**الجمهورية الجزائرية الديمقراطية الشعبية الجمهورية الجزائرية الديمقراطية الشعبية**

**وزارة التعليم العالي والبحث العلمي**

|  |  |  |
| --- | --- | --- |
| **جامعة باجي مختار – عنابـــــــــــــــة** |  | **Université Badji Mokhtar - Annaba**  **Badji Mokhtar – Annaba University** |
| **Faculté : Technologie** | | |
| **Département : Informatique** | | |
| **Filière : Informatique** | | |
| **Spécialité : Gestion et Analyse des Données Massives** | | |
|  | | |

* 2. **Projet du module Sécurité Informatique**

**Thème**

**Construction d’un modèle de classification capable**

**de différencier entre le trafic réseau normal et malicieux.**

**mobile pour aider à arrêter la consommation**

**de tabac**

**Présenté par**

Ferkous Imed Eddine

Rebiai Achref

|  |  |  |
| --- | --- | --- |
| **Professeur**  Abdelaziz Amara Korba |  | **Université**  Badji Mokhtar - Annaba |

**Année Universitaire : 2022/2023**

**TABLE DES MATIERES**

|  |
| --- |
| **Liste des figures ……………………………………………………………………………………….. 3** |
| **Introduction Générale …………………………………………………………………………………… 4** |  |
| **Contexte du projet …………………………………………...……………………………………………4** |  |
|  |  |
| **Chapitre I. Etat de l’art** |  |
| Introduction aux attaques DoS **……………………………………………………………………………..6** |  |
| 1. les différents types d'attaque **…………………………………………………………………………….7**  2. Modèles de classification basés sur l'apprentissage automatique pour la détection des attaques DoS **….7** |  |
|  |  |
| 4. Techniques de pré-traitement **…………………………………………………………………………….8** |  |
| Conclusion **………………………………………………………………………………………………….8** |  |
| **Chapitre II. Conception du modèle** |  |
| 1. Réalisation des attaques **………………………………………………………………………………..10** |  |
| 2. Construction du modèle **………………………………………………………………………………..11** |  |
| 2.1. Extraction et préparation des données **………………………………………………………………..11** |  |
| 2.2. Prétraitement sur les données**………………………………………………………………………....12** |  |
| 2.3. Apprentissage **…………………………………………………………...……………………………13** |  |
| 2.4. évaluation du modèle**…………………………………………………………………………………14** |  |
| 3. Essai du modele **………………………………………………………………………………………..14** |  |
| **Conclusion** |  |
|  |  |
|  |  |

**LISTE DES FIGURES**

|  |  |  |
| --- | --- | --- |
| **N°** | **Titre** | **Page** |
| **1** | Attaque dos avec MetaSploit | **8** |
| **2** | Attaque udp-flood avec HPING3 | **9** |
| **3** | Attaque icmp-flood avec HPING3 | **9** |
| **4** | Interface du CICFLlowMeter | **10** |
| **5** | 1er essai du modèle | **13** |
| **6** | 2ème essai du modèle | **13** |
| **7** | 3ème essai du modèle | **14** |

INTRODUCTION GÉNÉRALE

La sécurité des réseaux informatiques est devenue un enjeu crucial pour les entreprises, les gouvernements et les particuliers. Les menaces contre la sécurité des réseaux sont de plus en plus sophistiquées et peuvent avoir des conséquences catastrophiques pour les organisations et les individus. Les attaques de déni de service (DoS) constituent l'une des menaces les plus courantes et les plus nuisibles pour les réseaux informatiques.

Une attaque DoS vise à rendre un service indisponible pour les utilisateurs légitimes en submergeant les ressources d'un système cible avec une quantité massive de trafic ou de requêtes malveillantes. Ces attaques peuvent causer des pertes financières importantes, une détérioration de la réputation de l'entreprise, voire des impacts sur la sécurité physique des individus. Les attaques DoS sont en constante évolution et les attaquants utilisent des techniques de plus en plus sophistiquées pour masquer leur identité et rendre les attaques plus difficiles à détecter.

