中華大學

專題製作期末報告

電腦防毒軟體輔助系統

系所別：資訊工程學系

學號姓名：B10002059 李瑋哲、B10002085 呂宗霖

指導教授：劉懷仁 副教授

中華民國 一百零 四 年 一 月

摘要

隨著網際網路快速的發展，電腦病毒/網路攻擊的演化也日新月異，電腦病毒快速的傳播、變異、流竄於網路之間，因此如何抵擋電腦病毒/惡意攻擊成為資訊安全重要的議題。大多數防毒軟體系統是根據其資料庫現有的病毒資料、特徵來掃描電腦內部或封包內容，與其資料庫內容做比對以揪出潛藏的不速之客，但是，防毒軟體之更新速度往往不及電腦病毒/惡意攻擊的快速演進。此外，絕大多數的防毒軟體並不會告知使用者目前正在遭受網路上的惡意攻擊，而多數使用者也不知道該如何去判別通訊環境是否安全，若使用者仍然照常使用網路來交換、分享、下載資訊，在這種被惡意攻擊的通訊環境下，使用者身處險境，系統弱點因此很容易遭受攻擊而被入侵。於是本計畫提出了「電腦防毒軟體輔助系統」，透過監聽網路訊息交換時所傳送/接收的封包，逐一比對其封包內容，查驗並記錄該 IP 位址、時間. . .等多項資訊，告知網路使用者被攻擊入侵電腦的潛在危險性，防止不肖人士利用惡意攻擊侵犯使用者的隱私權。本程式針對可能危及資訊安全的讀或病毒入侵的寫兩動作亦會加以偵測並提出警訊。

目錄

圖目錄

第一章 研究背景與動機

在網路蓬勃發展的現今，電腦病毒快速的傳播、變異、流竄於網路之間，因此如何抵擋電腦病毒/惡意攻擊成為資訊安全重要的議題。一般使用者的防毒軟體並不會告知使用者當下使用的通訊環境是否安全，更甚的是，許多使用者皆已安裝防毒軟體，但仍被所屬公司/單位資安中心告知系統已中毒或被當作網路攻擊跳板。為了讓使用者能具體瞭解其所處網路環境的安全性，因此本計畫提出了「電腦防毒軟體輔助系統」，此計畫並非取代電腦中原有的防毒軟體，而是用來輔助電腦防毒軟體不足之處。

電腦病毒/惡意攻擊主要仍倚賴技術已相當成熟的防毒軟體，本計畫主要提供的是一個即時警示且友善查詢的介面。

本計畫研究電腦病毒多種攻擊模式，分析封包內容有無夾帶惡意資訊碼透過通訊寄生於通訊環境中，告知網路使用者被攻擊入侵電腦的潛在危險性，防止不肖人士利用惡意攻擊侵犯使用者的隱私權。本程式針對可能危及資訊安全的讀或病毒入侵的寫兩動作亦會加以偵測並提出警訊。

在封包的分析上，傳統防毒軟體僅檢查外部送進電腦內部的封包，本計畫提出之「電腦防毒軟體輔助系統」額外分析電腦內部向外送出的封包，經由「電腦防毒軟體輔助系統」的輔助，不但可以知道電腦目前正在遭受何處的攻擊，也可以檢測出電腦是否被當作網路攻擊跳板；記錄封包往返的 IP 位址、時間點、及封包交換量，具體的讓使用者知道當前通訊環境的概況，本計畫所提出的輔助系統可以輔助使用者來觀察判斷此通訊環境的安全性，更可以讓使用者自行決定是否要繼續此通訊。

圖 1.為 2014 年各大防毒軟體市佔率中，我們針對使用者市佔率最高的前四名 Microsoft Security Essentials、avast! Free Antivirus、Windows Defender、Avira Free Antivirus 等軟體，分別作 DoS、DDoS、PortScan、NetCut、Short Datagram、檔案讀寫之功能測試發現多數軟體皆無偵測與警示上述幾種功能，如圖 2 所示。因此，本專題提出一個整合性的輔助系統，讓使用者能方便了解自己身處所在環境的危險性。

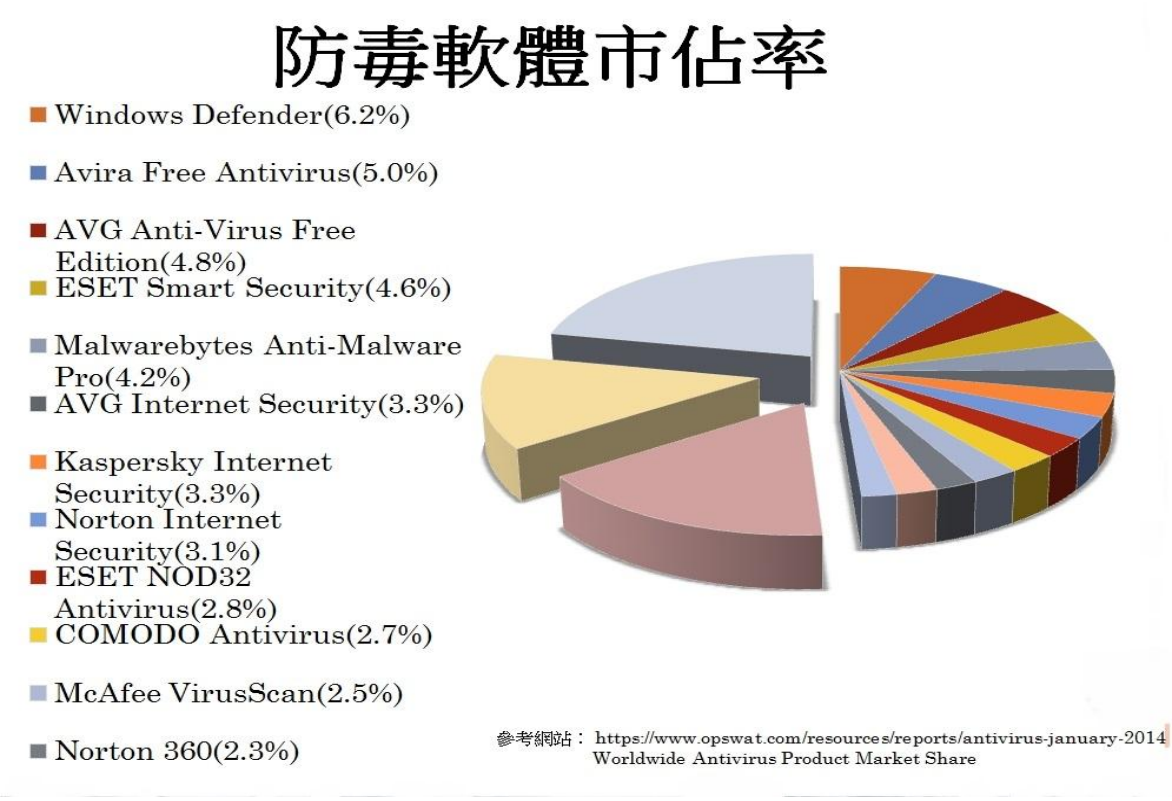

圖 1. 各大防毒軟體市佔率(2014)

軟體 / 功能	Microsoft Security Essentials	avast! Free Antivirus	Windows Defender	Avira Free Antivirus	我們的專題
DoS(IN) 偵測與警示	✗	✗	✗	✗	✓
DoS(OUT) 偵測與警示	✗	✗	✗	✗	✓
DDoS(IN) 偵測與警示	✗	✗	✗	✗	✓
DDoS(OUT) 偵測與警示	✗	✗	✗	✗	✓
PortScan 偵測與警示	✗	✗	✗	✗	✓
NetCut 偵測與警示	✗	✗	✗	✗	✓
Short Datagram 偵測與警示	✗	✗	✗	✗	✓
檔案讀寫 偵測與警示	✗	✗	✗	✗	✓

圖 2. 前四大防毒軟體目標功能比較

第二章 研究方法

Step 1. 研究通訊協定運作方式及封包格式。

Step 2. 定義所謂的攻擊：先定義已知的惡意攻擊如 DOS、DDOS、連線劫取、Spoofing ...，以 DOS/DDOS 為例，根據其攻擊行為，量化單位時間內封包接收量臨界值為 α，當單位時間內封包接收量 > α 時，則會跳出警示告知使用者目前通訊環境狀況，而 α 可由使用者自由變更。後續會有補充說明。

Step 3. 定義未知攻擊：通常封包內容都會帶有寫入這個動作相關的語法，截取封包逐一檢查其內容是否有 Write 這個動作指令，針對不同語言程式(Ajax, JavaScript)可能寫法也有所不同。個資的竊取則與 Read 動作指令有關。

Step 4. 撰寫監聽封包程式：程式內容包含 IP 位置、建立通訊方向、時間點、封包交換量、封包進出方向。並加入已定義的惡意攻擊內容、模式、語法等。提出警示，告知使用者，幫助使用者瞭解身處通訊環境目前的概況，並且讓使用者可自行決定是否繼續與該 IP 建立連結。

