Oracle Database Security Assessment: Das Werkzeug zur Erkennung von Sicherheits- und Datenschutzrisiken

Angreifer gehen bei ihrem Handeln sehr kreativ vor und verbringen viel Zeit damit das Angriffsziel zu verstehen. Sie verwenden mitunter illegale Werkzeuge zur Informationsgewinnung und halten sich nicht an Gesetze und Regeln. Diese Werkzeuge nutzen unter anderem Sicherheitslöcher und Fehlkonfigurationen ihrer Angriffsziele aus um die besten Angriffsvektoren zu erhalten. Haben die Angreifer genügend Informationen gesammelt, beginnen sie meist sehr diskret mit dem eigentlichen Angriff und gelangen so viel zu oft an sensible Daten.

Als Eigentümer, Verantwortlicher oder Verarbeiter von Daten hilft es ähnlich zu denken wie ein Angreifer, aber mit dem Ziel die Sicherheitslage so zu verbessern, dass ein Angreifer sein Ziel nicht erreicht. Viele Angriffsvektoren lassen sich durch einfache Sicherheitsmaßnahmen unterbinden. Datenbanken sollten so konfiguriert werden, dass sie ausschließlich nur Funktionen zulassen, die für den Betrieb der Anwendungen beziehungsweise der Verfahren notwendig sind.

Für jedes Datenbanksystem, welches personenbezogene Daten verarbeitet, muss entsprechend aktueller Gesetze und Richtlinien, wie zum Beispiel in der EU-Datenschutzgrundverordnung (EU- DSGVO) gefordert, ein Grundschutz implementiert werden. Für manche Regularien gibt es passende Kataloge oder Handlungsleitfaden, andere setzen auf angemessenen Schutz nach aktuellem Stand der Technik.

Gerade für Oracle Datenbanken sind eine Vielzahl an Sicherheitsmaßnahmen verfügbar, wie zum Beispiel bei der Konfiguration der Datenbank oder gar der Absicherung der Umgebung.

Oracle Database Security Assessment Tool

Oracle möchte bei der Umsetzung notwendiger Datensicherheitsmaßnahmen helfen und bietet ein Werkzeug zur Erkennung potenzieller Sicherheitsrisiken für Oracle Datenbanken an. Das Oracle Database Security Assessment Tool (DBSAT) überprüft Datenbankkonfigurationen, Datenschutzfunktionalitäten und gibt Sicherheitsempfehlungen gemäß Oracle Datenbanksicherheit Best Practices. In der Version 2 wurde es zusätzlich mit der Fähigkeit ausgestattet, auf einfachste Weise, sensitive Daten in Oracle

UNTERSTÜTZUNG FÜR

- Das Finden von Konfigurationsproblemen
- Das Aufspüren von Sensiblen Daten die ggf. gesondert geschützt werden müssen
- Das Erstellen von Datenbankreports zum Status Quo

TEST-BEREICHE

- Benutzerkonten
- Privilegien und Rollen
- Berechtigungskontrolle
- Datenverschlüsselung
- Zugriffskontrolle
- Passwortrichtlinien
- Datenbank-Konfiguration
- Listener-Konfiguration
- Dateiberechtigungen
- Sensitive Daten

Datenbanken zu suchen. Die hiermit aufgezeigten potenziellen Angriffsziele und Sicherheitsrisiken werden dokumentiert und können bei Bedarf und Notwendigkeit vom Datenbankadministrator behoben werden.

Das Oracle Database Security Assessment Tool ist für Kunden mit gültigem Datenbanksupport kostenfrei und dient in erster Linie zur kurzfristigen Identifizierung von Angriffszielen und hilft bei der Minimierung allgemeiner Risiken sowie bei der Umsetzung einer umfassenden Sicherheitsstrategie. Es ist sowohl für On-Premises als auch cloud-basierten Oracle Datenbanken einsetzbar. Für die Datenbank ist es nicht invasiv, d.h. es werden keine Objekte oder Strukturen in der Datenbank angelegt.

