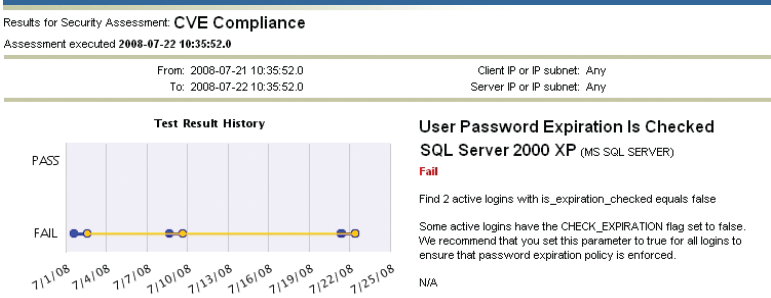
SECURE | IT

DATABASE VULNERABILITY ASSESSMENT



Database security vulnerability assessments evaluate your database environment and compare it with Federal Government configuration and security best practices. Security vulnerabilities are identified and prioritized so you remediate weaknesses and safeguard your critical enterprise data from both internal and external threats.

FEATURES

The database vulnerability assessment:

- Identifies all databases on your network
- Scans the selected databases for known vulnerabilities such as missing patches, weak passwords, misconfigured privileges and default vendor accounts
- Runs a series of over a hundred preconfigured tests in accordance with Defense Information System Agency (DISA) Security Technical Implementation Guide (STIG), National Institutes of Standard and Technology (NIST) and the Center for Internet Security (CIS) security standards.
- Generates security health report card and recommends concrete action plans to strengthen database security
- Combines three essential detection methods: database scanning, agent-based scanning and dynamic monitoring
- Provides complete coverage without impacting performance or stability
- Does not run intrusive exploits that can crash systems by imitating attacker behavior
- Supported platforms include:
  - Databases: Oracle, SQL Server, IBM DB2, Informix, Sybase and MySQL
  - Applications: SAP, Oracle Financials, PeopleSoft, Siebel, Business Objects

CLIENT REQUIREMENTS

The solution requires the following from the client to permit the assessment to be performed:

- IP address which is defined within its network. This address must be setup prior to start of task.
- Consultants will use a laptop to run the assessment. If customer does not permit contractor-owned equipment from attaching to the network, a customer-furnished laptop will need to be provided one week prior to the start of the task. The assessment laptop and its IP address must be able to communicate with all the required database instances.
- Client must create a user account on each database instance that is evaluated which will be used by the assessment team. The account will have limited privileges within the database to permit assessment of configuration, privileges and settings.
- Client must complete a Data Source worksheet at the time of order which specifies includes the server IP addresses, communication port, instance name, and the password for the assessment user account.

SERVICE AND DELIVERABLES

SecureIT offer a fixed price service to Federal government agencies. Deliverables:

- Database security health report on up to 50 database instances per engagement.
- Optional: Vulnerability assessment of underlying database service operating system including file permissions and external database configuration files.
- Optional: Real-time activity monitoring and report of behavioral vulnerabilities such as users sharing privileged credentials.
- Optional: Scan your databases for existence of sensitive information such as credit card numbers, social security numbers of information specific to your agency.

CONTACT

SECURE | IT

Phone: 703.464.7010
Email: info@SecureIT.com
Web: www.SecureIT.com