**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 (成大交管系) |
| 2.于京平 (南大資工系) |
| **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：OT 攻擊工具包**
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通信與中間人攻擊（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，我們設計了一套數據取得與竄改的工具，並利用中間人攻擊屏蔽Client對Server的連線。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。

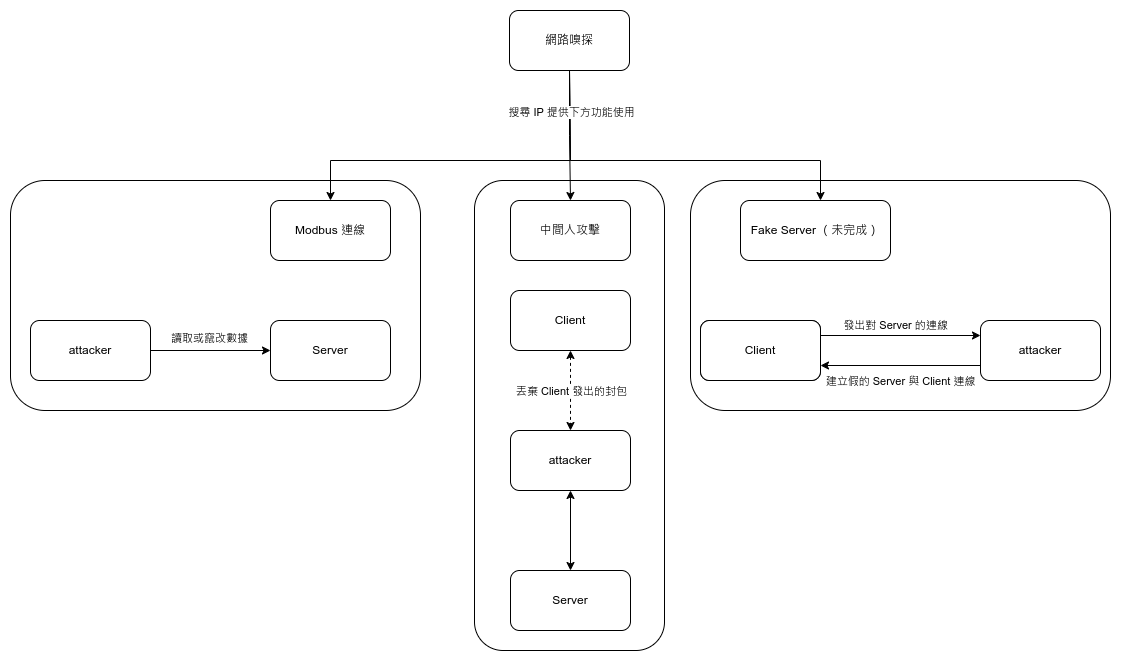
1. **內文(架構圖、實驗數據)**
2. **研究背景**

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 協議的連線和中間人攻擊（MITM）圖形化程式，以揭示和測試這些安全漏洞。

