

Inhaltsverzeichnis

Inhaltsverzeichnis für Security_II (c) 1998 - 2023 by Muniqsoft Training GmbH

1. Security II
© 2002-2022 by Muniqsoft Training GmbH

Kapitel 1 Einleitung

2. Übersicht
3. Denial of Service (DoS)
6. Rootkits
7. Einbruch im System
8. Tipps gegen Backdoors
9. Rootkits unter Oracle
10. Notizen

Kapitel 2 Database Vault

2. Einleitung
3. Einsatzmöglichkeiten
4. Voraussetzungen
5. Lizenzierung (Stand März 2016)
6. Installation
7. Installation in 11.2 (Software Installation)
8. Installation in 11.2 (Datenbank Installation)
9. Einschalten in Version 12c (Windows)
10. Ausschalten in Version 12c (Windows)
11. Ein- und Ausschalten (UNIX)
12. Allgemeines
14. Grundbegriffe: Realms
15. Grundbegriffe: Command Rules
16. Grundbegriffe: Factors
17. Grundbegriffe: Rule Sets
18. Grundbegriffe: Secure Application Role
19. Default-Parameteränderungen
20. Benutzer erzeugen/verändern
21. Was ändert sich?

23. SYSDBA
24. Anmelden im Browser
25. Rechte des neuen DV Admins

Inhaltsverzeichnis

- 26. Anmelden an der Weboberfläche
- 27. Web-Startseite (11.2)
- 28. Database Vault Berichts-Seite
- 29. Database Vault überwachen
- 30. Database Vault Realms
- 31. Besonderheiten bei Realms
- 32. Ablauf der Sicherheitsprüfung
- 35. Realm erstellen
- 37. Vordefinierte Realms
- 38. Database Vault Befehlsregeln
- 39. Database Vault: Regelgruppen
- 40. Database Vault Faktoren
- 41. Faktoren (Factors)
- 42. Factors über Weboberfläche einrichten
- 43. Bereich Allgemein
- 44. Bereich Faktor Identifikation
- 45. Bereich Abrufmethode
- 46. Bereich Validierungsmethode
- 47. Vordefinierte Faktor-Funktionen
- 51. Audit Optionen
- 52. Regelgruppen erstellen
- 54. Beispiele: Tabelle für andere schützen
- 55. Beispiele: Eigene Benutzer Tab Schutz
- 56. Beispiele: Befehle nur von einem Host
- 57. Beispiele: DBA Rolle vergeben
- 58. Beispiele: ALTER SYSTEM
- 59. VerwaltungsvIEWS
- 60. Neuerungen in 11.2.0.x
- 62. Notizen

Kapitel 3 Label Security

- 2. Einleitung
- 4. Installation

Inhaltsverzeichnis

- 6. Überprüfung der Installation
- 8. Deinstallation von Label Security
- 9. Zugriffskontrolle
- 11. Anwendungsbeispiel
- 19. Verwalten der Policy

Kapitel 4 Rootkits

- 2. Definition
- 3. Rootkit unter Unix
- 4. Wer greift mich an?
- 5. Was macht der Angreifer?
- 6. Wie komme ich in die Oracle Datenbank?
- 7. Wie komme ich in die Datenbank
- 11. Ich bin drin ...
- 12. Namensauflösung bei Objekten
- 13. Manipulation der VerwaltungsvIEWS
- 15. VerwaltungsvIEWS (V\$...)
- 18. Abweichungen bei Benutzertabellen
- 19. Abweichung von Public Synonymen
- 20. Abweichung bei Privilegien
- 21. SELECT führt DDL aus
- 22. Objekte als Oracle eigene ausgeben
- 23. Lösung
- 24. DDL Trigger
- 25. Wie kann man sich schützen?
- 26. PL/SQL Codes entschlüsseln