Contexte du projet :

L'objectif de ce projet est de créer un modèle de classification à l'aide des techniques d'apprentissage automatique, capable de distinguer entre le trafic réseau normal et malveillant, tout en étant capable de détecter le type d'attaque à partir de son trafic réseau.

I. ETAT DE L’ART

**Introduction aux attaques DoS :**

Les attaques de déni de service (DoS) sont une menace majeure pour la sécurité des réseaux informatiques. Ces attaques sont généralement menées en submergeant les ressources d'un système cible avec une quantité massive de trafic ou de requêtes malveillantes. Le but ultime de ces attaques est de rendre le service indisponible pour les utilisateurs légitimes, ce qui peut entraîner des pertes financières, une détérioration de la réputation de l'entreprise, voire des impacts sur la sécurité physique des individus.

Les attaques DoS ont plusieurs caractéristiques communes, notamment une forte intensité de trafic, une utilisation abusive de ressources, une variation de l'adresse IP source, etc. Les attaquants peuvent également utiliser diverses techniques pour masquer leur identité et rendre les attaques plus difficiles à détecter, comme l'utilisation de botnets, la falsification de l'adresse IP source, etc.

Les attaques de déni de service (DoS) se présentent sous différentes formes, notamment les attaques SYN flood, UDP flood et ICMP flood.

Les attaques SYN flood consistent à envoyer un grand nombre de requêtes de connexion SYN à un serveur cible, sans jamais finaliser la connexion. Cela peut saturer les ressources du serveur et le rendre indisponible pour les utilisateurs légitimes.

Les attaques UDP flood impliquent l'envoi d'un grand nombre de paquets UDP à un serveur cible, ce qui peut provoquer une saturation des ressources du serveur.

Les attaques ICMP flood consistent à envoyer un grand nombre de requêtes ICMP Echo Request à un serveur cible, ce qui peut provoquer une saturation des ressources du serveur ou une perturbation de la connectivité du réseau.

La détection des attaques DoS de différentes formes nécessite des approches de détection spécifiques. Dans ce projet, nous nous concentrerons sur la création d'un modèle de classification capable de détecter les attaques DoS en général, sans se limiter à une forme spécifique d'attaque.

Les conséquences des attaques DoS peuvent être graves, notamment des pertes financières, des temps d'arrêt des services, une diminution de la réputation de l'entreprise, des impacts sur la sécurité physique des individus, etc. Les entreprises doivent donc prendre des mesures pour détecter et prévenir les attaques DoS.

**Différents types d'attaques**

Les attaques de déni de service (DoS) se présentent sous différentes formes, notamment les attaques SYN flood, UDP flood et ICMP flood.

Les attaques SYN flood consistent à envoyer un grand nombre de requêtes de connexion SYN à un serveur cible, sans jamais finaliser la connexion. Cela peut saturer les ressources du serveur et le rendre indisponible pour les utilisateurs légitimes.

Les attaques UDP flood impliquent l'envoi d'un grand nombre de paquets UDP à un serveur cible, ce qui peut provoquer une saturation des ressources du serveur.

Les attaques ICMP flood consistent à envoyer un grand nombre de requêtes ICMP Echo Request à un serveur cible, ce qui peut provoquer une saturation des ressources du serveur ou une perturbation de la connectivité du réseau.

La détection des attaques DoS de différentes formes nécessite des approches de détection spécifiques. Dans ce projet, nous nous concentrerons sur la création d'un modèle de classification capable de détecter les attaques DoS en général, sans se limiter à une forme spécifique d'attaque.

**Modèles de classification basés sur l'apprentissage automatique pour la détection des attaques DoS**

Les modèles de classification basés sur l'apprentissage automatique sont des approches courantes pour la détection des attaques DoS. Ces modèles sont entraînés sur des ensembles de données comportant des exemples de trafic normal et des exemples de trafic malveillant, pour apprendre à différencier entre les deux. Les modèles de classification peuvent être basés sur différentes techniques d'apprentissage automatique telles que les réseaux de neurones, les arbres de décision, les méthodes de classification linéaire, ou encore les algorithmes de classification ensemblistes.

