國立交通大學

理學院網路學習學程

碩士論文

以 Snort 偵測並封鎖網路異常行為之研究

A Study on detecting abnormal network behaviors using Snort

研究生：吳金庭

指導教授：蔡文能　教授

中華民國九十八年六月

以 Snort 偵測並封鎖網路異常行為之研究
A Study on detecting abnormal network behaviors using Snort

研 究 生：吳金庭　　Student：Chin-Ting Wu

指導教授：蔡文能　　Advisor：Wen-Nung Tsai

國 立 交 通 大 學

理學院網路學習學程

碩 士 論 文

A Thesis

Submitted to Degree Program of E-Learning

College of Science

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Master

in

Degree Program of E-Learning

June 2009

Hsinchu, Taiwan, Republic of China

中華民國九十八年

以 Snort 偵測並封鎖網路異常行為之研究

研究生：吳金庭　　指導教授：蔡文能教授

國立交通大學理學院網路學習碩士在職專班

摘要

網路的發展越興盛，政府或企業利用網路來提供服務的頻率也越來越高。各項資料的 E 化雖帶來了不少便利，但也伴隨著各種危機。如駭客的入侵，導致學生資料外洩或成績遭到竄改等。

大部分的校園網路，通常以防火牆作為防止駭客入侵的第一道防線，但隨著網路技術的發展，駭客的攻擊方式與手法也越來越成熟且多樣化。面對層出不窮且變化多端的網路入侵攻擊，單靠防火牆的防禦是不夠的。因此，本研究以入侵偵測系統 Snort 及防火牆 Iptables 為基礎，搭配 PHP 開發出 ABBA System，協助網路管理人員有效的從眾多的警示訊息中分析出可疑的入侵行為，並透過防火牆加以封鎖。

本研究以實際在國小電腦教室所蒐集到的警示警訊，利用 ABBA System 進行統計分析，經由分析的結果，確實可以協助網路管理人員瞭解目前網路的異常狀況，藉此擬定因應的措施，以達到提升校園網路安全的目的。

關鍵字：網路安全、入侵偵測、異常行為

A Study on detecting abnormal network behaviors using Snort

student：Chin-Ting Wu　　Advisors：Dr. Wen-Nung Tsai

Degree Program of E-Learning
College of Science
National Chiao Tung University

ABSTRACT

The more prosperous development of the Internet, the higher frequency both the Government and enterprises use it to provide services. The electronization of different kinds of data in various applications has brought much convenience. However, the easy access of the Internet were accompanied with many risks, such as information leakage, system intrusion , etc.

Most of the campus networks use firewall to prevent hackers as the first line of defense. Since the approaches used by hackers have become more sophisticated and diversified with the great development of the Internet. Using firewall as the only defensive tool is not enough. Therefore, this study proposed a solid IPS and ABBA System, which utilized the network system administrator to detect suspicious intrusion effectively among abounding alerts, and furthermore blocked it by firewall.

In this study, we collected the data of invasion from the computers in computer classrooms in an elementary school. Then we employed the ABBA System to carry out statistical analysis. The result we obtained from the ABBA System did benefit the system administrators realize the present status of network anomalies and allowed them to take necessary actions ,which contributed to achieve the goal of upgrading the safety of campus .

keywords：Network Security, Intrusion Detection, Abnormal Behavior

致謝

在交大求學期間，首先要感謝蔡文能教授的諄諄教誨，讓我在研究的過程中學到了嚴謹的研究方法和正確的學習態度，使我獲益匪淺，在論文研究上由於老師的啟發與幫助，才使得本論文能夠順利完成，在此由衷的感謝。

另外，感謝所有教導過我的專班老師，由於你們的指導，讓我學習到了很多專業上的知識及研究方法。再來，要特別感謝我的同學—劉建德，有你的支援與協助，才能克服各種困境，完成此論文。同時也感謝我所服務學校的校長、主任及同事，謝謝你們在我就讀研究所期間的包容與幫助。

最後，感謝我的家人及女友虹羽，謝謝你們對我的關懷與鼓勵，在撰寫論文的這段時間，感謝你們的陪伴，謝謝你們的支持，讓我可以安心無後顧之憂的完成學業。

目錄

表目錄

圖目錄

第一章　緒論

近年來網路的蓬勃發展，改變了社會上人們的生活形態。網路的應用普及了各個領域，如：網路購物、網路交友、休閒娛樂、教育行政等等。網路的出現帶來了越來越多的便利，但也伴隨著越來越多的威脅，如：個人資料外洩、駭客入侵、病毒肆虐等等問題。如何能夠兼顧網路所帶來的方便，又能確保在瀏覽網頁的安全，預防入侵或病毒的破壞，是未來網路發展的重要課題。

教育部為推廣資訊科技融入教育，培養學生具備運用資訊科技主動學習與創新思考的基本能力，持續規劃建置校園有線與無線共構的資訊網路環境。至 1999 年，已達到所有國中小均有電腦教室，資訊課程一人一機的地步，2000 年人機比更提升至 19：1[1]。

在校園網路發展如此快速的情況下，校園網路安全及防護措施也就顯得更加的重要。如果沒有規劃好完善的安全防護措施，校園網路便容易遭到駭客的入侵威脅，或是受到病毒的破壞，尤其是現在校園中行政作業、學生資料成績大多已資訊化，若是遭到駭客入侵竊取或是病毒的破壞而毀損，將是無法估計的損失。

1.1　研究動機

隨著網際網路的盛行，校園師生使用網路的比率也隨著提高。以校園網路的使用來說，為了滿足教學所需或是學術研究，使得網路管理者對網路使用的管理比較難以落實。再者，如果校園的網路管理者對資訊安全沒有足夠的認知，學校網路不設防的暴露在不安全的環境中，常常會使得校園網路淪為駭客入侵的首要目標。

例如，常見的以「僵屍網路電腦」(botnet)的手法來控制校園網路內的電腦，來進行對特定目標的攻擊。所謂的僵屍網路即駭客利用病毒或其他的惡意程式感染電腦，取得控制權，使電腦運作看似一切正常，而使用者卻不自知。這些被控制的校園電腦成為駭客旗下僵屍網路電腦大軍的一員，被駭客操控，用以進行攻擊，執行如 DDoS 的攻擊行為[16]。

校園網路除了外部的駭客入侵的威脅之外，還有另一個威脅是來自於內部學生或行政人員的資訊安全素養不足，導致重要資料外洩或是遭到入侵。曾經發生過中部某所大學網站就曾因控管不當，使得學生的個人資料可以直接透過 Yahoo、Google 等搜尋引擎直接取得[17]。

大部分的校園網路安全防護主要都是仰賴防火牆來過濾網路的封包及阻擋威脅。而防火牆必須要能時時更新對威脅封包及來源的資料，才能達到防護的效果。

而校園網路管理者，常因為麻煩或疏忽，或是本身資訊能力不足，使得防火牆形同虛設，無法有效阻擋威脅。有些攻擊則是透過系統漏洞或是網路使用者使用電腦不小心，被植入後門程式來進行的[11]。所以防火牆的設定即使再周延也是無法防範所有的威脅。因此單單只依賴防火牆來維護校園的網路安全是不夠的。

為了提高校園網路的安全性，本研究希望能透過防火牆與入侵偵測系統結合，互相支援，互補不足，利用各自的優點，來降低網路入侵威脅的風險，以提升校園的資訊安全。

1.2 研究目的

為了能夠更完善的做好網路的安全防護，校園網路管理者能夠越早得知入侵威脅的警訊，是相當重要的。能夠及早發現並預防攻擊的發生，比事後的亡羊補牢更能夠減少損害。所以網路的管理人員，就得隨時的監測網路使用的狀況。

一般來說，網路的管理人員常透過網路的流量分析來得知目前網路的流量大小，藉以判斷網路使用的現況與提供服務的伺服器效能是否出現異常。但看似正常的流量，底下是否正有駭客在進行入侵或攻擊的動作，網路管理者並無法得知。

所以網路管理者使用入侵偵測系統（IDS），來協助瞭解網路上的封包傳輸，藉由入侵偵測系統的協助，可以早一步偵測出「惡意」的封包，向網路管理者提出「警告」，讓網路管理者在進一步的「入侵」或「危害」發生之前，能夠有足夠的時間採取適當的措施來防範阻止。

但網路管理者並非機器，無法時時刻刻監測著網路的異常狀況。因此本研究利用入侵偵測系統 Snort，來輔助網路管理者監測網路狀況。當 Snort 偵測到有封包符合其偵測的規則條件時，即針對該封包發出警訊，紀錄在資料庫中。並設計紀錄分析系統，來協助分析 Snort 紀錄，幫助網路管理者快速掌握網路狀況。

另外本研究為實現主動防禦的目的，以 Guardian 搭配 Snort 入侵偵測系統。Guardian 可以在 Snort 偵測到事件發生時，比對異常封包的目的主機 IP，呼叫防火牆程式即時封鎖住異常封包來源 IP，來阻止後續可能的入侵動作。

本研究之目的即在於使用 Snort 及 Guardian，在不增加學校成本及減輕系統管理人員負擔的原則下，配合 Snort 紀錄分析系統，結合原有的防火牆機制，來建構一個可快速偵測並封鎖異常行為的系統，以達到建構更安全的校園網路使用環境的目的。

1.3 研究範圍

Snort 入侵偵測系統（Intrusion Detective System，IDS）是一種基於主動策略的網路安全系統，可以在不影響及改變現有網路架構的情況下，對內部的不當存取及外部的可疑入侵行為，加以檢測，提高網路的安全性。對於校園網路的網路管理者來說，建構網路入侵偵測系統，網管人員可以得知目前的校園網路是否受到威脅，網頁服務及校務行政系統是否正常運作。本論文將研究如何利用 Snort 結合防火牆來提供校園網路更好的安全防護，並設計方便網路管理者分析 Snort 警訊及封鎖網路異常行為的系統程式。

1.4 論文架構

本論文共分六章，分述如下。

第一章　緒論

本章主要論述本研究的研究動機、研究目的、研究範圍及論文架構等四部分。

第二章　背景知識

本章探討的內容，包括常見的網路攻擊手法，入侵偵測簡介的及所使用的相關程式介紹。

第三章　相關研究

本章主要介紹入侵行為的分析、Snort 偵測異常行為的方式、異常行為特徵及 Snort 紀錄分析方式比較。

第四章　系統實作

ABBA System 系統設計與實作。

第五章　系統監測成果

實際監測分析從國小電腦教室所得到的 Snort 紀錄結果。

第六章　結論與建議

提出改善校園網路安全方法與建議，以及後續研究方向。

第二章　背景知識

本章內容主要介紹網路上常見的網路攻擊手法、入侵偵測系統的種類及優缺點，最後則是 BASE 與 Guardian 程式的簡介。常見的網路攻擊方式包括有 DoS（Denial of Service）、DDoS（Distributed Denial of Service）等。入侵偵測系統依照網路部署方式的不同而有網路型（NETWORK-BASED Intrusion Dection System，NIDS）、主機型（HOST-BASED Intrusion Dection System，HIDS）及混合型（Hybird IDS）三種方式。若依偵測方式不同則分為誤用偵測系統（Misuse Detection System）和非正常行為偵測系統(Anomaly Detection System)兩種。

