DETECTION D'INTRUSION SUR UN RESEAU : APPRENTISSAGE AUTOMATIQUE

Elfrid Tatiana ATEMKENG KAMDOM
Département de mathématiques, informatique et génie, Université du Québec à Rimouski-Campus de Lévis

CONTEXTE

La détection d'intrusion consiste à surveiller les activités du réseau pour identifier des comportements suspects ou malveillants qui pourraient indiquer qu'une attaque est en cours ou qu'un système informatique a été compromis.Les techniques de détection d'intrusion peuvent inclure l'analyse de signatures, qui utilise des règles préétablies pour identifier des modèles spécifiques d'activité malveillante, ou l'analyse comportementale, qui utilise l'apprentissage automatique pour identifier des modèles d'activité anormale qui pourraient indiquer une attaque. Elles peuvent également être utilisées en combinaison avec des techniques de prévention d'intrusion pour bloquer les attaques avant qu'elles ne compromettent les systèmes informatiques.

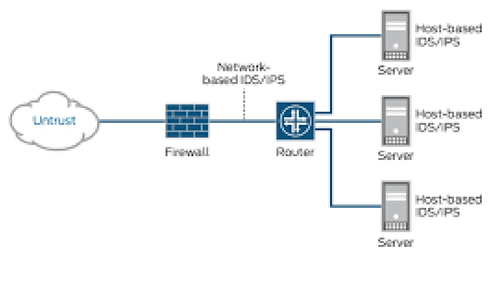

Fig. 1: Système de Détection d'Intrusion(IDS).

PROBLEMATIQUE

Avec le développement des systèmes d'information et l'utilisation d'outils informatiques, l'annalyse des donné es devient de plus en plus un processus necessaire afin d'avoir une vue globale sur l'ensemble du systeme :
- Fuites de données au sein des entreprises.
- Failles et problèmes de sécurité. Les méthodes de sécurité classiques ne suffisent plus.
- Tentatives de Connexions annormales au système
- Les données incomplètes, inexactes ou incorrectement étiquetées, peuvent entraîner des faux positifs ou des faux négatifs, ce qui peut compromettre la capacité de l'IDS à détecter les menaces.
Il est par conséquent primordial de mettre en place des mesures de sécurité robustes.

OBJECTIFS

- Faire une analyse des données d'un système de détection d'intrusion (IDS) afin de prévoir si un événement futur est susceptible d'être une attaque ou non, en utilisant un algorithme d'apprentissage automatique en fonction des caractéristiques,des événements et des modèles identifiés lors de l'entraînement.

DESCRIPTION DU SYSTEME

L'apprentissage automatique est une application de l'IA qui permet aux systèmes d'apprendre et de s'améliorer à partir de l'expérience sans être explicitement programmés

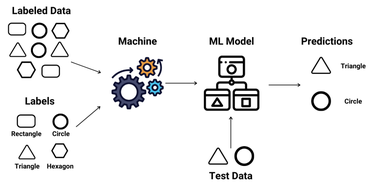

Fig. 2: Apprentissage et description du système

La matrice de confusion nous permet d'évaluer les performances du modèle d'apprentissage automatique de classification à l'aide de métriques plus polyvalentes , telles que l'exactitude, la précision, le rappel, etc.Une matrice de confusion a quatre composants:
- Vrai positif (TP) - Ce sont les prédictions correctes faites qui sont étiquetées comme positives. Vous pouvez entrer ceci et les valeurs ci-dessous dans la première section du calculateur de matrice de confusion.
- Faux négatif (FN) - Ce sont les mauvaises prédictions faites qui sont étiquetées comme négatives.
- Faux positif (FP) - Ce sont les mauvaises prédictions faites qui sont étiquetées comme positives.
- Vrai négatif (TN) - Ce sont les prédictions correctes faites qui sont étiquetées comme négatives.

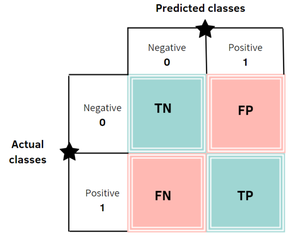

Fig. 3: Prédiction et matrice de confusion.

Il résume les résultats d'un problème de classification à l'aide de quatre métriques : vrai positif, faux négatif, faux positif et vrai négatif. À l'aide de ces quatre composants, nous pouvons calculer diverses métriques pour analyser les performances du modèle d'apprentissage automatique :
+ accuracy- La précision est la proportion des prédictions correctes dans la matrice de confusion sur toutes les prédictions faites.
+ precision- La précision est la proportion des prédictions correctes dans la matrice de confusion sur toutes les prédictions positives.
+ recall- Le rappel est la proportion de prédictions correctes dans la matrice de confusion parmi toutes les classes positives.
+ F1 score- Le score F1 permet de comparer des modèles à faible précision à des modèles à rappel élevé, ou vice versa.

METHODOLOGIE D'EVALUATION

- La base de données de référence Network Intrusion Detection dataset a été téléchargée à partir de Kaggle.
- collection de données de trafic réseau générées à partir d'un environnement de réseau simulé, étiquetées avec le type d'attaque qu'elles représentent, et a un total de 42 types d'attaques différents, un total de 23 fonctionnalités pour chaque paquet réseau, comprenant des informations telles que le type de protocole, les adresses IP source et destination, les numéros de port source et destination, ainsi que l'heure du paquet
- Durant les évaluations, l'arbre de decision qui a été adopter comme algorithme classification binaire.

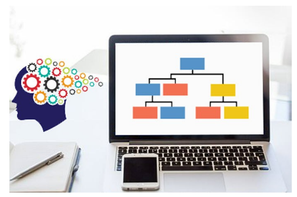

Fig. 4: Arbre de decision.

RESULTATS

Les scores attribués à chaque prédiction reflètent également cette tendance, avec des scores positifs élevés et des scores négatifs faibles.

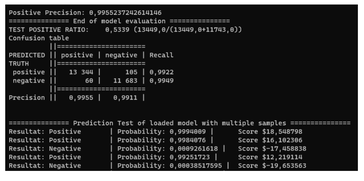

Fig. 5: Prédiction et Matrice de confusion.

CONCLUSION

Obtention de résultats intéressants avec la l'utilisation de l'algorithme Decision tree
- Améliorer le processus de pré-traitement pour avoir une prediction meilleur.

REFERENCES

[1] SANTOS, Frédéric. Arbres de décision. cours université de Bordeaux (CNRS, UMR 5199 PACEA), 2015, p. 1-5.
[2] Poterie, Audrey. Arbres de décision et forêts aléatoires pour variables groupées. Diss. INSA de Rennes, 2018.