1. **架構**

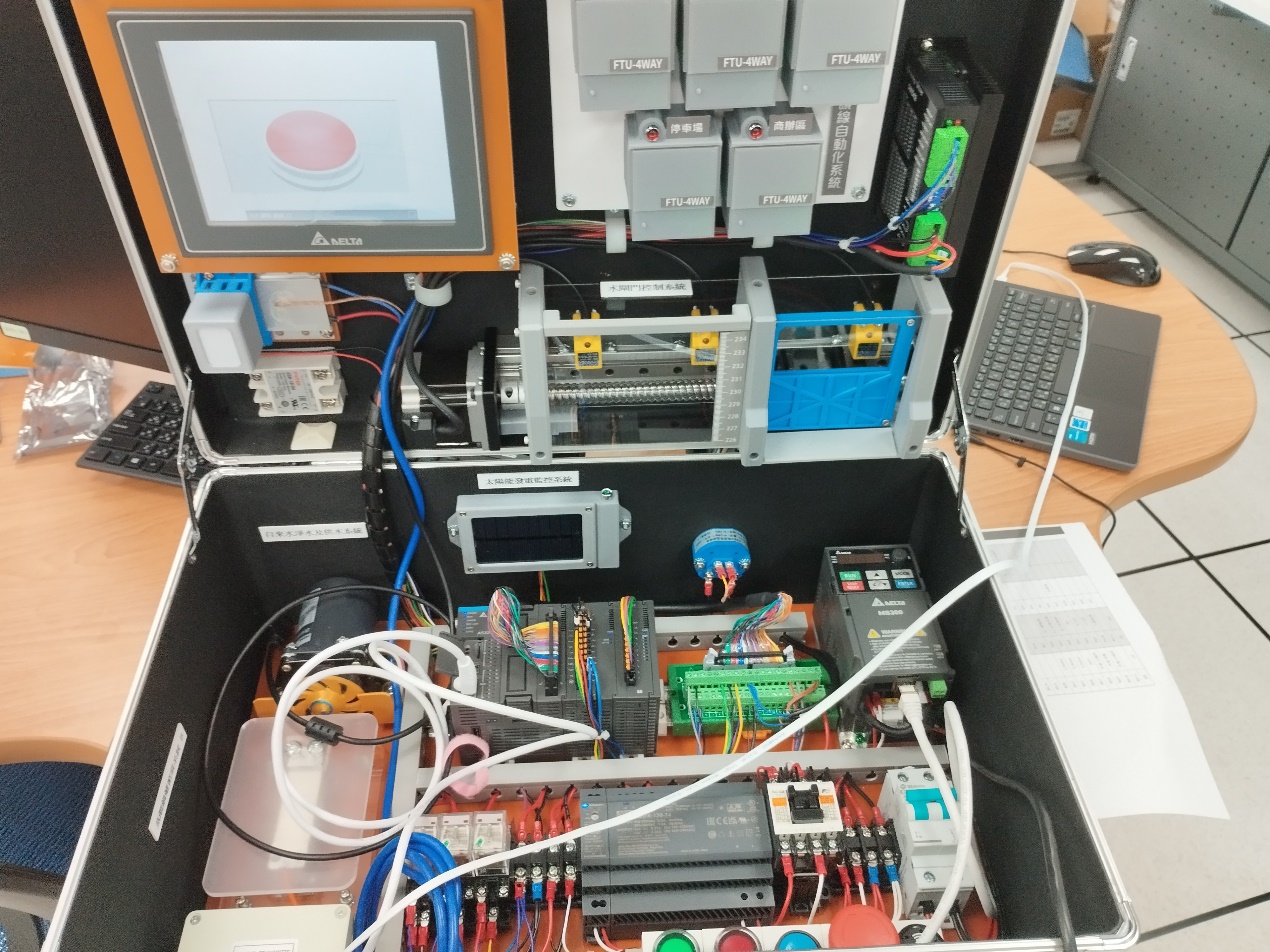
本專題攻擊程式架構如下，分成四個主要模組：

1. **圖形化模組**：建構直覺易操作的圖形化攻擊介面。
2. **網路模組：使用** namp進行網路嗅探與掃描潛在工控裝置。
3. **中間人攻擊模塊**：使用 ettercap 發起中間人攻擊進行 arp 欺騙，並對 Client 傳出的封包進行屏蔽，這項功能將使得 Client 失去對 Server 的連線，防止 Client 修復竄改的數據。
4. **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。

