

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique



Université des Sciences et de la Technologie Houari Boumediène

Faculté d'Electronique et d'Informatique
Département Informatique

Mémoire de projet de fin d'études
Pour l'obtention du diplôme d'ingénieur d'état en informatique

Option
Sécurité informatique et Réseaux

Thème

Conception et réalisation
d'un système de détection d'intrusion web

Proposé par : **Dr D. Tandjaoui (CERIST)**

Encadré par : **Mr T. Kenaza (EMP)**

Réalisé par :

Benabdelatif Mohamed Nassim

Devant le jury composé de :

Président : **Mr K. Benabadji**

Membre : **Mr M. Guerroumi**

Membre : **Mr S. Hamrioui**

Promotion 2008/2009-N°89

Résumé

Le travail effectué dans ce projet a pour objectif la conception et la réalisation d'un système de détection d'intrusion web permettant la détection des attaques web à partir du trafic réseau http. La technique de détection utilisée est basée sur la classification bayésienne qui permet de classer chaque donnée http modélisée par un réseau bayésien en un événement normal ou malveillant. L'association du problème de détection d'intrusion au problème de classification a fait des réseaux bayésiens l'un des outils les plus puissants pour la représentation des comportements normaux et des comportements malveillants.

Mots clés : Détection d'intrusion, IDS, attaques web, sécurité informatique, réseau bayésien.

SOMMAIRE

Introduction générale	Erreur ! Signet non défini.
Organisation du mémoire	Erreur ! Signet non défini.

Partie Etat de l'art

Chapitre I : La sécurité informatique

1. Introduction.....	Erreur ! Signet non défini.
2. Définition	Erreur ! Signet non défini.
3. Objectifs de la sécurité informatique	Erreur ! Signet non défini.
4. Politique de sécurité.....	Erreur ! Signet non défini.
4.1. Définition	Erreur ! Signet non défini.
4.2. Mise en place d'une politique de sécurité	Erreur ! Signet non défini.
4.3. Normes d'établissement d'une politique de sécurité	Erreur ! Signet non défini.
5. Outils de sécurisation d'un réseau informatique.....	Erreur ! Signet non défini.
5.1. Firewall	Erreur ! Signet non défini.
5.2. Les serveurs proxy	Erreur ! Signet non défini.
5.3. Les scanners de vulnérabilités.....	Erreur ! Signet non défini.
5.4. Les systèmes de détection d'intrusion	Erreur ! Signet non défini.
6. Conclusion	Erreur ! Signet non défini.

Chapitre II : Vulnérabilité des applications web

1. Introduction.....	Erreur ! Signet non défini.
2. Le World Wide Web (WWW).....	Erreur ! Signet non défini.
3. Les applications web.....	Erreur ! Signet non défini.
3.1. Définition	Erreur ! Signet non défini.
3.2. Fonctionnement d'une application Web.....	Erreur ! Signet non défini.
3.2.1. Traitement des pages Web statiques	Erreur ! Signet non défini.
3.2.2. Traitement des pages dynamiques	Erreur ! Signet non défini.
3.3. Langages de programmation des applications web.....	Erreur ! Signet non défini.
3.3.1. Les langages coté serveur	Erreur ! Signet non défini.
3.3.2. Les langages coté client	Erreur ! Signet non défini.
3.4. Les risques dans les applications web.....	Erreur ! Signet non défini.

4. Les attaques web	Erreur ! Signet non défini.
4.1. Classification des attaques web.....	Erreur ! Signet non défini.
4.1.1. Attaques par validation d'entrée.....	Erreur ! Signet non défini.
4.1.2. Attaques contre les mécanismes d'authentification/autorisation.....	Erreur ! Signet non défini.
4.1.3. Scans de site Web et floodings	Erreur ! Signet non défini.
5. Conclusion	Erreur ! Signet non défini.

Chapitre III : Les Systèmes de détection d'intrusion

1. Introduction.....	Erreur ! Signet non défini.
2. Définitions.....	Erreur ! Signet non défini.
3. Caractéristiques des IDSs.....	Erreur ! Signet non défini.
4. Architecture d'un IDS	Erreur ! Signet non défini.
5. Classification des IDSs	Erreur ! Signet non défini.
5.1. Méthodes de détection	Erreur ! Signet non défini.
5.1.1. Approche par scénario	Erreur ! Signet non défini.
5.1.2. Approche comportementale (détection d'anomalies)	Erreur ! Signet non défini.
5.2. Source de données.....	Erreur ! Signet non défini.
5.2.1. La détection d'Intrusion basée sur l'hôte (HIDS)	Erreur ! Signet non défini.
5.2.2. La détection d'Intrusion basée sur réseau (NIDS).....	Erreur ! Signet non défini.
5.3. Comportement après détection.....	Erreur ! Signet non défini.
5.4. Fréquence d'utilisation	Erreur ! Signet non défini.
6. Efficacité d'un IDS.....	Erreur ! Signet non défini.
7. Les limites des systèmes de détections existants	Erreur ! Signet non défini.
8. Tendances et constantes sur la détection d'intrusions	Erreur ! Signet non défini.
9. Conclusion	Erreur ! Signet non défini.