2.1　常見的網路攻擊方式

駭客為了要達成其入侵的目的，常會借用駭客軟體的幫助，如利用木馬程式，竊取檔案或密碼。有些攻擊行為則是利用系統的安全漏洞或是程式的弱點，發起攻擊，阻斷系統的服務。以下為網路常見的攻擊方式介紹。

2.1.1　DoS(Denial of Service)阻斷服務

根據 CERT/CC(2001)及 Mirkovic & Reiher (2004)的定義，主要是指試圖讓某個網路服務的合法使用者，無法正常的使用該服務[12]。DoS 是一對一的網路攻擊方式，攻擊者藉由不當方式佔用系統分享資源(CPU、網路、硬碟…)，達到干擾正常系統運作的進行。不同於一般網路入侵，DoS 不一定需要取得系統使用的權力，即可達到目的。最常見的 DoS 方式即是透過所謂的訊息洪泛(Message Flood)，向攻擊對象送出大量且無意義的網路訊息，不管被攻擊對象是否回應，都會因頻寬的被佔用，而導致不正常運作[18]。如果駭客利用大量的封包，不斷的要求系統提供的服務，正常的使用者就會發現他所要連結的網站無法連上，或是反應相當的緩慢。

要避免 DoS 攻擊的損害，可透過網路的即時監控與異常封包的過濾來著手進行。透過網路監控程式，隨時監控區域網路中的封包數量，配合動態的封包過濾，以達到防禦 DoS 攻擊的目的[19]。

2.1.2 DDoS（Distributed Denial of Service）分散式阻斷服務

DDoS 則是 DoS 的特例，駭客利用多台機器同時攻擊來達到妨礙正常使用者使用服務的目的。駭客預先入侵大量主機以後，在被害主機上安裝 DDoS 攻擊程式控制被害主機對攻擊目標展開攻擊；有些 DDoS 工具採用多層次的架構，甚至可以一次控制高達上千台電腦展開攻擊，利用這樣的方式可以有效產生極大的網路流量以癱瘓攻擊目標。早在 2000 年就發生過針對 Yahoo, eBay, Buy.com 和 CNN 等知名網站的 DDoS 攻擊，阻止了合法的網路流量長達數個小時[20]。

DDos 攻擊的模式並非一對一，而是多對一的方式，多台電腦同時對同一個目標發動攻擊[9]。而這些發動攻擊的電腦，往往都是已遭受入侵而不自知的電腦系統。由於這種攻擊方式大多是利用替死鬼行兇，不僅難以防範，更是難以追查主要發動攻擊者。

常見的 DDoS 攻擊方式有 TNF DDos、TNF 2k DDoS、Trin00 DDoS 及 Stacheldraht 等。使用的協定包括 UDP、ICMP ECHO 及 TCP 與 UDP 並用。攻擊模式如下：

1. 利用作業系統、網路協定、應用程式設計上的漏洞入侵電腦系統。
2. 在入侵的系統中安裝攻擊程式。
3. 由主控端下達攻擊指令，遙控被入侵的系統對特定的目標發動攻擊。

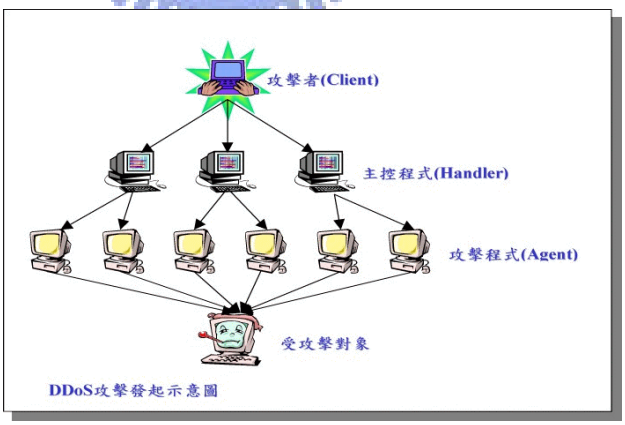

圖 1　DDoS 攻擊發起示意圖
資料來源：[18]

為避免電腦成為 DDoS 攻擊的的跳板，系統管理者必須要常注意更新系統漏洞、隨時注意系統安全，避免被植入 DDoS 攻擊程式，以免成為駭客攻擊的幫兇。

2.1.3 電腦病毒（Virus）

電腦病毒是指故意設計來干擾電腦的作業、紀錄、毀損或刪除資料，或散佈至其他電腦與網際網路上流竄的軟體程式，這類的軟體程式通常會減緩電腦的運作速度，並在過程中造成其他問題[21]。電腦病毒會將本身複製到其他乾淨的檔案或是開機磁區，當電腦使用者沒注意的情況下，執行到已受到病毒感染的檔案或程式，病毒就會以相同的方式散佈或共用出去。

為避免電腦病毒的感染，必須要時時注意電腦系統的程式更新，安裝防毒軟體並更新病毒碼，在瀏覽網路、下載檔案或開啟電子郵件附件時，需確切的確認附件內容，避免開啟陌生人所寄來的電子郵件附件。[22]

2.1.4 電腦蠕蟲（Worm）

電腦蠕蟲和電腦病毒相似，是一種能夠自我複製的電腦程序。蠕蟲程序常駐於一台或多台電腦中，本身會像西遊記裡面的孫悟空，複製許多分身，像蠕蟲般在電腦網路中爬行，感染多台電腦。電腦蠕蟲通常會掃瞄其他機器是否感染同樣的蠕蟲病毒，如果否，就會透過內置的傳播手段進行感染，以達到使電腦癱瘓的目的。常用的方法就是透過區域網路（LAN）、網際網路（Internet）或是 E-mail 來散佈自己。著名的電腦蠕蟲如「VBS_LOVELETTER」[23][24]。

預防感染的方式為不要輕易開啟不認識的人所傳來的電子郵件及附件檔，也不要隨便從網際網路下載程式，並執行它。

2.1.5 特洛伊木馬程式（Trojan Horse）

特洛伊木馬程式，顧名思義就是像希臘神話中所描述的一樣，看起來是平平無奇的程式，執行他結果卻是突擊你電腦系統的士兵。特洛伊木馬程式不像其他電腦病毒一樣會感染其他檔案，特洛伊木馬程式通常都會以一些特殊管道進入使用者的電腦中，然後伺機執行其惡意行為，例如：格式化硬碟、刪除檔案、竊取密碼等）。特洛伊木馬程式看起來就像是有用軟體的電腦程式，但卻會對電腦的安全性造成許多損害。例如：以電子郵件形式偽裝的特洛伊木馬程式，其附件檔案宣稱為是系統的更新檔，執行它之後，即化身為病毒危害系統安全[24][25]。

防範的方式為不要任意安裝下載不明軟體及執行來路不明的電子郵件附件。

2.1.6 連接埠掃瞄（Port Scan）

每台電腦在提供或是連結網路服務的時候，如瀏覽網頁（Port：80），都要經過連接埠的連接，才能使用電腦所提供的服務。駭客通常都會掃瞄要攻擊主機的 Port，來檢視主機提供那些服務，如果提供服務的程式有漏洞未經修補，駭客會利用該服務的漏洞進行攻擊。因此，Port Scan 常是駭客攻擊前的前置手段。

2.1.7 IP Spoofing

IP Spoofing 簡單來說就是偽造網路封包的表頭，讓路由器（Router）或者是防火牆（Firewall），以為是來自安全可信任的網域，而被允許進入內部網路，直接攻擊網路主機[26]。

2.1.8 緩衝區溢位（Buffer Overflow）

緩衝區溢位(Buffer Overflow)是由於程式撰寫的疏忽，使得攻擊者利用程式設計上的缺失而進行攻擊，造成緩衝區容量的不足，導致系統執行攻擊者欲執行的攻擊程式[29]。這是近年來最常見到的網路攻擊手法。攻擊者通常具備相當的程式設計基礎。例如：處理一個長度為 80 字元的字串，程式設計師設定字串變數長度為 100，如果攻擊者將一個長度超過 100 的字串送入程式中處理，這樣超出的變數就可能會覆蓋其他程式的片段，造成程式執行無效[2]。

2.2 入侵偵測系統（Intrusion Detection System，IDS）

入侵偵測系統（IDS）就是一種網路安全監測工具，可以即時偵測出網路上的不當使用行為或是違反使用者自訂的網路安全規則功能的系統[10]。藉由解讀電腦系統上的稽核檔或網路上的封包內容，並對其進行安全分析，判斷是否違反安全規則或是攻擊行為，即時回報給系統管理人員。

入侵偵測依部署方式的不同主要可以分成三類：

（1）網路型入侵偵測系統（NETWORK-BASED Intrusion Dection System，NIDS）

網路型的入侵偵測系統，主要是擷取每一個經過的網路封包作為資料來源，通常將網路卡設定為雜亂模式（Promiscuous Mode），來偵測分析流經網路層(Network Layer)的封包資訊[2][3]。如果所偵測的封包資料與系統內置的安全規則吻合，入侵偵測系統就會發出警報。每個偵測器檢查每個連接網段所傳送的封包，可以保護多個連到該網段的主機。傳統的網路型偵測系統是由一個或多個可以執行本機分析與回報攻擊資訊到集中式主控台的偵測器所組成。

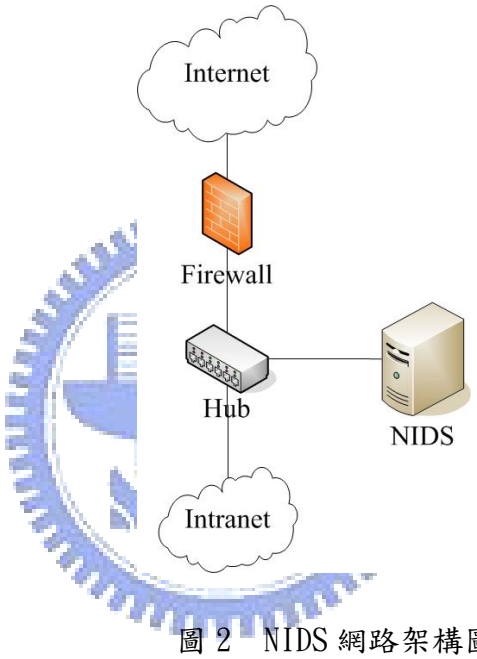

圖 2　NIDS 網路架構圖

資料來源：[15]

網路型偵測系統（NIDS）的優點如下[2][3]：

1. 設置的成本較低。在不需更改現有網路的架構及作業系統情況下，只需設置一部 NIDS 即可偵測同一區域網路內可能的入侵行為。
2. 隱形在網路上偵測。入侵者無法得知偵測系統的存在，其入侵／攻擊行為記錄無法湮滅。
3. 可同時偵測多個重要主機的傳輸資訊。一部 NIDS 可以同時偵測同一區域網路內的所有主機的網路傳輸資訊。
4. 可偵測來自網路封包的攻擊模式。例如：DoS，DDoS。
5. 不會影響網路的傳輸效率。NIDS 只是在傳輸網路上監測，不需像防火牆一樣管制所有進出的資料，因此不會影響網路的傳輸速度。
6. 資料更新只需作一次即可，不需個別機器一一更新。