Step 5. 在環境下利用惡意攻擊行為多次重複實驗測試、並且校正程式錯誤和缺點，察看記錄每次實驗後的結果。

Step2 定義所謂的攻擊之補充說明：在惡意攻擊上，目前已納入考量的包含 DOS(Denial of Service) 阻斷服務攻擊和 DDOS(Distributed Denial of Service) 分散式阻斷服務攻擊，都是透過大量的請求佔用大量網路資源，以達到癱瘓網路以及系統的目的。我們必須針對這些惡意攻擊給予量化描述以方便程式監控。

DOS 阻斷服務攻擊的主要特性是單位時間內接收同一來源地 IP 位址的封包量過大。若是中了殭屍病毒，自身變成攻擊來源，主要特性是單位時間內傳送同一目的地 IP 位址的封包量過大。

DDOS 阻斷服務攻擊的主要特性是單位時間內接收不同來源地 IP 位址的封包量過大。若是中了殭屍病毒，自身變成攻擊來源，主要特性是單位時間內傳送封包量過大。

連線劫取攻擊的主要特性是單位時間內接收同一來源地 TCP RST(reset)封包量過大。截至目前為止尚無此種殭屍病毒的報告，但本系統仍然可以給予偵測：單位時間內傳送同一目的地 TCP RST(reset)封包量過大。

Spoofing 攻擊得主要特性是扮演其他用戶或主機，透過利用 ARP Spoofing/IP Spoofing 傳送封包，要求目標電腦修改的 MAC 位址指向駭客電腦的 MAC 位址，進行資料竊取。

第三章 系統實作

3.1 系統介面

圖 3.1 使用者開啟介面有十秒鐘的初始化時間，程式在此段初始化時間用來讀取資料，並顯示到各個介面上，呈現給使用者。

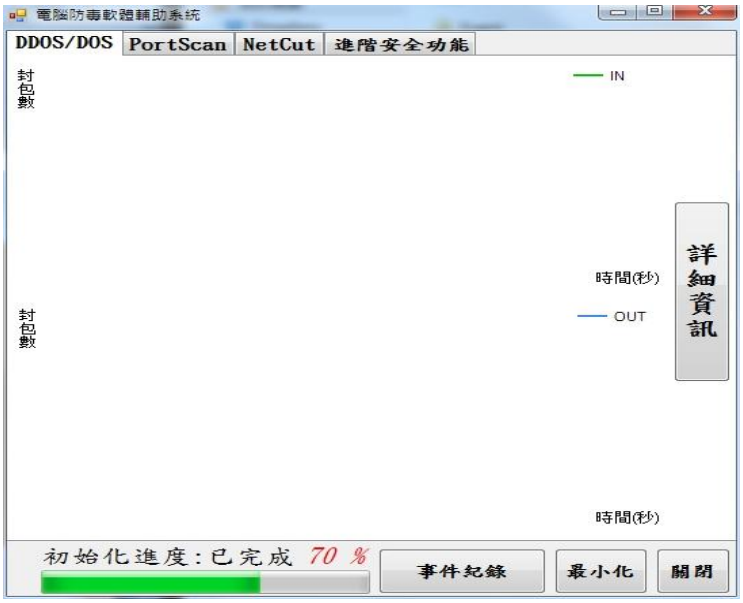

圖 3.1 初始化界面

所有曾經發生過的事件警示將被記錄在本專題之事件紀錄介面中，如圖 3.2。

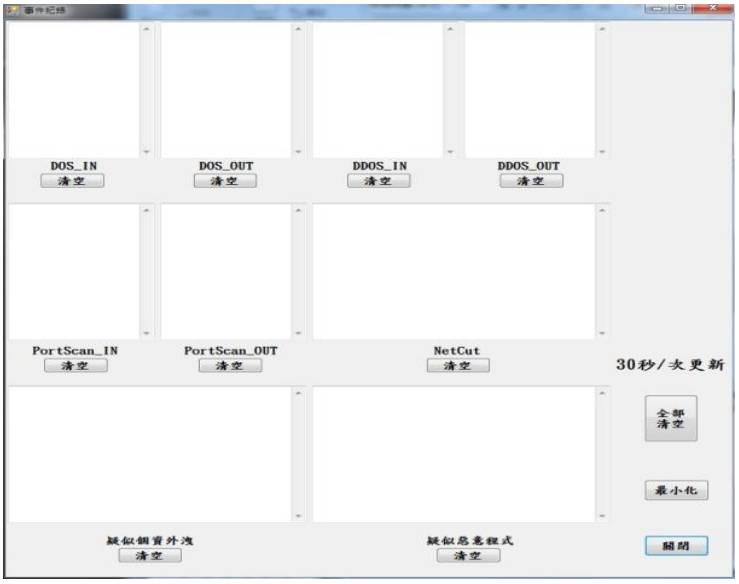

圖 3.2 事件紀錄介面

圖 3.3 為 DDoS/DoS 介面，此介面顯示目前一秒至十秒前各個時間點當下的封包接收/發送之總量。

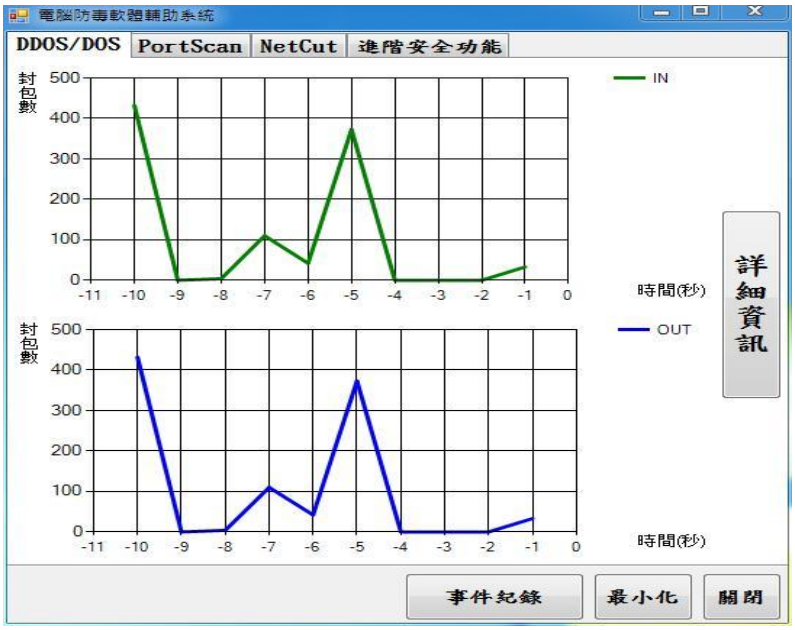

圖 3.3 DoS/DDoS 介面

圖 3.4 為 PortScan 介面，此介面 IN 方向紀錄接收的封包，他人之 IP 位址，和該 IP 位址掃描過本機埠號之數量；OUT 方向紀錄發送的封包，發送出去之 IP 位址，和本機掃瞄過該 IP 位址埠號之數量。