Cependant, la création de modèles de classification efficaces pour la détection des attaques DoS peut être un défi en raison de la complexité et de la diversité des attaques. Les modèles de classification doivent être entraînés sur des ensembles de données de grande taille et représentatifs de différentes formes d'attaques pour garantir leur généralisation et leur précision. De plus, l'ingénierie de caractéristiques est une étape importante pour améliorer la qualité de l'ensemble de données et la précision du modèle de classification.

**Techniques de pré-traitement**

Les techniques de pré-traitement sont essentielles pour améliorer la précision des modèles de classification contre les attaques DoS. Ces techniques visent à sélectionner et à transformer les caractéristiques les plus pertinentes et informatives du trafic réseau pour améliorer la qualité de l'ensemble de données et la performance du modèle de classification.

Les techniques de pré-traitement incluent le nettoyage des données, la normalisation, la discrétisation et la réduction de dimension. Le nettoyage des données consiste à éliminer les données erronées, manquantes ou dupliquées. La normalisation vise à réduire les écarts entre les valeurs des caractéristiques pour les rendre comparables. La discrétisation consiste à transformer les caractéristiques continues en variables catégorielles pour faciliter leur traitement. La réduction de dimension permet de réduire la taille de l'ensemble de données en éliminant les caractéristiques redondantes ou peu pertinentes.

L'utilisation de techniques de pré-traitement et d'ingénierie de caractéristiques est cruciale pour améliorer la précision des modèles de classification contre les attaques DoS. Ces techniques peuvent contribuer à améliorer la qualité de l'ensemble de données et la performance du modèle de classification en réduisant le bruit, en éliminant les caractéristiques peu pertinentes et en extrayant des caractéristiques plus discriminantes.

**Conclusion**

La détection des attaques DoS est un défi important pour la sécurité des réseaux informatiques. Les approches basées sur les signatures et les anomalies sont souvent inefficaces pour détecter les attaques DoS modernes, ce qui a conduit au développement de modèles de classification basés sur l'apprentissage automatique. Ces modèles peuvent être améliorés en utilisant des techniques de pré-traitement et d'ingénierie de caractéristiques pour améliorer la qualité de l'ensemble de données et la performance du modèle de classification. Les recherches récentes ont montré que les modèles de classification basés sur l'apprentissage automatique sont prometteurs pour la détection des attaques DoS, mais il reste des défis à relever pour améliorer leur efficacité et leur robustesse face aux attaques sophistiquées.

II. CONCEPTION DU MODELE

**Réalisation des attaques**

Dans le cadre de notre projet, nous avons mis en place un environnement comprenant deux machines virtuelles : une pour la réalisation des attaques et l'autre pour simuler la machine victime. Nous avons réalisé plusieurs attaques courantes telles que l'attaque SYN Flood, l'attaque UDP Flood et l'attaque ICMP Flood. Nous avons utilisé différents outils et scripts pour réaliser ces attaques, notamment Hping3 et MetaSploit. Nous avons ensuite mesuré les effets de ces attaques sur la machine victime et observé les résultats en utilisant Wireshark qui est un outil de capture et d'analyse de trafic réseau gratuit et open source. Il permet de capturer et d'analyser les paquets de données qui circulent sur un réseau.