7. 可即時偵測入侵活動，不必等到封包進到機器才發現。
8. 風險較低。網路入侵偵測系統如果故障，不會影響正常業務的進行。

缺點如下[3]：

1. 僅能偵測事先定義的規則與封包特徵，無法偵測新型的攻擊行為。
2. 網路流量過大或超出能處理的範圍時，NIDS 則無法完全偵測所有網路封包的傳輸狀況。
3. 無法偵測經過加密的傳輸資訊內容。
4. 無法判斷入侵／攻擊行為是否成功。
5. 不能檢測在不同網段的網路封包。在使用交換乙太網路的環境中就會出現監測範圍的侷限。

（2）主機型入侵偵測系統（HOST-BASED Intrusion Dection System，HIDS）

這種系統的軟體必需要直接載入主機並加以監控。主要偵測該主機的網路即時連接及系統檔案、程序與日誌檔中是否有可疑的活動。某些主機型的 IDS 會監測使用者權限是否有改變。內部網路攻擊者常用的手法為：取得最高權限或設定新使用者的帳號。在重要的伺服器上監測是否有使用者濫權濫用是很重要的。可以與網路型偵測結合使用，達成完整的入侵偵測。

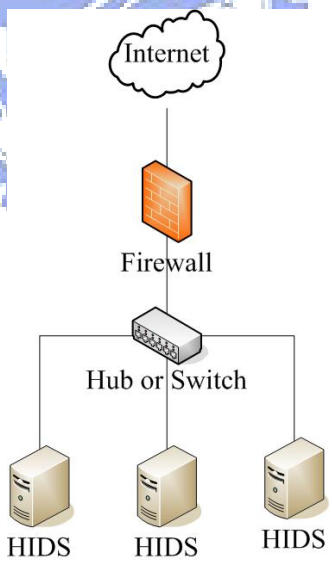

圖 3　HIDS 網路架構圖

資料來源：[15]

主機型入侵偵測系統（HIDS）優點如下[3]：

1. HIDS 可以根據日誌記錄，判斷入侵／攻擊行為是否成功。
2. HIDS 主要偵測 OSI 第七層，適用於有加密式或交換式（Switch）網路環境。

3. 能分析“可能的攻擊行為”。入侵者試圖執行哪些危險指令、執行什麼程式、開啟什麼文件等。
4. 誤報率比網路入侵偵測系統低。檢測主機上的執行命令序列比檢測網路流量簡單。
5. 不需另外增加硬體設備。

缺點如下[3]：

1. HIDS 會暴露在網路上，行蹤可能被發現，而遭攻擊損毀。
2. 僅偵測事先定義的規則與特徵行為，對新型的攻擊型態無法偵測。
3. 可能無法相容於所有不同主機的作業平台，使得部署及維護工作比較複雜，且無法防護作業系統本身的安全漏洞，若駭客入侵／攻擊這些系統安全漏洞，將使 HIDS 失去效用。
4. 無法偵測主機所在網域的所有電腦主機，HIDS 僅偵測其所在主機所接收的封包資訊。
5. 在伺服器本身上安裝入侵偵測系統會降低應用系統的效率。
6. 本來不允許安全管理員有權限訪問的伺服器變成可訪問的。
7. 如果伺服器沒有配置日誌的功能，則需重新配置日誌檔蒐集的問題。

（3）混合型入侵偵測系統（Hybird IDS）

結合 HIDS 和 NIDS 技術的入侵偵測，Hybird IDS 係以主機系統為基礎，會辨識網路封包流向或是來自某主機的封包攻擊。它不像 NIDS 會檢查每一個經過的封包，所以它減緩了某些因為流量分析而造成的效能降低問題。Hybird IDS 藉由監控系統的事件、資料、目錄及登錄檔中的攻擊行為，提供更多的防護，也較不易發生誤報的情形。但作業平台的限制與部署位置的爭議，仍是一個問題，且耗費較多的系統資源，所以一般不被採用[3][27]。

入侵偵測系統依偵測方式的不同分為兩類：

（1）誤用偵測系統（Misuse Detection System）

誤用偵測系統又稱為特徵型偵測（Signature-based Detection），檢測的方法類似電腦病毒的檢測方式，對已知的網路攻擊手法及入侵行為，包含系統的缺陷，經由分析整理成入侵特徵（Signature）模式庫。入侵偵測系統藉由比對從主機或是網路中所蒐集到的資料特徵，是否在所收集到的入侵特徵模式庫中出現，如果有符合攻擊者入侵行為的特徵時，即發出警告（Alert）。

誤用偵測系統的應用主要是建立在入侵特徵模式庫上，遇到符合入侵特徵的行為，才會被視為入侵行為。所以要能偵測出所有網路上已經被知道的入侵行為，就必須要有一個完整且時時更新的入侵偵測模式庫。而誤用入侵偵測系統的偵測

能力，也取決於入侵偵測模式庫的完整性和更新程度。

透過入侵偵測模式庫，誤用入侵偵測系統可以詳細且準確的對已知的入侵行為發出警告訊息，因此有較低的誤判率(False Alert)，但對於未知的攻擊特徵則無法準確的偵測出來。

（2）非正常行為偵測系統(Anomaly Detection System)

非正常行為入侵偵測系統主要在於先建立電腦或網路正常活動的統計記錄，將正常活動的統計記錄與現行的網路活動進行比較，如果現行網路活動有違反正常正常活動規律時，該活動即被認為是可能入侵行為。

因此，非正常行為入侵偵測系統要先透過統計、具有學習能力的類神經網路或資料採礦等技術，將正常使用時的電腦 CP 利用率、記憶體利用率、歷史活動資料、客戶端正常使用的訪問時間和次數等行為作一個統計並記錄起來，以作為與現行行為比較的依據，藉此判斷出是否為入侵行為。

此種偵測方式的優點在於可以檢測到未知或是較複雜的入侵行為，但誤報率(False Alert)也高。例如用戶行為的突然改變，極有可能被視為入侵行為。

2.3 BASE（Basic Analysis and Security Engine）

BASE 的主要功能在於能從遠端觀測 Snort 在校園網路內所偵測到的警告訊息，透過 BASE，可以得知「誰在攻擊」、「誰被攻擊」、「用什麼方式攻擊」、「什麼時間」攻擊等資訊。BASE 可說是 Snort 的前端管理介面。

BASE 的發展是基於原本的 ACID（Analysis Console for Intrusion Database）Web 界面管理程式而來，依照 ACID 的架構再往上發展。主要具有以下功能：

◆警示資訊的快速檢索

能夠快速的列出警示資料中的資訊，包含「來源 IP」、「目的 IP」及最近發生的警告訊息。

◆搜尋功能

自訂搜尋的條件，對警告訊息搜尋。

◆統計圖表功能

能將警示訊息統計繪製成「圓餅圖」、「長條圖」及「折線圖」。

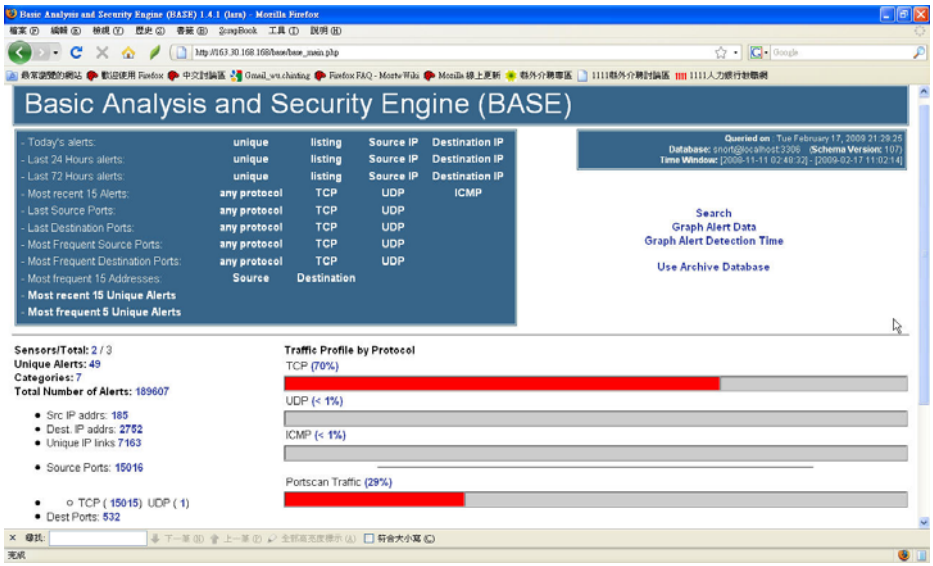

圖 4　BASE 主要畫面

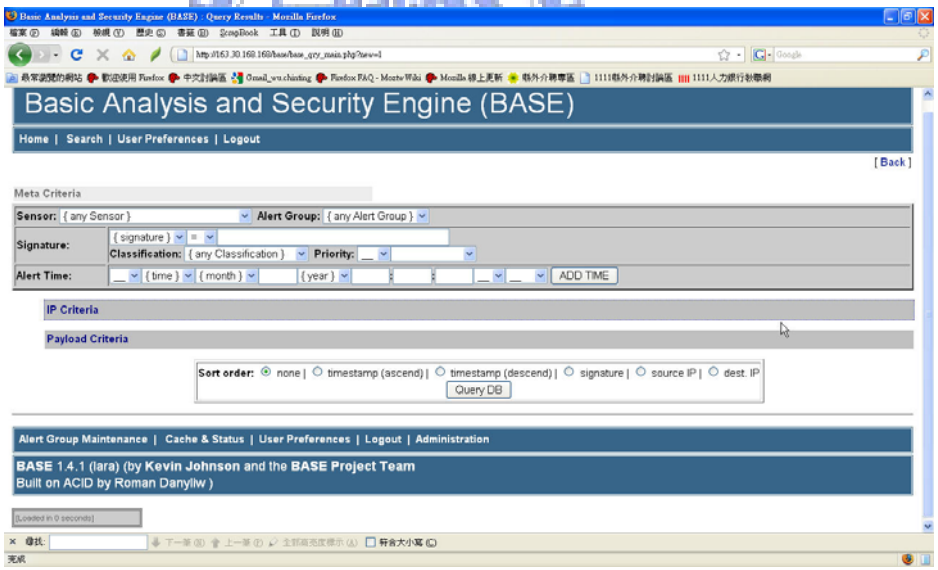

圖 5　BASE 搜尋

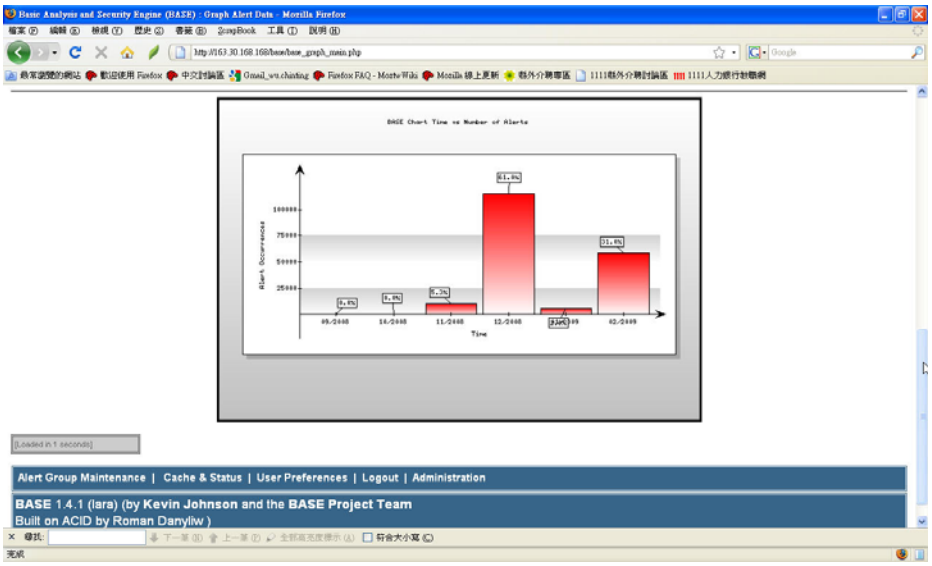

圖 6　BASE 統計長條圖

雖然 BASE 已經擁有讓網路管理者可以瞭解網路上入侵警告的資訊，但隨著資訊量的累積，資料庫內的警告訊息越來越多，要從眾多的訊息中，分析出攻擊者 IP、攻擊類型、攻擊次數及攻擊的時間，單靠 BASE 並不容易。因此，本研究另外利用 PHP 設計 ABBA 系統，以利網路管理者，能在眾多的資訊中，快速的得知目前網路所存在的威脅。

