



République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université des Sciences et de la Technologie Houari BOUMEDIENE

FACULTE DE ELECTRONIQUE & INFORMATIQUE
DEPARTEMENT D'INFORMATIQUE

Mémoire du projet de fin d'études

Pour l'obtention du diplôme
D'ingénieur d'état en Informatique

Option : Systèmes & Réseaux

Thème :

Systeme de Détection d'Intrusion Comportemental

Thème proposé et encadré par : **Mr NACI Djamel**

Etudié par : **AKIF Yacine & BELHOCINE Farouk**

Devant le Jury composé de :
Mr BELKHIR Président
Mr BEHLOUL Membre
Mr BERBAR Membre

Organisme d'accueil :
Centre de Recherché sur l'Information Scientifique et Technique



PROMOTION 2004/2005
N° 90

Résumé

Le travail à effectuer est dans le domaine de la sécurité réseau, et a pour objectif la conception et la mise en œuvre d'un Système de détection comportemental dans un environnement d'entreprise, ce système s'intéresse aux intrusions internes c'est-à-dire qu'on tente de détecter les attaques réalisées depuis le réseau interne de l'entreprise. Ce qui justifie le choix de se baser sur les attaques internes est le rapport « *Computer Crime and Security Survey* » publié par la **CSI** (*Computer Security Institute*) pour l'année 2000, et qui indique que 90% des responsables de sécurité ont détecté des attaques, il indique également que seulement 25% d'entre eux ont décelé des attaques provenant de l'extérieur. Cette étude montre aussi que 78% des responsables de sécurité ont découvert des accès non autorisés provenant de l'intérieur. De son côté L'ICSA (*International Computer Security Association*) considère que 80% des problèmes de sécurité proviennent de l'intérieur même de l'organisation.[SEC03].

Lors de l'exploitation de la machine, Chaque utilisateur a un comportement unique, On va donc essayer en premier lieu de construire un profil unique pour chaque utilisateur qui définit ce comportement, pour cela on utilisera les événements générés dans le système par cet utilisateur, et la fréquence de chaque événement va constituer une variable aléatoire; ensuite toutes ces variables aléatoires vont être représentées par un histogramme, et ce dernier n'est que le profil.

Le profil est le noyau de l'approche comportementale, puisque la détection se fera en le comparant au comportement courant. Dans notre Système on compare le profil de l'utilisateur type avec le profil courant; et cette comparaison est réalisée grâce aux fonctions de calcul de distance entre les histogrammes, si cette distance est supérieur a un seuil donné une alerte est générée.

Pour renforcer ce profil on va ajouter des *Sensors* (sondes) réseau et système qui vont fournir des informations supplémentaires sur cet utilisateur comme les sites qu'il a visité, les services qu'il utilise, et le taux de charge du processeur...etc.

Pour prouver l'efficacité de cette méthode (calcul de distance), nous allons effectuer des tests de détection d'intrusion, permettant aussi de fixer quelques paramètres comme la valeur du seuil de détection, la meilleur fonction de calcul de distance...etc.

Mots Clés : Sécurité informatique, attaques réseaux, Intrusion, Profil référentiel, Profil temporaire, Comportement, Fichiers Logs, événements, Distances statistiques, Histogrammes.

SOMMAIRE

Introduction générale

Résumé

Chapitre I : La Sécurité informatique

I.1	Introduction	1
I.2	Caractéristiques d'un système sécurisé	2
I.3	Les menaces et les ennemis	3
	I.3.1 Les Menaces.....	3
	I.3.2 Pirates informatiques.....	3
I.4	Les Attaques.....	4
	I.4.1 Classification des attaques.....	4
	I.4.2 Les différentes techniques d'attaques	7
	I.4.2.1 Le Sniffing.....	7
	I.4.2.2 Le spoofing	7
	I.4.2.3 Le DoS (Le Deni de Service)	9
	I.4.2.4 Le social engineering.....	10
	I.4.2.5 Le Crackage de mot de passe	10
	I.4.2.6 Virus	11
	a- Les différents types de virus	11
	b- Les catégories de virus.....	12
I.5	Les Outils de protection	13
	I.5.1 Les Firewalls	13
	I.5.1.1 Le fonctionnement d'un système pare-feu	14
	I.5.1.2 Les méthodes de filtrage de paquet	15
	I.5.1.3 Les méthodes de filtrage applicative	15
	I.5.1.4 Qu'est-ce qu'un firewall ne peut pas faire	16
	I.5.2 Les Antivirus	16
	I.5.2.1 Comment fonctionne un antivirus	16
	I.5.2.2 Comment reconnaître un virus	16
	I.5.3 La cryptographie	17
	I.5.3.1 Le cryptage asymétrique ou à clé publique	18
	I.5.3.2 Le cryptage symétrique	18
	I.5.3.3 Signature	18
	a- Signature numérique	18
	b- Les certificats	19
	I.5.4 L'Audit	19
	I.5.5 Les VPN	20
	I.5.5.1 Fonctionnement des VPN	21
	I.5.6 Le DMZ (dé-militerazed zone)	22
	I.5.7 Les IDS (Système de détection d'intrusion)	22
I.6	Exemple d'une architecture sécurisée.....	23
I.7	Conclusion	24