1. MetaSploit avec la commande ‘use auxiliary/dos/tcp/synflood’ pour effectuer le syn-flood

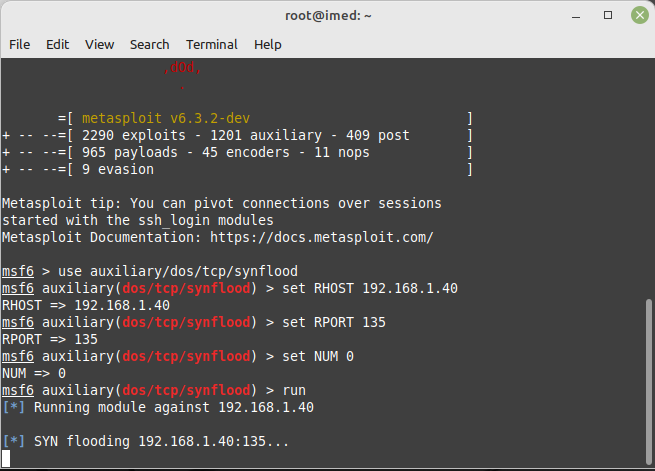


Figure 1. Attaque dos avec MetaSploit

1. Hping3 avec la commande ‘hping3 -2 –flood (adress du la machine victime)’ pour udp-flood

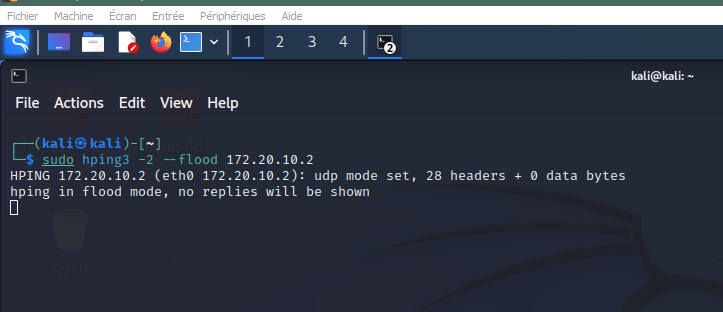


Figure 2. Attaque udp-flood avec HPING3

3. Hping3 avec la commande ‘hping3 -1 –flood (adress du la machine victime)’ pour udp-flood

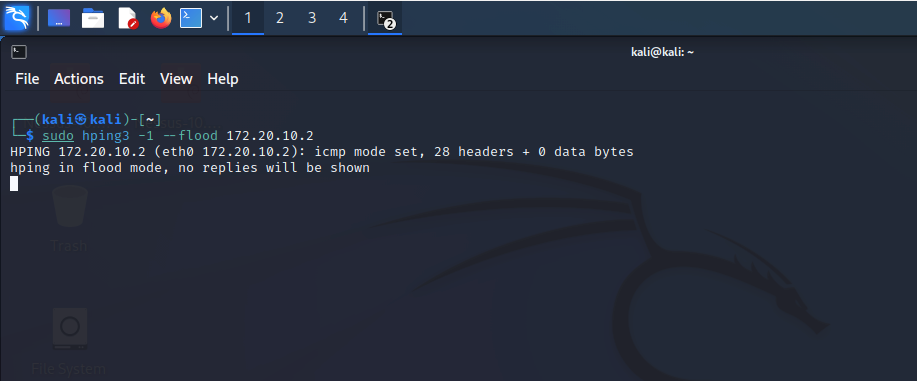


Figure 3. Attaque icmp-flood avec HPING3

**2.Construction du modèle**

* 1. **. Extraction et préparation des données**

Dans cette partie du projet, nous avons extrait les données nécessaires à la construction de notre modèle de classification à partir du trafic réseau capturé à l'aide de Wireshark. Nous avons ensuite utilisé l'outil CICflowmeter pour convertir le fichier pcap en un fichier csv exploitable pour l'analyse. Cet outil a permis de transformer les données de base en une version plus raffinée, tout en ajoutant des caractéristiques spécifiques à la détection des attaques DoS. Le fichier csv obtenu contenait des informations sur chaque paquet de données capturé, telles que les adresses IP source et destination, les ports source et destination, les protocoles utilisés, ainsi que des caractéristiques de flux, telles que la durée, le nombre de paquets, la taille du flux, etc.

