基於機器學習之低速緩慢 DDoS 攻擊偵測
A Slow DDoS Attack Detection Based On Machine Learning

指導教授：張燕光; 專題成員：張原愷、張辰凱

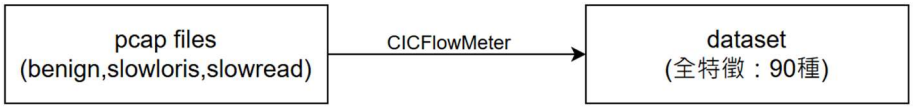
開發工具：Python, Scapy, CICFlowMeter; 測試環境：Ubuntu 22.04 LTS

一、 簡介：

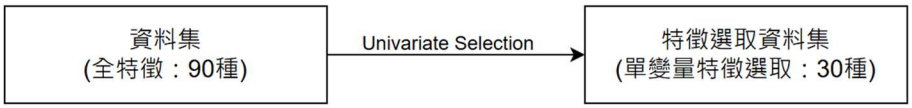
Slow HTTP Attack DDoS 是一種網路攻擊方式，透過發送大量低速、持續的 HTTP 請求使得伺服器資源耗盡，進而使其無法處理正常用戶的 HTTP 請求。與其他 DDoS 攻擊不同，低速緩慢攻擊通常利用合法的 HTTP 請求，但攻擊者會故意以非常緩慢的速度發送這些請求，以耗盡伺服器資源。在我們這組的專題中，我們修改並利用 CICFlowMeter[1]提取機器學習所需的 flow 特徵，之後參考論文[2]做資料前處理，最後實現基於機器學習的 Slow HTTP Attack 攻擊偵測，偵測的攻擊有兩種 (1) Slowloris (2) Slow Read。

(一)資料前處理：

特徵選取：透過特徵選取降低模型複雜度以及減少對訓練資料集的過擬合(Overfitting)。



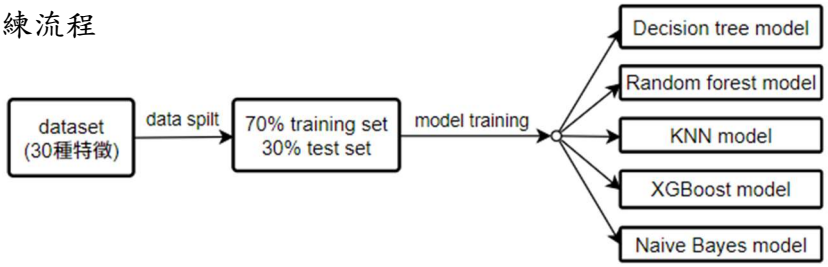
單變量特徵選取，我們採取 SelectKBest 方法：選取 K 個最好的特徵，K=30。



(二)模型訓練：

資料集(種類)	訓練樣本數	測試樣本數	標籤
Benign	55591	10103	benign
Slowloris	21453	5901	slowloris
Slow Read	24369	5871	slowread

訓練流程



(三)花費時間：

Total feature extraction time	33m 20s
Total feature selection time	46s
Total training time	4m 45s

二、 測試結果：

(一) 訓練結果：以下是針對三個 Label 分析後的各個結果數值。

Model	Precision	Recall	F1-score	True positive rate	False positive rate
DecisionTree	0.9999	0.9998	0.9998	0.9998	0.0001
RandomForest	0.9999	1.	0.9999	1.	0.0001
KNN	0.9996	0.9999	0.9997	0.9999	0.0004
XGBoost	0.9999	1.	0.9999	1.	0.0001
Naïve Bayes	0.9674	0.9569	0.9621	0.9569	0.039