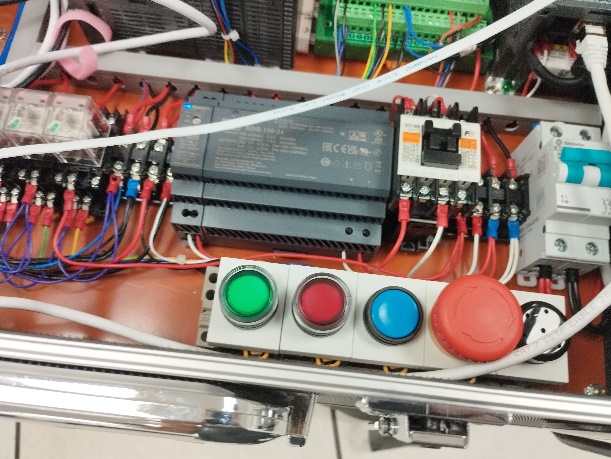


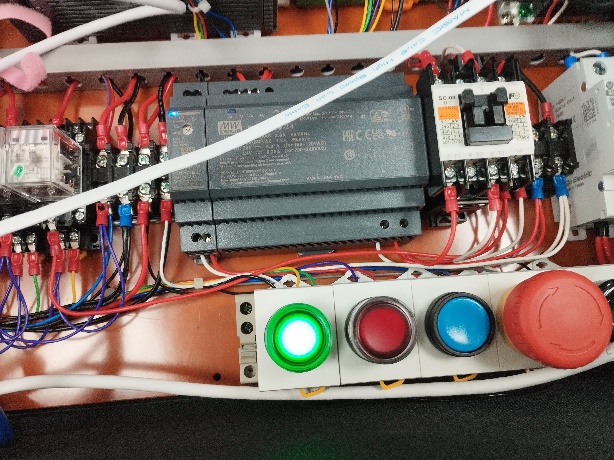
1. **實驗數據**

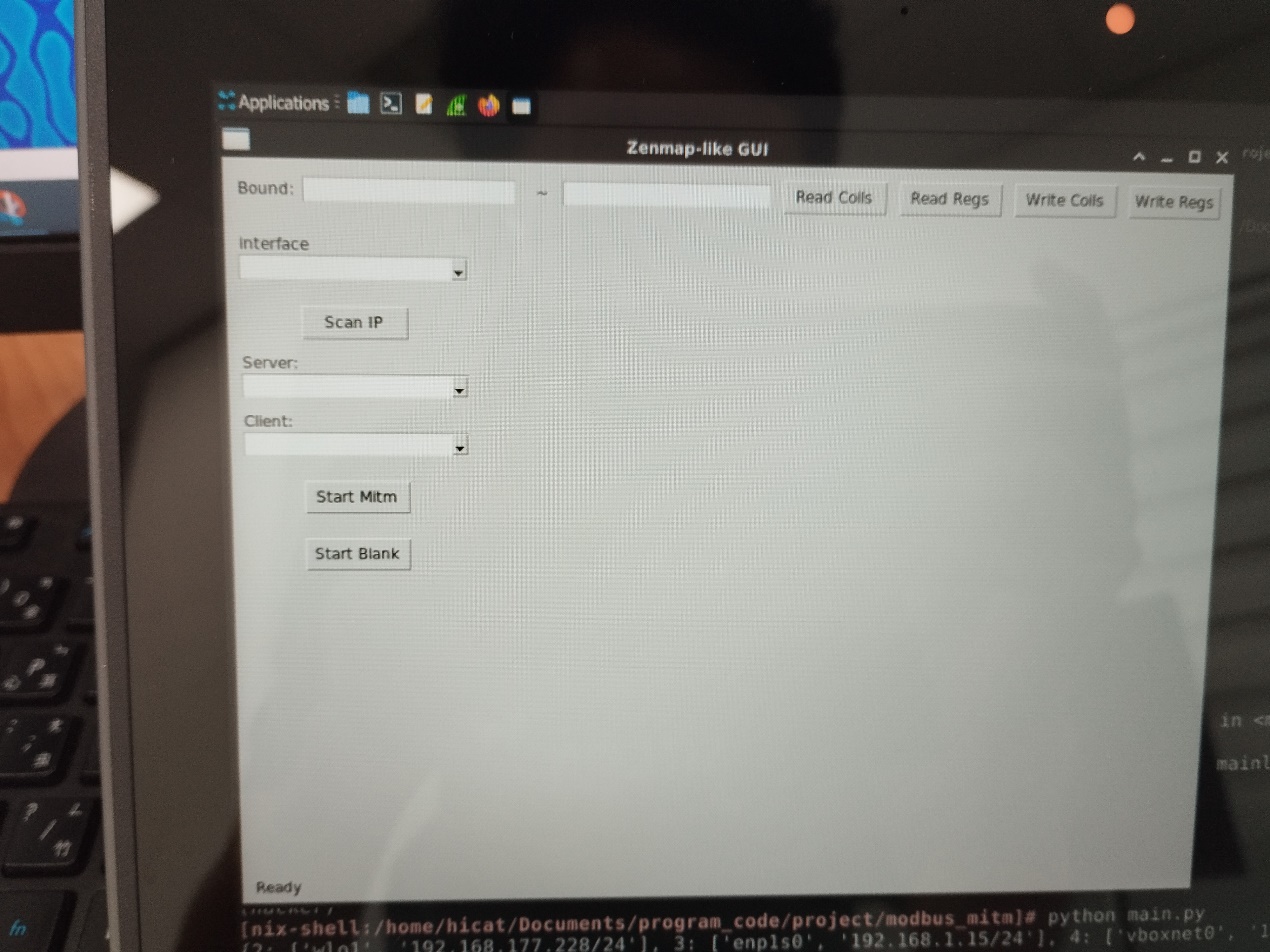
我們先來介紹工控箱環境



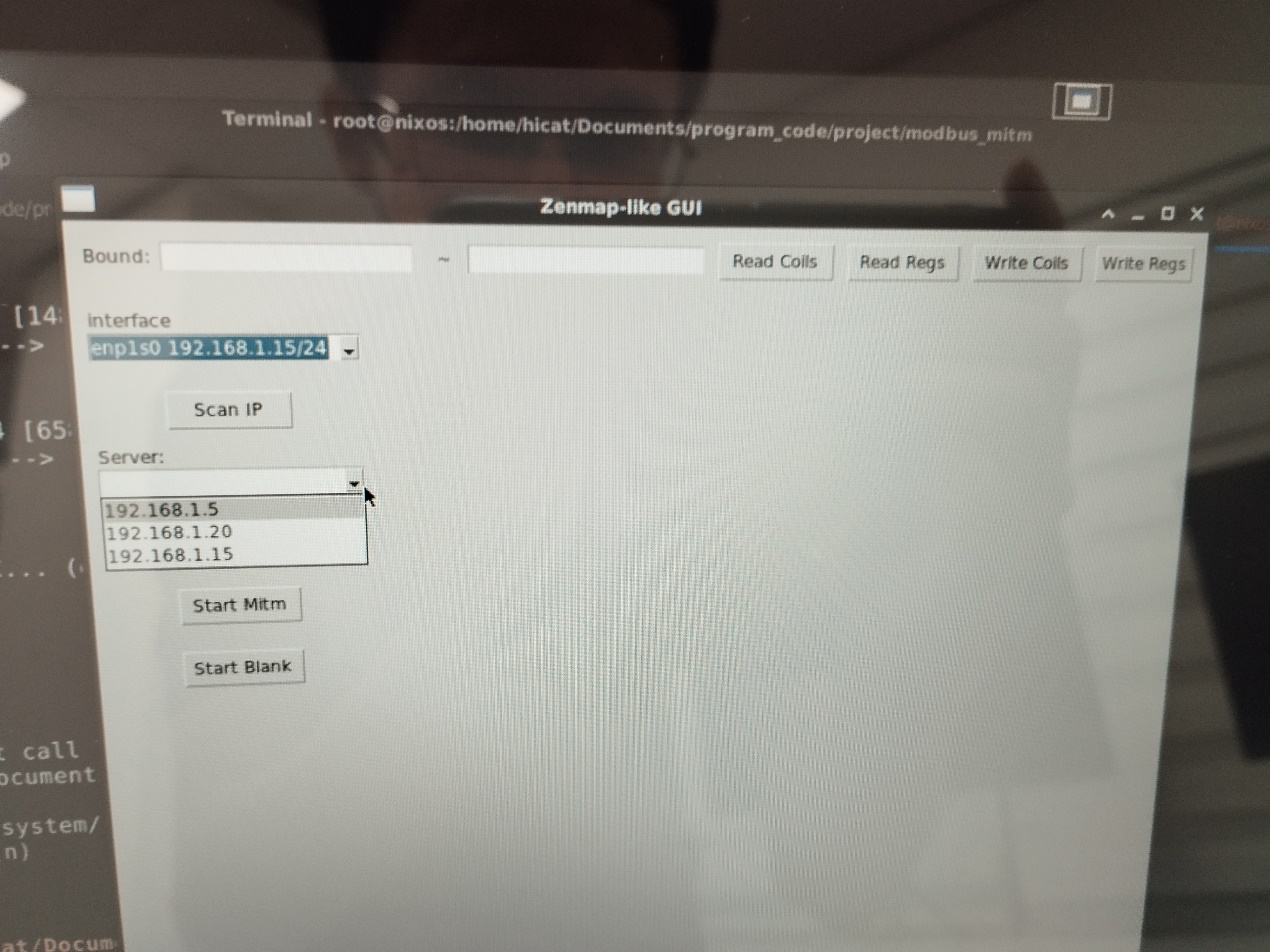
我們會使用到工控箱中的Delta PLC與HMI和下方的綠紅藍按鍵燈中的綠色按鍵

