

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

INSTITUT DE

Mémoire du Projet de fin d'études

Pour l'obtention du diplôme
d'ingénieur d'état en informatique

Option :

SUJET :

Conception et mise en œuvre d'un système de
détection à base de cas

Thème proposé par :

Etudié par :

Encadré par : Mme Aliane, Mme Benmeziane

OUCHEN Mohamed
TEHARI Mohamed

Soutenu le :

Devant le jury composé de :

Président,
Rapporteur,
Examineur,
Examineur,

PROMOTION :

SOMMAIRE

INTRODUCTION GENERALE.....-1-

CHAPITRE 1 : INTELLIGENCE ARTIFICIELLE

| | |
|---|------------------------------------|
| I. INTRODUCTION | ERREUR ! SIGNET NON DEFINI. |
| II. DEFINITION | ERREUR ! SIGNET NON DEFINI. |
| III. BREF HISTORIQUE | ERREUR ! SIGNET NON DEFINI. |
| IV. LES DOMAINES D'APPLICATIONS | ERREUR ! SIGNET NON DEFINI. |
| 1. Les robots et systèmes autonomes | Erreur ! Signet non défini. |
| 2. Les systèmes experts..... | Erreur ! Signet non défini. |
| 3. Le raisonnement basé sur le cas..... | Erreur ! Signet non défini. |
| 4. La reconnaissance de la parole | Erreur ! Signet non défini. |
| 5. Le traitement du langage naturel (TLN)..... | Erreur ! Signet non défini. |
| 6. La vision par ordinateur..... | Erreur ! Signet non défini. |
| V. LES SYSTEMES A BASE DE CONNAISSANCE (SBC) . | ERREUR ! SIGNET NON DEFINI. |
| 1. Définition (La connaissance) | Erreur ! Signet non défini. |
| 2. Types de connaissances | Erreur ! Signet non défini. |
| 2.1. Connaissances empiriques..... | Erreur ! Signet non défini. |
| 2.2. Connaissances théoriques..... | Erreur ! Signet non défini. |
| 3. Représentation des connaissances | Erreur ! Signet non défini. |
| 3.1. Représentation procédurale | Erreur ! Signet non défini. |
| 3.2. Représentation déclarative | Erreur ! Signet non défini. |
| 3.3. Représentation structurée | Erreur ! Signet non défini. |
| 3.3.1 Les réseaux sémantiques..... | Erreur ! Signet non défini. |
| 3.3.2 Les schémas (frames)..... | Erreur ! Signet non défini. |
| 3.4. L'orienté objets (OO)..... | Erreur ! Signet non défini. |
| 4. Exemples des systèmes à base de connaissance | Erreur ! Signet non défini. |
| 4.1 Les systèmes expert..... | Erreur ! Signet non défini. |
| 4.1.1 Base de Connaissances | Erreur ! Signet non défini. |
| 4.1.2 Moteur d'Inférence | Erreur ! Signet non défini. |
| 4.1.3 Module d'acquisition de connaissances..... | Erreur ! Signet non défini. |
| 4.1.4 Module d'explication..... | Erreur ! Signet non défini. |
| 4.1.5 Interface avec l'utilisateur | Erreur ! Signet non défini. |
| 4.2 Les systèmes à base de cas | Erreur ! Signet non défini. |
| 4.2.1 Principes de base..... | Erreur ! Signet non défini. |
| 4.2.2 Composantes d'un système à base de cas..... | Erreur ! Signet non défini. |
| VI. CONCLUSION | ERREUR ! SIGNET NON DEFINI. |

