SQL Server audit uses Extended Events to help create an audit (https://msdn.microsoft.com/en-us/library/bb630282(v=sql.110).aspx)