

IDS Réseau basé sur le Deep Learning

CHEFROUR Abbes & ZIANI Salah Eddine

Projet de fin d'études pour l'obtention du
diplôme de Post-Graduation Spécialisée en
Sécurité Informatique.

Encadré par :

Mr Amira Abdelouahab
Mr Boulemtafes Amine

Devant le jury :

Président : Krinah Abdelghani
Examineur : Djedjig Nabil
Examineur : Hadjar Samir

INTRODUCTION GENERALE -----	6
I- RESEAUX ETHERNET, ATTAQUES RESEAUX ET IDS -----	7
I.1. LES RESEAUX ETHERNET -----	8
I.1.1. <i>La trame Ethernet II</i> -----	8
I.1.2. <i>Le paquet ip</i> -----	8
I.1.3. <i>Le segment (un paquet encapsulé au niveau de la couche transport)</i> -----	11
I.2. LES ATTAQUES RESEAUX : -----	12
I.2.1. <i>Fuzzers</i> -----	12
I.2.2. <i>Analyse ou scan de ports</i> -----	12
I.2.3. <i>Portes dérobées ou backdoors</i> -----	12
I.2.4. <i>Déni de service (DoS) et Déni de service distribué (DDoS)</i> -----	13
I.2.5. <i>Exploits</i> -----	13
I.2.6. <i>Reconnaissance</i> -----	13
I.2.7. <i>Shellcode</i> -----	14
I.2.8. <i>Worms ou vers</i> -----	14
I.3. SYSTEME DE DETECTION D'INTRUSION -----	15
I.3.1. <i>Techniques de détection:</i> -----	15
I.3.1.1. <i>Analyse basée sur les signatures :</i> -----	15
I.3.1.2. <i>Analyse basée sur la détection d'anomalies :</i> -----	15
I.3.2. <i>Types d'IDS</i> -----	16
I.3.2.1. <i>Les nids (IDS Réseau)</i> -----	16
I.3.2.2. <i>Les HIDS (IDS basé Hôte):</i> -----	16
I.4. <i>Conclusion :</i> -----	8
II- MACHINE LEARNING & DEEP LEARNING -----	18
II.1. MACHINE LEARNING : -----	19
II.1.1. <i>Principes de fonctionnement :</i> -----	19
II.1.1.1. <i>Les données :</i> -----	19
II.1.1.2. <i>Le modèle</i> -----	20
II.1.1.3. <i>La décision</i> -----	20
II.1.2. <i>Exemples d'algorithmes d'apprentissage automatique :</i> -----	21
II.1.2.1. <i>La régression linéaire :</i> -----	21
II.1.2.2. <i>La régression logistique:</i> -----	21
II.1.2.3. <i>Support vecteur machine (svm) :</i> -----	21
II.1.2.4. <i>Naïve bayes :</i> -----	22
II.1.2.5. <i>Arbres de décision :</i> -----	22
II.1.2.6. <i>Réseau de neurones :</i> -----	22
II.1.2.7. <i>K-means :</i> -----	23
II.2. DEEP LEARNING : -----	23
II.2.1. <i>Applications du deep learning :</i> -----	25
II.2.2. <i>Fonctionnement des réseaux de neurones profonds</i> -----	25
II.2.3. <i>Principales architectures des réseaux profonds :</i> -----	27
II.2.3.1. <i>Perceptron multicouche (multilayer perceptron - MLP):</i> -----	28
II.2.3.2. <i>Réseaux de neurones convolutifs ou à convolution (CNN) :</i> -----	28
II.2.3.3. <i>Les réseaux de neurones auto-encoder</i> -----	30
II.2.3.4. <i>Les réseaux de neurones de type GAN :</i> -----	30
II.2.3.5. <i>Réseaux de neurones récurrents (RNN) :</i> -----	31
II.2.3.6. <i>Réseaux long short-term memory LSTM:</i> -----	32
II.3. CONCLUSION -----	32
III- METHODOLOGIE ET CONCEPTION -----	33
III.1. ÉTAPES ET METHODOLOGIE SUIVIES -----	34
III.2. DATASET (JEU DE DONNEES) -----	34
III.2.1. <i>Dataset originale</i> -----	34
III.2.2. <i>Traitement de la dataset :</i> -----	37
III.3.1. <i>Prétraitement</i> -----	39
III.3.1.1. <i>Sélection des fonctionnalités du training</i> -----	39
III.3.1.2. <i>Numérisation</i> -----	39
III.3.1.3. <i>Normalisation</i> -----	39

III.3.1.4.	Remodélisation de la dataset	39
III.3.1.5.	Partitionnement de la dataset	41
III.3.2.	Architecture du modèle proposé	42
III.3.2.1.	Construction du modèle :	43
IV-	IMPLÉMENTATION	47
IV.1	ENVIRONNEMENT DE TRAVAIL	48
IV.1.1	- Environnement matériel :	48
IV.1.2	- Environnement logiciel :	48
IV.2	IMPLEMENTATION DES PHASES DE DEPLOIEMENT DE LA SOLUTION:	49
IV.2.1	Prétraitement de la dataset	49
IV.2.1.1	Lecture du fichier dataset des flux :	49
IV.2.1.2	Sélectionner les fonctionnalités du training :	49
IV.2.1.3	Numérisation :	49
IV.2.1.4	Normalisation :	51
IV.2.1.5	Remodeler la dataset :	52
IV.2.1.6	Partitionnement de la dataset	53
IV.2.2	Training (Entraînement)	54
IV.2.2.1	Construction du modèle :	54
IV.2.3	Compiler le modèle :	57
IV.2.3.1	Entraîner le modèle :	57
IV.2.3.2	Enregistrement du modèle	60
IV.3	Conclusion	60
V-	ÉVALUATION	61
V.1	METRIQUES :	62
V.2	TESTS EFFECTUES ET RESULTATS	64
V.2.1	Phase d'apprentissage	64
V.2.1.1	Lancement de la phase d'apprentissage	66
V.2.1.2	Démarrage de l'entraînement du modèle	67
V.2.1.3	La fin de l'entraînement du modèle :	68
V.2.1.4	Visualisation du graphe de précision et de perte :	69
V.2.1.5	Rapport des performances de classification	70
V.2.1.6	Matrice de confusion	71
V.2.1.7	Analyse des scores des métriques de la phase d'apprentissage:	72
V.2.2	Phase de test du modèle	72
V.2.2.1	Chargement du modèle :	72
V.2.2.2	Prédiction :	73
V.2.2.3	Rapport de classification	74
V.2.2.4	Matrice de confusion :	75
V.2.2.5	Analyse des scores de la phase de test:	75
V.2.3	Discussion des résultats	76
VI-	CONCLUSION GENERALE ET PERSPECTIVES	78