2.4　Guardian Active Response for Snort

Guardian 主要是結合 Snort，依據 Snort 所產生的警訊來自動更新防火牆的規則，以達到自動防護的安全程式[30]。透過 Guardian 可以即時更新防火牆規則，阻擋所有來自攻擊主機 IP 位址的封包。Guardian 是由 Perl 所寫成的程式，其所支援的防火牆包括 ipchains、iptables、ipfwadm、FreeBSD using IPFW、ipfilter、Checkpoint Firewall、PixFirewall 等。Snort 與 Guardian 的結合，可以讓原本只是單純的入侵偵測系統，變成具有主動阻擋異常行為 IP 的入侵防禦系統。

Guardian 的設定檔主要有兩個，介紹如下：

1. guardian. ignort

主要為設定經常存取本系統主機的 IP，為網路管理者所信任的 IP，可以避免在連線時遭到 guardian 以防火牆封鎖封包。例如 DNS 主機、getways、郵件主機等，網路管理者也可自行加入信賴的主機 IP。

2. guardian. target

這個檔案主要紀錄了所要防護的主機 IP，包含主機 IP。當 Snort 所偵測到的封包，符合了 Snort 的規則條件，觸發了 Snort 的警告，而其目的 IP 為列表中的 IP 時，則 guardian 就會呼叫防火牆，封鎖來源 IP 所發送的封包。

Guardian 可以依據網路管理者需求，設定封鎖 IP 的時間。當封鎖時間限制一到，即解除該 IP 的封鎖。對於區域網路內部電腦發生異常狀況時，相當具有彈性。

第三章　相關研究

所謂：「知己知彼，百戰不殆。」，要能正確且成功的判斷可疑的入侵偵測，必須要對入侵行為的模式及特徵，有相當的瞭解。除此之外，對於負責偵測入侵行為的 Snort 系統，對其偵測的方式及系統的架構也要有一定的認識。因此本章主要分為四個小節。在 3.1 節中介紹駭客入侵主機前的前置作業分析。3.2 節介紹 Snort 入侵偵測系統的架構、偵測方式及規則的語法。3.3 節則介紹異常行為特徵的分析方式。最後，3.4 節則對本研究所提 Snort 警訊資料分析方式與其他研究做一個比較整理。

3.1　入侵行為的分析

一個網路攻擊事件的發生，並非偶然。駭客要攻擊一個網路或是系統，必須是先收集相關的訊息，經過詳盡的分析，擬定周全的計畫，才會開始行動。而隨著網路安全等級的不同，收集訊息與攻擊方式的複雜度也有所差異。在攻擊初期，駭客通常會利用掃瞄程式來對目標進行資訊蒐集的工作，但如果是盲目的試探，不僅容易被察覺攻擊的意圖，也容易使網路或系統的管理者產生警覺而加強防範。所以駭客在選定目標後，針對不同的作業系統或是不同的伺服器，會擬定不同的攻擊方式，以減少被察覺而失敗的機會。沈文吉（2001）在網路安全監控與攻擊行為之分析與實作中將入侵行為分成四個階段，如下[2]：

3.1.1　資訊的蒐集

駭客利用一些現成的工具或是技術來對目標主機進行資訊蒐集的動作。例如目標主機的防火牆配置，是否有部署 IDS 偵測系統，系統使用者資訊，內部 IP 的分配等等。透過這些情報，駭客可以決定入侵的方式。以下是常見的一些資訊蒐集的方式：

1. finger、whois 指令：為 unix 內建的指令，可以取得系統使用者的資料。
2. traceroute：Linux 系統為 traceroute，Windows 系統為 tracert。是一種電腦網路工具，可以顯示封包在網路上傳送時，所經過的路由器 IP 位址或可能存在的防火牆
3. 砍站軟體：如 Teleport Pro、HTTrack 等。砍站軟體就是將整個網站複製到使用者的硬碟中，方便使用者離線瀏覽。但駭客入侵時可以透過複製整個網站，進而分析裡面的資訊，以得到有利的攻擊資訊。

3.1.2 網路掃瞄

網路掃瞄就是要找出目標主機所提供的服務 Port，藉此找尋可供入侵的通道及漏洞。Portscan 是駭客入侵時常用的偵測行為，利用 Portscan 可以找出網路上運行的機器及其所開啟的服務 Port。Portscan 有下列兩種方式：

1. 掃瞄整個網路：逐一掃瞄 IP 位址，可以得知網路上有多少機器在運行。
2. 掃瞄單一機器的 Port：掃瞄主機上的 Port，可以得知主機所提供的服務。

3.1.3 弱點攻擊

收集到了網路上主機的資訊，瞭解主機所使用的作業系統及提供的服務，就可以利用已知的弱點攻擊程式來進行入侵攻擊的工作。例如：開啟 Port23 的主機，表示其可能提供 Telnet 服務，利用網路竊聽工具，抓取網路上的封包，很容易可以得知該主機相關的帳號或密碼，藉此進行進一步的攻擊。

3.1.4 取得使用權

入侵的最終目的，就是要取得入侵主機的最高使用權限（root），有了這個權限便可主宰整部主機，竊取機密資料，安裝後門程式或是利用這部主機進一步入侵其他機器。

3.2 Snort 偵測異常行為偵測的方式

Snort 入侵偵測系統是 Marty Tosech 於 1988 年所創造出來的 Open Source（開放原始碼）入侵偵測軟體，是一套免費而且使用者可自行修改發展的入侵偵測系統[1]。主要運行在 Libpcap 的函數基礎上，並支援多種系統軟硬體平台。Snort 入侵偵測系統是一個輕量級的入侵偵測系統，具有擷取網路封包，分析封包內容，並以規則為主（Rule-based）的模式對封包內容進行比對，對符合規則的封包判定其具有入侵行為，進而提出警告，提醒網路管理者。Snort 也可以將警告的訊息寫入 Syslog 指定的日誌文件檔。Snort 用來比對封包規則的語言相當的靈活有彈性，因此可以迅速的對入侵行為作出反應。且 Snort 具有模組化的擴展能力，能搭配其他軟體，如防火牆(firewall)或自己編寫的模組，來強化入侵偵測及防禦的功能[6]。

3.2.1 Snort 的運作模式

Snort 與入侵偵測相關的主要有四種模式：

1. 封包監聽模式（Sniffer mode）
   監聽網路上封包所傳輸的內容，並將所監聽到的封包內容顯示於螢幕上。
2. 封包記錄模式（Packet Logger mode）
   將所監聽到的封包記錄到硬碟中。
3. 網路入侵偵測系統模式（Network Intrusion Detection System mode，NIDS）
   分析網路上的封包內容，如果有符合使用者所定義的規則（Rules），則依規則內容採取相應的動作。
4. Inline mode
   從防火牆(Iptables)來擷取封包而非透過 libpcap，如果遇到符合 Snort 規則選項的封包，則由規則設定的動作來告訴 Iptables 丟棄封包或是放行。

3.2.2 Snort 的運行架構

Snort 的主要運行架構如下圖：

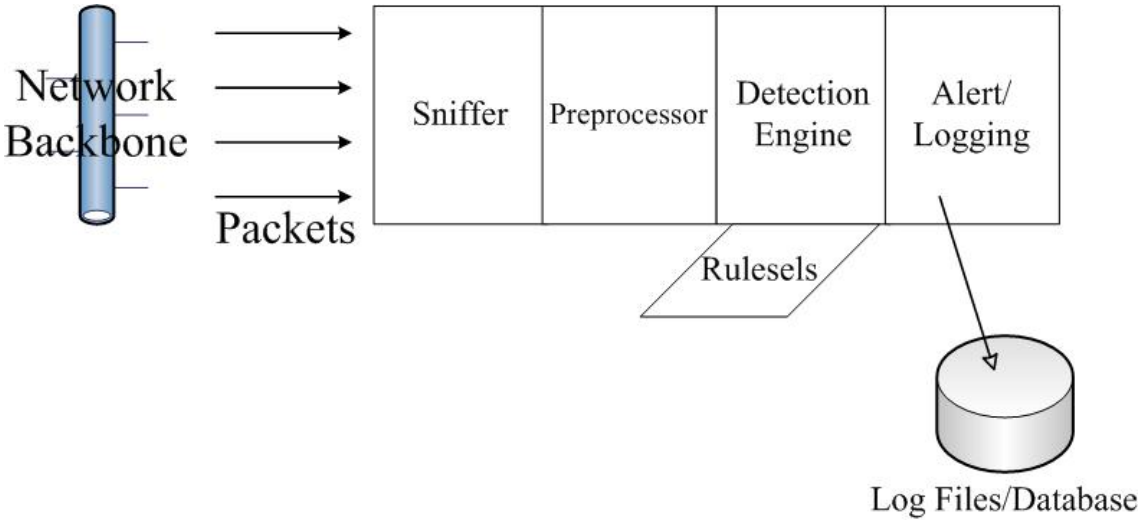

圖 7　Snort 主要架構圖

資料來源：[2]

Snort 主要由四個部分組成：封包擷取與解碼器（Packet Capture and Packet Decoder）、前處理器(Preprocessor)、偵測引擎(Detection Engine)及記錄與警示系統（Logging and Alerting System），分述如下：

1. 封包擷取與解碼器（Packet Capture and Packet Decoder）：

主要功能為從網路上擷取封包，並載入封包解碼器進行解碼來對封包分析。Snort 利用 Libpcap 函數庫擷取封包[14]，並按照 TCP/IP 協定的不同層次對封包進行解析，也可設置封包過濾器來擷取指定封包。