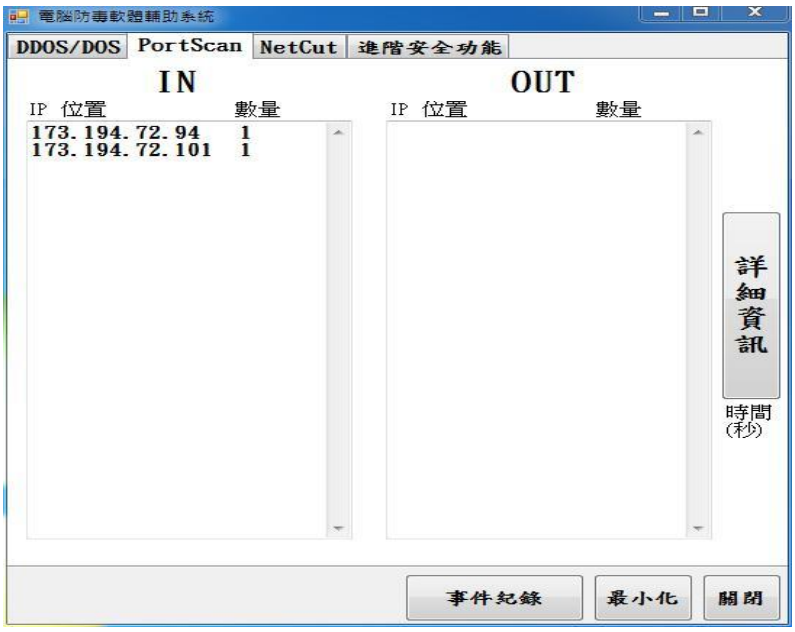

圖 3.4 PortScan 介面

圖 3.5 NetCut 介面，此介面紀錄當下發生異動的原 IP 位址和 MAC 位址。

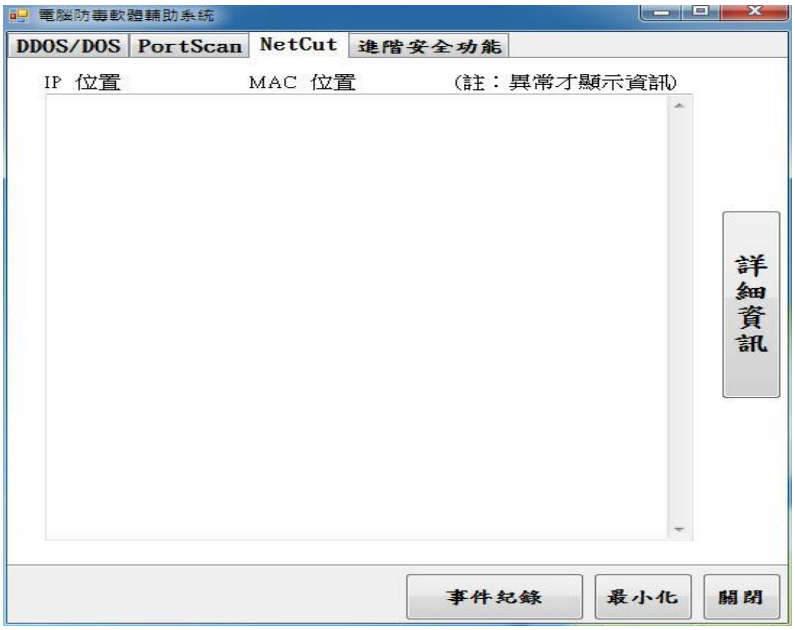

圖 3.5 NetCut 介面

圖 3.6 進階安全功能介面包含兩個部分。上半部呈現 Short Datagram 功能，呈現方式有三種，綠色表是正常狀態無偵測發現危險，黃色表示該封包大小小於 γ 值，顯示一級危險，紅色表示該封包大小小於 γ 值且符合定義特徵，顯示二級危險；下半部呈現檔案讀寫功能，綠色表示正常狀態無偵測發現危險，紅色則表示疑似危險。

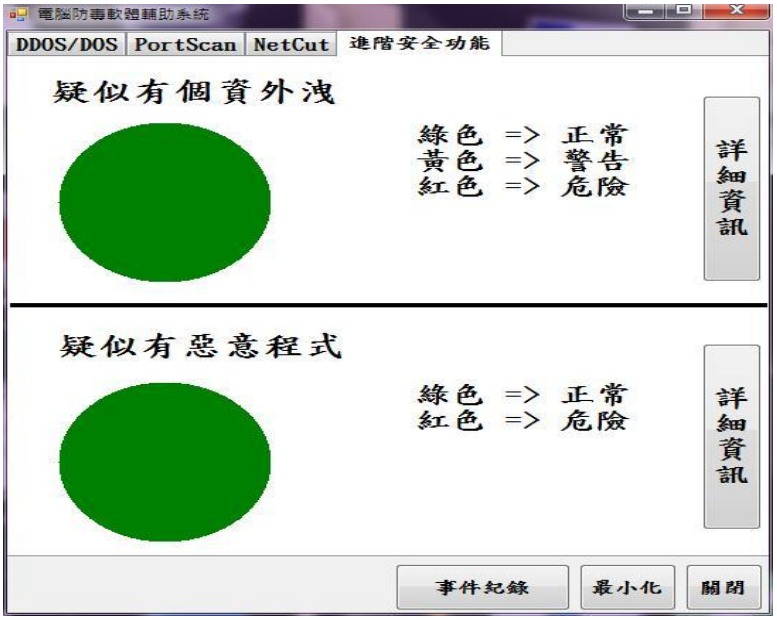

圖 3.6 進階安全功能介面

第四章 系統成果展示

4.1.1 DoS 偵測

圖 4.1 模擬被 DoS 攻擊時呈現出來的所有畫面，包含點選詳細資料，呈現主機 IP 位址和傳送/接收之封包數量，若點選事件紀錄則會顯示歷史紀錄曾遭攻擊的時間點。

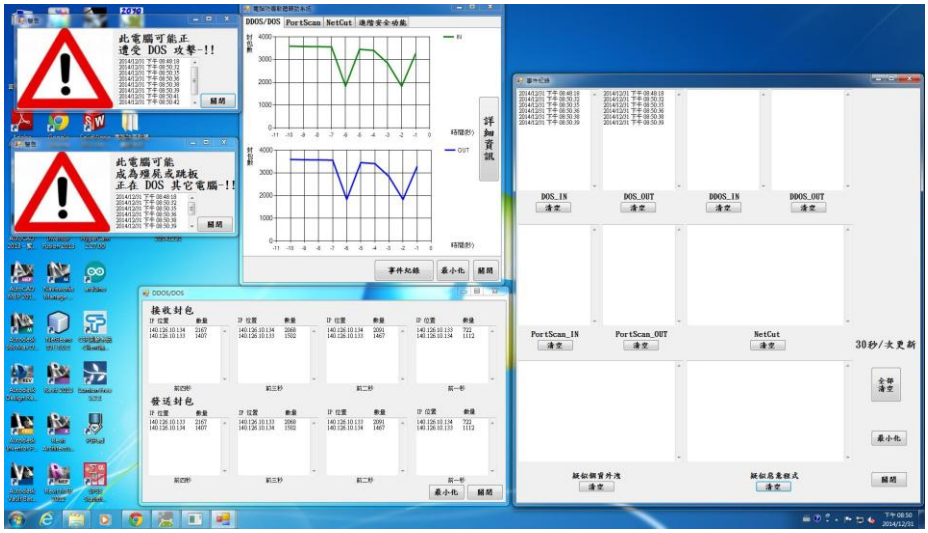

圖 4.1 DoS 全畫面截屏

若點選圖 4.1 之詳細資訊，則出現圖 4.2，內容顯示個別主機 IP 位址，和該 IP 位址發送/接收本機之封包數量。

圖 4.2 DDoS/DoS 接收和發送封包介面

若接收的封包量大於定義臨界值α且來自同一主機，則會顯示如圖 4.3 之警示

圖 4.3 遭受 DoS 攻擊警示圖

若發送的封包量大於定義臨界值α且來自同一主機，則會顯示如圖 4.4 之警示

圖 4.4 可能成為跳板正在 DoS 他人電腦警示圖

若點選圖 4.1 之事件紀錄圖則出現 4.5 事件紀錄介面，內容呈現所有曾經被攻擊過之發生時間點。

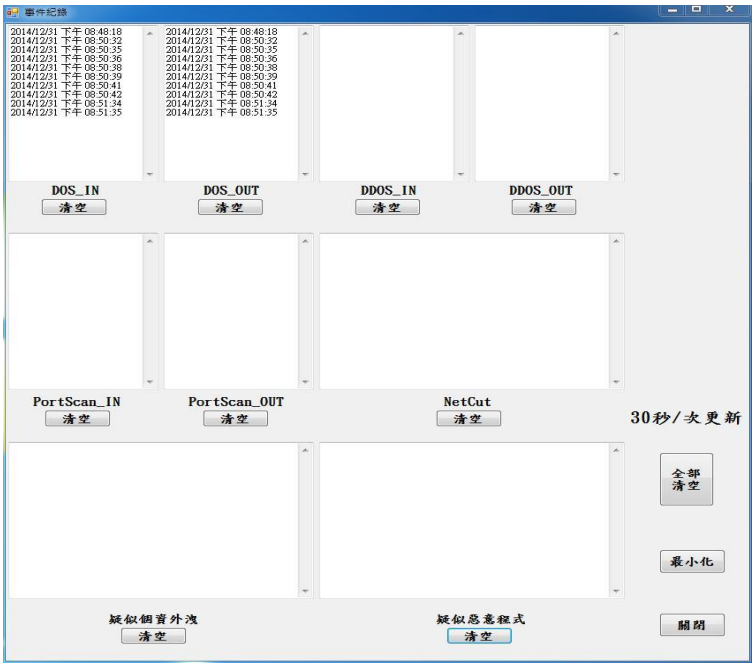

圖 4.5 DoS 事件紀錄介面呈現

4.1.2 DDOS 偵測

圖 5.1 模擬遭受 DDoS 攻擊時呈現出來的所有畫面，包含點選詳細資料，則出現個別主機 IP 位址和傳送/接收之封包數量，若點選事件紀錄則會顯示歷史紀錄曾經遭受攻擊的各個時間點。