 HMI中有一個按鈕圖示能控制綠色按鈕的燈亮起或關閉(此時為關閉)

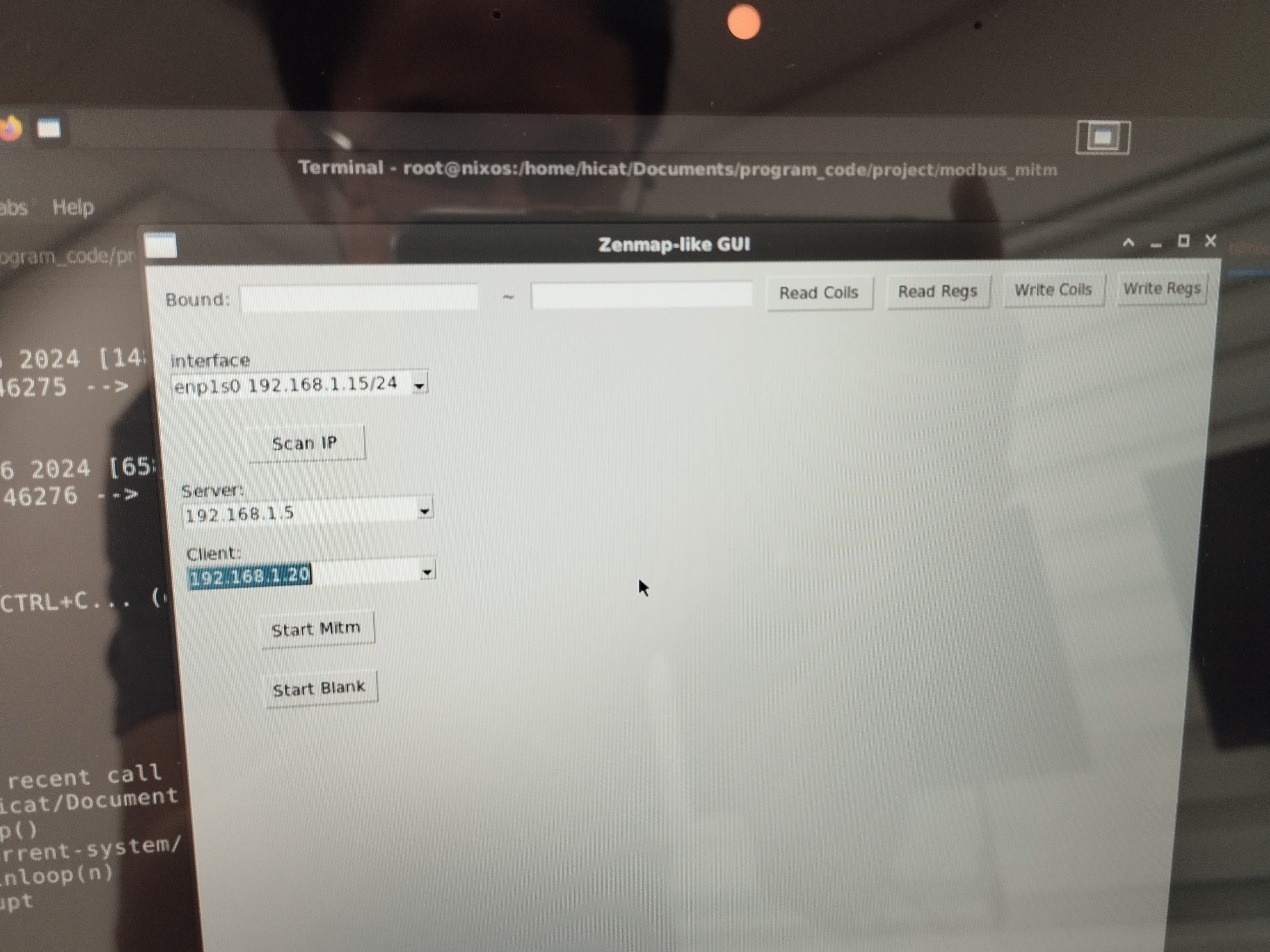
  (此時為亮起)



