

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/ Mira de Bejaia

Faculté des Sciences et Sciences de l'Ingénieur

Département d'Informatique

Ecole Doctorale d'Informatique



Mémoire de Magistère

en Informatique

Option

Réseaux et Systèmes Distribués

Thème

*Etude critique des méthodes d'optimisation
pour la détection d'intrusion dans un
système informatique.*

Soutenu le 12/11/2005

par

Noudjoud KAHYA

Devant le jury composé de:

A. Belmehdi	Professeur, Université de Béjaia	Président
L. Talbi	Professeur, Université de Québec (Canada)	Directeur de Mémoire
K. Adi	Professeur, Université de Québec (Canada)	Co-Directeur de Mémoire
MS. Radjef	Professeur, Université de Béjaia	Examineur
K. Benatchba	Docteur, INI, Alger	Examinatrice

Table des matières :

INTRODUCTION	01
I. LES ATTAQUES INFORMATIQUE	
I.1. Introduction.....	04
I.2. Historique des attaques réseaux.....	05
I.3. Les pirates et leurs objectifs.....	07
I.3.1 Définition du Hacking.....	07
I.3.2 Types de pirates.....	07
I.3.3 Rôles des hackers.....	08
I.4. L'aspect technique de hacking.....	09
I.4.1. Prise d'empreinte.....	09
I.4.2. Le balayage.....	11
I.4.3. Le recensement.....	13
I.5. Les types d'attaques.....	13
I.5.1. Classification des attaques.....	13
I.5.2. Les différentes attaques.....	15
I.6. Conclusion.....	25
II. TECHNIQUES DE DEFENSE ET DE SECURITE	
II.1. Introduction.....	27
II.2. Principales techniques de défense et de sécurité.....	27
II.2.1. Authentification.....	27
II.2.2. Cryptographie.....	28
II.2.2.1. Le chiffrement.....	28
II.2.2.2. Signature.....	29
II.2.3. Proxy.....	30
II.2.4. Firewalls (Par-Feu).....	30
II.2.5. Antivirus.....	31
II.2.6. VPN.....	32
II.2.7. IDS (Intrusion Detection System).....	33
II.3. Conclusion.....	33
III. LES SYSTEMES DE DETECTION D'INTRUSION.	
III.1. Introduction.....	34
III.2. Les différent techniques anti-intrusion.....	35
III.2.1. Préemption.....	36
III.2.2. Prévention.....	36
III.2.3. Dissuasion.....	37
III.2.4. Détection.....	37
III.2.5. Déflexion.....	38
III.2.6. Contre-mesures.....	38
III.3. Activités liées à l'audit de sécurité.....	39
III.4. Les système de détection d'intrusion.....	41
III.4.1. Modules de base d'un IDS.....	42
III.4.2. les Caractéristiques souhaitées d'un IDS.....	44
III.4.3. Qu'est ce qu'un IDS ne peut pas faire ?.....	46
III.5. Classification des IDS.....	47

III.5.1. Principes de détection.....	49
A- L'approche comportementale.....	50
B- L'approche par scénarios (IDS à Bibliothèques de signatures).....	57
C- Avantages et inconvénients des deux approches.....	63
III.5.2. Comportements en cas d'attaque détectée.....	65
III.5.3. Sources des données à analyser.....	65
III.5.4. Fréquence d'utilisation.....	70
III.5.5. Architecture.....	71
III.6. Placement des IDS.....	74
III.7. Conclusion	76
IV. LES METHODES D'OPTIMISATIONS POUR LA DETECTION D'INTRUSION	
IV.1. Introduction.....	77
IV.2. Détection d'intrusion par analyse de fichiers d'audit de sécurité.....	79
IV.2.1. Analyse modèle par modèle.....	79
IV.2.2. Analyse simplifiée d'un fichier d'audit de sécurité.....	80
IV.3. Définition du Problème de l'Analyse Simplifiée de Fichiers d'Audit de sécurité «PASFAS».....	81
IV.4. Durée des sessions d'audit.....	84
IV.5. Application des méthodes d'optimisation pour la détection d'intrusion.....	85
IV.5.1. Introduction.....	85
IV.5.2. Définitions préliminaires.....	85
A- Méta heuristiques multi solutions.....	87
A-1 L'application des algorithmes génétiques au problème de l'analyse simplifiée d'un fichier d'audit de sécurité (PASFAS).....	87
A-1.1. Introduction.....	87
A-1.2. Codage des individus.....	90
A-1.3. Fonction sélective.....	90
A-1.4. Expérimentations.....	93
A-1.5. Qualité des résultats.....	97
A-1.6. Conclusion.....	99
IV.6. Les inconvénients de l'approche génétique.....	99
B- Méta heuristiques mono solution.....	99
B-1. Le Recuit Simulé (RS)	100
B-1.1. Introduction.....	100
B-1.2. Principe.....	100
B-1.3. Algorithmes du Recuit Simulé (RS)	101
B-1.4. Formulation du problème PASFAS.....	102
B-1.5. Expérimentations.....	103
B-1.5.1. Benchmarks de teste.....	104
B-1.5.2. Comportement réel de l'algorithme Recuit Simulé.....	104
B-1.6. Conclusion.....	109
B-2. La recherche Tabou (RT).....	109
B-2.1. Introduction.....	109
B-2.2. Les paramètres de la méthode Tabou.....	110
B-2.3. Algorithme de la méthode Tabou.....	111
B-2.4. Comportement réel de la recherche Tabou.....	111
B-2.5. Expérimentations.....	112
B-2.6. Conclusion	116
B-3. Recherche à Voisinage Variable (RVV).....	117

B-3.1. Introduction.....	117
B-3.2. Algorithmes de la Recherche à Voisinage Variable (RVV).....	117
B-3.3. Comportement réel de la Recherche à Voisinage Variable.....	118
B-3.4. Expérimentations.....	119
B-3.5. Conclusion	121
IV.6. Etude critique des méthodes d'optimisation pour la détection d'intrusion.....	122
IV.7. Conclusion.....	126
CONCLUSION GENERALE	128
ANNEXE	131
BIBLIOGRAPHIE	