Inhaltsverzeichnis

- 27. View Definitionen mit Hash-Wert speichern
- 28. Rootkit Version 2
- 29. Rootkit Version 2 aufspüren
- 30. Honeypot
- 31. Oracle Würmer
- 32. Vorsichtsmaßnahmen
- 34. Notizen

Kapitel 5 Neu in 12c

- 2. Neue Benutzer
- 3. Neue Parameter für Passwort-Datei
- 4. Neue Passwort-Prüffunktion
- 5. Abschalten des alten PWD Algorithmus
- 7. Neue Passwortverschlüsselung in 12.1.0.2
- 8. Hinweis zur Passwortverschlüsselung
- 9. System Benutzer in der Passwortdatei
- 10. Übersicht der Rechte pro Benutzer
- 11. SYSDBA Ersatz
- 12. Anmeldung als SYSBACKUP
- 13. Anpassungen für neue Benutzer unter UNIX
- 14. Erweitertes CREATE USER Kommando
- 15. Benutzer anlegen in CDB
- 16. Fehlerhafter Login / Login Zeit
- 17. Rollenänderungen
- 18. Neue Rollen
- 19. Neue Rollen (Database Vault)
- 20. Neue Rechte in 12.1.0.1
- 21. Neue Rechte in 12.1.0.2
- 22. Inherit Privileges
- 24. Beispiel zu inherit Privileges
- 26. Neuerung bei Rechten in 12.1.0.2
- 27. Weitere neue Rechte
- 28. Oracle Maintained Rollen/Benutzer

Inhaltsverzeichnis

Kapitel 6 APEX Security

2. Übersicht des Security Bereichs
3. Was lässt sich in APEX schützen ?
4. Einrichtung der Prüfung
6. Ideen für Prüfungen
7. Beispiele für Prüfroutinen
8. Liste der nutzbaren Seite in Tabelle
9. Sicherheitsprüfung einer Seite
10. Sicherheitsprüfung bei Reports
11. Sicherheitsprüfung bei Items/Buttons/Spalten
12. Manipulationsmöglichkeiten
13. Session State Protection
14. Session State Protection: Einstellungen
15. Prüfsummen
16. Itemwerte selbst verschlüsseln
17. Gefälschte Formularwerte
18. Gefälschte Formularwerte: Lösung
19. Länge der Eingabefelder
20. Benutzergruppen
22. Benutzerauthentifizierung
23. Benutzerauthentifizierung durch LDAP
25. Eigene Authentifizierung der Benutzer
26. Verfügbarkeit der Applikation
27. Session Timeout
28. SQL Injection
31. SQL Injection Beispiel:
32. SQL Injection Tipps & Tricks
33. Gefährliche Module für SQL Injection
34. Beispiel SQL Injection
35. SQL Injection: Lösungen
39. SQL Injection und reguläre Ausdrücke
40. Cross Site Scripting
41. HTTP Packages gegen Cross Site Scripting
42. HTF Escaping Beispiel
43. White List / Black List

Inhaltsverzeichnis

- 44. Formularschutz
- 45. Seite Access Control
- 48. Allgemeine Sicherheitsbetrachtungen
- 49. Einrichtung von SSL Verbindungen
- 50. Wallet
- 52. Internes Gateway mit SSL
- 53. Oracle 11g und ACL
- 54. DBMS_NETWORK_ACL_ADMIN (ab 12c)
- 55. Fine Grain Access für andere Rechner (12c)
- 56. Package dbms_network_acl_admin (12c)
- 57. APPEND_HOST_ACE Beispiel 12c
- 58. APPEND_HOST_ACE Parametererklärung 12c
- 59. ACL Views ab 12c
- 60. Benutzer und Passwörter
- 61. Neuer Admin für Internal Workspace
- 62. Überwachung von Logins
- 63. Hidden & Protected
- 64. APEX und VPD (nur in Enterprise Ed.)
- 65. APEX VPD Beispiel
- 70. APEX Repository (Prozesse)
- 71. APEX Repository (Reports)
- 72. APEX Repository (List of Values)
- 73. APEX Repository (Flash Grafiken)
- 74. Anmeldung über mehrere Apps hinweg
- 75. Diverse APEX Security Tipps
- 78. APEX Runtime Installation
- 79. Diverse Security Tipps
- 80. Apache Security Tipps
- 81. APEx Security Check Tools
- 82. Notizen