啟動成功後會出現視窗介面，選擇好interface後即可按Scan IP進行掃描



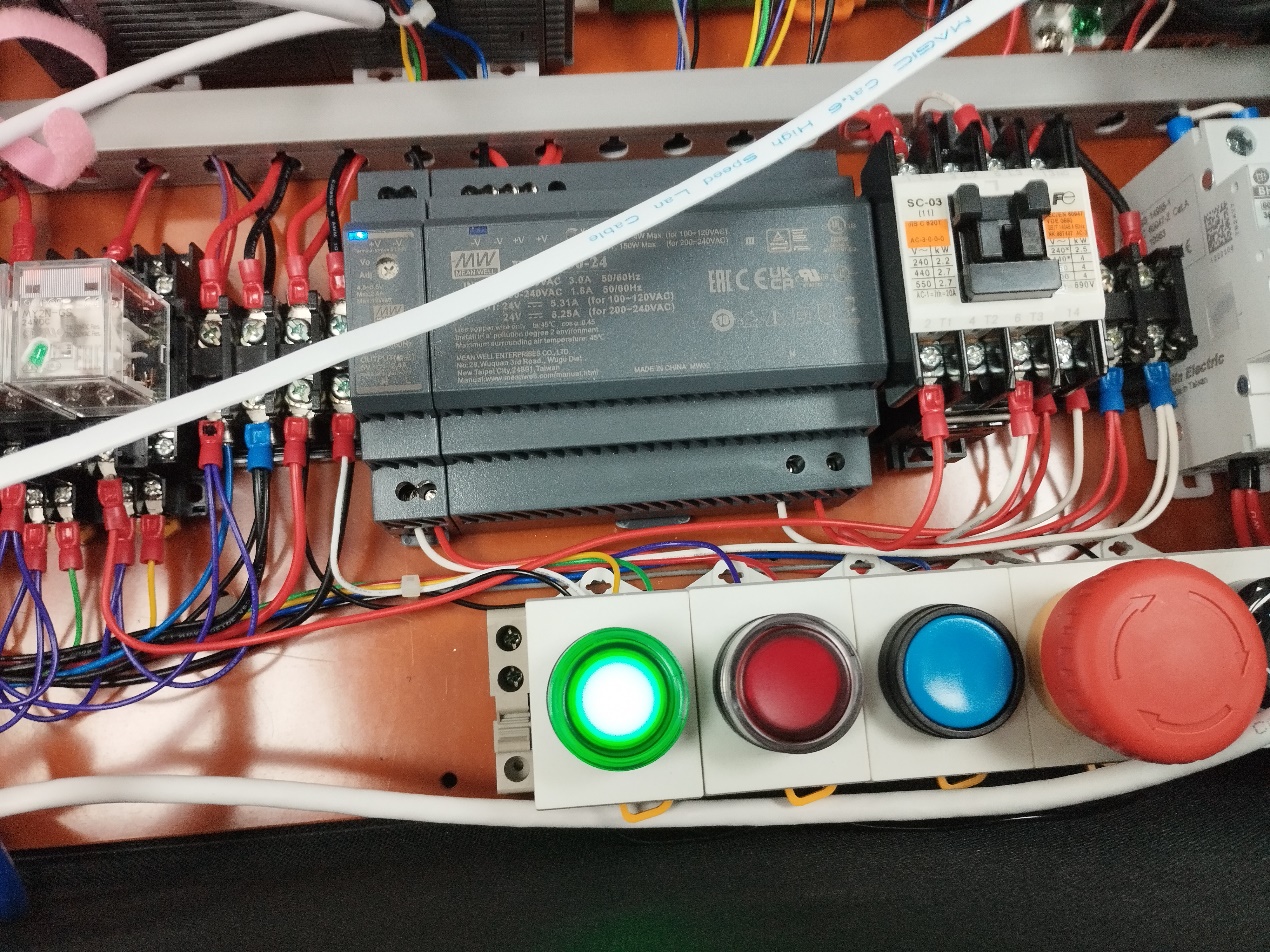
掃描好後即可選擇Server和Client所屬IP



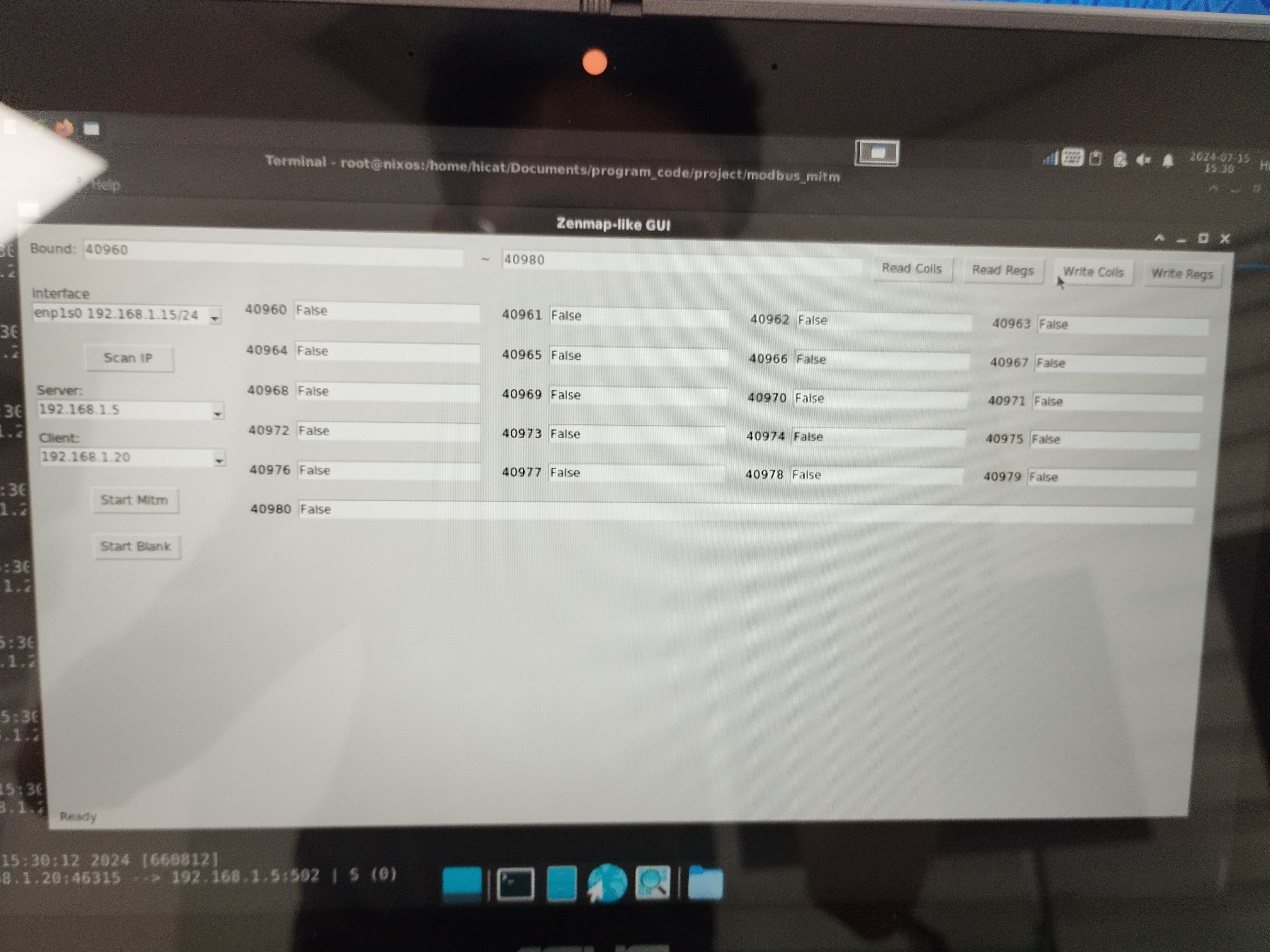
