

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et la Recherche
Scientifique
Centre de Recherche sur l'Information Scientifique et
Technique



Mémoire de fin d'étude pour l'obtention du diplôme
de Post-Graduation Spécialisée en Sécurité Informatique

Thème

**La Détection d'Intrusion dans Les Applications
Bases de Données**

• *Présenté par :*

- Mr AISSAOUI Hamid

• *Encadré par:*

-Mme. BESSAI Fatma Zohra.

• *Devant le jury:*

Mr DERHAB

Melle H.BENSEFAI

Mr BELHOUL

Président

Membre

Membre

Promotion 2010

SOMMAIRE

Introduction générale.....	1
Chapitre I : Sécurité des bases de données	
1. Introduction	4
2. La sécurité informatique	4
3. Terminologie de la sécurité informatique.....	6
3.1. Types d'attaques	6
3.2. Anatomie d'une attaque.....	7
4. Confidentialité	8
4.1 Politiques et modèles d'autorisation discrétionnaires (DAC).....	9
4.2 Politiques et modèles d'autorisation obligatoires (MAC).....	9
4.2.1 Modèle de Bell et LaPadula.....	10
4.3 Politiques et modèles de sécurité par rôles (RBAC).....	11
5. Intégrité	12
5.1. Modèle Biba.....	12
6. Disponibilité	13
7. L'Audit	14
7.1 Audit de base de données	15
8. Cryptographie	17
8.1 Cryptage de la base de données	17
8.2 Sécurité trafics réseaux.	19
9. Conclusion	22
Chapitre II : Les Systèmes de détection d'Intrusion	
1. Introduction.....	24
2. Intrusions et attaques informatiques.....	24
2.1. Définition Intrusion	24
2.2. Définition Détection d'intrusion	25
2.3. Définition Faux positifs	25
2.4. Définition Faux négatifs	25
3. Systèmes de détection d'intrusions	25
4. Classification des IDS	26
4.1. Approches de détection	27
4.1.1. Approche par scénario.	27
4.1.2. Approche Comportementale	28
4.2. Système protégé	30
4.2.1. Basé réseau (NIDS : Network Intrusion Detection System).....	30
4.2.2. Basé hôte (HIDS : Host Intrusion Detection System).....	32
4.2.3 IDS d'application.....	33
4.2.4 IDS Hybride	34
4.3. Classification selon la source d'information.....	34
4.3.1. Par Audit	34
4.3.2. Par Paquet	34
4.4 Fréquence d'utilisation	34
4.4.1 Périodique.....	34

4.4.2. Continue.	35
4.5 Comportement après détection.....	35
4.6 Architecture d'unIDS	35
4.6.1. Centralisée	35
4.6.2. Partiellement distribuée	36
4.6.3. Entièrement distribuée.....	36
5. La standardisation des systèmes de détection d'intrusion.....	37
5.1 Le modèle CIDF	38
5.2 Les travaux de l'IDWG	40
6. Critères de tests d'un IDS	41
7. Techniques anti-IDS.....	41
8. Conclusion	42

Chapitre III : IDS pour application Base de données

1. Introduction	44
2. Collecte des données pour les IDS applications base de données	45
2.1. Utilisation des fonctionnalités d'audit du SGBD	45
2.2. Interception des communications (sniffer).....	46
2.3 Solution proposée pour une collecte optimale des données	46
3. Méthode pour détection d'intrusion dans les applications bases de données.....	47
3.1 Détection d'intrusion dans une base de données avec l'utilisation d'empreinte de transaction	47
3.2 IDS avec Approche comportementale.....	52
3.3 IDS avec Approche comportementale basée sur les rôles	57
3.4 IDS commercial versus IDS Open-Source	60
4. Conclusion	61

Chapitre IV : Solution de détection envisagée

1. Introduction	64
2. Description de la solution	64
3. IDS avec approche comportementale (IIDD)	66
4. IDS avec approche par scénario Snort	68
4.1 Installation et configuration de Snort	69
4.2 Outils d'analyse et de gestion	69
4.2.1 ACID (Analysis Console for Intrusion Database	69
4.2.2 BASE	70
4.3 IDScenter	70
4.4 Les règles	72
5. Conclusion	73
Conclusion générale	75
Référence Bibliographique	77
Annexe I : Les attaques	I
Annexe II : Outils open source	X