DBSAT führt Tests und Scans in folgenden Kategorien durch:

- Benutzerkonten, Privilegien und Rollen
- Berechtigungskontrolle
- Datenverschlüsselung
- Zugriffskontrolle
- Passwortrichtlinien
- Datenbank-Konfiguration
- Listener-Konfiguration
- Betriebssystem-Dateiberechtigungen
- Sensitive Data Discovery (Data-Dictionary)

Im Wesentlichen besteht das Werkzeug aus drei Komponenten:

- DBSAT Discoverer (Aufspüren sensitiver Daten)
- DBSAT Collector (Sammeln von Konfigurations-Informationen)
- DBSAT Reporter (Erstellung des DBSAT Berichts)

Der DBSAT Discoverer lässt sich unabhängig vom DBSAT Collector und DBSAT Reporter verwenden.

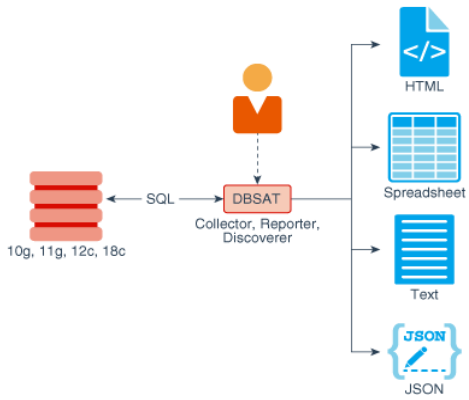


Abbildung 1: Database Assessment Tool Architektur

Folgende Schritte sind bei Verwendung des Oracle Database Security Assessment Tools notwendig:

- Herunterladen des Oracle Database Security Assessment Tools von Oracle Support (Document ID: 2138254.1)
- Schaffen der Ablaufumgebung und Zuweisen der Privilegien
- Sammeln der Informationen, indem Sie 'dbsat collect' bzw. 'dbsat discover‘ auf dem Ziel ausführen
- Ausführung des ‘dbsat report’ Kommandos, um die Berichte zu erstellen (Wird nur im Zusammenhang mit dem DBSAT Collector benötigt)

Die aktuelle Vorgehensweise zur technischen Ausführung des Tools finden Sie in der Dokumentation: Security Assessment Tool User Guide Release 2.0.1.

Hinweis

DBSAT hilft sensitive Daten und potenzielle Schwachstellen in Ihrem Datenbanksystem zu identifizieren. Sowohl die Ausführung des Tools und eventuell negative Folgen durch Behebungen identifizierter Probleme obliegt in der Verantwortung des Kunden. Die von diesem Werkzeug erzeugte Ausgabe kann potenziell sensible Systemkonfigurationsdaten und Informationen enthalten, die von einem Angreifer missbraucht werden könnten. Der Ausführer ist dafür verantwortlich, die Ausgabe dieses Tools, einschließlich aller generierten Berichte vor Missbrauch zu schützen.

Suchen von sensitiven Daten

Die Komponente **DBSAT Discoverer**, dient zum Aufspüren sensitiver Daten. Verordnungen wie die EU-DSGVO verlangen von Unternehmen, dass sie personenbezogene Daten schützen. Unternehmen müssen jedoch zuerst wissen, welche persönlichen Daten verarbeitet werden und wo sich diese befinden.