選擇好後就可以使用數據讀取寫入與中間人兩項功能



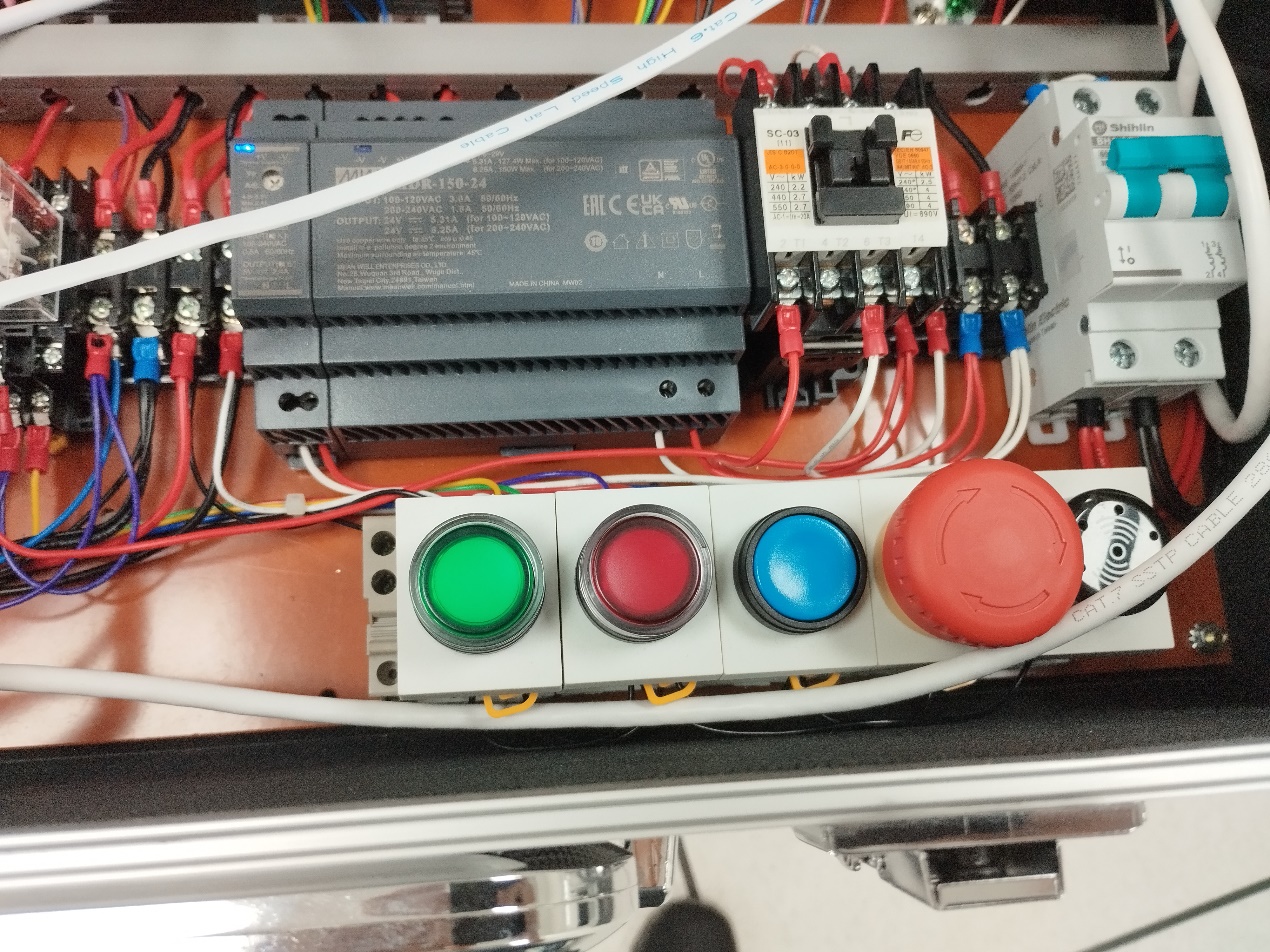
讀取Server中的coil資料可發現地址40969的數據為True(此地址記錄綠色按鈕為亮起還是關閉，此時為True代表亮起)