Chapitre IV: Les Réseaux Bayésiens

1. Introduction.....	Erreur ! Signet non défini.
2. Calcul probabiliste	Erreur ! Signet non défini.
3. Les réseaux bayésiens	Erreur ! Signet non défini.
4. Apprentissage des réseaux bayésiens.....	Erreur ! Signet non défini.
4.1. L'apprentissage de structure	Erreur ! Signet non défini.
4.2. L'apprentissage de paramètres.....	Erreur ! Signet non défini.
5. Classification bayésienne.....	Erreur ! Signet non défini.
6. Classifieurs bayésiens naïfs	Erreur ! Signet non défini.
7. Réseaux bayésiens naïfs pour la détection d'intrusion	Erreur ! Signet non défini.

8. Conclusion	Erreur ! Signet non défini.
---------------------	-----------------------------

Partie Conception et Réalisation

Chapitre I : Architecture et fonctionnement du système

1. Introduction.....	Erreur ! Signet non défini.
2. Choix de l'approche.....	Erreur ! Signet non défini.
3. Principe et méthode de détection	Erreur ! Signet non défini.
4. Architecture générale du système	Erreur ! Signet non défini.
5. Architecture détaillée	Erreur ! Signet non défini.
5.1. Le module Sonde	Erreur ! Signet non défini.
5.1.1. Capture.....	Erreur ! Signet non défini.
5.1.2. Reconstruction des données http.....	Erreur ! Signet non défini.
5.1.3. Formatage.....	Erreur ! Signet non défini.
5.2. Module Apprentissage	Erreur ! Signet non défini.
5.3. Module Analyse et Interprétation	Erreur ! Signet non défini.
5.4. Module Stockage.....	Erreur ! Signet non défini.
6. Définition d'attributs pour la détection d'attaques Web	Erreur ! Signet non défini.

Chapitre II : Modélisation UML

1. Introduction.....	Erreur ! Signet non défini.
2. Architecture logicielle.....	Erreur ! Signet non défini.
2.1. Le système de détection	Erreur ! Signet non défini.
2.2. Module de persistance.....	Erreur ! Signet non défini.
3. Diagramme de déploiement	Erreur ! Signet non défini.
4. Système de détection.....	Erreur ! Signet non défini.
4.1. Diagramme cas d'utilisation	Erreur ! Signet non défini.
4.2. Description des cas d'utilisation	Erreur ! Signet non défini.
4.3. Diagramme de classe	Erreur ! Signet non défini.

Chapitre III : Implémentation

1. Introduction.....	Erreur ! Signet non défini.
2. Environnement de développement.....	Erreur ! Signet non défini.
2.1. Langage de programmation	Erreur ! Signet non défini.
2.2 La bibliothèque Winpcap.....	Erreur ! Signet non défini.
3. Présentation de l'application.....	Erreur ! Signet non défini.

3.1. Authentification de l'administrateur	Erreur ! Signet non défini.
3.2. Interface principale	Erreur ! Signet non défini.
3.3. Onglet « Détection/Formatage en ligne »	Erreur ! Signet non défini.
3.4. Onglet « Détection hors ligne »	Erreur ! Signet non défini.
3.5. Onglet « Apprentissage»	Erreur ! Signet non défini.
3.6. Onglet « Journal des alertes»	Erreur ! Signet non défini.
3.7. Configurer le système	Erreur ! Signet non défini.
3.8. Mise à jour de la base d'apprentissage.....	Erreur ! Signet non défini.

Chapitre IV : Test

1. Introduction.....	Erreur ! Signet non défini.
2. Métriques et critères d'évaluation	Erreur ! Signet non défini.
3. Evaluation du système	Erreur ! Signet non défini.
3.1. Test n°1	Erreur ! Signet non défini.
3.2. Test n°2	Erreur ! Signet non défini.
3.3. Test n°3	Erreur ! Signet non défini.
4. Conclusion	Erreur ! Signet non défini.

Conclusion générale & Perspectives.....	Erreur ! Signet non défini.
--	------------------------------------

Bibliographie

Annexes

A. La suite des protocoles Internet.....	I
B. Le protocole http.....	VIII
C. Les données de test.....	XIII