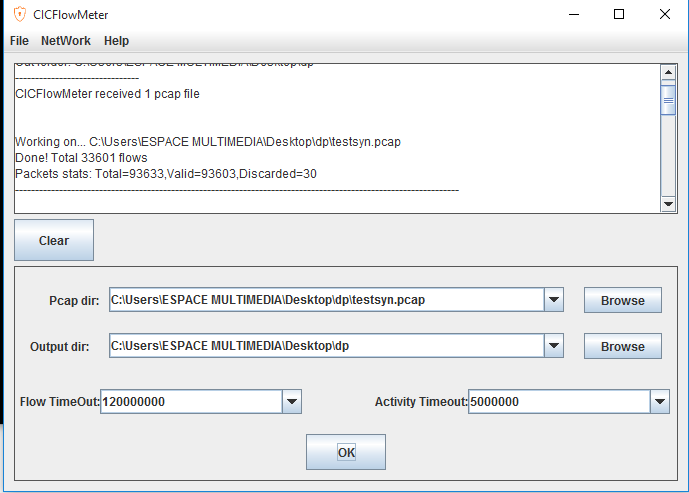


Figure 4. Interface du CICFLlowMeter

**2.2 .Pré-traitement sur les données**

Dans cette partie du projet, nous avons effectué un prétraitement sur les données pour les rendre plus adaptées à l'utilisation d'algorithmes d'apprentissage automatique.

1. L’équilibrage les classes de notre ensemble de données en utilisant la technique de sous-échantillonnage (ou "drop"), qui consiste à supprimer des exemples de la classe majoritaire jusqu'à ce que les classes soient équilibrées.
2. La conversion les étiquettes des données de leur format d'origine en utilisant un encodage différent pour chaque type d'attaque. Plus précisément, nous avons utilisé la valeur 0 pour le trafic normal, 1 pour les attaques UDP, 2 pour les attaques SYN et 3 pour les attaques ICMP.
3. La concaténation les quatre fichiers CSV résultants en un seul fichier CSV.
4. La suppression des valeurs infinies.
5. La suppression de différents paramètres qui pourrait ne pas être utile pour détecter les attaques DoS :

* Adresses IP source et destination qui peuvent être masquées ou falsifiées, ce qui rend difficile l'identification de l'attaquant réel.
* Port source et destination : De nombreux types d'attaques DoS ne dépendent pas des ports spécifiques utilisés pour la communication.
* Timestamp : Les horodatages peuvent être utiles pour analyser les modèles de trafic et détecter les anomalies, mais ils ne sont pas indispensables pour la détection des attaques DoS. Par conséquent, les inclure ou les enlever du modèle dépend de la nature de l'attaque et des données disponibles pour l'analyse.

1. L’utilisation du model Lasso regression pour la selection des paramètres les plus utiles : Le modèle de régression Lasso est un type de régression linéaire qui ajoute une contrainte de pénalité à la fonction de coût afin de pénaliser les coefficients des paramètres moins importants, les conduisant à être réduits à zéro. Cela permet de sélectionner automatiquement les paramètres les plus utiles pour la classification en éliminant les paramètres moins importants qui peuvent affecter la performance du modèle. En utilisant cette méthode, nous avons pu sélectionner les caractéristiques les plus importantes pour notre modèle de classification contre les attaques DoS.

**2.3. Apprentissage**

Après avoir préparé les données et sélectionné les caractéristiques les plus importantes à l'aide de la régression Lasso, nous avons procédé à l'apprentissage en utilisant l'algorithme de l'arbre de décision. L'arbre de décision est un modèle d'apprentissage automatique qui prend en entrée les caractéristiques de données et les utilise pour prendre des décisions en suivant une hiérarchie de règles de décision. L'algorithme d'arbre de décision apprend ces règles à partir des données d'entraînement et peut ensuite être utilisé pour classer de nouvelles données en fonction de la hiérarchie de règles.

Nous avons utilisé la bibliothèque de machine learning Scikit-learn en Python pour entraîner notre modèle d'arbre de décision. Nous avons divisé notre ensemble de données en un ensemble d'entraînement et un ensemble de test, où l'ensemble d'entraînement est utilisé pour entraîner le modèle et l'ensemble de test est utilisé pour évaluer sa performance.