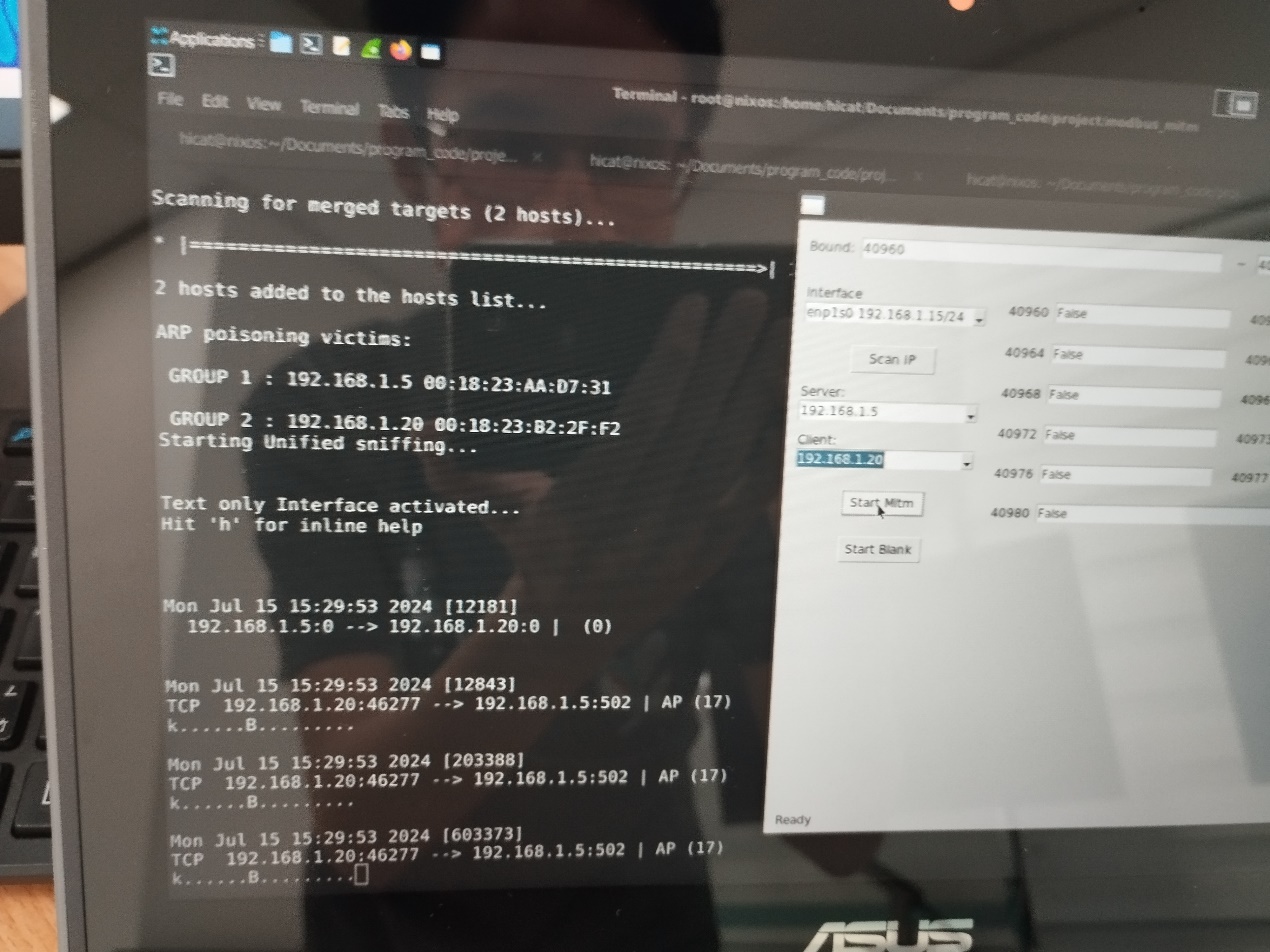
觀察工控箱也可發現綠色按鈕此時為亮起



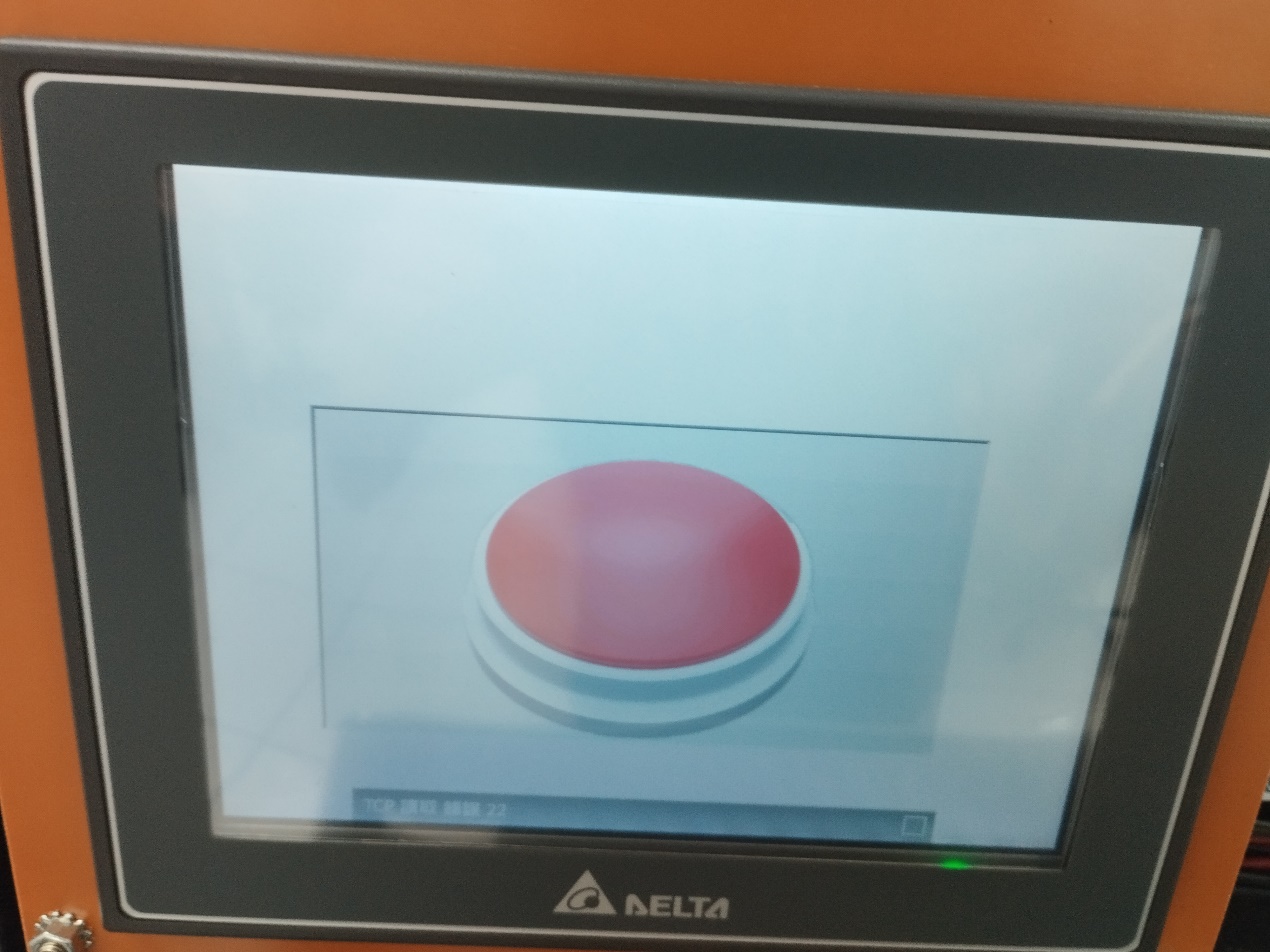
通過直接修改上面數據並上傳即可進行數據竄改(將地址40969數據改為False代表關閉)



