109550073 陳宥安

Network System Capstone – Final Project
Project Proposal
Network monitoring and warning system

1. 主題

本project旨在開發一個網路監控系統，用於實時監視和分析網路流量，並提供有關網路性能、安全性和運營狀況的實時報告和警示。

2. 預期功能

- 網路流量監視：系統將實時監視網路流量中的封包，將出入的封包記錄並統計信息，例如流量大小、流量來源和目的地、協議類型等。
- 網路性能分析：系統將分析網路性能指標，例如頻寬使用率、延遲時間、丟包率等，並可以生成報告或圖以便於分析和評估網路性能。
- 網路安全監視：能夠檢測網路中的異常流量、潛在風險和安全事件，並發出警報通知。
- 歷史紀錄：能夠將捕獲到的封包和相關分析結果保存，以便後續查詢和分析。

3. 詳細說明

題目的想法來自於我們homework 1時所作的packet capture，我想將它以python改寫，把功能擴充並加入安全偵測的功能。改寫的部份我預計使用pyshark來改寫，並用他來完成封包捕獲、封包解析、統計分析等功能，方便進行網路流量的監控和分析。安全偵測的部份，我想要使用有提供python api的偵測library，然後如果有能力的話，加入機器學習的部份來讓安全偵測更加準確，在識別的部份使用Yara等Python函式庫來識別網路流量和檔案中的惡意特徵，例如病毒特徵、惡意URL、命令與控制（C2）通信特徵等，以增加對已知威脅的識別能力，並在識別到安全問題後，提供即時的報警和通知功能。

4. 實驗/開發環境

開發語言：Python
系統：Ubuntu 22.04
機器學習庫：Scikit-learn、TensorFlow等
可視化庫：Matplotlib