Inhaltsverzeichnis

Kapitel 7 Forensik

2. Was ist Forensik?
3. Tools für die Forensik
4. Interessante Trace Files
5. Trace Views/Tables
6. Vorgehensweise
7. Befehle zur Überwachung
9. SYS.USER\$
10. Alte Passwörter
11. SYS.WRH\$_ACTIVE_SESSION_HISTORY
12. Welche Programme haben sich angemeldet?
13. Änderungen an wichtigen Tabellen
14. Weitere interessante Tabellen
15. Listener.log in External Table
16. Auswertungen der listener.log
17. Blöcke auslesen
18. Die SCN als Dokumentation des Zeitpunkts
19. Checkpoint Nummer wandeln
20. SCN Nummern in Blöcken
21. Interessante Auswertungen bzgl der SCN
22. Flashback Row History
23. Inhaltliche Änderungen feststellen
24. Notizen

Kapitel 8 Log Miner

2. Einleitung
3. Anwendungsfälle des Logminers
4. Vorbereitungen
6. Anwendungsmöglichkeiten
7. 1. Externe Data Dictionary Mapping Tabelle
11. 2. Extrahieren der Mapping-Infos in Redologs
14. 2. Logminer mit Redolog-Mapping starten
15. Zeitbereiche angeben
16. 3. Verwenden des Online Data Dictionary

Inhaltsverzeichnis

- 17. Einsatz des Logminers
- 18. Beispiele
- 22. DDL Kommandos im Logminer
- 23. Optionen des Logminers
- 27. Tipps & Tricks
- 28. Supplemental Logging
- 29. Datenbankweites Supplemental Logging
- 32. Zurücksetzen des Supplemental LOGGING
- 33. Tabellen Identification Key Logging
- 35. DBA_LOG_GROUPS View
- 36. DBA_LOG_GROUP_COLUMNS View

Kapitel 9 Kerberos

- 2. Einführung
- 3. Einrichtung mittels Win AD
- 4. Wichtige Konfigurationseinstellung
- 5. Einrichtung mittels Win AD
- 7. Datenbank auf Unix
- 8. Einrichtung mittels Win AD
- 9. Kerberos Konfigurationsdatei
- 10. Einrichtung mittels Win AD
- 11. Testen der Verbindung
- 13. Troubleshooting
- 15. Troubleshooting mit Tracing
- 16. Bestehender Accounts

Inhaltsverzeichnis

Kapitel 10 Real Application Security

2. Real Application Security
4. Dimensionen der effektiven Sicherheit
5. Real Application Security
6. PL/SQL Packages
7. SQL Funktionen
8. Data Dictionary Views
9. Neue Rollen für RAS
10. RAS Komponenten - Principal
11. XS_PRINCIPAL.CREATE_USER Package
12. XS_PRINCIPAL.SET_PASSWORD Package
13. XS_PRINCIPAL.CREATE_ROLE Package
14. XS_PRINCIPAL.CREATE_DYNAMIC_ROLE
15. XS_PRINCIPAL.GRANT_ROLE Package
16. XS_PRINCIPAL.REVOKE_ROLE Package
17. Rollen und Benutzer löschen
18. Applikationsrollen
19. Applikationsbenutzer
20. Applikationssessions
24. Security Class
25. Data Security Policy (Teil 1)
26. Data Security Policy (Teil 2)
27. Data Security Policy (Teil 3)
28. RAS in APEX
30. RAS und Oracle Firewall
31. Notizen