



Mémoire de Post-graduation spécialisée

En sécurité Informatique

Thème

**Implémentation d'un IDS comportemental optimisé par
l'algorithme K-means pour sécuriser une application Web**

**Présenté par : M. ALBANE Abdelkader
M. FAID Samir**

Soutenu le 03 Mai 2016
devant le jury composé de :

Mme	Lynda ZEGHACHE	Maitre de recherche, CERIST	Président
Mr	Abdelghani KRINAH	Attaché de recherche, CERIST	Examineur
Mr	Nabil DJEDJIG	Attaché de recherche, CERIST	Examineur
Mr	Abdelhakim Nacef	<i>Maitre de conférence associé, UFC</i>	Encadreur

Sommaire

Liste des figures	5
Introduction générale	6
<i>Chapitre 1</i>	8
<i>Sécurité des réseaux et des systèmes</i>	8
1. Introduction.....	9
2. La protection des données	9
3. La protection contre des attaques	11
4. Les domaines d'application de la sécurité informatique	11
4.1 La sécurité physique	12
4.2 Sécurité de l'exploitation.....	12
4.3 Sécurité logique.....	12
4.4 Sécurité applicative.....	13
4.5 Sécurité des télécommunications	13
5. Les causes pour sécuriser les réseaux.....	14
5.1 Les enjeux.....	14
5.1.1 Enjeux économiques	14
5.1.2 Enjeux politiques	14
5.1.3 Enjeux juridiques	14
5.2 Les vulnérabilités.....	15
5.2.1 Vulnérabilités humaines.....	15
5.2.2 Vulnérabilités technologiques.....	15
5.2.3 Vulnérabilités organisationnelles	16
5.2.4 Vulnérabilités mise en œuvre	16
5.3 Les menaces.....	16
5.3.1 Origine opérationnel	16
5.3.2 Origine physique.....	16
5.3.3 Origine humaine	16
5.3.4 Les risques.....	17
6. Les facettes de la sécurité	17
6.1 Diriger la sécurité.....	17
6.2 Importance du juridique dans la sécurité des systèmes d'information.....	19

6.3 Éthique et formation.....	19
7. Architecture de sécurité.....	20
8. Profils et capacités des attaquants.....	22
8.1 Réalisation d'une attaque.....	22
8.2 Attaques actives et passives	23
8.3 Attaque fondées sur l'usurpation de mots de passe	23
8.4 Attaques fondées sur le leurre.....	25
8.5 Attaques fondées sur le détournement des technologies	25
8.6 Attaques fondées sur la manipulation d'information	25
9. Politique de sécurité	26
10. Différentes sources de menaces	26
11. Quels moyens pour l'entreprise ?.....	27
12. Solutions techniques.....	27
12.1 Pare-feu	27
12.2 VPN (réseau privé virtuel).....	27
12.3 Antivirus.....	28
12.4 Anti-spywares et anti-spams.....	28
12.5 Solutions de contrôle d'accès et d'authentification	28
12.6 IDS	28
12.7 IPS	28
13. Conclusion.....	29
<i>Chapitre 2.....</i>	<i>30</i>
<i>Les systèmes de détection d'intrusion.....</i>	<i>30</i>
1. Introduction.....	31
2. Définitions	31
2.1 Intrusion.....	31
2.2 Attaque.....	31
2.3 Mécanisme d'audit.....	31
2.4 Journal d'audit.....	31
2.5 Événement.....	32
2.6 Flux d'audit élémentaire	32
2.7 Flux d'audit	32

2.8 IDS	32
3. Architecture classique d'IDS	32
3.1 Le capteur	33
3.2 L'analyseur.....	33
3.3 Le manager	34
4. Classification des IDS	34
4.1 IDS Réseaux (NIDS)	34
4.2 IDS Systèmes (HIDS).....	35
4.3 IDS Hybrides.....	36
5. Méthodologie de détection.....	37
5.1 Les IDS à signatures (ou à scénarios)	37
5.1.1 Principe.....	37
5.1.2 Systèmes Experts.....	37
5.1.3 "Pattern matching" (Reconnaissance de formes)	37
5.1.4 Algorithmes génétique.....	38
5.1.5 Discussion	39
5.2 Les IDS comportementaux.....	40
5.2.1 Approche probabiliste	40
5.2.2 Approche statistique	41
5.2.3 Discussion	41
6. Classification par type de réaction :	42
6.1 Détecteurs d'intrusions passifs	42
6.2 Détecteurs d'intrusions actifs	42
7. Classification par mode d'utilisation.....	42
7.1 Analyse en temps réel.....	42
7.2 Analyse en temps différé.....	43
8. Quelques systèmes de détection d'intrusions.....	43
8.1 Prelude-NIDS.....	43
8.2 Snort-NIDS	43
9. Conclusion :.....	44
Chapitre 3.....	45
Implémentation d'un IDS comportemental	45

1. Introduction.....	46
2. Outils de réalisation	46
2.1 Microsoft SQL Server version 2008	46
2.2 Développement en couche (N-Tier)	47
2.3 Relation entre les couches	47
2.4 Avantages de cette architecture	48
Séparer l'application en 3 couches a de nombreux avantages, en voici une liste non exhaustive:.....	48
3. Définition de la gestion de carrière.....	49
4. Description de l'application Web de la gestion de carrière	50
5. Sécurisation de l'application Web	52
5.1 Implémentation d'un IDS :.....	52
5.1.1 Phase d'apprentissage	52
5.1.1.1 Modélisation de la phase d'apprentissage	53
5.1.2 Phase de détection	55
5.1.2.1 Détermination de changement entre l'ancien et le nouveau profil	56
5.1.2.2 Modélisation de la phase de détection	57
6. Optimisation de la solution par l'algorithme de K-means	58
6.1 Définition de K-means.....	58
6.2 Etapes d'application de l'algorithme K-means	59
6.3 Organigramme	59
6.4 Implémentation de l'algorithme K-means	59
7. Etude comparative	63
8. Implémentation du processus de réapprentissage automatique	64
9. Conclusion.....	66
Conclusion générale.....	67
Références bibliographiques.....	69
Liste des abréviations.....	71

Liste des figures

Figure.1.1	Les différentes dimensions d'une architecture de sécurité	21
Figure 1.2	Etapes de réalisation d'une attaque	22
Figure 1.3	Critères de sécurité touchée par l'attaque	23
Figure.2.1	Architecture classique d'un IDS	33
Figure.2.2	Architecture d'un NIDS	34
Figure. 2.3	Déploiement de plusieurs IDS	35
Figure.2.4	Architecture d'un HIDS	36
Figure.2.5	Principe de l'IDS hybride	37
Figure.2.6	Architecture d'un IDS utilisant le pattern matching	38
Figure. 2.8	Principe de l'algorithme génétique	39
Figure 3.1	Présentation des 3 couches logicielles	47
Figure 3.2	Niveau de communication entre couche	48
Figure 3.3	Les informations d'un fonctionnaire	50
Figure 3.4	Saisie une promotion de grade	51
Figure 3.5	Liste des absences	51
Figure 3.6	Organigramme de l'algorithme K-means	59
Figure 3.7	Résultat de l'algorithme K-means	61
Figure 3.8	Graphe comparatif des faux positifs de chaque étape de la solution	64
Figure 3.9	Lancement de réapprentissage	65