May, 2019

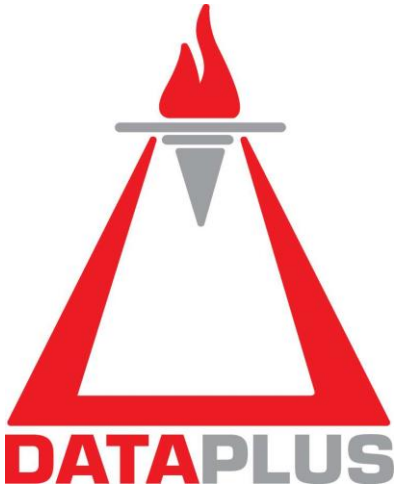
Whitepaper

Omega DB Scanner ™

Professional Edition

For Oracle Database, with built-in SIEM integration

Database security posture assessment and scan results comparison



Introduction

The database is usually the central point of enterprise's most valuable informational assets, data on customers, partners, transactions, financial and much more. With the arrival of the information age, millions of such records owned by the company are being confronted with an ever increasing number of attacks from insider and/or outsider sources who are trying to gain unauthorized access to steal, destroy, compromise or retrieve industrial espionage data. Database security is one of the top concerning priorities of the information owners that needs to comply with more internal and external regulatory compliance practices and standards that require stronger information security controls.

The database remains today one of the less protected point of the enterprise's information, which traditionally has been focused mostly in protecting perimeter networks, or operating systems which do indeed create some barriers, but which are few effective against insider threats, especially from privileged account holders, who not only are within the internal network, but by nature of their jobs may access information bypassing application security, or own a high security clearance on it. Furthermore the traditional network and OS protection has been modeled with the concept in mind of the once "isolated" database within the internal network, but due to their increasing business services and interfaces, today's databases are much more open toward the external networks and internet, and the number and sophistication level of the attacks has since then increased.

In all of the recent studies performed by the authoritative bodies of the field, inside breaches account for more than 50% of data breaches, usually with higher impact than breaches from outside.

The Challenge

Implementation of stronger information security controls requires implementation of stronger database security measures, on top of which is the performing of an in-depth assessment of the security posture of the Oracle database on the following important security areas:

- Authentication
- Authorization
  - System Privileges
  - Important system object privileges
  - Role Privileges
- Audit
- Backup-Availability
- General Security

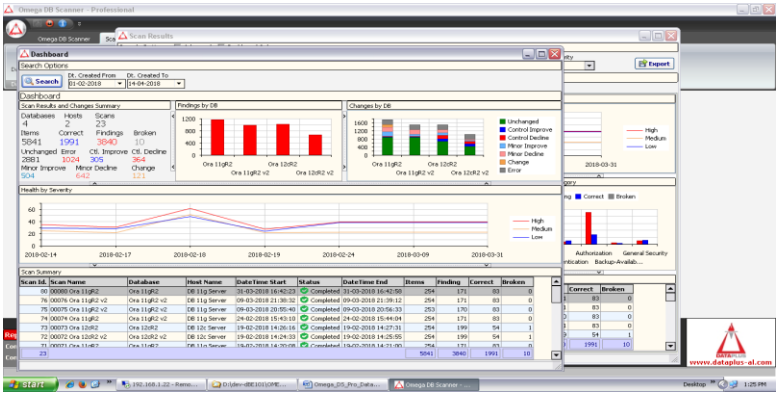
What is needed?

- Scan of the security posture of the database on the above topics
- Ability to compare scan result at item level to detect changes
- Tailoring according to the specific database environments
- Integration with SIEM (where applies)
- Automated processing

Introducing Omega DB Scanner Professional

Omega DB Scanner is a security auditing tool and vulnerability assessment scanner for Oracle databases. It has been designed to give the user the **automated knowledge** in performing the complex task of assessment, evaluation and improvement of the security posture of his mission critical Oracle database.

Omega DB Scanner is an out-of-box, software-only solution. The Professional Edition features a Repository (built on Oracle Express Edition) that contains system configurations and scan results, with a Task Scheduler as a NT Service application, and a Windows desktop application that manages the whole solution. Target databases are scanned from both the application and Scheduler and results are saved to Repository. Automatic e-mail alerting for scan results can be configured for each database. Manual and transactional scan item's comparison highlights any item change through DB scans.



Omega DB Scanner is not just a scanner, but also an inventory of your Oracle database's security posture. It is Agent-less and accesses the target database in read-only mode.