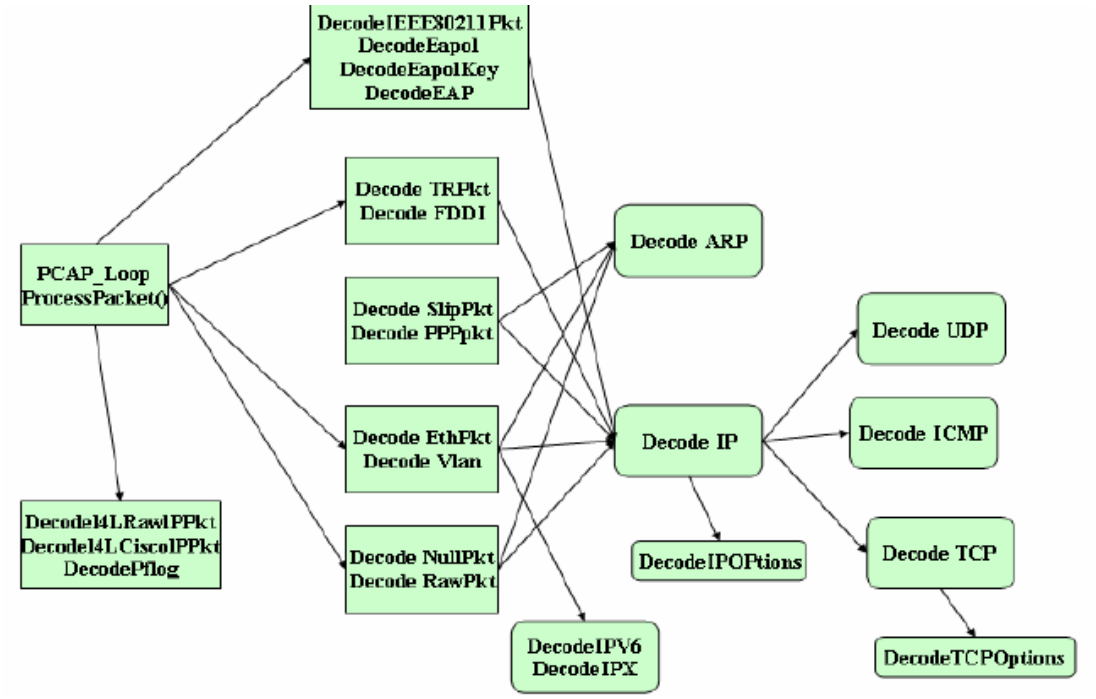

圖 8　Snort 解碼封包之架構

資料來源：[7]

2. 前處理器(Preprocessor)：

Snort 的前處理器主要有兩個作用。它可以協助檢查透過特徵匹配所無法偵測出來的攻擊行為；另一個作用為通過對流量的模式進行標準化處理，以便偵測引擎能準確的匹配特徵，使攻擊無法逃避 Snort 偵測引擎的偵測。

經由解碼器分析後的封包，便送至前處理器。前處理器能將封包分段、重組 TCP Stream、編碼的轉換等。同時也能判斷某種類型的攻擊，如果有偵測到攻擊，便直接產生警告訊息。所以前處理器處理完封包之後，會將資料送到偵測引擎進行規則比對，或是直接輸出警告。其處理流程如下圖

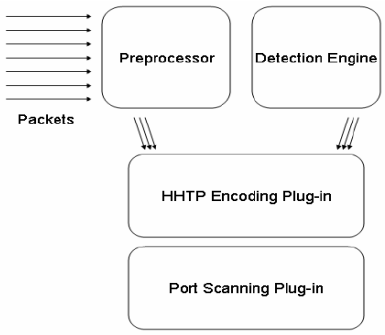

圖 9　Snort 前處理器

資料來源：[7]

3. 偵測引擎(Detection Engine)：

偵測引擎主要有兩個功能：規則分析與特徵偵測。Snort 載入規則並比對每個封包，若發現有符合規則的封包，則依據該規則所定義的動作進行處理，若所有規則都不符合，則丟棄該封包。處理流程如下圖：

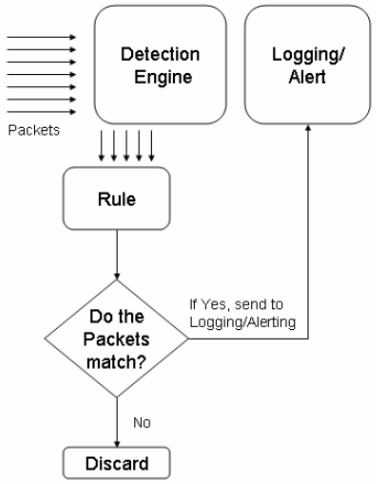

圖 10　Snort 封包解碼架構圖

資料來源：[7]

4. 紀錄與警示系統（Logging and Alerting System）

Snort 能夠在偵測到入侵行為的同時，產生即時的警告及紀錄。其採取 TCPDUMP 的格式記錄信息，並向 Syslog 發送警告信息，以通知網路管理人員。其訊息可儲存在檔案或是資料庫中。

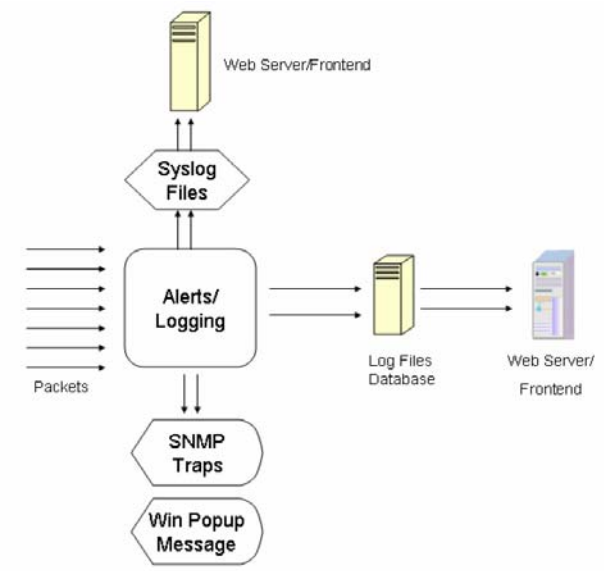

圖 11　Snort 記錄與警示架構圖

資料來源：[7]

3.2.3　Snort 規則匹配方式

Snort 入侵偵測系統檢測封包的方式為規則匹配，及透過本身的規則庫，分析封包的資料內容。如果能夠匹配就產生警告訊息，或者保留準備更多情況的分析。規則的匹配包括了下面的匹配類型：

1.協定匹配（Protocol Match）

Snort 針對 IP、TCP、UDP、ICMP 協定進行分析，透過協定分析模組，將封包按照協定分析的結果對協定相應的部分進行檢測。例如：TCP 封包的標記（flag）位元，協定異常等。一般 TCP 的連結有一個或多個標記，標記是用來說明這個連結的用途，TCP 的位元如 F（FIN）、S（SYN）、R(RESET)、P（PUSH）、A（ACK）、U（URGENT）。如下例為某一規則的定義，其中 flags 為對各種 TCP 標記位元作協定位置的匹配。

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN SYN
FIN";flags:SF,12;reference:arachnids,198;
classtype:attempted-recon;sid:624; rev:2;)
```

2.字串匹配（Signature Match）

字串匹配模式是 Snort 偵測系統最主要的匹配模式，事件定義者根據某個攻擊的封包或者攻擊的原因，提取其中的封包字串特徵。通常入侵偵測系統經過協定分析後，進行字串的匹配。例如以下的規則定義：

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS
(msg:"WEB-CLIENT readme.eml download attempt";
flow:from_client,established; uricontent:"/readme.eml"; nocase;
classtype:attempted-user; sid:1284;
reference:url,www.cert.org/advisories/CA-2001-26.html; rev:9;)
```

這條規則中所要進行定義的字串為「/readme.eml」。另外，Snort 入侵偵測系統在預處理（Preprocessors）中有 Fragment Reassembly 功能，可以避免攻擊者使用分裂(fragmentation)來阻撓或躲避規則匹配，尤其是針對字串匹配。

3.大小匹配

這可以歸屬於字串匹配中的一種。這種匹配方式主要是對資料封包中的某段資料的長度進行匹配，而非針對具體的字串。例如，透過資料長度的限制來對緩衝區溢出攻擊進行檢測：如以下規則所示：

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS
(msg:”WEB-IIS ISAPI .ida attempt”; uricontent:”.ida?”;
nocase;dsize:>251;
flow:to_server,established;reference:arachnids,552;classtype:web-a
pplicationattack;
reference:bugtraq,1065;reference:cve,CAN-2000-0071;sid:1243; ev:6;)
```

其中的關鍵字“dsize”就是對資料封包的負載進行匹配，如果請求的命令總長度大於 251，那麼就檢測出緩衝區溢出攻擊的事件。

4.邏輯匹配

對不同類型的事件組合來進行判斷，從而獲得新的事件。有少數的入侵偵測系統對多種事件的組合來構成邏輯推理，增強檢測的智慧。

5.累積匹配

通過對某些事件出現的量或單位時間出現的次數來產生新的事件。例如，某 IP 在 1 分鐘內產生了 100 個 CGI 事件，那麼就屬於一次 CGI 掃瞄事件。[2][6]

3.2.4 Snort 的規則

Snort 入侵偵測系統主要是以「規則」來判斷網路上的可能入侵行為，是以攻擊特徵為基礎的入侵偵測系統（Signature-Based IDS）。利用已經建立好的規則庫，來比對封包內容，如果規則的定義不夠完善或是定義不夠明確，將直接影響到 Snort 對入侵偵測判斷的結果。Snort 的偵測規則是以開放式的方式來發展的，可以自行撰寫規則，以符合自己的需求。

Snort 的規則語言是用簡單、靈活且強大的描述語言來撰寫的，只需依照幾個簡單的原則就可以發展。Snort 的規則主要分成兩部分，規則頭（rule header）及規則選項(rule options)。規則頭主要包含了規則的動作、通訊協定、來源位址及目的位址的 IP 及所使用的 Port 等資訊。規則選項則包含了警告訊息及封包檢查的內容範圍，可由一個或多個條件組合而成[28] 。其結構如下：

```
alert tcp any any -> 192.168.1.0/24 111 (content:" |00 01 86 a5| "; msg:" mountd access";)
|   規則頭（rule header）   |          規則選項（rule options）          |
```

圖 12　Snort 規則範例

資料來源：[28]

規則頭（rule header）

Snort 的規則頭定義了對符合規則封包的動作(action)、通訊協定（Protocol）、來源 IP 及 Port、目的 IP 及 Port 及封包流向等資訊。介紹如下：

◆動作(action)：

主要是告訴 Snort 當發現有封包符合規則條件時，所該採取的反應。Snort 常用的動作如下：

- alert 產生警告訊息並記錄。
- log 記錄封包。
- pass 忽略封包。
- activate 產生警告並啟動另一條規則處理。
- dynamic 等待直到另一條規則被執行才啟動。

◆通訊協定（Protocol）：

Snort 目前支援的通訊協定包括了 TCP、UDP、ICMP 和 IP。

◆IP 及 Port：

Snort 使用「any」這個字來表示「任一位址」，也可以直接指定 IP 位址，如「192.168.1.3」。如果要表示區域網路，則使用「CIDR」模式，「192.168.1.0/24」表示從 192.168.1.1 到 192.168.1.255 這段區域網路。使用「!」則表示「非」何

種網路 IP，如！192.168.1.0/24，表示非 192.168.1.1 到 192.168.1.255 這段網路。

Port 可以以好幾種方式表示，如用「any」表示任意 port。指定特定的 port，如 telnet 的 23、http 的 80。或是以「：」表示特定的 port 範圍，如下圖