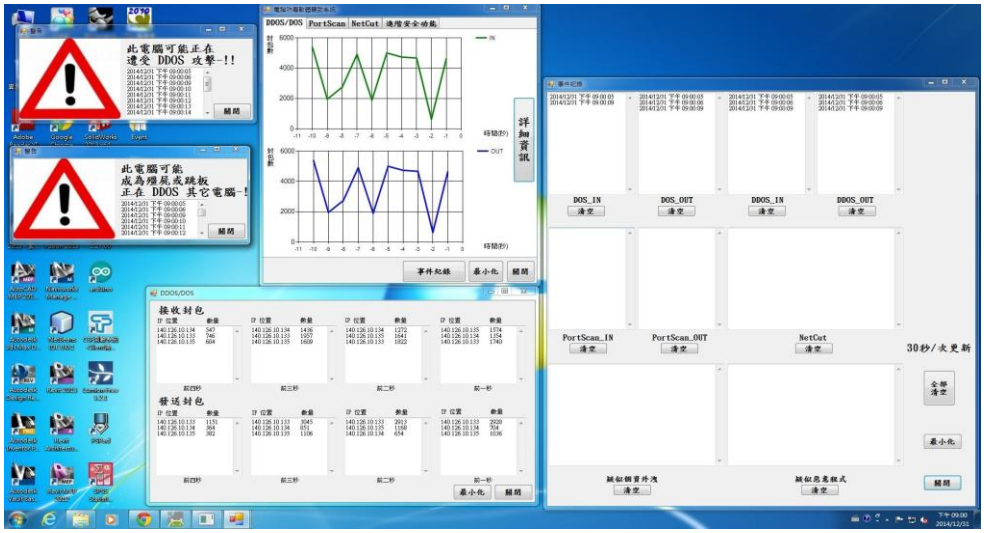

圖 5.1 DDoS 全畫面截屏

若點選圖 5.1 之詳細資訊，則出現圖 5.2，內容顯示個別主機 IP 位址，和該 IP 位址發送/接收本機之封包數量。

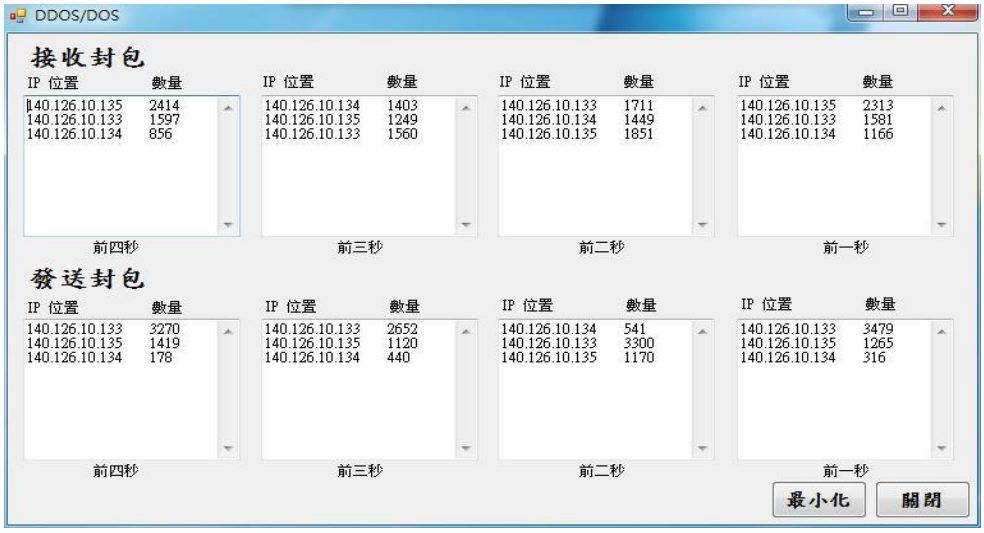

圖 5.2 DDoS/DoS 接收和發送封包介面

若來自不同主機，但接收的封包總量大於定義臨界值α，則會顯示如圖 5.3 之警示。

圖 5.3 遭受 DDoS 攻擊警示圖

若發送的封包總量大於定義臨界值α，則會顯示如圖 5.4 之警示。

圖 5.4 可能成為跳板正在 DDoS 他人電腦警示圖

若點選圖 5.1 之事件紀錄圖則出現 5.5 事件紀錄介面，內容呈現所有曾經被攻擊過之發生時間點。

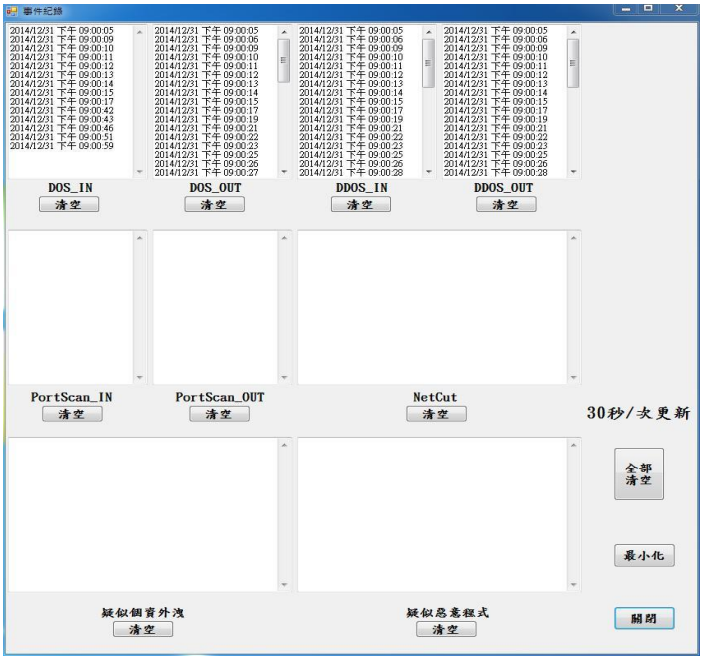

圖 5.5 DDoS 事件紀錄介面呈現

4.1.3 PortScan 偵測

圖 6.1 模擬遭受 PortScan 攻擊時呈現所有的畫面，包含點選詳細資料，則出現個別主機 IP 位址和掃描/被掃描過的埠號總數量，若點選事件紀錄則會顯示歷史紀錄曾經遭受攻擊的各個時間點。左圖為 Wireshark 軟體，用來比對 PortScan 資料是否有誤。

