

Module : Sécurité des bases de données

Code

ING-4-SSIR-S8-P2

Période

Semestre 2

Volume horaire

31.5h

ECTS

3

Responsable

AYARI Hattab

email

le_hattab@yahoo.fr

Equipe pédagogique

AYARI Hattab

1. Objectifs de Module (Savoirs, aptitudes et compétences)

L'objectif est d'évaluer les attaques dans les base de données, de créer et maintenir les lignes de base et la configuration sécurisée des bases de données.

Acquis d'apprentissage :

A la fin de cet enseignement, l'élève sera capable de :

- Maîtriser, la configuration d'une base de données (**C1.2**)
- La classification des meilleures pratiques de la sécurité des bases de données. (**C1.1**)
- Simuler la création et la signature des comptes utilisateurs (**C1.3**)
- Maitriser l'audit et l'utilisation des qualificateurs d'audit. (**C5.2**)

Compétences

C1.3 Tester les politiques FGA**C5.2 configuration de Oracle Audit Vault****C1.2 Maitriser les privilèges et les autorisations**

2. Pré-requis(autres UE et compétences indispensables pour suivre l'UE concernée)

- TCP/IP
- SQL

3. Répartition d'Horaire de Module

<i>Intitulé de l'élément d'enseignement</i>	<i>Total</i>	<i>Cours</i>	<i>TD</i>	<i>Atelier</i>	<i>PR</i>
Module :... Sécurité des bases de données	31.5	16.5		15	

4. Méthodes pédagogiques et moyens spécifiques au Module

(pédagogie d'enseignement, ouvrages de références, outils matériels et logiciels)

- Supports de Cours
- Projecteur et Tableau
- Travaux dirigés
- Logiciels de simulation : Oracle DB

Bibliographie

Titre	Auteur(s)	Edition
Les étapes de sécurité globale des bases de données	https://s3-us-west-2.amazonaws.com/itworldcanada/archive/Documents/whitepaper/ITW135FGestiondel'information.pdf	2021
Introduction aux outils de sécurité pour les bases de données.	https://www.lemagit.fr/conseil/Introduction-aux-outils-de-securite-pour-bases-de-donnees	2022

5. Contenu (Descriptifs et plans des cours/Déroulement / Détail de l'évaluation de l'activité pratique¹)	Durée allouée

Séance 1

- I. Introduction
 - 1. Pourquoi sécuriser les données?
 - 2. Classification des meilleures pratiques de la sécurité des bases de données.
 - 3. préparation sur la sécurité Oracle

Cours 3H

TD 0

TP 0

Séance 2

- II. Renforcement de la base de données
 - 1. Elaborer une stratégie directrice de durcissement
 - 1.1 Database STIG (Database Security Technical Implementation Guide)
 - 1.2 CIS Oracle Benchmark (Center for Internet Security)
 - 2. Evaluation de la vulnérabilité
 - 3. Créer et maintenir une ligne de base (baseline) de la configuration sécurisée
 - 4. Gestion des mises à jour critiques des correctifs (patch update)
 - 5. Sécuriser les données pour les environnements de tests

Cours 1.5H

TD -

TP 1.5H

Séance 3

- III. Sécurité Listener
 - 1. sécuriser l'accès à lsnrctl

Cours 1.5H

TD -

TP 1.5H

 1

<p>2. limiter la possibilité de modifier les propriétés de LISTENER</p> <p>3. Sécuriser EXTPROC</p> <ul style="list-style-type: none"> 3.1 les procédures externes 3.2 Sécuriser les procédures externes 3.3 limiter les sources utilisées pour les connexions 3.4 Inspection des journaux et des traces LISTENER 3.5 Combattre les attaques de protocole TNS 		
Séance 4	Cours	1.5H
IV. Sécurité du compte	TD	0
1. créer, modifier, supprimer et verrouiller les comptes d'utilisateurs	TP	1.5H
2. le processus d'ouverture de session standard		
3. les règles de mot de passe		
4. complexité du mot de passe		
5. Vérification des mots de passe faibles et par défaut		
6. Définir le mot de passe		
7. Limiter les ressources système utilisées par les utilisateurs		
8. utilisateurs / profils		
Séance 5		
V. Authentication	Cours	1.5H
1. O3 / O5 LOGON et l'authentification OS	TD	-
2. Utilisation fichiers mot de passe	TP	1.5H
3. Configurer les clients pour utiliser un mot de passe externe		
4. authentification SSL à l'aide d'ASO (Advanced Security Options)		
5. Configurer l'authentification Kerberos à l'aide d'ASO		
6. RADIUS et l'authentification à deux facteurs à l'aide d'ASO		
Séance 6	Cours	1.5H
VI. Audit standard	TD	-
1. Activer l'audit standard	TP	1.5H
2. Utiliser les qualificateurs d'audit		
3. Utilisation de l'audit d'états		
4. Utiliser l'audit d'objet		
5. Utiliser l'audit de privilège		
6. Audit des erreurs inattendues dans la couche réseau		
7. Lire les enregistrements d'audit		
8. Utiliser NOAUDIT		
Séance 7	Cours	1.5H
VII. Audit obligatoire	TD	-
1. Utiliser l'audit obligatoire		

	2. Activer l'audit administrateur 3. Utiliser l'audit Syslog	TP	1.5H
Séance 8	VIII. Fine-Grained Audit (FGA) 1. Définir les politiques FGA 2. Gérer les politiques FGA 3. Lire les tableaux et les vues FGA	Cours	1.5H
		TD	-
		TP	1.5H
Séance 9	IX. Audit des valeurs avant / après et surveillance des données sélectionnées 1. Utiliser les déclencheurs pour capturer les valeurs avant / après 2. Utiliser Oracle Streams pour capturer des valeurs avant / après 3. Utiliser les requêtes SCN et Flashback 3.1 Lois de notification 3.2 Utilisation de requêtes Flashback: un exemple 3.3 Obtenir des versions en utilisant Flashback 3.4 Prérequis pour Flashback 4. Utiliser les archives de données Flashback	Cours	1.5H
		TD	-
		TP	1.5H
Séance 10	X. Privilèges et autorisation 1. Gérer les privilèges d'objet et de colonne 2. Gérer les privilèges système 3. Utiliser les rôles pour gérer les privilèges 4. Utiliser des rôles d'application sécurisés 5. Gérer le rôle PUBLIC 6. Utiliser les listes de contrôle d'accès (ACL) pour limiter l'accès aux services de réseau de base de données	Cours	1.5H
		TD	-
		TP	1.5H
Séance 11	XI. Examen TP	Cours	-
		TD	-
		TP	1.5H

6. Mode d'évaluation de Module(nombre, types et pondération des contrôles)
Eléments d'enseignement
Coeff DS EX TP PR

Module - Sécurité des bases de données	2	30%	50%	20%	
--	---	-----	-----	-----	--

Pour valider le module, les étudiants passeront un examen dont le coefficient est de 50%, un DS dont le coefficient est de 30% et un TP 20% .

La durée de tous les examens (Examen, DS et TP)est de 1h30.

Le DS est planifié 7 semaines après le début du module testera les connaissances acquises .

Quand à l'examen, il est planifié après l'écoulement des 10 semaines et portera sur toutes les thématiques enseignées tout au long des 30 heures.

L'examen TP est planifié la dernière séance (1h 30).

Le module est validé si l'étudiant obtient une moyenne supérieure ou égal à 10 sur 20.