```
log udp any any -> 192.168.1.0/24 1:1024 log udp
traffic coming from any port and destination ports ranging from 1 to 1024

log tcp any any -> 192.168.1.0/24 :6000
log tcp traffic from any port going to ports less than or equal to 6000

log tcp any :1024 -> 192.168.1.0/24 500:
log tcp traffic from privileged ports less than or equal to 1024 going to ports
greater than or equal to 500
```

圖 13　Port 範圍表示範例

資料來源：[28]

◆封包流向（Direction）：

「->」的符號表示封包由來源 IP 的 port 往目的 IP 的 port 方向傳送，如下：

圖 14　Snort 封包流向圖

「<>」則表示不分來源位址及目的位址。

規則選項（rule options）

規則選項組成了 Snort 入侵偵測引擎中的核心部分，主要是由一個或幾個選項的條件組合。規則選項有四個分類，分述如下：

◆general

主要是提供此規則的相關資訊，無關入侵偵測的功能。

◆payload

比對資料封包中的內容。

◆non-payload

用來比對各種協定的欄位值。

◆post-detection

當封包內容比對符合時，除了所定義的動作之外，所採取的其他行動。

規則選項主要的關鍵字整理如下表：

表 1　規則選項關鍵字

分類	關鍵字
general	msg、reference、gid、sid、rev、classtype、priority、metadata
payload	content、nocase、rawbytes、depth、offset、distance、within、http_client_body、http_cookie、http_header、http_method、http_uri、fast_pattern、uricontent、urilen、isdataat、pcre、bype_test、byte_jump、ftpbounce、asnl、cvs
non-payload	fragoffet、ttl、tos、id、ipopts、fragbits、dsize、flags、flow、flowbits、seq、ack、window、itype、icode、icmp_id、icmp_seq、rpc、ip_proto、sameip、stream_size
post-detction	logto、session、resp、react、tag、activates、activated_by、count

資料來源：[28]

3.3 異常行為特徵

在判斷正常行為與異常行為的方式上，最直接的方式就是觀察行為特徵的表現。在 Snort 所蒐集的警示訊息中，如何能過濾且判斷出異常行為，是網路管理者所必須思考的問題。在莊振宏（2003）針對網路銀行之異常偵測模組研究[9]中提到，異常行為特徵的分析，主要是利用人類的習慣原則來作為依據。因為這些習慣不容易改變，所以在異常偵測的理論中，行為特徵成為一個很重要的偵測依據。透過行為特徵的分析，可以判斷出異常行為。主要以三個面向來作分析。

1.行為特徵時間分析

行為特徵時間分析指的就是做某件事情的時間與做該件事情所使用的時間。舉例來說，有一個人上班習慣八點出門，八點半到公司，每天都固定花半小時時間。其行為特徵可以記錄如下：

User Behavior:{WORK;8:00;8:30;30min}

當某一天，該上班族八點出門，九點才到公司，到公司花了一個小時，我們可以判斷，該上班族有異常行為發生。所以分析行為特徵的時間，是用來判斷使用者行為習慣的重要特徵依據。

另外，行為特徵時間分析還有另一種使用方式，即偵測某段時間內，某個事件的次數，在網路攻擊的事件中，如 DoS，就是利用單位時間內，讓某個事件負載超過極限，致使系統發生問題。

2.行為特徵次數分析

行為特徵次數分析就是透過使用者對某事件的次數，通常都會配合時間分析一起進行，也就是單位時間內進行的次數。例如有一個人每週平均跑步四次，我們可將其行為模型記錄如下：

User Behavior:{RUN ; a week; 4 times}

若此事件屬於公眾次數，則可以將次數計算成分數的模式，也就是說，公眾平均次數五次，而該使用者四次，則該使用者的行為模型可以轉換如下：

User Behavior:{RUN ; a week; 4/5}

3.行為特徵順序分析

行為特徵順序分析，變化較大，因為這是組合事件分析，而非單一事件。行為特徵分析中，會有一個起始事件，也就是一開始要記錄的事件特徵。舉例來說，「某人從家裡到公司」這個事件，首先會有一個離開家的動作與時間，皆下來是搭乘交通工具的種類與時間，到達公司的動作與時間等等。其特徵模型如下：

User Behavior:{[home;07:40],[bus;08:00],[office;08:40]}

User Behavior:{[home;07:30],[car;07:35],[office;08:30]}

由以上的紀錄，可以知道每一事件的動作與發生的時間，也可記錄同一事件內部不同動作的變化，多重記錄使用者行為。

我們藉由來源 IP 或目的 IP（使用者）所引發的警告事件時間、次數與事件的組合，來觀察 IP（使用者）的動向。透過 IP（使用者）所引發的事件組合及資料庫內的次數統計，我們可以藉此判斷 IP 所引發的事件是否具有入侵的企圖或具有其他危險。藉由單位時間內的次數統計，我們可以列出可疑 IP 的事件行為，藉此加以防範。

3.4 Snort Log 分析方式比較

大部分對入侵偵測系統的研究，大多著重在於如何提高入侵偵測系統的效能及提升警訊的正確率上，很少針對警示訊息作分析，以瞭解駭客背後入侵的模式與現行的網路系統是否安全。在李為漢（2005）網際網路惡意程式之活動調查—以某企業對外網路連線為例[7]論文中，提到實際利用網路入侵偵測系統（Snort）所蒐集的紀錄加以分析與研究的方法，其透過自行設計的分析程式來輔助入侵偵測系統，主要目的是瞭解網路上惡意程式的活動為何（指網路上駭客攻擊的行為），藉以分析駭客攻擊網路的行為特性與意圖，以有效的防護網路安全。