CHAPITRE 2 : SECURITE INFORMATIQUE

| | |
|---|------------------------------------|
| I. INTRODUCTION | ERREUR ! SIGNET NON DEFINI. |
| II. CONCEPTS DE SECURITE | ERREUR ! SIGNET NON DEFINI. |
| 1. Le domaine de la sécurité..... | Erreur ! Signet non défini. |
| 2. Les Aspects de la sécurité informatique..... | Erreur ! Signet non défini. |
| 2.1 Confidentialité des données..... | Erreur ! Signet non défini. |

| | |
|---|------------------------------------|
| 2.2 Intégrité des données | Erreur ! Signet non défini. |
| 2.3 Disponibilité de service | Erreur ! Signet non défini. |
| 3. Méthodologie | Erreur ! Signet non défini. |
| III. LES MENACES..... | ERREUR ! SIGNET NON DEFINI. |
| 1. Que peut faire une attaque ? | Erreur ! Signet non défini. |
| 2. Pourquoi il y a des menaces ? | Erreur ! Signet non défini. |
| 3. Classification des menaces | Erreur ! Signet non défini. |
| 3.1. Les menaces accidentelles | Erreur ! Signet non défini. |
| 3.2. Les menaces intentionnelles (les attaques) | Erreur ! Signet non défini. |
| 3.2.1 Les attaques passives | Erreur ! Signet non défini. |
| 3.2.2 Les attaques actives | Erreur ! Signet non défini. |
| 4. Quelques types d'attaques | Erreur ! Signet non défini. |
| 4.1 Le déni de service (DoS) | Erreur ! Signet non défini. |
| a) Syn flooding | Erreur ! Signet non défini. |
| b) Smurf | Erreur ! Signet non défini. |
| d) Déni de service distribué | Erreur ! Signet non défini. |
| 4.2 Le spamming | Erreur ! Signet non défini. |
| 4.3 Les chevaux de Troie | Erreur ! Signet non défini. |
| 4.4 Les bombes logiques | Erreur ! Signet non défini. |
| 4.5 Les vers | Erreur ! Signet non défini. |
| 4.6 Les virus | Erreur ! Signet non défini. |
| 4.7 Le sniffing | Erreur ! Signet non défini. |
| IV. LES SERVICES DE SECURITE | ERREUR ! SIGNET NON DEFINI. |
| 1. La confidentialité des données | Erreur ! Signet non défini. |
| 2. L'intégrité des données | Erreur ! Signet non défini. |
| 3. L'authentification | Erreur ! Signet non défini. |
| 4. Le contrôle d'accès | Erreur ! Signet non défini. |
| 5. La non répudiation | Erreur ! Signet non défini. |
| V. LES MECANISMES DE SECURITE | ERREUR ! SIGNET NON DEFINI. |
| 1. La cryptographie | Erreur ! Signet non défini. |
| 1.1 Chiffrement symétrique | Erreur ! Signet non défini. |
| 1.2 Chiffrement asymétrique | Erreur ! Signet non défini. |
| 1.3 Signature numérique | Erreur ! Signet non défini. |
| 2. L'authentification | Erreur ! Signet non défini. |
| 3. Le contrôle d'accès | Erreur ! Signet non défini. |
| 4. Sécurité de communication | Erreur ! Signet non défini. |
| VI. QUELQUES OUTILS DE SECURITE..... | ERREUR ! SIGNET NON DEFINI. |
| 1. Les firewalls | Erreur ! Signet non défini. |
| 2. Les systèmes de détection d'intrusion | Erreur ! Signet non défini. |
| VII. CONCLUSION..... | ERREUR ! SIGNET NON DEFINI. |

CHAPITRE 3 : LES SYSTEMES DE DETECTION D'INTRUSIONS

| | |
|---|------------------------------------|
| I. INTRODUCTION | ERREUR ! SIGNET NON DEFINI. |
| II. DEFINITIONS..... | ERREUR ! SIGNET NON DEFINI. |
| 1. L'intrusion | Erreur ! Signet non défini. |
| 2. La détection d'intrusion | Erreur ! Signet non défini. |
| 3. Système de détection d'intrusion | Erreur ! Signet non défini. |