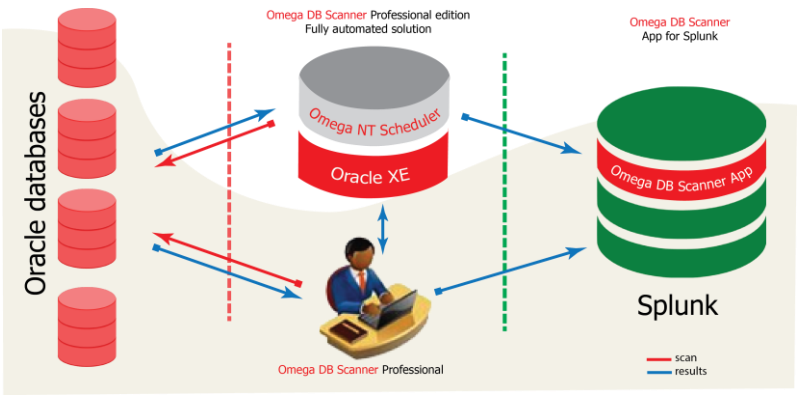
Key features & benefits

- Scheduled scans
- E-Mail alerts for scans
- In-depth view of Oracle security combining:
  - Account Status
  - Role hierarchy
  - Full audit syntax support
  - Public privilege highlights
- Effective privilege evaluation (with role hierarchy)
- Account based evaluation [roles optional]
- Intelligent Scan - ex. Audit of system privileges by effective privilege
- DB repository storage
- Scan Comparison - Run vs. Baseline
- Transactional Comparison
- Over 250 advanced in-depth controls
- Rich and intuitive GUI
- Easy and simple operation
- Quick and minimal setup
- Agentless and read-only DB Scan
- Unicode character set support
- Built-in SIEM integration for Splunk

Omega DB Scanner Architecture

Omega DB Scanner Professional has four main components:

- **Omega DB Scanner Engine**: An Oracle PL/SQL software package featuring e-Mail Alert notification and SIEM/LMS integration, installed on the XE repository under the SYS schema and running with its privileges.
- **Omega DB Scanner Repository**: An Oracle Express Edition (XE) Schema Repository containing all system data - configurations and scans results.
- **Omega DB Scanner Scheduler**: A Windows NT Service application implementing scheduled scans.
- **Omega DB Scanner Application**: A Windows-based client desktop Application, managing the whole solution.



Deployed Vulnerabilities (Security Controls)

Omega DB Scanner deploys 254 (in this version) vulnerabilities – alias security controls – that can be used to scan and assess the security posture of your Oracle database.

These controls assess the following Oracle database areas of security interest:

- System Privileges authorization
- System Privileges audit
- System Roles authorization
- System Packages authorization
- System Tables authorization
- System Views authorization
- System Parameters
- User Profiles - Password
- User Profiles - Resources
- System accounts status
- Others

In-Depth scan of security posture

"In-depth" in Omega DB Scanner means evaluating:

- Account status — whether the account is effectively LOCKED or not at assessment time
- Effective privilege — assessing not only the direct grant of the privilege, but also when it is in force granted through role-grants hierarchy
- Account based — allows focusing (by Effective Privilege) on user accounts only – as the "real" operating entities of the privilege; Roles also assessed as an option
- Others: — PUBLIC grants on privilege, full support of the AUDIT command syntax

Authorization

Authorization is the process of allowing acceptances to the vulnerability control's finding either at a whole or at entity level, depending on each vulnerability control. This means that the control will not fire a Finding for an already declared holder, or holders, of the (for example) DBA Role authorized according to system's Database Administrator[s] – at least one DBA has to be. But it must fire a Finding whenever a non-authorized account is found granted with the DBA role.

Scans Comparison

Use the scan comparison feature to highlight changes between two different scans, changes that are evaluated at each control between current run and the baseline. Automatic (transactional) comparison is also performed at the repository level for each vulnerability vs the previous scan result of the same.

Scheduled Scans

The solution's Scheduler features scheduled scanning of target databases.

E-Mail Alert

E-Mail alert for scans with summary of results and transactional comparison.

SIEM and Log Management Systems integration

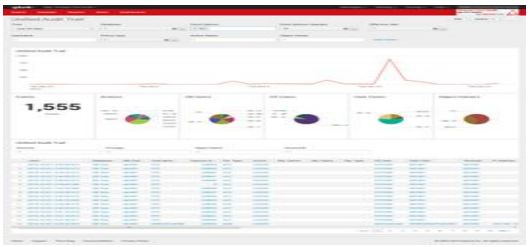
Omega DB Scanner's open structure allows and enables automatic delivery of scan records to SIEMs and Log Management Systems that support records ingest through one of:

- "Push" directly through TCP in XML format - built-in supported by the LMS module
- "Pull" by Oracle query - supported by its open structure and as specifically by each SIEM

Splunk

Automatically send your scan records straight to Splunk SIEM from Omega DB Scanner; thus enabling storage of your scans results in a central location, visualization and quick access of scan data history.

Delivery of scan records to Splunk is built-in supported; it can also be with Splunk DB Connect App.



Monitor and assess the security posture of your Oracle database via the graphical interface of our next solution **Omega DB Scanner App for Splunk***, running on top of the Splunk system.

Available at SplunkBase:
https://splunkbase.splunk.com/app/3753/

* Omega DB Scanner App for Splunk is a Splunk Application made by DATAPLUS and free to all Omega DB Scanner users!

Compatibility:

- Target database — Oracle Database 10g R2 - 18c, all editions
- Target database OS — Target database OS independent
- Application & Scheduler — All Win NT-based systems

About DATAPLUS

DATAPLUS is an information security consulting and solution provider company, founded in October 2007 in Tirana, Albania. We provide Oracle database software solutions and services.

Contact us

For more information about Omega DB Scanner please visit www.dataplus-al.com, or contact us at:

DATAPLUS
Tirana, Albania
Street Address: Bul. Zog I, P. "Edicom", 8F.
E-Mail: info@dataplus-al.com
Cel: +355 68 2061664
Tel: +355 42419275