其分析方式主要分為四個面向：

（1）時間特性分析：

1. 以上下班時間與網路被攻擊次數統計表來得知網路遭受攻擊的情形。
2. 每日攻擊的次數統計。
3. 來源 IP 攻擊的持續時間分析：以時間為區間，統計與分析發生攻擊事件最多的前十名。
4. 同一個來源 IP 的攻擊是否曾在不同的日期重複出現？

（2）空間特性分析：

1. ICMP Ping 與 Trace Route 測試:針對來源 IP 進行 ICMP Ping 與 Trace Route 測試(隨機抽樣 50 個，總共抽樣 3 次)。
2. 來源 IP 個數統計。
3. 來源 IP 地區分析。
4. 網路被攻擊目標之次數統計。

（3）攻擊者與被攻擊目標之特性分析

1. 攻擊的事件與分類。
2. 駭客攻擊網路之意圖與分析（嘗試獲取資訊、取得系統權限、拒絕存取服務、執行任意目的程式）。

3.網路攻擊類型分析（ICMP，WEB，Database，Netbios）。

4.駭客攻擊網路之目標系統分析。

（4）駭客使用攻擊工具與方式分析

李為漢（2005）的研究藉由入侵偵測系統所偵測到的攻擊事件與統計數據，來使網路管理者可以藉此判斷網路是否遭到駭客的入侵，同時也藉由攻擊事件的組合，成功的分析駭客的行為與意圖，讓網路管理者知所警戒，加以防範，以提高網路的安全性。

其研究方法與本研究比較如下表：

表 2　網際網路惡意程式之活動調查—以某企業對外網路連線為例與本研究比較表

論文名稱	網際網路惡意程式之活動調查—以某企業對外網路連線為例	以 snort 偵測並封鎖網路異常之研究
資料蒐集方式	以 Snort 監聽 A 公司對外網路的進出流量，蒐集外部網路的攻擊訊息。	以 Snort 蒐集國小電腦教室的進出流量,所有電腦皆透過 nat（安裝 Snort）連接外部網路。
資料儲存方式	以 Snort 紀錄檔為主，先將入侵資料作篩選，將其中重要資料存於資料庫中。	以 Snort 紀錄檔,透過 Base 系統將資料存於資料庫中，未經篩選。
處理資料方式	透過輔助程式分析發生事件最多的來源 IP，可以自有選擇分析的時間區間。	利用 ABBA 系統,來統計分析來源 IP、目的 IP、及攻擊事件，並可透過防火牆針對可疑 IP 進行封鎖。
資料分析	1.時間特性：駭客攻擊行為與時間的關聯。 2.空間特性：網路被攻擊的目標次數統計。 3.攻擊者與攻擊目標特性分析：分析駭客攻擊行為特性與目的。 4.駭客使用的攻擊工具分析：瞭解目前駭客使用的攻擊工具為何。	1.行為特徵時間分析：藉由時間的分析，判斷可能的攻擊行為。 2.行為特徵次數分析：藉由時間次數的統計,判斷 IP 是否可疑。 3.行為特徵順序分析：藉由事件的發生組合，判斷是否有入侵的可能。

李為漢（2005）對 Snort Log 的分析研究著重於事後對駭客攻擊方式、時間、手法的分析，其資料來源主要為外部對內的 Snort 警訊，所分析的 Snort Log 經過事先所定義的過濾清單篩選，再儲存於資料庫。而本研究所著重的在於內部網路對外的存取所發生的即時事件分析與監測。利用 Base 系統直接將 Snort 所產生的警告訊息儲存於資料庫中，並透過 ABBA 系統觀察監測警訊發生時間、警訊次數與其行為特徵的分析組合，來判斷該 IP 是否有異常的行為活動。若有則透過防火牆加以封鎖該 IP 的封包進出。

兩者的分析方式雖然不同，但同樣藉由 Snort 警訊的發生時間與產生警訊的 IP 及警告次數的統計，來瞭解網路異常行為的活動狀態，同樣也透過警訊事件的組合，來判斷是否有可能的入侵行為，或是執行不當的程式。

第四章　系統實作

本研究所提出的系統主要目的在於不改變校園現有網路架構下，利用現有的工具與技術，在不增加成本、減少網路管理者負擔的原則下，來提升校園網路的安全性。

國小電腦教室常因為使用者（學生）的錯誤使用或下載不當程式與檔案，常常發生中毒或是被植入木馬程式的情況。而這些遭到中毒或植入木馬的電腦，往往成為校園網路內最大的潛在威脅。這些遭受感染或入侵的電腦可能透過網路的傳播造成重要伺服器（如：Web Server）的中毒，或是成為入侵者的跳板（僵屍電腦），變成攻擊其他電腦的幫兇，造成校園網路的癱瘓。在國小各項重要資料（學籍成績、學生個人資料）越趨資訊化的情況下，校園網路的安全性，也就更需重視。

大多數國小的電腦教室都使用虛擬 IP 上網，要連結對外的網路，必須經由 NAT 伺服器的 IP 轉換。因為電腦教室內的網路封包都需經過 NAT 伺服器，因此我們在 NAT 伺服器上安裝 Snort 入侵偵測系統、ABBA System 及 Iptables。Snort 主要是對進出電腦教室的封包作檢測與紀錄的動作，ABBA System 則是監測分析 Snort 所產生的警示訊息，Iptables 則是針對可疑 IP 封鎖其異常行為。

4.1　系統簡介

本研究以國小電腦教室為實作環境，將 ABBA System 建置在電腦教室對外連線的 Nat 主機上，該主機同時安裝了 Snort、MySQL 及 IPtables，系統示意圖如下。

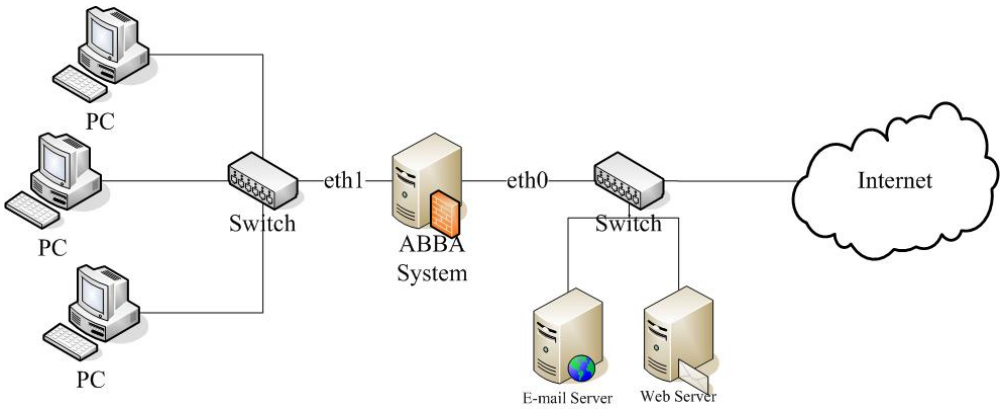

圖 15　系統示意圖

電腦教室內的電腦設定虛擬 IP(192.168.0.X)透過 eth1 與 Snort 主機連線，Snort 透過 eth0 實體 IP（163.30.168.X）對外連線。當 Snort 偵測到電腦教室內有電腦有異常行為或是發送不當封包時，若其目的 IP 是對校園內重要主機（如：Web Server）發送，則即時透過防火牆機制來阻止不當封包的傳送。藉此避免電腦教室的電腦成為攻擊或感染校園內重要伺服器的幫兇。

封包進出流程圖如下

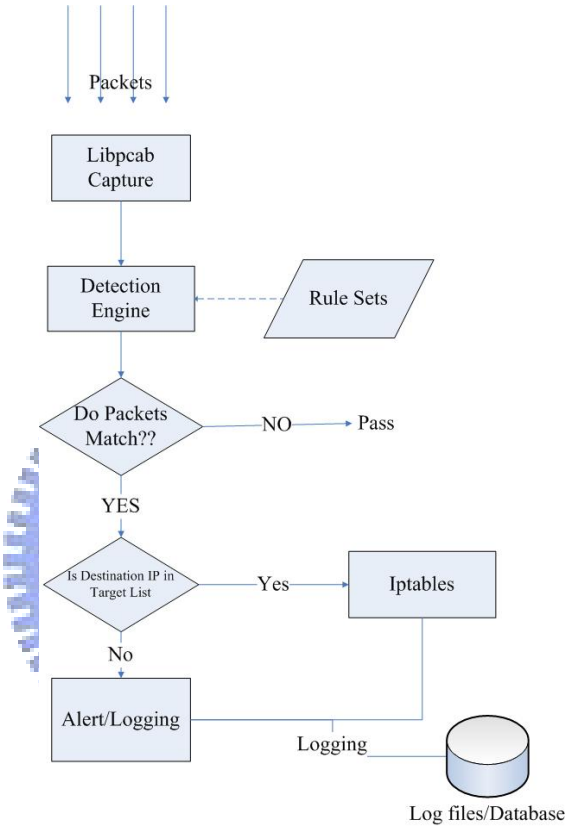

圖 16　封包進出流程圖

封包經由 Libpcab 擷取之後，透過偵測引擎(Detection Engine)比對規則(Rules)，若是封包並未符合規則，則放行；若是發現符合規則的封包，且其目的 IP 在防護主機的列表內，則通知防火牆（Iptables）阻擋封包的通行，同時發出警告並記錄在資料庫中，以便日後追蹤防範。若其目的 IP 不在防護主主機列表中，則發出警告並紀錄在資料庫中。