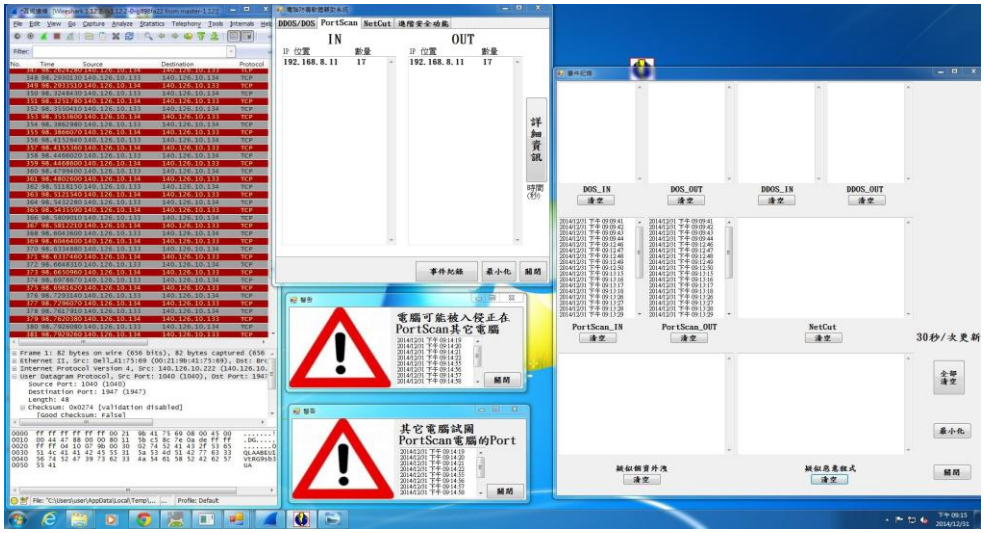

圖 6.1 PortScan 全畫面截屏

若點選圖 6.1 之詳細資訊，則出現圖 6.2，內容顯示個別主機 IP 位址，和該 IP 位址掃描/被掃描之埠號總數量。

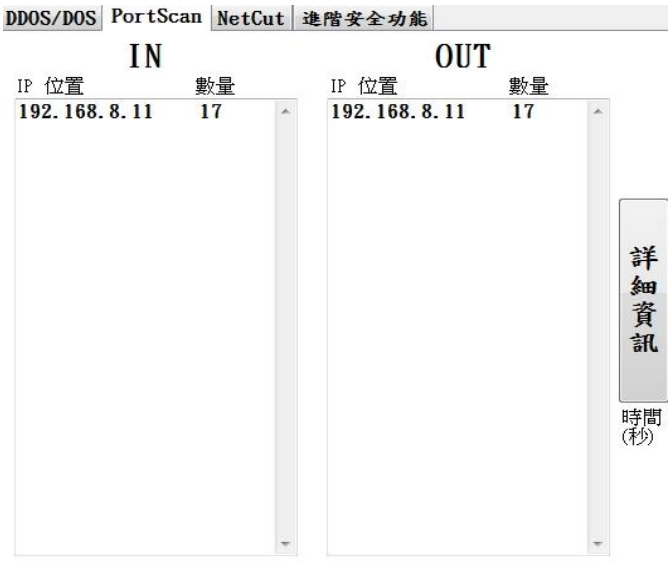

圖 6.2 PortScan 詳細資訊介面

單位時間內他人電腦掃描本機埠號總數量大於 β ，則會顯示如圖 5.3 之警示。

圖 6.3 本機可能被 PortScan 警示圖

圖 6.3 表示本機可能成為跳板，單位時間內掃描他人電腦埠號總數量大於 β

圖 6.4 本機 PortScan 他人電腦警示圖

若點選圖 6.1 之事件紀錄圖則出現 6.5 事件紀錄介面，內容呈現所有曾經被攻擊過之發生時間點。

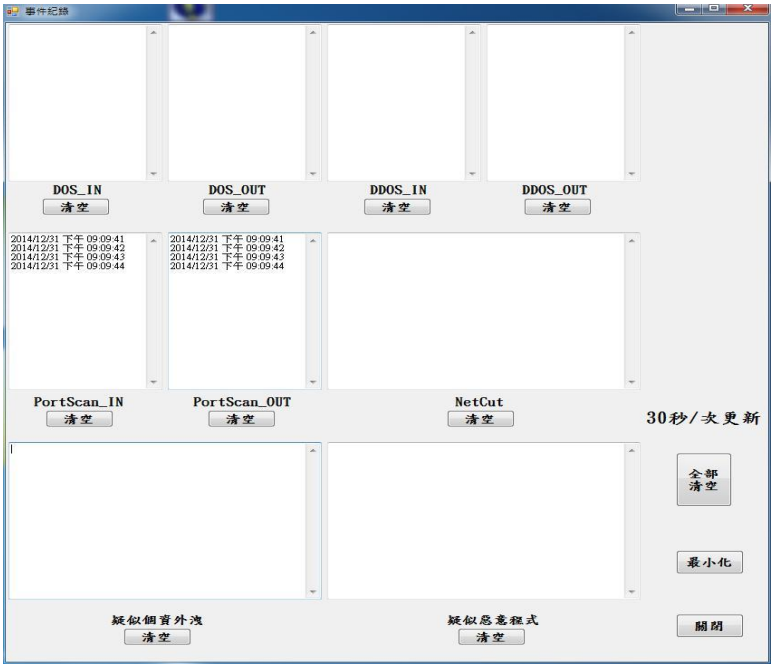

圖 6.5 PortScan 事件紀錄介面呈現

4.1.4 NetCut 偵測

圖 7.1 模擬遭受 NetCut 攻擊時呈現出來的所有畫面，包含點選詳細資料，則出現個別主機 IP 位址和相對應的 MAC 位址，若點選事件紀錄則會顯示歷史紀錄曾經遭受攻擊的各個時間點。