**2.4. Évaluation du modèle**

Après avoir entraîné notre modèle de classification en utilisant l'algorithme de l'arbre de décision, nous avons évalué sa performance en utilisant un ensemble de données de test séparé. Nous avons calculé plusieurs métriques de performance telles que l’accuracy, le recall et le score F1 pour évaluer la qualité de la classification du modèle.

Voici les résultats sous forme de tableau.

|  |  |  |
| --- | --- | --- |
| Accuracy | Recall | F1-Score |
| 99,99% | 99.99% | 99.99% |

1. **Essai du modèle :**

Pour essayer ce modèle nous avons utiliser trois nouvelles bases de données contenant chaque une un type d’attaques différents et on a utilisé la fonction predict du modèle pour savoir le type de chaque attaque.

Le modèle Affiche de bons résultats pour chaque un des essais et pour n’importe quel type d’attaques

**Détection d’Udp flood**

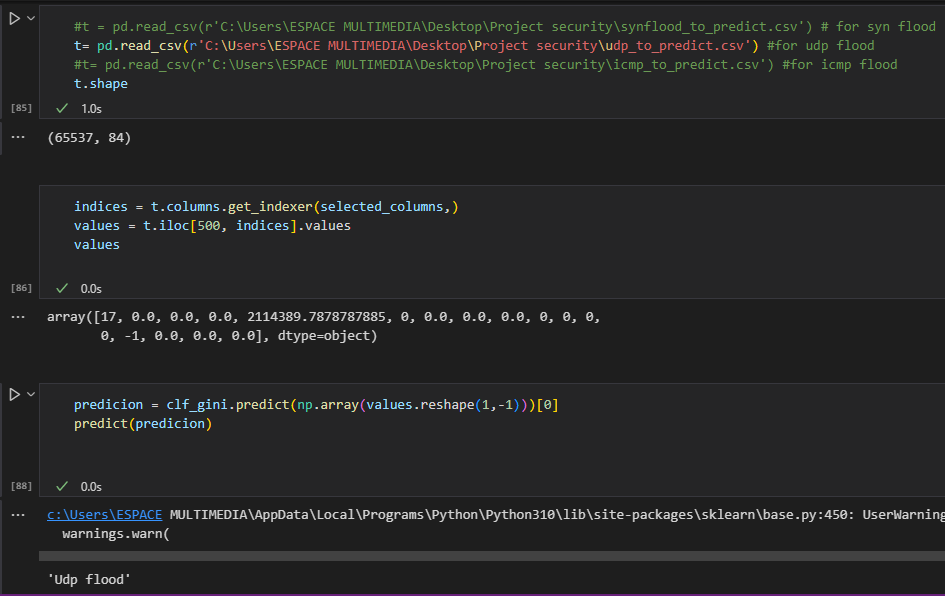


Figure 5. 1er essai du modèle

**Détection de Syn flood**

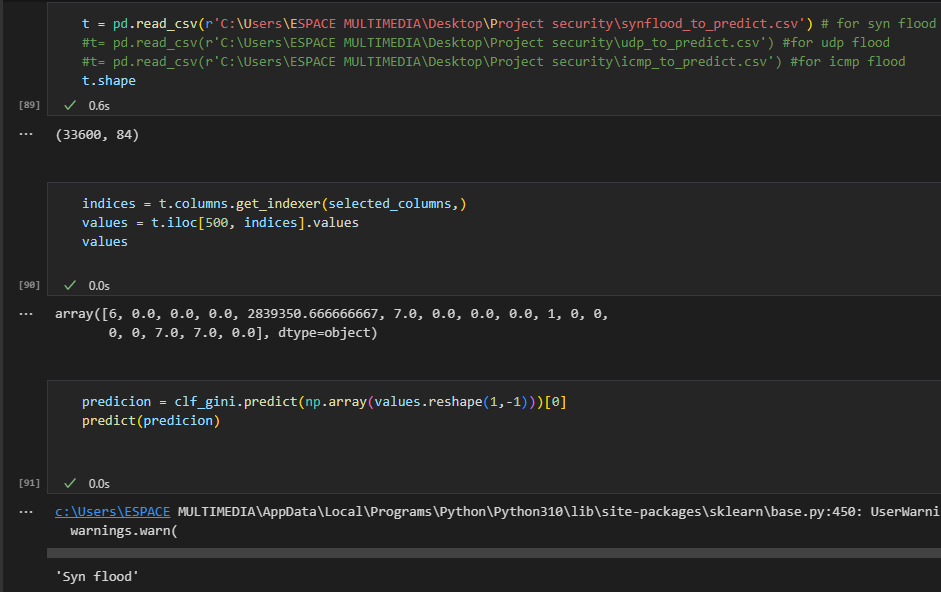


Figure 6. 2ème essai du modèle

**Détection de ICMP flood**

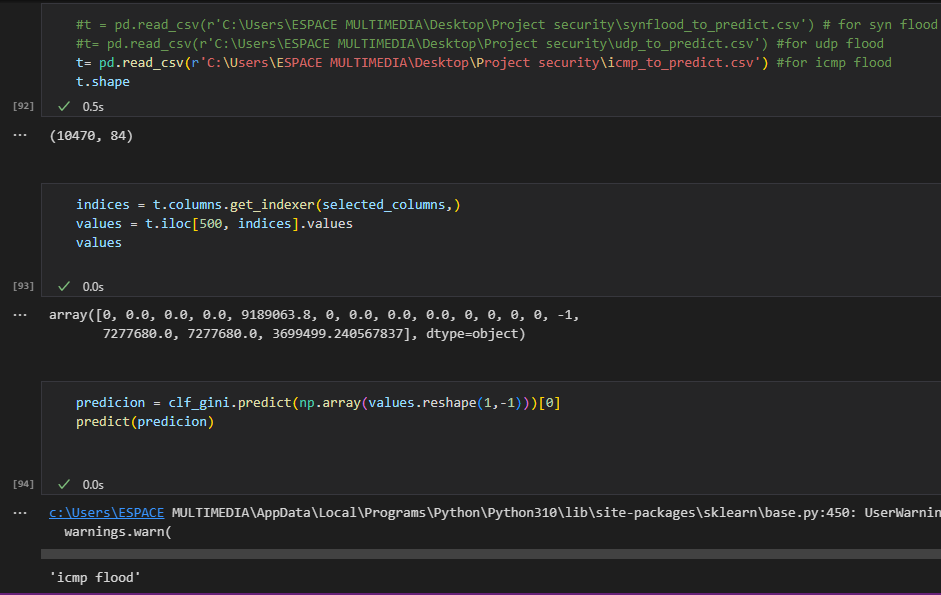


Figure 7. 3ème essai du modèle

**Conclusion**

Au terme de ce rapport, nous avons présenté les différentes techniques et méthodes utilisées pour la conception et l'implémentation d'un modèle de classification d'attaques DoS. Nous avons commencé par présenter l'état de l'art dans ce domaine, en mettant en évidence des techniques utilisées. Ensuite, nous avons présenté la conception générale de notre modèle, ainsi que les différentes étapes du prétraitement et de l'apprentissage des données. Nous avons également évalué la performance de notre modèle en utilisant différentes métriques telles que l'accuracy, le recall et le f1-score. Enfin, nous avons testé notre modèle sur une base de données contenant des attaques différentes, ce qui a permis de vérifier l'efficacité de notre modèle dans la détection des attaques.

En conclusion, ce projet a permis d'approfondir notre compréhension des techniques d'apprentissage automatique appliquées à la détection des attaques DoS, ainsi que de mettre en évidence les différentes étapes nécessaires à la conception d'un modèle efficace et performant.