Der DBSAT Discoverer selber ist ein Java-Programm und benötigt zur Ausführung eine Java Runtime Environment (JRE) 1.6 oder höher

DBSAT unterstützt hier durch das Scannen der Datenbankmetadaten auf Basis von Spalten-Namen und Spalten-Kommentaren. Die Suchmuster lassen sich flexibel durch Verwendung regulärer Ausdrücke in entsprechenden Konfigurationsdateien anpassen.

```
#U.S. Social Security Number (US SSN)
[SOCIAL_SECURITY_NUMBER]
COL_NAME_PATTERN = SOC.*SEC|^SSN$|NATIONAL.*ID|SSID
COL_COMMENT_PATTERN = Social Security Number
SENSITIVE_CATEGORY = PII - IDs
```

Abbildung 2: Angabe der Metadaten Suchmuster in der Konfigurationsdatei

Da die Suche nach sensitiven Daten ausschließlich im Data-Dictionary durchgeführt wird, werden keine Zugriffsrechte auf die Daten selber benötigt. Die Suche ist lokalisierbar, für „deutsch“ beispielsweise gibt es auf Anfrage ein entsprechendes anpassbares Template.

Der mit dem Discoverer erstellte Bericht enthält Informationen über den genauen Speicherort (Schema > Tabelle > Spalte) von potenziell sensitiven Daten. Zudem wird eine

CSV-Datei mit allen notwendigen Informationen erstellt. Alle Ausgabedateien sind durch ein Kennwort verschlüsselt.

Sensitive Daten werden natürlich nicht im Bericht angezeigt.

Schema Name	Table Name	Column Name	Column Comment	Sensitive Category	Sensitive Type
DEMOAPPS	EMP	EMAIL	--	PII	EMAIL
DEMOAPPS	EMP	FIRSTNAME	--	PII	FIRST_NAME
DEMOAPPS	EMP	LASTNAME	--	PII	LAST_NAME
DEMOAPPS	EMP	LOCATION	--	PII - IT DATA	LOCATION
DEMOAPPS	EMP	PHONEFAX	--	PII	PHONE
DEMOAPPS	EMP	PHONEFIX	--	PII	PHONE
DEMOAPPS	EMP	PHONEMOBILE	--	PII	PHONE
DEMOAPPS	EMP	POSITION	--	JOB DATA	JOB_TITLE
DEMOAPPS	EMP	SALARY	--	JOB DATA	INCOME
DEMOAPPS	EMP	USERID	--	PII - IT DATA	USERID
DEV	COUNTRIES	COUNTRY_ID	Primary key of co…	PII - ADDRESS	COUNTRY
DEV	COUNTRIES	COUNTRY_NAME	Country name	PII - ADDRESS	COUNTRY

Abbildung 3: Genauer Speicherort der Daten

Sollen auch die Daten hinsichtlich eventueller sensibler Inhalte analysiert werden, kann Oracle Sensitive Data Discovery eingesetzt werden. Dieses Werkzeug ist Bestandteil des Database Masking and Subsetting Packs. Weiterführende Links sind im Abschnitt „Weitere Informationen“ aufgeführt.

Sammeln von Konfigurationsdaten und Erstellung des Berichts

Der **DBSAT Collector** führt Tests in Form von SQL-Abfragen (nur gegen das Oracle Datenbank Dictionary) und Betriebssystembefehle (für Listener Konfiguration, SQLNET.ORA usw.) aus, um die notwendigen Informationen aus dem System zu sammeln. Die gesammelten Daten werden in eine durch ein Passwort verschlüsselte JSON-Datei geschrieben. Diese Datei wird dann von der zweiten Komponente, dem DBSAT Reporter, während der Analysephase verwendet. Der DBSAT Collector kann für Oracle Datenbanken ab der Version 10.2.0.5 und für die folgenden Betriebssysteme verwendet werden:

- Solaris x64 and Solaris SPARC
- Linux x86-64
- Windows x64
- HP-UX IA (64-bit)
- IBM AIX & zSeries Based Linux

Die Datenerfassung aus den Kategorien Listener-Konfiguration und Betriebssystem-Dateiberechtigungen werden auf Windows-Plattformen momentan nicht unterstützt.

