Omega DB Security Reporter ™

For Oracle Database

July 2024 | Version 2.4

Assessment comparison with Tenable Nessus Professional

Omega DB Security Reporter
vs
Nessus Professional

Comparison of Security Assessments for Oracle Database

www.dataplus-al.com

TABLE OF CONTENTS

1 Overview

This document describes a comparison between assessing the security of Oracle Database version 19 with:

Omega DB Security Reporter, version 2.4 – by DATAPLUS
Nessus Professional, version 10 – by Tenable

… the later using the CIS Oracle Database 19c Benchmark version 1.1.0 – published by Center for Internet Security (CIS) in December 2022.

Omega DB Security Reporter and Nessus Professional assess only those controls that can be performed with SQL commands.

The paragraphs of this document have been compiled adhering to the structure of CIS Oracle Database 19c Benchmark.

Document Information:

Document Author:	Altin Karaulli – DATAPLUS Founder
Document Date:	July-2024

2 Comparison

2.1 Database Security Parameters

Description: Many Oracle database initialization parameters are related to security and must be assessed for proper values.

Feature	Feature Description	Nessus	Omega
DB Parameters	Assessment of security-related DB initialization parameters	Yes (1)	Yes (2)

Notes:

1. Nessus Professional assesses 16 security-related parameters.

2. Omega DB Security Reporter assesses 17 security-related parameters.

2.2 User Profiles - Resources

Description: Password resource parameters are part of User Profiles and control passwords settings and management. Resource parameters do the same for system resources.

Feature	Feature Description	Nessus	Omega
Password Parameters	Assessment of Password security for database users	Yes	Yes (1)
Resource Parameters	Assessment of Resource parameters for database users	Yes (2)	No

Notes:

1. Both Nessus Professional and Omega DB Security Reporter assess 8 out of 9 password resources. The PASSWORD_ROLLOVER_TIME (introduced in 19c) is not included.

2. Nessus Professional also assesses a single Resource Parameter - SESSIONS_PER_USER.

2.3 Users

Description: This category, named as such by CIS Oracle Database 19c Benchmark, contains some individual controls related to user security settings.

Feature	Feature Description	Nessus	Omega
User	Assessment of different aspects of user security	Yes (1)	No

Notes:

1. Kind of: users with default password, existence of sample user schemas, existence of externally identified users, existence of SYS.USER$MIG table, user's authentication type, … etc.

2.4 Privileges

Description: Privilege is the right to execute a particular type of SQL statement.

For both Nessus Professional and Omega DB Security Reporter, the types of privileges assessed are:

System Privileges	right to perform actions on system level or on schema-wide objects.
Object Privileges	right to perform a certain operation on a specific object.
Role Privileges	groups of privileges and other roles.

2.4.1 Basic Assessment

Feature	Feature Description	Nessus	Omega
System Privileges	Assessment of System Privileges grants	Yes (1)	Yes
Object Privileges	Assessment of Object Privileges grants	Yes (1)	Yes
Role Privileges	Assessment of Role Privileges grants	Yes (1)	Yes
Public Grant	Assessment of privileges granted to Public	Yes	Yes
Proxy User	Assessment of Proxy Users	Yes (2)	No

Notes:

1. Nessus Professional is limited to specific privileges and for direct grants only.

2. Limited to Role Privileges only.

2.4.2 Advanced Assessment

Feature	Feature Description	Nessus	Omega
Indirect Grant	Assessment by granted through a role, or several ones (chain)	No	Yes (1)
Account Status	Assessment by user account status – locked/unlocked	No	Yes (2)
Grantable	Assessment by Grantee able to grant own granted privilege	No	Yes (3)
Grantee selection	Selection of specific grantees for assessment	No	Yes (4)
Any Item	Assessment of any System Privilege, Object Operation and Role	No	Yes (5)

Notes:

1. Users are the operative entities. Behind every user stands either a human, or an interface that interacts with the database, the later of every kind in respect to the infrastructure, like the application DB user (working on behalf of many application users). It is the DB Users that do use the privileges. While Roles are no operative entities, they are just groups of privileges. The security assessment must highlight not only the privileges granted directly to a Grantee (be this a User or Role), but also those being effective through a granted role (to which the privilege is granted). And to also support the case when a privilege is granted to a role, which is granted to another role (and so on), and the last one is granted to a Grantee – no limit on the "chain" nodes.

2. An unlocked Grantee of a privilege has a higher criticality compared to a locked Grantee of the same.

3. A Grantee that can grant its granted privilege to another User/Role has a higher criticality compared to a Grantee that cannot.

4. Nessus Professional assesses all users that are not created by Oracle – indiscriminately. Omega DB Security Reporter can assess any user, providing the possibility to compile automatic, manual (include/exclude), and combined lists from both Oracle and non-Oracle users.

5. Omega DB Security Reporter is not limited to specific privilege items only – it can assess all available. The last two (Object Operation and Role) enable assessment of user's application objects and roles, not being limited to Oracle Dictionary objects and roles only.

Reminder:

It is precisely the information on user's application tables that every intruder looks to access, change, or destroy!

2.5 Audit

2.5.1 Traditional Audit

Description: Traditional Audit is the legacy audit on Oracle Database. It is deprecated in Oracle 21c and de-supported in Oracle 23ai.

