**關鍵基礎設施資安學程**

**實務選修專題課程-實作專題報告**

|  |  |
| --- | --- |
| **操作方式** | □個人　　　　□小組 |
| **組員名單**  **(請列出學校、系所、姓名)** | 1.佘俊霖 |
| 2. |
| **修讀課程** | □水資源資安實務專題  □石化資安實務專題  □電網資安實務專題 |

1. **專題名稱：針對modbus通訊協議的中間人攻擊圖形化程式設計與實作**
2. **摘要**

本專題旨在研究Modbus通訊協議的安全性，設計並實作一個針對該協議的中間人攻擊（MITM）圖形化程式，以模擬和測試可能存在的安全漏洞。通過詳細分析Modbus通訊協議的工作機制，我們設計了一套針對不同場景的中間人攻擊方法。最終，我們開發了一個易於操作的圖形化工具，並進行了一系列實驗以驗證其有效性。

1. **內文(架構圖、實驗數據)**
2. **研究背景**

Modbus通訊協議是工業控制系統中常用的協議之一，廣泛應用於各類自動化設備的數據傳輸。然而，由於其設計上的簡單性和透明性，Modbus協議在安全性方面存在一定的風險。本研究針對這些潛在風險，設計並實作一個針對Modbus協議的中間人攻擊（MITM）圖形化程式，以揭示和測試這些安全漏洞。

1. **架構**

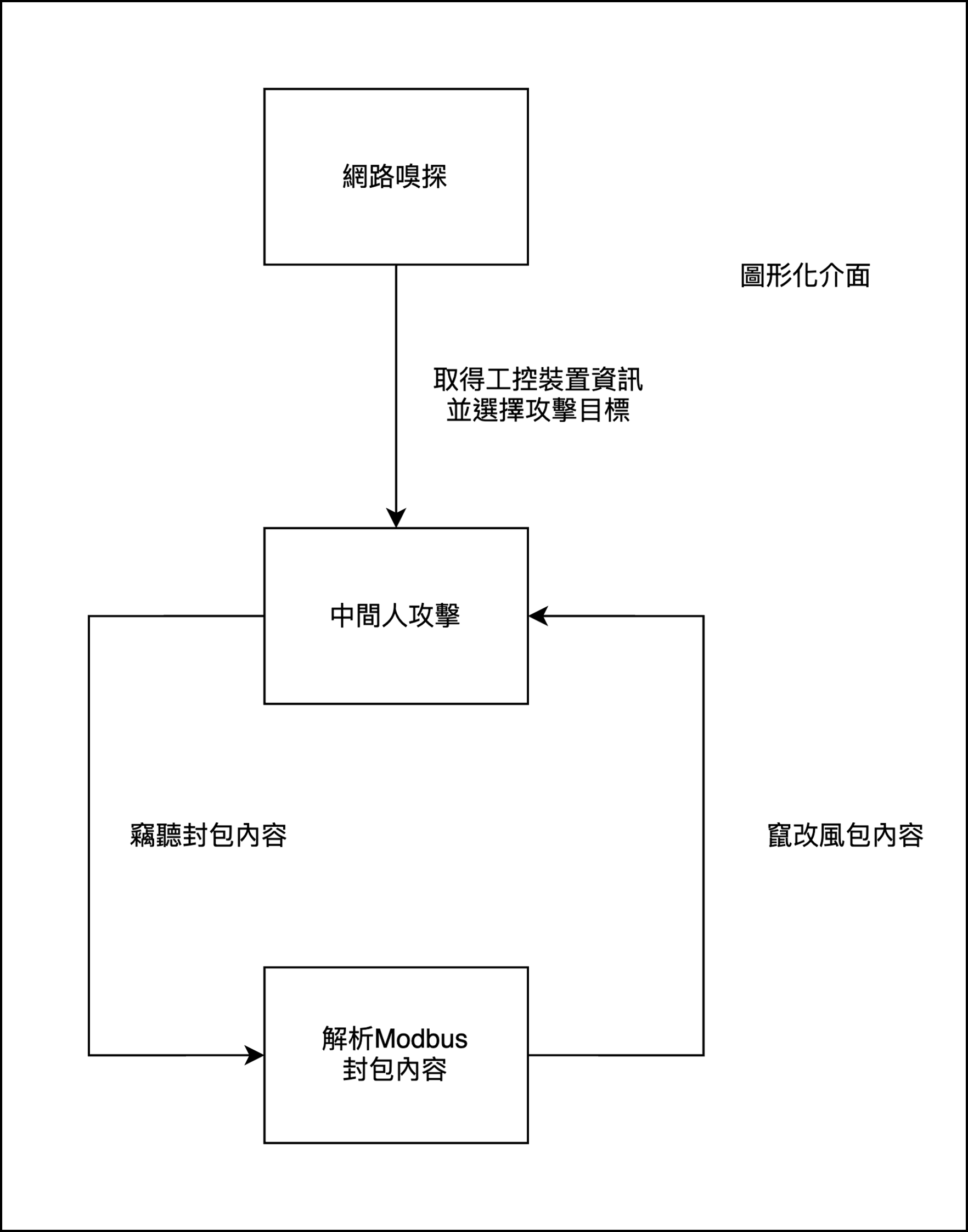
本專題攻擊程式架構如下，分成四個主要模組：

**圖形化模組**：建構直覺易操作的圖形化攻擊介面。

**網路模組：**進行網路嗅探與掃描潛在工控裝置。

**中間人攻擊模塊**：使用中間人攻擊進行 arp 欺騙，竊聽並竄改modbus 協議封包。

**Modbus解析模組：**解析modbus協議，並透過圖形化介面讓攻擊者取得並修改傳輸數據。

****

1. **成果**

建議題目：

1. 智慧農業中的PLC自動化灌溉系統
2. 水處理廠SCADA系統的設計與實施
3. 智慧城市中的交通信號控制系統
4. 能源管理系統在智能建築中的應用
5. 風力發電廠的監控與控制系統
6. 太陽能光電的監控與控制系統
7. 化工廠安全監控與預警系統設計
8. 工業物聯網在化工廠中的應用
9. 基於SCADA的化工廠能效管理系統
10. 溫溼度空氣監控系統