| | |
|--|------------------------------------|
| III. IDS : BREF HISTORIQUE | ERREUR ! SIGNET NON DEFINI. |
| IV. LES COMPOSANTS D'UN IDS | ERREUR ! SIGNET NON DEFINI. |
| V. LES CARACTERISTIQUES SOUHAITEES D'UN IDS | ERREUR ! SIGNET NON DEFINI. |
| VI. LA CLASSIFICATION DES IDS | ERREUR ! SIGNET NON DEFINI. |
| 1. Méthode d'analyse | Erreur ! Signet non défini. |
| 1.1 Approche comportementale | Erreur ! Signet non défini. |
| a) Méthodes statistiques | Erreur ! Signet non défini. |
| b) Systèmes experts | Erreur ! Signet non défini. |
| c) Réseaux de neurones | Erreur ! Signet non défini. |
| 1.2 Approche par scénarios | Erreur ! Signet non défini. |
| a) les systèmes experts | Erreur ! Signet non défini. |
| b) Pattern Matching | Erreur ! Signet non défini. |
| 2. Source de données | Erreur ! Signet non défini. |
| 2.1 La détection d'intrusion basée sur un hôte (HIDS) | Erreur ! Signet non défini. |
| 2.2 La détection d'intrusion réseau (NIDS) | Erreur ! Signet non défini. |
| 3. Réaction après détection | Erreur ! Signet non défini. |
| 4. Fréquence d'utilisation | Erreur ! Signet non défini. |
| VII. FORCES ET LIMITATIONS DES IDS | ERREUR ! SIGNET NON DEFINI. |
| 1. Les forces des systèmes de détection d'intrusion | Erreur ! Signet non défini. |
| 2. Les limitations des IDS | Erreur ! Signet non défini. |
| VIII. UTILISATION DU RAISONNEMENT A BASE DE CAS POUR LA DETECTION D'INTRUSION | ERREUR ! SIGNET NON DEFINI. |
| IX. CONCLUSION | ERREUR ! SIGNET NON DEFINI. |

CHAPITRE 4 : LA CONCEPTION DU CBRIDS

| | |
|--|------------------------------------|
| I. INTRODUCTION | ERREUR ! SIGNET NON DEFINI. |
| II. NOTATION | ERREUR ! SIGNET NON DEFINI. |
| III. ARCHITECTURE GLOBALE | ERREUR ! SIGNET NON DEFINI. |
| IV. ARCHITECTURE DETAILLEE | ERREUR ! SIGNET NON DEFINI. |
| 1. Gestion des paquets fragmentés | Erreur ! Signet non défini. |
| 2. Fournisseur des paquets | Erreur ! Signet non défini. |
| 3. Détection des attaques par signatures | Erreur ! Signet non défini. |
| 3.1 La base des signatures d'attaques | Erreur ! Signet non défini. |
| 3.1.1 Les types des signatures d'attaques | Erreur ! Signet non défini. |
| 3.1.2 Les sous bases des signatures d'attaques | Erreur ! Signet non défini. |
| 3.2 Le moteur de recherche et de similarité | Erreur ! Signet non défini. |
| 4. Contrôleur de l'intégrité | Erreur ! Signet non défini. |
| 5. Gestion des alertes | Erreur ! Signet non défini. |
| V. CONCLUSION | ERREUR ! SIGNET NON DEFINI. |

CHAPITRE 5 : IMPLEMENTATION DU CBRIDS

| | |
|------------------------------|------------------------------------|
| I. INTRODUCTION | ERREUR ! SIGNET NON DEFINI. |
|------------------------------|------------------------------------|

| | |
|---|-----------------------------|
| II. ENVIRONNEMENT DE DEVELOPPEMENT | ERREUR ! SIGNET NON DEFINI. |
| 1. Choix du langage de programmation | Erreur ! Signet non défini. |
| 2. La capture des paquets..... | Erreur ! Signet non défini. |
| III. PRESENTATION DU CBRIDS | ERREUR ! SIGNET NON DEFINI. |
| 1. Description de l'interface..... | Erreur ! Signet non défini. |
| 1.1 Gestion de la base des signatures..... | Erreur ! Signet non défini. |
| 1.2 La configuration | Erreur ! Signet non défini. |
| 1.3 La Visualisation des alertes | Erreur ! Signet non défini. |
| 2. Test du CbrIDS..... | Erreur ! Signet non défini. |
| IV. CONCLUSION | ERREUR ! SIGNET NON DEFINI. |