

Database Security Tools

S.S. Sarma

Amarjot Walia

Pankaj Sharma

CERT-In

- Best Practices Analyzer Tool for Microsoft® SQL Server™ 2000 is a database management tool used to verify compliance of a database with common best practices for SQL Server operation and management.
- Prerequisites
 - Platforms:
 - Microsoft Windows® 2000 Server
 - Microsoft Windows XP
 - Microsoft Windows Server™ 2003
 - Microsoft SQL Server Best Practices Analyzer requires:
 - Microsoft Internet Explorer 6.0 or later
 - Microsoft .Net Framework 1.1 (1.1.4322)

- Adding a SQL Server Instance

The SQL Server Instances page allows you to add a SQL Server instance to the BPA Repository for analysis. Once an instance is identified for analysis, this can be added instance to a Best Practice Group. A Best Practice Group binds a set of rules to a group of SQL Server instances. SQL BPA analyzes each of the SQL Server instances against the set of rules included in the group. The results of the SQL BPA analysis are included in a compliance report.

- Creating a Best Practice Group

Select the rules to include in the Best Practice Group. Each rule encapsulates a widely accepted best practice

- Analyzing SQL Server Instances
- Working with Compliance Reports

SQL BPA generates a compliance report for each executed Best Practice Group. A compliance report provides details on the level of compliance of each of the SQL Server instances included in the group against the set of rules defined for the group. The report also provides workarounds to achieve compliance in the case of noncompliant and partially compliant SQL Server instances.
- Reporting services

For rich reporting capabilities, including printing, report, and query customization, plus the ability to export to other formats, you can use SQL Server 2000 Reporting Services with SQL BPA

Microsoft Baseline Security Analyzer version 1.1.1 checks for the following security settings during a full scan.

SQL checks

- Check if Administrators group belongs to sysadmin role
- Check if CmdExec role is restricted to sysadmin only
- Check if SQL Server is running on a Domain Controller
- Check if sa account password is exposed
- Check SQL installation folders access permissions
- Check if Guest account has database access

Microsoft Baseline Security Analyzer version 1.1.1 checks for the following security settings during a full scan.

SQL checks

- Check if the Everyone group has access to SQL registry keys
- Check if SQL service accounts are members of the local Administrators group
- Check if SQL accounts have blank or simple passwords
- Check for missing SQL security updates
- Check the SQL Server authentication mode type
- Check the number of sysadmin role members

Graphical tools for setting up and managing the native audit functions of the database system (system audit). The system audit functions can be used to record various events that have or will occur in the monitored database, primarily for auditing and improving system security, detecting penetration of the system and misuse of resources.

Graphical and non-graphical tools for setting up mechanisms and functions for tracing data changes in the database tables (data-change audit). The data-change audit functions can be used to capture data-change events in database tables and record the "before" and "after" values. DB Audit Expert also allows setting up automated email alerts that can notify data owners about the data-change events.

- DB Audit Expert enables the tracking of data changes made to a database. DB Audit Expert can record what changes were made and who, when, and from where they were made. Any number of tables or columns may be selected for auditing. Different types of auditing can be specified for different tables.
- Actual auditing of the database is implemented by installing audit triggers on each table selected for auditing and also creating audit trail tables to store data from the changed records.

- AppDetective™ is a network-based vulnerability assessment tool that rates the security strength of databases. AppDetective™ can be used to locate, examine, report, and help fix the security holes and misconfigurations.

Features:

- Audit and penetration testing methodology/tactics
- "agent-less" security audits.
- Automated inventory, information gathering, and analysis features
- Reporting facilities to communicate application vulnerabilities and security holes
- Extensive and continuously updated library of vulnerabilities and misconfigurations

SQL Server Password Auditing Tool

features of v2.0 are:

- Easy Command-Line Control
- Dictionary Attack
- Brute Force Attack

This tool needs the IP address or machine name of the SQL Server and the user ID to be checked.

- Usage :
 1. For the Dictionary Attack:

```
forceSQL [IP] [UserID] -d
```
 2. For the Brute Force Attack:

```
forceSQL [IP] [UserID] -b [length]
```
- If Port is other than default port 1433, you can specify port by inserting it into IP seperated by ','. Otherwise it will use the default port

- Best Practices Analyzer
<http://www.microsoft.com/downloads/details.aspx?FamilyID=b352eb1f-d3ca-44ee-893e-9e07339c1f22&DisplayLang=en>
- Microsoft Baseline Security Analyzer
<http://www.microsoft.com/technet/security/tools/mbsahome.mspx>
- DB Audit 2.0
<http://www.softtreetech.com/dbaudit/index.htm>
- AppDetective
<http://www.appsecinc.com/products/appdetective/>
- forceSQL v2.0
<http://www.nii.co.in/tools.html>

Thank You

ssarma@mit.gov.in

amarjot.walia@hub.nic.in

pankaj.sharma@hub.nic.in

<http://www.cert-in.org.in>