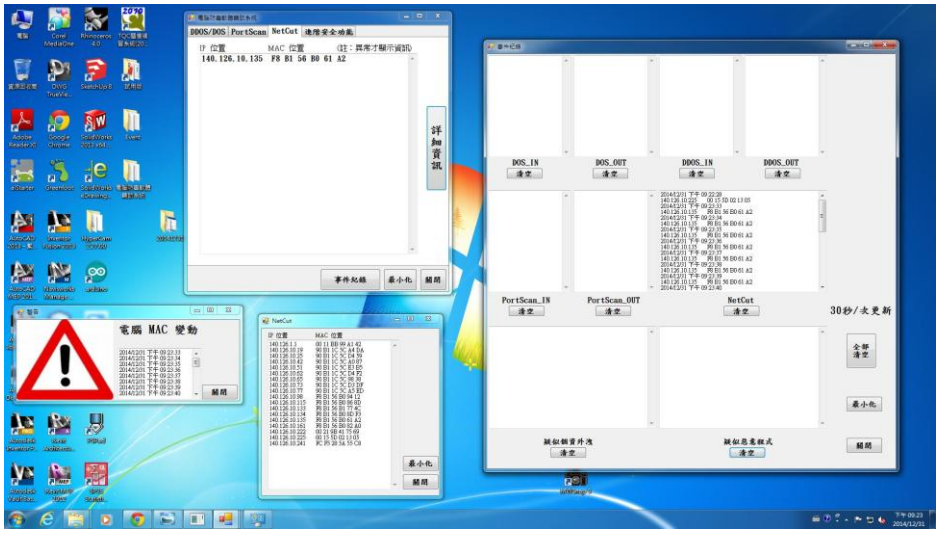

圖 7.1 NetCut 全畫面截屏

若點選圖 7.1 之詳細資訊，則出現圖 7.2，內容顯示個別主機 IP 位址和 MAC 位址。

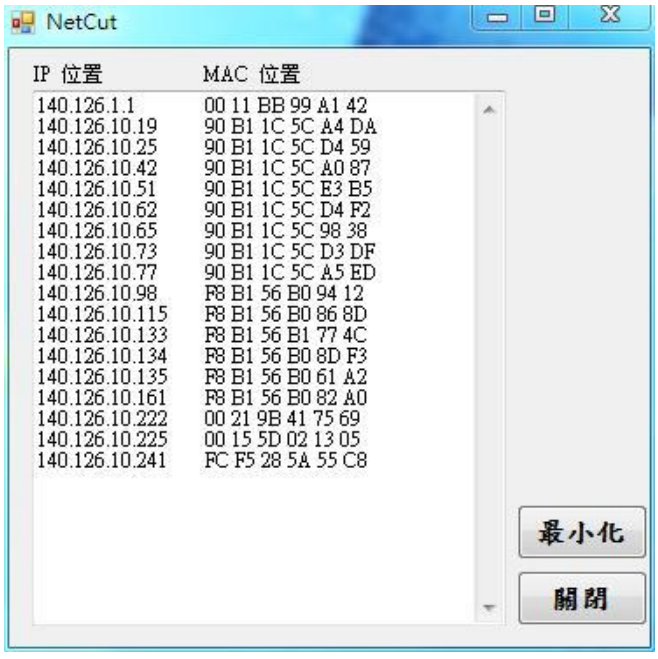

圖 7.2 NetCut 詳細資訊介面

當 IP 位址和 MAC 位址對應關係發生異動時，顯示此一警示，如圖 7.3 所示。

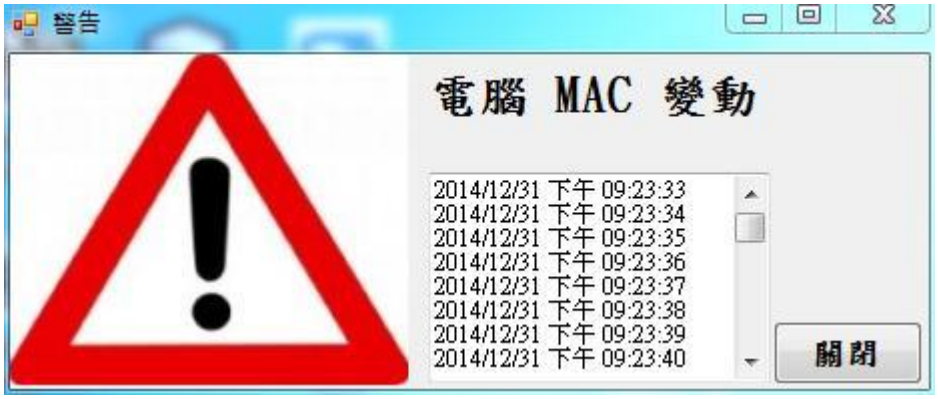

圖 7.3 IP 和 MAC 位址異動警示圖

若點選圖 7.1 之事件紀錄圖則出現 7.4 事件紀錄介面，內容呈現所有曾經被攻擊過之發生時間點。

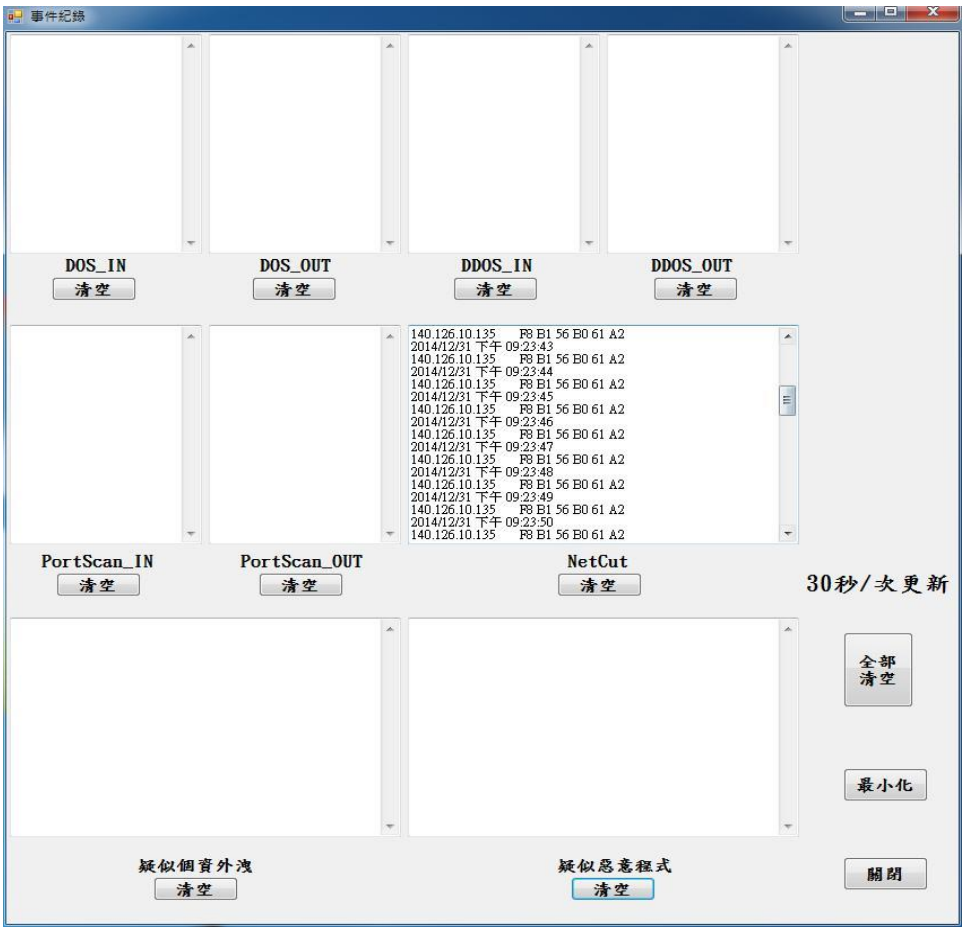

圖 7.4 NetCut 事件紀錄介面呈現

4.1.5 小量資料偵測

圖 8.1 模擬遭受 Short Datagram 攻擊時呈現所有的畫面，包含點選詳細資料，則出現發生事件的檔案名稱，若點選事件紀錄則會顯示歷史紀錄曾經遭受攻擊的各個時間點和發生疑似之檔案名稱。