Feature	Feature Description	Nessus	Omega
User Statements	Assessment of SQL User Statements	Yes (1)	Yes
System Privileges	Assessment of System Privileges	Yes (1)	Yes
Object Operations	Assessment of Object Operations	Yes (2)	Yes

Notes:

1. Nessus Professional is limited to specific items and on audit for All Users only.

2. Object operations audit is limited to SYS.AUD$ table only.

2.5.2 Unified Audit

Description: Unified Audit is the new audit on Oracle Database, starting with Oracle 12c.

Feature	Feature Description	Nessus	Omega
System Actions	Assessment of System Actions	Yes (1)	Yes
System Privileges	Assessment of System Privileges	Yes (1)	Yes
Object Operations	Assessment of Object Operations	Yes (1)	Yes
By-Except User	Assessment of users included/excluded in/from the audit policy	No	Yes (2)
By Granted Role	Assessment of users because granted an (audited) role	No	Yes (3)
By Role	Assessment for every System Privilege granted to a Role	No	Yes (4)

Notes:

1. Nessus Professional is limited to specific items only and on audit for All Users only. Object operations audit is limited to AUDSYS.AUD$UNIFIED table only.

2. Unified Audit Policies, other than applied for All Users, can also be applied to specific users (audit clause BY USER), or can exclude specific users (audit clause EXCEPT USER).

3. Unified Audit Policies can be enabled on every user that has been granted a specific role – directly or indirectly (audit clause BY_USERS_WITH_ROLES).

4. Unified Audit Policies can monitor the exercise of all system privileges granted directly to a role (audit clause ROLE_AUDIT).

Reminder:

The last two points (By Granted Role and By Role) enable auditing the user's application roles!

2.5.3 Advanced Audit

Description: Audit assessment options valid for both Traditional and Unified Audit

Feature	Feature Description	Nessus	Omega
Account Status	Assessment by user account status – locked/unlocked	No	Yes (1)
Partial Audit	Assessment by Audit being Partial or Full	No	Yes (2)
FGA	Assessment of FGA Audit Policies	No	Yes (3)
Cumulative Audit	Combining different audit options (Traditional) or policies (Unified)	No	Yes (4)
Any Item	Assessment of any Item – Statement (Traditional) or System Action (Unified), System Privilege, and Object Operation	No	Yes (5)

Notes:

1. An un-audited user that is locked has a lower criticality compared to an un-audited unlocked user.

2. Audit is considered partial for a user when (for the specific audited item):

* User is audited either on Success or on Failure only.
* User is audited for Top-SQL commands only – ALL STATEMENTS clause on Traditional Audit and ONLY TOPLEVEL clause on Unified Audit.
* User is audited conditionally on Unified Audit – clause AUDIT_CONDITION.

3. Fine-Grained (FGA) Audit Policies enable conditional audit, protection and alerting on TABLE/VIEW objects.

4. Example: User is audit for some item for Success in one configuration, and failure only in another; the net result is a Full Audit.

5. Omega DB Security Reporter is not limited to specific privilege items only – it can assess all available.The last (Objects Operations) enables assessment of user's application objects (hacker's target), not being limited to Oracle Dictionary objects only.

2.6 Advanced Features

2.6.1 Level I

Description: Features good to have.

Feature	Feature Description	Nessus	Omega
Granularity	Item assessed and reported individually for each Subject	No	Yes (1)
Detailed Result	Result is given with 5 levels of Criticality	No	Yes (2)
Authorization	Authorization of exceptions.	No	Yes (3)
Editable Templates	User can edit existing templates or create new ones	No	Yes (4)

Notes:

1. Every item (be a user profile, privilege, or audit option) is assessed and reported separately for every Subject(User, or Role where applies). This, differently from many scanners that return multiple Subjects inside the result of the same assessed item, allows for a very-detailed result, that is very suitable for further analysis.

2. The result for each assessed item and subject is evaluated and reported with 5 levels: Generic, Info, Low, Medium, High - and not a simple Correct/Finding.

3. In practical situations certain findings need to be except, either as accepted risks, or when mitigated outside Oracle. This is implemented as a pre-declared entries of item-subjects couples at user's will.

4. User can edit existing templates or create new one, not being limited to predefined items for assessment only. This his highlighted in the previously mentioned "Any Item" listings.

2.6.2 Level II

Description: Features very good to have.

Feature	Feature Description	Nessus	Omega
All applying Audits	Combine Traditional, Unified and FGA	No	Yes (1)
Cross check	All Privileges vs All Audits	No	Yes (2)

Notes:

1. Combination of all applying audits for a combined result is the only way to reach a definitive result. For example, when assessing system privilege audits for a user, both the Traditional Audit and Unified Audit is evaluated for the user. In the audit of object operations, the FGA is also added when applies (TABLEs/VIEWs).

2. Revoking un-required privileges is the easy part. The question is on how to handle privileges granted to users who need them for their daily tasks – ex. Developers, or Interfaces, …, etc. What is need is to know, for every item – ex. an object operation – and every user, all applying privileges and all applying audits, to know the standing balance between privileging (grant) and accountability (audit).

Example: assessing the SELECT privilege on a TABLE for a specific user. User can have this right either by being granted SELECT on this specific object, or by being granted the SELECT ANY TABLE System Privilege. Meanwhile, the audit can result by a Statement/System Action (TD/UN) Audit on the user, or by a System Privilege being audited, or by audit on the operation of the object itself – all valid for both Traditional and Unified Audit, and FGA.