上傳成功後即可觀察到工控箱中的綠色按鈕關閉



接下來測試中間人攻擊，當設定好Server和Client後即可按下Start mitm，可以從終端中看見執行成功與否



此時觀察工控的HMI會發現已與PLC連線失效，此時HMI中的操作都無法控制到綠色按鈕，但攻擊工具包還是能讀取與控制PLC中的數據，此功能可以防止攻擊者的篡改遭到管理者使用HMI修復

以上為完整的OT攻擊工具包功能展示。

1. **成果**

**專題github倉庫:** [**https://github.com/TriangleSnake/modbus\_mitm**](https://github.com/TriangleSnake/modbus_mitm)

以下為使用方式與須知，也可在倉庫中的README.md文件中取得:

**modbus\_mitm**

modbus\_mitm 是一個工業控制（OT）網路連線的攻擊工具包，針對 modbus 協議進行竊聽與竄改等功能等功能

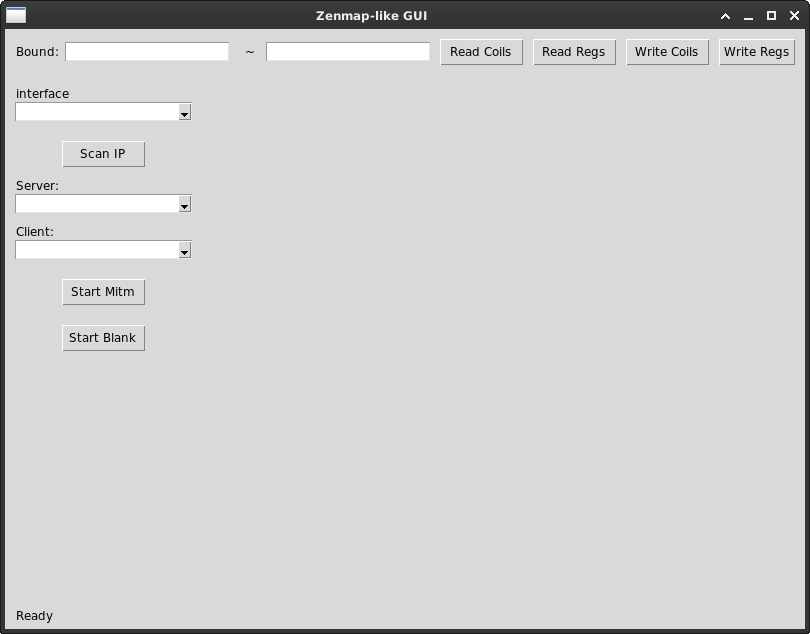
* **使用須知**

1. **Requirement**
   1. python 套件
      * tkinter
      * psutil
      * pyModbusTCP
      * scapy
   2. 外部工具
      * Nmap
      * Ettercap
2. **開啟方式**

程式還處於開發初期，須照著只是使用，否則可能會出現錯誤

**python main.py**

執行後將會開啟下方視窗



啟動後選擇 interface 並按 Scan IP，左下角的 Ready 會轉成 Scanning...，等到變回Ready即可在 Server 和 Client 選擇掃描到的 IP。

當選擇好 Server 就可以使用上方列的Server功能，填入 Bound 並選擇要讀取 coil 或 register，按下後及會在右下角空白處生成列表顯示左邊界到右邊界內的 coil 或 register 數據，可以直接修改其上面的數據（coil 請輸入 True、1 或 False、0，register 請輸入整數），填好要修改的數據後，即可按 Write Coils 或 Write Registers（Coils 或 Registers 須與讀取時一致）。

選擇好 Server 和 Client 後，即可按下 Start Mitm，此時會啟動 Server 和 Client 的中間人攻擊，並將 Client 發出的封包進行屏蔽。

Start Blank 預定是讓 Client 與 Fake Server 進行連線，但還未製作完成。