表一：Benign

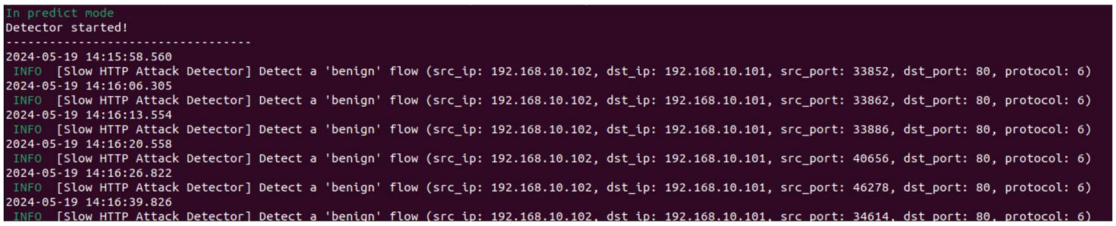
Model	Precision	Recall	F1-score	True positive rate	False positive rate
DecisionTree	0.998	0.9971	0.9976	0.9971	0.0004
RandomForest	0.9988	0.9985	0.9986	0.9985	0.0003
KNN	0.9983	0.9961	0.9972	0.9961	0.0004
XGBoost	0.998	0.998	0.998	0.998	0.0004
Naïve Bayes	0.8792	0.9194	0.8988	0.9194	0.033

表二：Slowloris

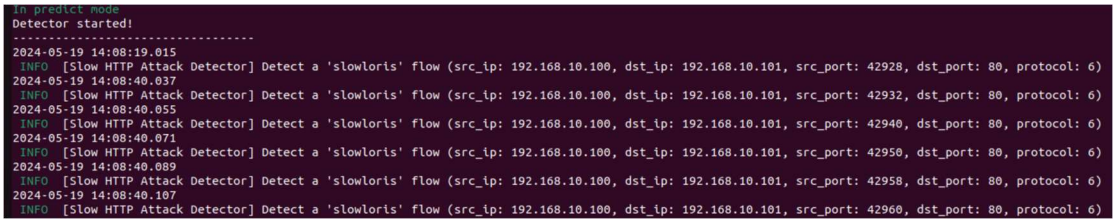
Model	Precision	Recall	F1-score	True positive rate	False positive rate
DecisionTree	0.9975	0.9985	0.998	0.9985	0.0008
RandomForest	0.9987	0.9987	0.9987	0.9987	0.0004
KNN	0.9969	0.9981	0.9975	0.9981	0.0009
XGBoost	0.9983	0.9981	0.9982	0.9981	0.0005
Naïve Bayes	1.	0.9856	0.9927	0.9856	0.

表三：Slow Read

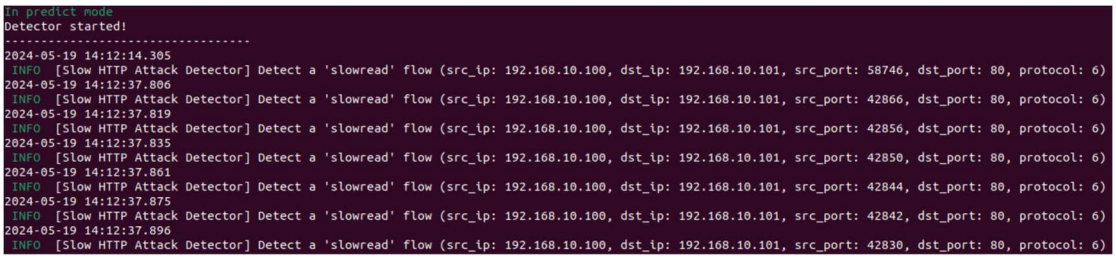
（二）實際偵測：以下分別是正常訪問網頁以及利用 slowhttptest 攻擊網站的結果。



圖一：Benign 偵測



圖二：Slowloris 偵測



圖三：Slow Read 偵測

三、 參考文獻：

[1] ”CICFlowMeter”, 2020, https://gitlab.com/hieulw/cicflowmeter.

[2] Yin Mon Swe, Pye Pye Aung, Aye Su Hlaing, “A Slow DDoS Attack Detection Mechanism using Feature Weighing and Ranking”, the 11th Annual International Conference on Industrial Engineering and Operations Management, 2021. 03.