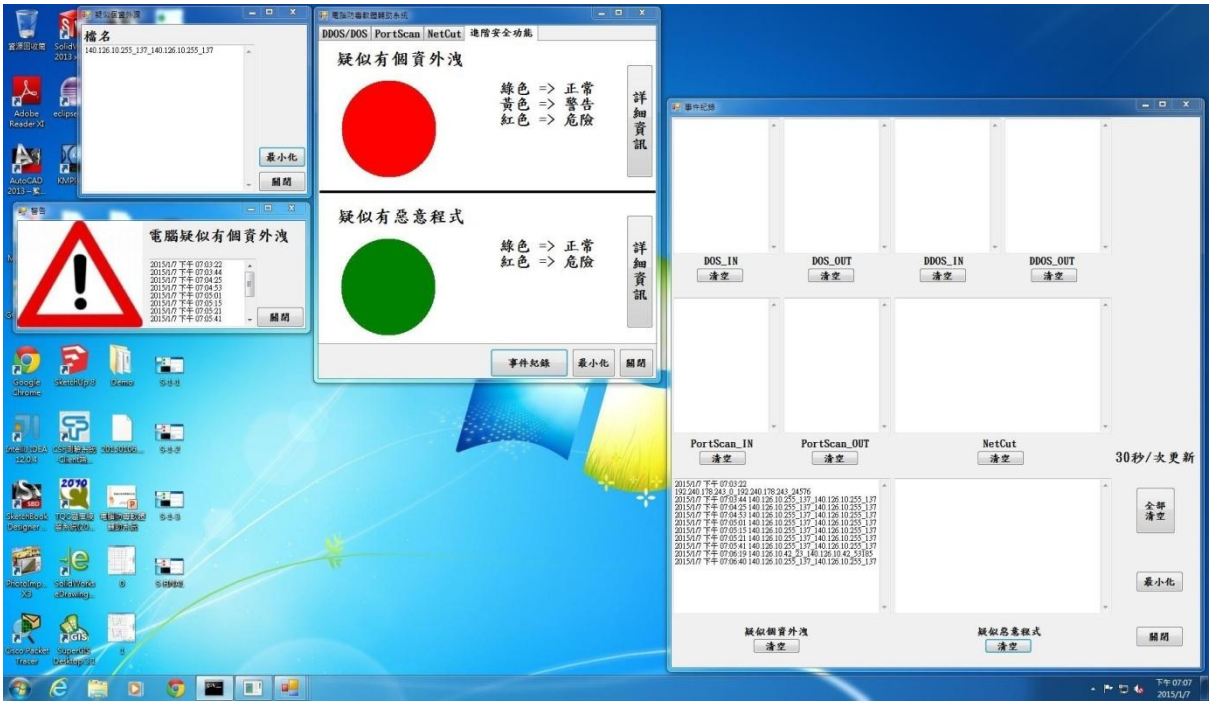

圖 8.1 Short Datagram 全畫面截屏

圖 8.2 上半部為 Short Datagram 介面，顯示黃色表示封包大小小於 γ ，但無符合定義特徵時，顯示黃色警告。

圖 8.2 Short Datagram 黃色警告圖

圖 8.3 上半部為 Short Datagram 介面，顯示紅色表示封包大小小於 γ ，並且符合定義特徵時，顯示紅色警告。

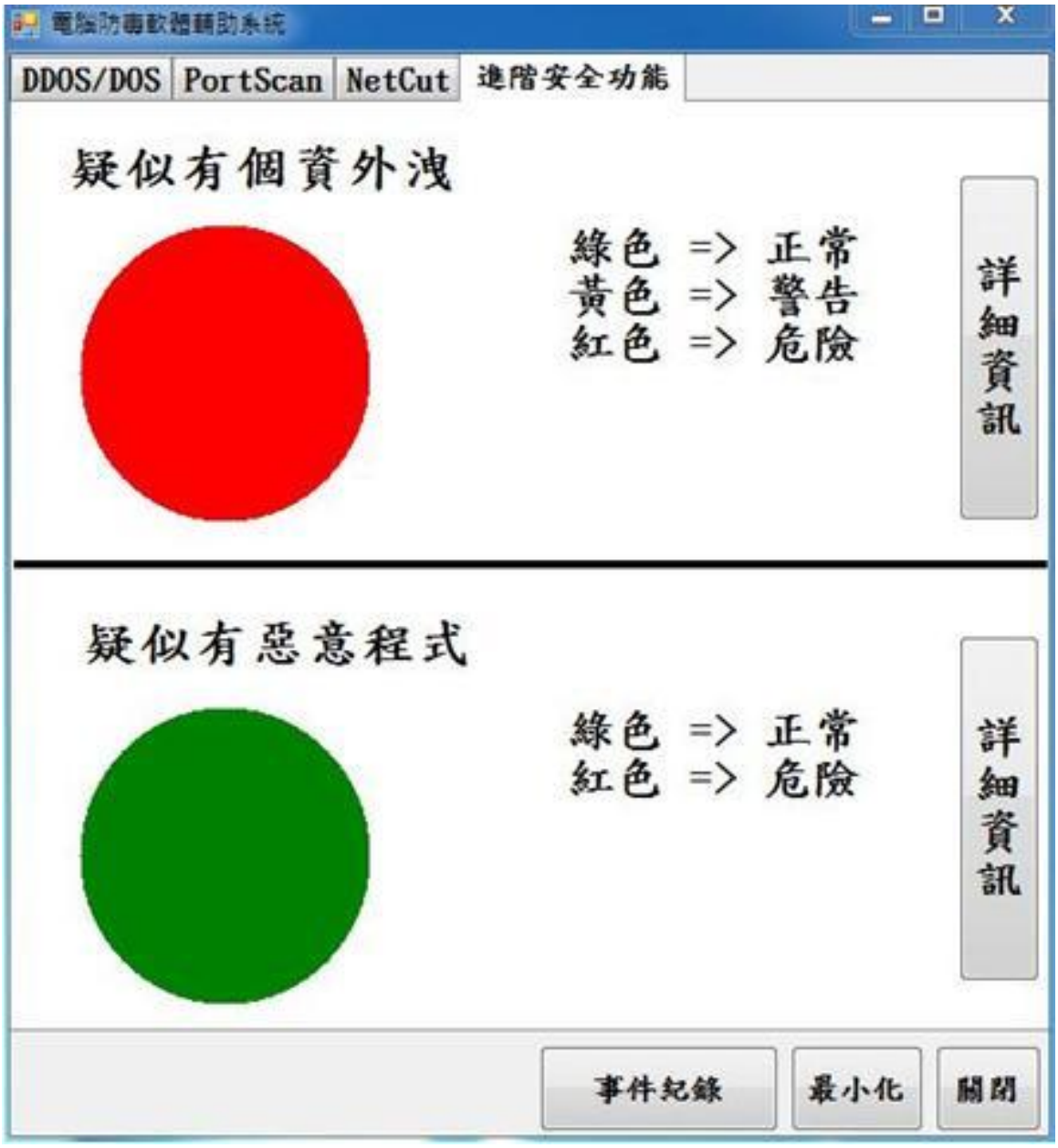

圖 8.3 Short Datagram 紅色警告圖

當有封包大小小於γ且符合定義特徵時，顯示此一警示，如圖 8.4 所示。

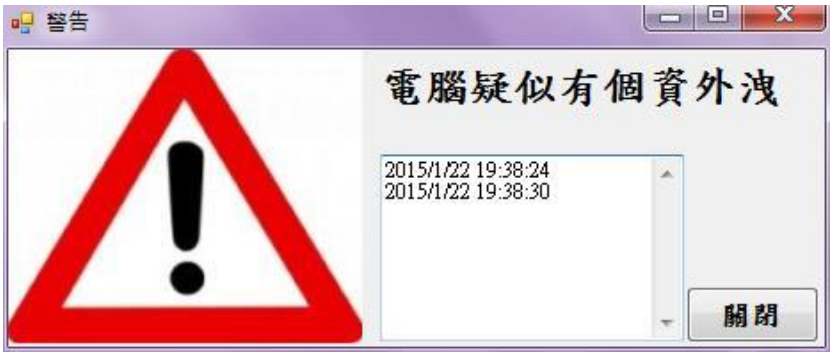

圖 8.4 有小資料封包警示圖

若點選圖 8.1 之詳細資訊，則出現圖 8.5，內容顯示疑似個資外洩的檔案名稱

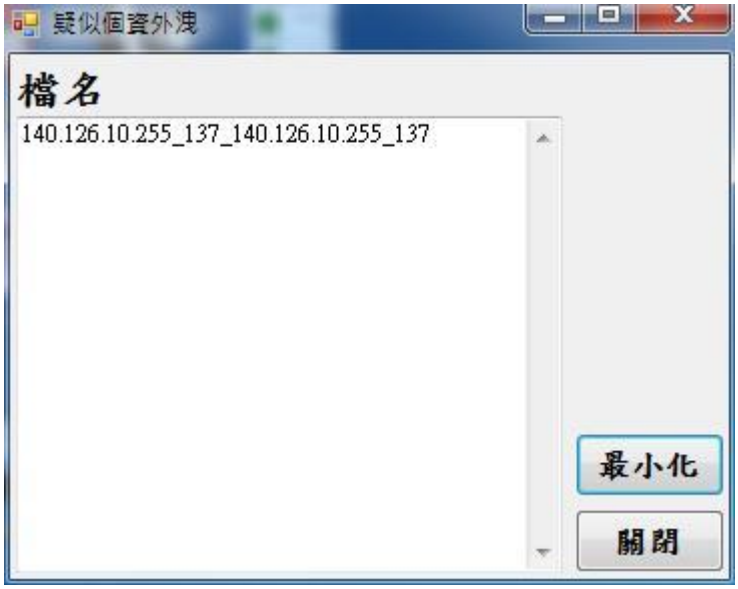

圖 8.5 Short Datagram 詳細資訊介面

若點選圖 8.1 之事件紀錄圖則出現 8.6 事件紀錄介面，內容呈現所有曾經被攻擊過之檔案名稱。

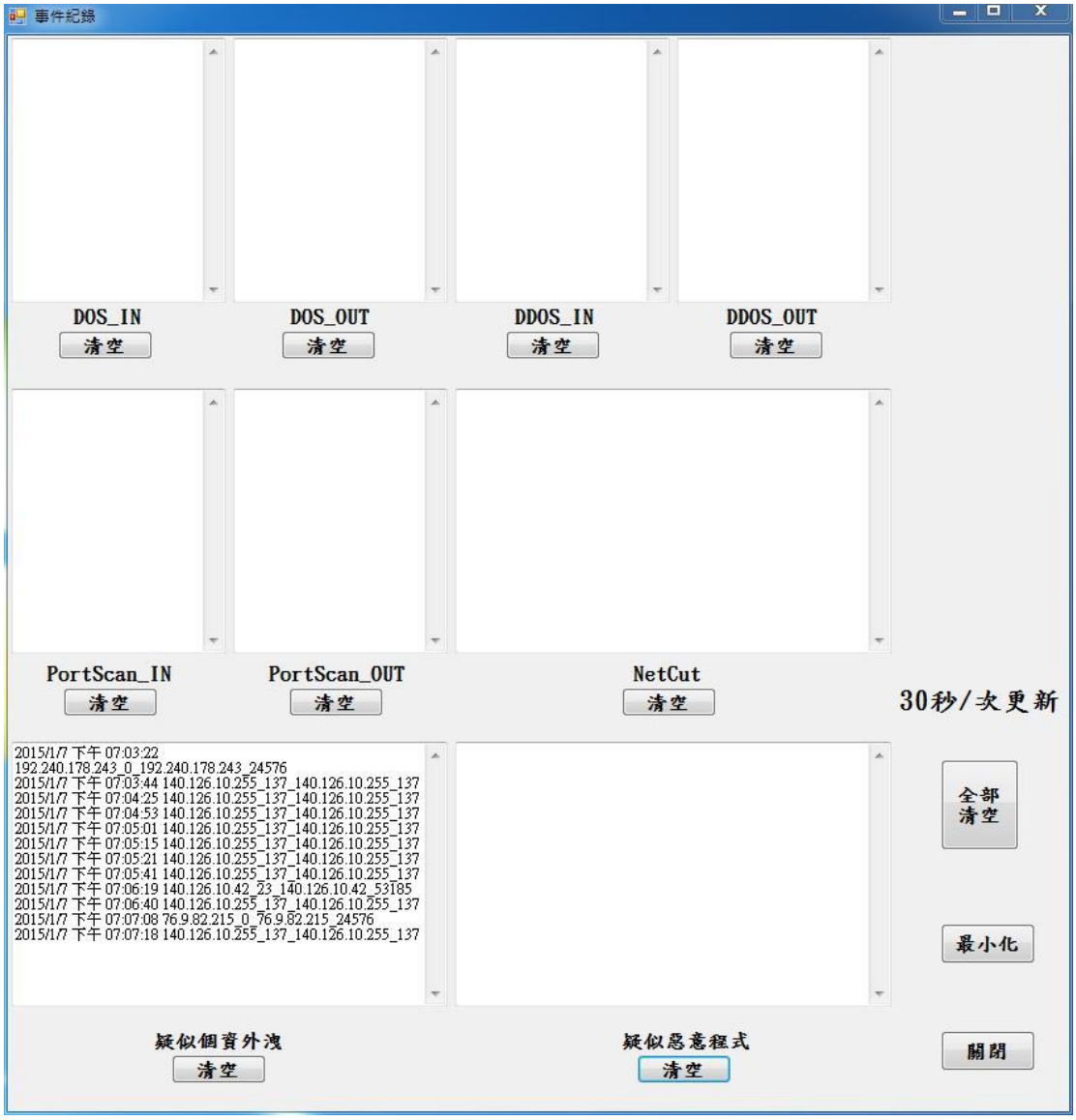

圖 8.6 Short Datagram 事件紀錄介面呈現

4.1.6 檔案讀寫偵測

圖 9.1 模擬發生檔案讀寫時呈現所有的畫面，包含點選詳細資料，則出現發生事件的檔案名稱，若點選事件紀錄則會顯示歷史紀錄曾經遭受攻擊的各個時間點和發生疑似之檔案名稱。

