31. RDBMS Incident Response (V2)

When working an incident involving a database, the IR team should be sure to understand several key data points about the database itself.

1. What role does the RDBMS provide to the organization, the data it contains, data flow to/from the RDBMS (like an extract), and the sensitivity of that data?
2. Is the data in the RDBMS encrypted, and how secure or tamper evident is the keystore?
3. For authentication: Does the RDBMS utilize localized accounts, centralized accounts, or some mix of authentication models? Is login/logout actually logged (user access)?
4. What is the exposure of the RDBMS and the server(s) it resides on – open services, shares, TCP/UDP ports, trusted authentication?

Microsoft SQL Server Specific Points

1. Presence of database tools on DMZ assets and *most*, not *all* servers/systems can be suspicious. For example `sqlping` found on a DMZ server is of concern, as `sqlping` is a SQL server scan tool.
2. Look for "output" or "extract" files found on SQL servers. It is likely normal for some output/extracts, but files like "myfile1.txt" or "tableout.csv". Files that have unexplainable names can be suspicious.
3. By default, members of the "Administrators" group have elevated access to the RDBMS; this isn't necessary, and should be avoided. Attackers can dump the SAM database using tools like `pwdump7`, and then work on cracking the hashes.
4. Authentication model and login auditing is configured on the Server Properties page (use the Enterprise Manager utility).
5. Incident response scripts can be created with "`sqlcmd.exe`". You can script up select statements, and then package them in WFT!

Filesystem and Registry Notes

The version of SQL server affects, or defines, the default options, logging, and encryption level. The log file can contain login auditing, the method for user authentication (Windows/Mixed), startup information, version information, and other fact data about the instances. A new log is created each time SQL server is started. Up to 6 prior logs are stored in the \LOG\ directory.

Error Log: By default, the error log is located at Program Files\Microsoft SQL Server\MSSQL.n\MSSQL\LOG\ERRORLOG and ERRORLOG.n files.
Version: HKLM\Software\Microsoft\MSSQLServer\MSSQLServer\CurrentVersion
Instances: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\Inst2\MSSQLServer\CurrentVersion <<< Inst2 is the instance identifier; there may be multiple instances on the server.

Table 51 File Extension Types

Extension	Type
MDF	Primary DB; User and objects
NDF	Secondary DB; stores data so the database can be spread across several volumes
LDF	Transaction log; will store transient data like `insert/update/delete`; supports `rollback` for recovery and `commit` operations once a tran completes. Tran log entries are registered with a Server Process ID (SPID), which *tracks a given session*.
TRC	Trace file; will contain DDL commands like `create`, `alter`, `truncate`, and `delete`.
BAK	Backups
CSV	Commonly used for comma delimited exports.
SQL	Commonly used for Structured Query Language (SQL) commands.