Chapitre II : Les systèmes de détection d'intrusions

II.1	Introduction.....	26
	II.1.1 Définition d'une intrusion.....	26

II.1.2	La détection d'intrusions.....	27
II.2	L'audit de sécurité	27
II.2.1	Les fichiers logs.....	28
II.2.2	Analyse du journal d'audit.....	29
II.3	Le Rôle d'un système de détection d'intrusion.....	29
II.3.1	Définition d'une alerte.....	29
II.3.2	Niveaux d'alerte d'IDS.....	29
II.3.3	Faux positifs.....	31
II.3.4	Faux négatifs.....	31
II.4	Architecture de base d'un IDS.....	31
II.5	Conditions de fonctionnement des systèmes de détection d'intrusions.....	32
II.6	Classification des IDS.....	33
II.6.1	Méthode de détection.....	33
II.6.1.1	Les approches par scénarios (Knowledge – based).....	33
a-	les techniques à base de règle (i.e. les systèmes expert).....	34
b-	Pattern matching	34
c-	les algorithmes génétiques.....	34
Avantages de l'approche par scénarios.....	34	
Inconvénients de l'approche par scénarios.....	34	
II.6.1.2	L'approche comportementale (Behavior-based).....	35
a-	Les méthodes statistiques.....	35
b-	Méthode probabiliste.....	36
c-	Les systèmes experts Réseau de neurones.....	36
d-	Méthode des Profils Propres	37
e-	Les générateurs de forme prédictive.....	37
f-	Approche immunologique.....	38
Les Avantages.....	38	
Les Inconvénients.....	38	
II.6.2	Système protégé.....	39
II.6.2.1	IDS basé Hôte (HIDS).....	39
a-	Avantages.....	40
b-	Inconvénients.....	40
II.6.2.2	IDS basé réseau (NIDS).....	40
II.6.2.2.1	Quelque méthode pour déjouer les NIDS.....	41
Avantages.....	43	
Inconvénients.....	44	
II.6.4	Source de données.....	44
II.6.4.1	Sources d'information système.....	44
II.6.4.2	Sources d'information applicatives.....	45
II.6.4.3	Sources d'information réseau.....	45
II.6.5	Comportement après détection.....	45
II.6.5.1	Passif.....	45
II.6.5.2	Actif.....	45
II.6.6	Fréquence d'utilisation.....	46
II.6.6.1	périodique.....	46
II.6.6.2	Continue.....	46
II.6.7	Classification par Architecture	46
II.6.7.1	L'approche par agent mobile dans les systèmes distribués.....	47
Avantages de l'approche par agent mobile.....	47	
Inconvénients de l'approche par agent mobile.....	48	

II.7	Caractéristiques souhaités des IDS	49
II.8	Les IDS existants	49
II.9	Conclusion.....	54

Chapitre III : La Conception du système de détection comportemental

III.1	Introduction.....	56
III.2	Objectif du travail.....	56
III.3	Choix de l'approche du travail.....	57
	III.3.1 Contrainte sur la période du calcul du profil.....	57
	III.3.2 Exploitation de la méthode statistique pour le calcul du profil.....	57
	III.3.3 L'Idée générale du travail.....	61
III.4	Architecture générale du système BIDS.....	63
	III.4.1. Module interface d'échanges.....	66
	III.4.2. Module de Gestion de la BD.....	66
	III.4.3. Module Réseau.....	67
	III.4.4. Module Authentification.....	69
	III.4.5. Module Comportement.....	70
	III.4.6. Module Analyse et détection.....	72
	III.4.7 Module Contrôle.....	74
III.5	Conclusion.....	75

Chapitre IV : La mise en œuvre du système de détection comportemental

IV.1	Introduction	77
IV.2	Environnement de développement	77
	IV.2.1 Système d'exploitation	77
	IV.2.2 Langage de programmation	77
IV.3	L'implémentation des différents modules	78
	IV.3.1 Module Gestion des bases de données	78
	IV.3.1.1 Les tables de la base	78
	a- La Table Session	78
	b- La Table Profil	79
	c- La Table Personnel	79
	d- La table des Applications utilisées	79
	e- La Table des Services utilisés	80
	f- La Table des rapports d'analyse	80
	IV.3.2 Module Authentification	81
	IV.3.3 Module Sonde Réseau	81
	IV.3.3.1 La capture de paquets	81
	IV.3.3.2 L'analyse des paquets	84
	IV.3.4.1 Etablissement du profil de référence.....	86
	IV.3.4.2 Etablissement du profil temporaire	87
	IV.3.4.3 Mise à jour du profil de référence	88
	IV.3.5 Le Module Analyse	88
	IV.3.6 Module Interface d'échange	89
	IV.3.7 Module Contrôle et Configuration	91
IV.4	Présentation de l'interface.....	91
	IV.4.1 La partie hôte.....	91
	IV.4.2 La partie administrateur	91

IV. 4.2.1 La fenêtre du contrôle de tout le système	92
IV.4.2.3 la fenêtre de Scanner de Ports.....	93
IV.4.2.4 La fenêtre Capture de paquets	94
V.5 Conclusion	94

Chapitre V : Tests de la méthode comportementale

V.1 Introduction	96
V.2 Présentation du profil en histogramme	96
V.3 Explication des tests	97
V.3.1 La période d'apprentissage	97
V.3.2 L'utilisation des distances statistiques	97
V.4 Déroulement des tests	97
V.5 Les tableaux des tests de la méthode comportementale.....	99
V.6 Analyse des tests	107
V.6.1 Les tests de la distance euclidienne Forme L1	107
V.6.2 La distance Euclidienne Forme L2	110
V.6.3 La Distance Quadratique	111
V.6.4 Quelques remarques	111
⁹ V.6.5 Contrainte sur la période d'apprentissage	113
V.7 Limite de cette méthode	115
V.8 Conclusion	115

Conclusion générale

Annexe I : La Pile TCP/IP	118
Annexe II : Le langage de modélisation unifié (UML)	140