Table des matières

Introduction générale.....I

Chapitre 1 : SECURITE DES RESEAUX INFORMATIQUE ET CAH

1. Généralités sur la sécurité informatique……3

1.1. La sécurité informatique 3

1.**2.** Principaux services de la sécurité 3

1.3. Différents types d'attaques 4

1.3.1. Les attaques réseaux 4

1.3.2. Les attaques applicatives 5

1.3.3. Le Déni de service (Denial of Service) 6

1.3.4. Les attaques virales 6

1.4. Mécanismes de sécurité 7

1.4.1. Authentification et contrôles d'accès aux ressources 7

1.4.2. La Cryptographie 7

1.4.3**.** Pare-feu (fire-well) 8

1.4.4. Scanners de vulnérabilités 8

1.4.5. Protection anti-virus 8

1.4.6. VPN 9

1.4.7. Détection et prévention d'intrusions..... 9

2. Système de détection d'intrusion……9

2.1. Définition 10

2.2. Terminologies..... 10

2.3. Architecture d'un IDS 11

2.4. Mode de fonctionnement d'un IDS 12

2.4.1. Mode de détection 12

a) La détection d'anomalies 12

b) La reconnaissance de signature 12

2.4.2. Réponse passive et active 13

a) La réponse passive 13

b) La réponse active 13

2.5. Classification des systèmes de détection d'intrusions : 13

2.5.1. Méthode de détection 14

a) Approche par scénario 14

b) Approche comportementale 15

2.5.2. Sources de données à analyser 16

a) Sondes réseau 16

b) Sondes systèmes 17

c) IDS hydrides (NIDS+HIDS) 19

2.5.3. Réponses des IDS 19

2.5.4. Paradigme de détection 19

2.5.5. La fréquence d'utilisation 19

3. La classification automatique..... 19

3.1. Le Clustring 20

3.2. Domaines d'Application 20

3.3. Mesures d'éloignement 22

3.3.1. Indice de ressemblance, ou similarité 22

3.3.2. Indice de dissemblance, ou dis similarité 22

3.3.3. Distances 23

3.4. Les types des méthodes de classification 23
3.5. Les algorithmes de clustering 25
3.5.1. K-Means 25
3.5.2. Classification Ascendante Hiérarchique (CAH) 26
a) Mesure des Distances 28
a) Règles d'Agrégation 30
3.6. La Classification et la détection d'intrusion 31
3.7. Les limites de Clustering 32
Conclusion : 33

Chapitre 2 : ETAT DE L'ART

Introduction : 35
1. Les IDS basé sur la technique de Machine à vecteurs de support (SVM) 35
2. Data mining et les systèmes de détection d'intrusion 36
3. Optimisation de l'algorithme de k-mean 37
4. La construction des modèles pour la détection d'intrusion 38
5. La détection d'intrusion dans les réseaux sans fils 39
6. D'autres domaines d'application et méthodes pour la détection d'intrusion 40
7. Les critiques 42
Conclusion 44

Chapitre 3 : CONCEPTION DE SYSTEME

Introduction 46
1. Présentation 46
2. Problématique 46

3. Démarche 46
4. Etapes de conception 47
4.1. Normalisation des données 47
4.2. Classification Ascendante Hiérarchique (CAH) 48
4.3. Critère d'agrégation 48
5. L'algorithme CAH 49
6. Exemple 50
7. Le dendrogramme 51
8. Organigrammes de système 52
Conclusion 55

Chapitre 4 : IMPLEMENTATION

Introduction 57
1. jeux de données 57
2. Outils utilisés 57
2.1. NetBeans 57
2.2. Winpcap 58
2.3. Wireshark 58
2.4. WampServer 59
3. Description de notre système 59
4. Résultats 59
4.1. Expérimentation du modèle sur un échantillon de 300 connexions en utilisant les trois critères d'agrégations 60
4.2. Mesure des performances 62
4.3. Validation 64

5. Discussion 65

Conclusion 66

Conclusion générale.……67

Bibliographies……..……69