Zur Ausführung des DBSAT Collectors werden folgende Datenbank Privilegien benötigt:

- CREATE SESSION
- SELECT on SYS.REGISTRY$HISTORY
- Rolle SELECT_CATALOG_ROLE
- Rolle DV_SECANALYST (wenn Database Vault aktiviert ist)
- Rolle AUDIT_VIEWER (ab 12c)

- Rolle CAPTURE_ADMIN (ab 12c)
- SELECT on SYS.DBA_USERS_WITH_DEFPWD (11g und 12c)
- SELECT on AUDSYS.AUD$UNIFIED (ab 12c)

Zur Ermittlung der Betriebssystem-Informationen werden Leseberechtigungen für das entsprechende Oracle-Home Verzeichnis benötigt.

Für einen dauerhaft sicheren Betrieb sollte ein entsprechender Prozess zur fortwährenden Sicherstellung der Sicherheit und ein automatisiertes Monitoring etabliert sein, um die Datenbank hinsichtlich Konfiguration, Patching und Nutzung zu überwachen. Dieses ist zum Beispiel mit dem Lifecycle Management Pack von Oracle Enterprise Manager möglich.

Der **DBSAT Reporter** analysiert die gesammelten Daten und bietet die Ergebnisse und Empfehlungen in mehreren Ausgabeformaten an: PDF, XLS und Text. Der DBSAT Reporter ist ein plattformunabhängiges Python-Programm und benötigt Python 2.6 oder höher. Als Ergebnis erstellt DBSAT Berichte in drei unterschiedlichen Formaten – HTML, XLS und TEXT - für verschiedene Zielgruppen und Verwendungszwecke.

Ausschnitte der Ergebnisse

Der HTML-Bericht liefert detaillierte Ergebnisse in einem einfach zu navigierenden Format.

Die folgende Abbildung zeigt die ersten drei HTML-Tabellen einer Zusammenfassung:

Oracle Database Security Assessment

Highly Confidential

Assessment Date & Time

Date of Data Collection	Date of Report	Reporter Version
Mon Jan 22 2018 09:36:00	Mon Jan 22 2018 11:29:57	2.0.1 (December 2017) - d526

Database Identity

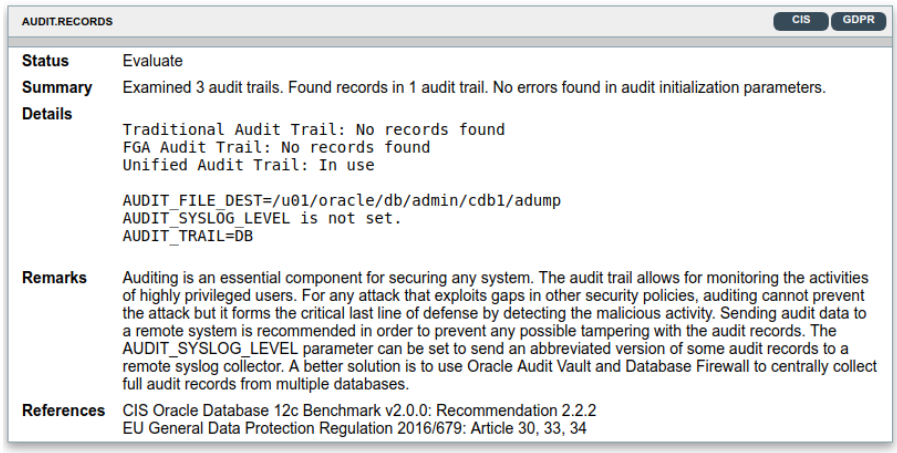
Name	Container (Type:ID)	Platform	Database Role	Log Mode	Created
CDB1	PDB1 (PDB:3)	Linux x86 64-bit	PRIMARY	NOARCHIVELOG	Wed Jan 04 2017 15:09:00

Summary

Section	Pass	Evaluate	Advisory	Low Risk	Medium Risk	High Risk	Total Findings
Basic Information	1	0	0	0	0	0	**1**
User Accounts	4	0	0	5	2	1	**12**
Privileges and Roles	4	14	0	1	0	0	**19**
Authorization Control	0	0	2	0	0	0	**2**
Data Encryption	0	1	1	0	0	0	**2**
Fine-Grained Access Control	0	1	4	0	0	0	**5**
Auditing	3	5	1	0	3	0	**12**
Database Configuration	7	3	0	1	1	1	**13**
Network Configuration	1	0	0	1	3	0	**5**
Operating System	0	2	0	2	1	0	**5**
Total	**20**	**26**	**8**	**10**	**10**	**2**	**76**