圖 9.1 檔案讀寫全畫面截屏

圖 9.2 下半部為檔案讀寫介面，當偵測到定義特徵時，顯示紅色發出警告。

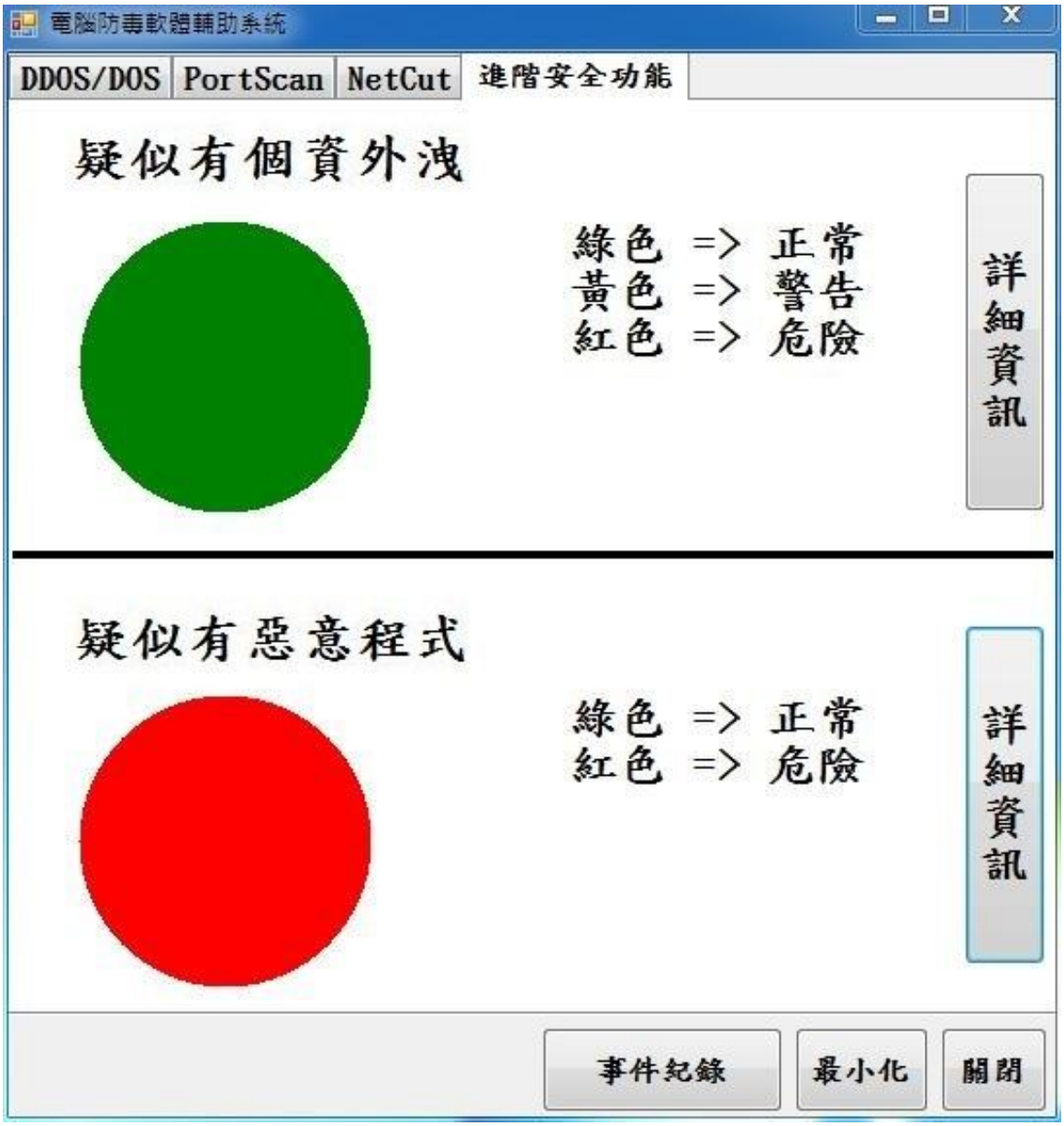

圖 9.2 檔案讀寫紅色警告圖

當封包內容出現開啟檔案/讀取檔案之語法偵測到定義特徵時，顯示此一警示，如圖 9.4 所示。

圖 9.3 疑似惡意程式警示圖

若點選圖 9.1 之詳細資訊，則出現圖 9.4，內容顯示並記錄疑似惡意程式的檔案名稱

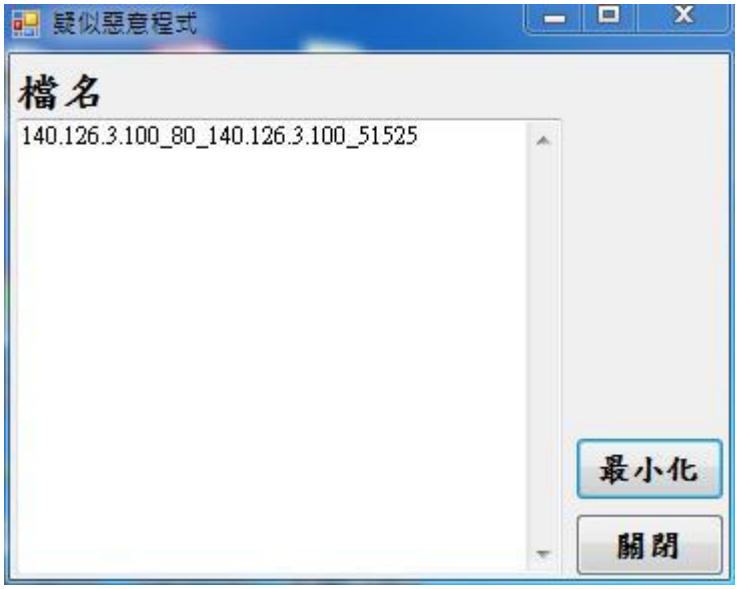

圖 9.4 Short Datagram 詳細資訊介面

若點選圖 9.1 之事件紀錄圖則出現 9.5 事件紀錄介面，內容呈現所有曾經被攻擊過之檔案名稱及時間點。

圖 9.5 檔案讀寫事件紀錄介面呈現

第五章 結論與未來展望

許多使用者皆已安裝防毒軟體，但仍被所屬公司/單位資安中心告知系統已中毒或被當作網路攻擊跳板。本計畫提出了「電腦防毒軟體輔助系統」，此系統並非取代電腦中原有的防毒軟體，而是用來輔助電腦防毒軟體不足之處。

電腦病毒/惡意攻擊主要仍倚賴技術已相當成熟的防毒軟體，本計畫主要提供的是一個即時警示且友善查詢的介面。

本計畫所提出的「電腦防毒軟體輔助系統」將可以輔助電腦防毒軟體揪出潛在危險性的通訊環境，將會逐一提出警示告知使用者，讓使用者能瞭解當下所處通訊環境之安全性。除此之外，利用本程式所收集到之網路行為，亦可作為未來研究電腦病毒/惡意攻擊的幫助。

檔案讀寫的 method/function 若有加密則無法被本程式偵測內容。

進階功能中之偵測與警示可能會產生誤報，由於大部分正常網頁執行檔案讀寫應會出現選單。供用戶確認，所以在正常情況下，此一誤報只會引起操作上的困擾，在未來可能的改善方式上，則可能將此區分開，減少誤報情形。

在 Short Datagram 偵測與警示上，亦可能產生誤報，但現行大部分的應用，很少有少量資料量傳輸，所以此一誤報應為罕見，惟資料超出臨界值的竊取，無法被偵測出來。

參考文獻

[1] 顏新晨，“行為比對感知技術之於網路攻擊漏洞偵測”，臺灣大學，碩士論文，民國一百年

[2] 郭溥村，“殭屍網路攻擊路徑的重建與分析”，崑山科技大學，碩士論文，民國九十九年

[3] 劉恩榜，“Android 上的殭屍網路攻擊偵測”，交通大學，碩士論文，民國一百年

[4] 李俊祥，“智慧型網路攻擊模式之研究”， 國防大學中正理工學院，碩士論文，民國九十一年

[5] 林昭名，“部署分散式虛擬蜜網偵測網路攻擊”，佛光大學，碩士論文，民國九十九年

[6] 許浩屏，“植基於網路攻擊行為模式進行數位蒐證機制之研究”，國防大學管理學院，碩士論文，民國九十八年六月

[7] 王品鈞，“無線區域網路攻擊與防禦機制之設計與實作”，長庚大學，碩士論文，民國九十九年七月

[8] 何俊德，“偵測網際網路攻擊之基於熵的網路行為模式建立演算法”，交通大學，碩士論文，民國九十七年

[9] 李政廣，“網路攻擊來源追蹤技術應用之研究”，樹德科技大學，碩士論文，民國九十八年六月

[10] 李慶憲，“網際網路攻擊來源回溯之研究—分段式機率封包標記”，中央警察大學，碩士論文，民國九十四年

[11] 許曉青，“網際網路攻擊來源回溯之研究”，中央警察大學，碩士論文，民國九十三年

[12] 莊伯言，“不同類型網路攻擊對樹狀多重播送行動隨意網路之影響研究”，中國科技大學，碩士論文，民國九十六年七月

[13]陳崇葦，“於 Ad-hoc 感應器網路系統上使用 Blom 方法抵抗網路攻擊”，清華大學，碩士論文，民國九十三年

[14]林玉峰，“網路攻擊與防護評比指標”， 樹德科技大學，碩士論文，民國九十三年

[15]呂智群，“XML 為基礎的網路攻擊系統設計與實作”，清華大學，碩士論文，民國九十年六月

[16]葉耀中，“XML 為基礎的狀態化網路攻擊產生器”，清華大學，碩士論文，民國九十年