Abbildung 4: HTML-Bericht Zusammenfassung

Die einzelnen „Findings“ werden im Weiteren detailliert angezeigt:



AUDIT.RECORDS CIS GDPR

Status	Evaluate
Summary	Examined 3 audit trails. Found records in 1 audit trail. No errors found in audit initialization parameters.
Details	Traditional Audit Trail: No records found FGA Audit Trail: No records found Unified Audit Trail: In use AUDIT_FILE_DEST=/u01/oracle/db/admin/cdb1/adump AUDIT_SYSLOG_LEVEL is not set. AUDIT_TRAIL=DB
Remarks	Auditing is an essential component for securing any system. The audit trail allows for monitoring the activities of highly privileged users. For any attack that exploits gaps in other security policies, auditing cannot prevent the attack but it forms the critical last line of defense by detecting the malicious activity. Sending audit data to a remote system is recommended in order to prevent any possible tampering with the audit records. The AUDIT_SYSLOG_LEVEL parameter can be set to send an abbreviated version of some audit records to a remote syslog collector. A better solution is to use Oracle Audit Vault and Database Firewall to centrally collect full audit records from multiple databases.
References	CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 2.2.2 EU General Data Protection Regulation 2016/679: Article 30, 33, 34

Abbildung 5: HTML-Bericht Beispiel eines „Findings“

Im Bereich der „Findings“ finden Sie:

Titel
Eindeutige ID des einzelnen Tests, hier AUDIT.RECORDS.

Status
Der Status kann als Empfehlung zur Priorisierung der Problembehebung verstanden werden. Ein schweres Risiko könnte sofortige Abhilfemaßnahmen erfordern, während andere Risiken bei einer geplanten Ausfallzeit beziehungsweise bei Wartungsaktivitäten behoben werden können.

Es existieren 6 Status:

- Pass: kein Problem gefunden
- Evaluate: Muss manuell beurteilt werde
- Some Risk: geringes Risiko
- Significant Risk: mittleres Risiko
- Severe Risk: hohes Risiko. Sollte umgehend behoben werden.
- Opportunity: Eine Verbesserung der Sicherheit durch zusätzliche Sicherheitsmaßnahmen sollte bedacht werden.

Summary
Hier steht eine kurze Zusammenfassung der Test-Ergebnisse.

Details
Hier finden sich konkrete Angaben zu den betroffenen Objekten.

Remarks
Detaillierte Problembeschreibung und Empfehlung zur Behebung des Problems.

References
Bietet Informationen darüber, ob sich das Finding auf das CIS Benchmark bezieht oder im Zusammenhang mit einem DSGVO-Artikel beziehungsweise Erwägungsgrund steht.

Das xls-Format bietet die Zusammenfassung der einzelnen Ergebnisse ohne die detaillierte Ausgabe aus dem HTML-Bericht. Es bietet Ihnen aber die Möglichkeit, eigene Spalten hinzuzufügen, beispielsweise für Verfolgungs- und Priorisierungszwecke.

Inactive Users	Some Risk	1 unlocked user(s) have been inactive for more than 30 days.	If a user account is no longer in use, it increases the attack surface of the system unnecessarily while providing no corresponding benefit. Furthermore, unauthorized use is less likely to be noticed when no one is regularly using the account. Accounts that have been unused for more than 30 days should be investigated to determine whether they should remain active.
Users with Expired Passwords	Some Risk	1 unlocked user(s) with password expired for more than 60 days exist.	Password expiration is used to ensure that users change their passwords on a regular basis. If a user's password has been expired for more than 60 days, it indicates that the user has not logged in for at least that long. Accounts that have been unused for an extended period of time should be investigated to determine whether they should remain active.
User Accounts in SYSTEM or SYSAUX Tablespace	Significant Risk	5 non-Oracle supplied user(s) use SYSTEM or SYSAUX tablespace.	The SYSTEM and SYSAUX tablespaces are reserved for Oracle-supplied user accounts. To avoid a possible denial of service caused by exhausting these resources, regular user accounts should not use these tablespaces.
Sample Schemas	Significant Risk	6 sample schema(s) are found.	Sample schemas are well-known accounts provided by Oracle to serve as simple examples for developers. They generally serve no purpose in a production database and should be removed because they unnecessarily increase the attack surface of the
Users with Default Password		0 user(s) are using default password with account status open.	Default account passwords for predefined Oracle accounts are well known. Open accounts with default passwords provide a trivial means of entry for attackers, but well-known passwords should be changed for locked accounts as well.

Abbildung 6: xls-Bericht Details

Ein weiterer Bericht im Textformat bietet die Möglichkeit Teile der Ausgabe für andere Verwendungszwecke ohne Formatierung einfach weiterzuverarbeiten.

```
### Oracle Database Security Assessment - Highly Confidential ###

* Assessment Date & Time *
Date of Data Collection  Date of Report           Reporter Version
------------------------ ------------------------ ----------------------------
Mon Jan 22 2018 09:36:00 Mon Jan 22 2018 11:29:57 2.0.1 (December 2017) - d526

* Database Identity *
Name Container (Type:ID) Platform         Database Role Log Mode     Created
---- ------------------- ---------------- ------------- ------------ ------------------------
CDB1 PDB1 (PDB:3)        Linux x86 64-bit PRIMARY       NOARCHIVELOG Wed Jan 04 2017 15:09:00

### Summary ###

Section                    Pass Evaluate Advisory Low Risk Medium Risk High Risk Total Findings
-------------------------- ---- -------- -------- -------- ----------- --------- --------------
Basic Information             1        0        0        0           0         0              1
User Accounts                 4        0        0        5           2         1             12
Privileges and Roles          4       14        0        1           0         0             19
Authorization Control         0        0        2        0           0         0              2
Data Encryption               0        1        1        0           0         0              2
Fine-Grained Access Control   0        1        4        0           0         0              5
Auditing                      3        5        1        0           3         0             12
Database Configuration        7        3        0        1           1         1             13
Network Configuration         1        0        0        1           3         0              5
Operating System              0        2        0        2           1         0              5
Total                        20       26        8       10          10         2             76
```

Abbildung 7: Text-Bericht

Quelle für das Oracle Database Security Assessment Tool

Kunden die einen gültigen Oracle Support Account haben, können das Oracle Database Security Assessment Tool unter der Support Note (Doc ID 2138254.1) beziehen

Weitere Informationen

- Einstieg mit einer Funktionsübersicht und der Dokumentation:
  http://www.oracle.com/technetwork/database/security/dbsat/overview/index.html
- Download über Oracle Support Document 2138254.1 (Oracle Database Security Assessment Tool (DBSAT)):
  https://support.oracle.com/epmos/faces/DocumentDisplay?id=2138254.1
- Database Security und EU-DSGVO Whitepaper
  https://go.oracle.com/LP=54366
- Application Data Modeller und Oracle Data Masking:
  http://www.oracle.com/technetwork/database/options/data-masking-subsetting/overview/index.html
- Oracle Datenbank Security Informationen:
  http://www.oracle.com/technetwork/database/security/index.html
- Oracle Database Security Best Practice Guide:
  http://docs.oracle.com/database/122/nav/security.htm
- Weiterführende Informationen zu Security & Oracle:
  http://www.oracle.com/security

CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/oracle

twitter.com/oracle

oracle.com

FOR MORE INFORMATION

Contact: 1.800.ORACLE1

ORACLE

Integrated Cloud Applications & Platform Services