4.2 ABBA System（ABnormal Behavior Aspirin System）

為了能更快速的瞭解 Snort Log 背後所隱藏的資訊，我們結合 BASE 的資料庫，開發了 ABBA System。ABBA System 主要是針對 BASE 所儲存在資料庫中的警告資訊進行統計與查詢，讓網路管理者可以透過統計與查詢的方式，快速瞭解網路內所遭遇到的攻擊類型，藉此制訂防禦的措施與方法。

ABBA System 主要以 PHP 程式語言寫成，以 MySQL 為後端資料庫，其系統模組架構如下圖。

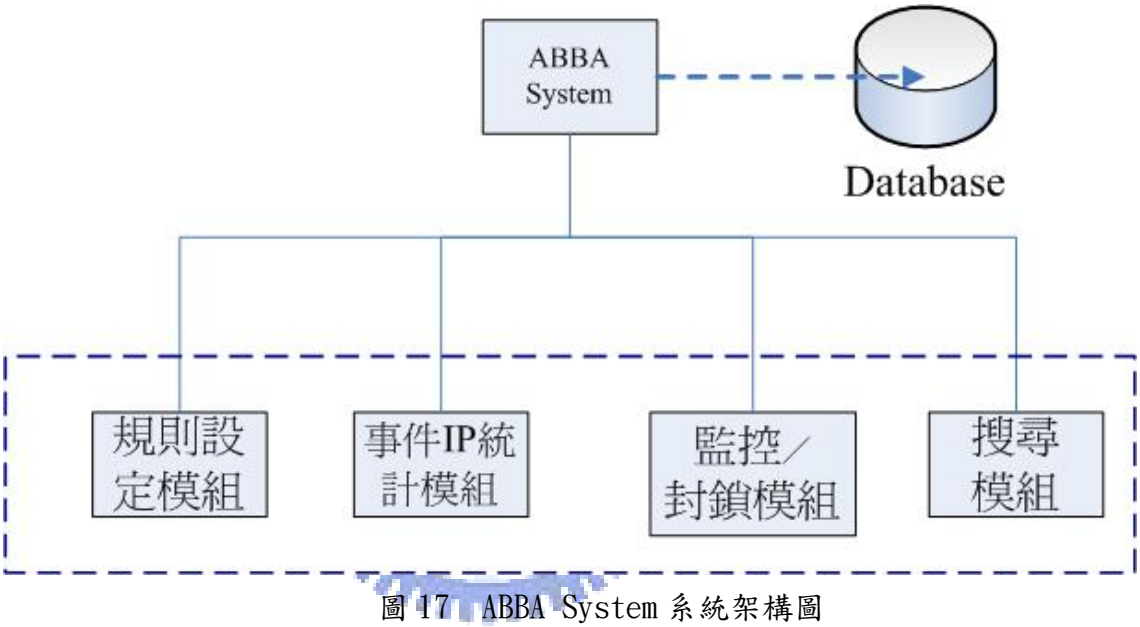

圖 17 ABBA System 系統架構圖

本系統主要由四個模組所組成，分別是規則設定模組、事件 IP 統計模組、監控封／鎖模組與搜尋模組。以下分別對各項模組功能進行說明。

4.2.1 規則設定模組

規則設定模組主要提供一個 Web 界面供網路管理者自行設定 Snort rule 規則。rule 規則是 Snort 入侵偵測系統用來比對封包，藉此產生警告事件的主要依據。Snort 本身使用了一種靈活的規則語言來描述網路封包，使用者可以根據其規則語言自訂規則，讓 Snort 可以對新的攻擊做出快速的反應，具有即時警報的能力。

設定規則主要分成規則頭（Rules Header）及規則選項(Rule Options)兩方面。規則頭設定包含了封包動作、通訊協定、來源 IP、來源 PORT、封包流向、目的 IP、目的 PORT 等欄位。規則選項設定則包含了警示名稱(Msg)、封包內容(Content)及警示編號（Sid）等欄位。

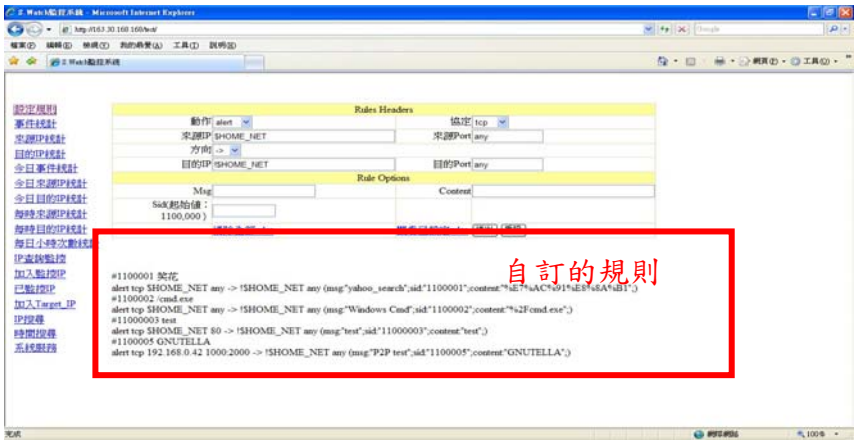

圖 18　設定規則

規則選項中的 content，主要是設定 Snort 在封包檢查中所要檢查的特定字串，如果是二進位的資料，則需以「|」括起來區隔。以下列規則為例：

#1100005 GNUTELLA
alert tcp 192.168.0.42 1000:2000 -> !$HOME_NET any (msg:"P2P test";sid:"1100005";content:"GNUTELLA";)

此規則意思為只要是從 192.168.0.42 發出的封包，使用 PORT 為 1000 到 2000 之間，要去讀取網段外的 IP，且內容包含有「GNUTELLA」，當 Snort 比對封包內容，若有比對到符合的選項時，則發出「P2P test」的警告訊息。如下圖。

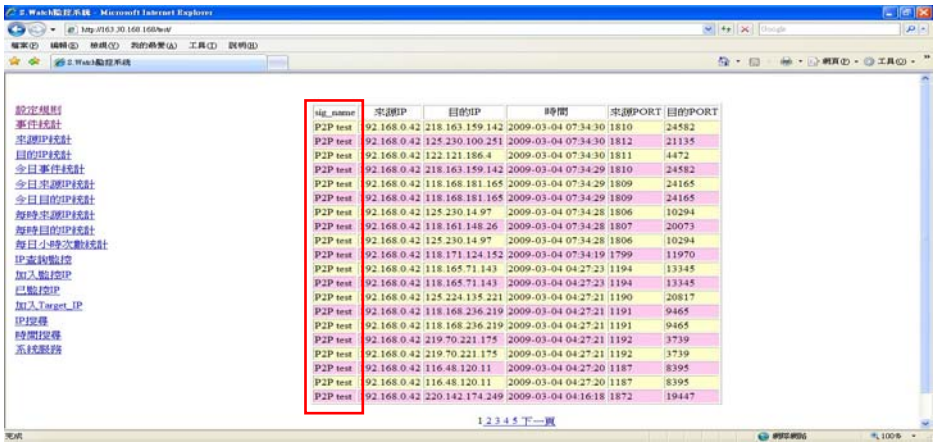

圖 19　以自訂規則偵測到的 P2P 警訊

4.2.2 事件 IP 統計模組

此模組主要是以不同的時間區隔方式，來觀察所發生的事件、來源 IP、目的 IP 的次數統計。統計 Snort 所發生的所有警告訊息，依照事件警告次數或發生時間先後進行排序，讓網路管理者可以清楚的掌握網路發生的事件及狀況。

為了能快速的瞭解 Snort 警告訊息及掌握處理時效，因此我們將統計方式依時間區隔分成總數統計、今日統計、及每時統計等三種方式。

（一）總數統計

總數統計的方式是為了瞭解全部所發生過的警告事件及 IP，並透過統計排序，可以知道引發事件最多的 IP 及事件，提供網路管理者相關資訊藉以預防可能的入侵及危害。

圖 20　所有警訊事件統計

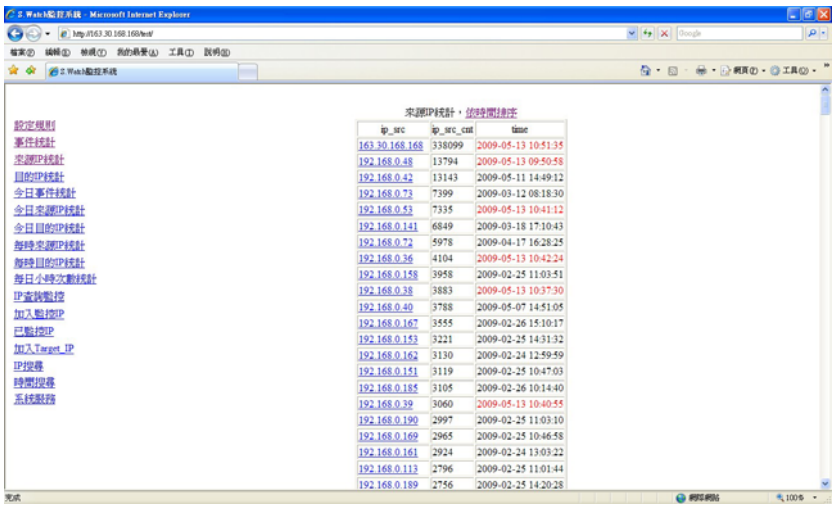

圖 21　全部來源 IP 統計，依次數

（二）今日統計

以今日為時間區隔的統計，可以讓網路管理者針對即時發生事件的 IP 做快速的反應及處理。若是屬於區域網路內的 IP，可以藉由引發的事件來觀察電腦是否遭受到入侵或是感染病毒。若是區域網路外的 IP，則可交由監測封鎖模組，來封鎖其行為。

圖 22　今日事件統計

圖 23　今日來源 IP 統計

網路管理者能快速得知今日區網內所發生的事件數及 IP 數量，即可透過時間排序，明確的掌握系統所引發的最新事件與 IP 位址，讓網路管理者可以透過事件的監測，快速的反應及防制不法的行為與存取。

（三）每時統計

每日小時次數統計可以知道一天之中，引發 Snort 警告次數最多的時段，利用資料庫資料的分析，可以比較出過去每個星期每小時所引發的警告事件數目的差異。提供管理者作為判定是否網路有異常狀況的參考。

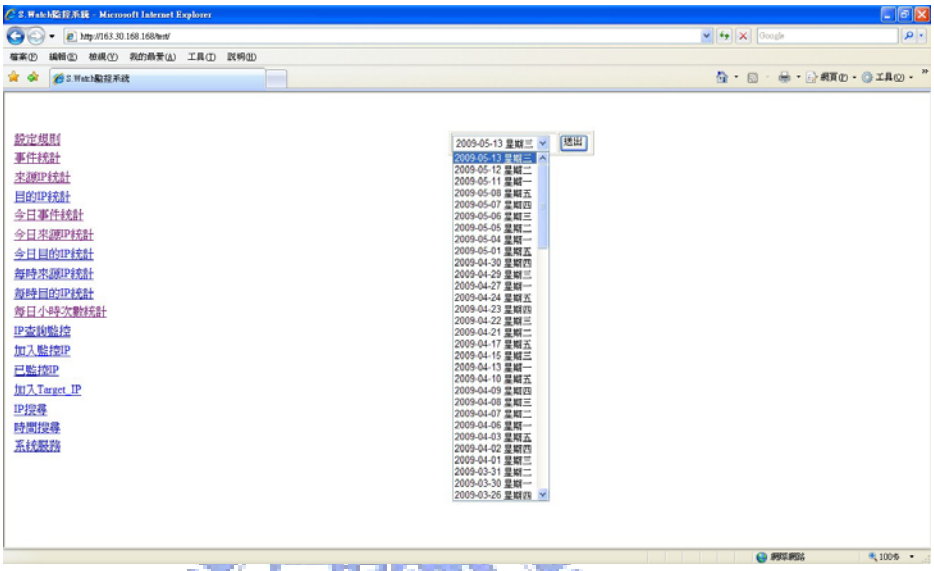

圖 24　每日小時警告次數統計

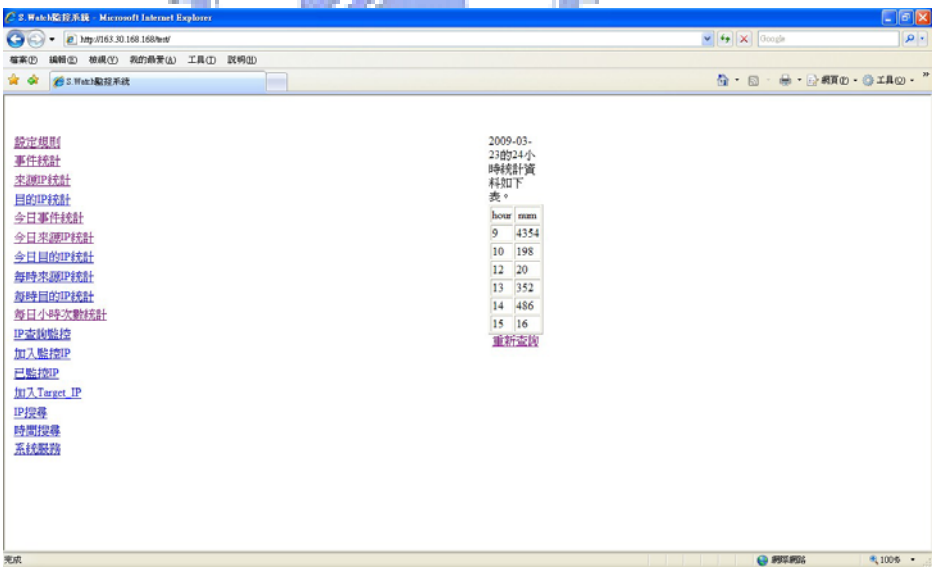

圖 25　每日小時次數統計列表

4.2.3 監控／封鎖模組

監控／封鎖模組主要有兩種功能，一是透過 Guardian，針對引起警訊的封包來源 IP 的做主動的封鎖。二是透過網路管理者監測判斷並封鎖可疑 IP。運作流程如下圖。

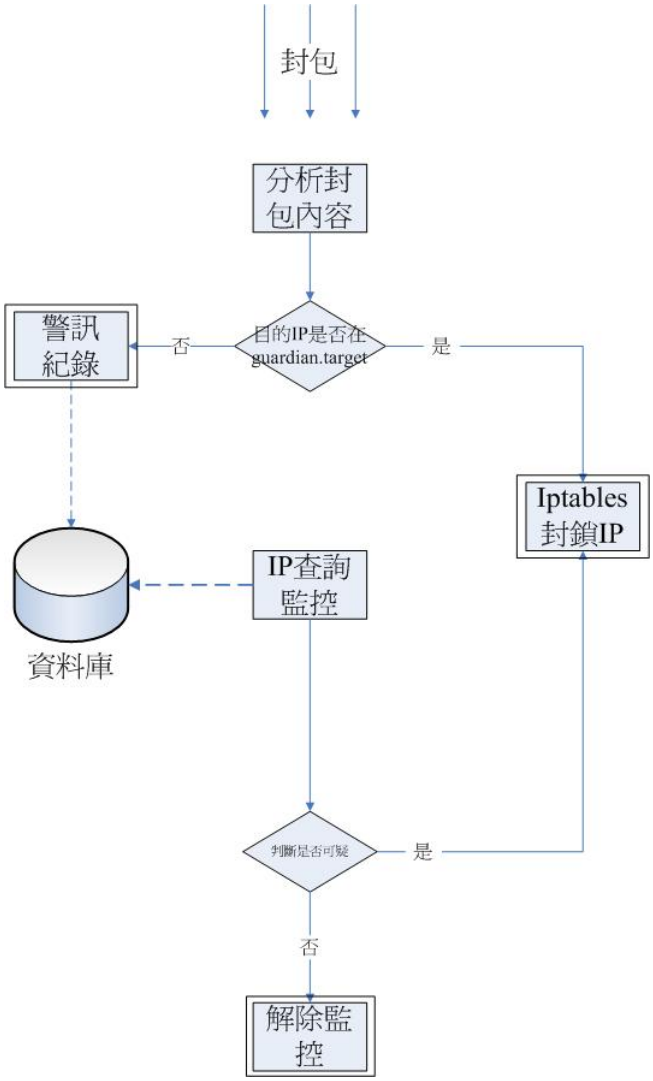

圖 26　IP 監控／封鎖模組流程圖

封包進入主機後，監測封鎖模組會先檢查封包的目的 IP 是否在 guardain.target 的主機名單中，若存在，且該封包同時觸發 Snort 的警訊，則直接以 Iptables 封鎖其來源 IP，並紀錄下來。若不存在於 guardian.target 中，則發出警訊，並交由網路管理人員監測判斷是否為可疑的 IP。若是，則同樣透過 Iptables 封鎖來源 IP，拒絕可疑 IP 存取。

監控／封鎖模組針對單位時間內所偵測到的警訊次數，針對警訊次數過於頻繁，超過一定數量的 IP 做監測及封鎖的動作。可疑 IP 列表預設為時間八小時內，警訊次數超過 100 次的 IP。網路管理者自己也可以依據網路狀況，自訂查詢的時間與次數。

在發現異常行為之後，網路管理者必須評估異常行為可能造成的後續影響及危害程度，必要時須加以封鎖並阻止其異常行為的發生。在本研究中，我們將封鎖異常行為的方式分成監測 IP 事件及封鎖 IP 活動兩階段來進行。監測 IP 事件為觀察 IP 所引發的警訊及次數，藉此來判斷其危害程度。封鎖 IP 活動則是透過防火牆將該 IP 所有網路封包加以封鎖，直到異常狀況解除才開放。

在 Snort 的警訊事件中，有些事件發生並非十分需要持續關注的，例如：(ftp_telnet) Telnet traffic encrypted，是紀錄使用者使用 telnet 的行為警訊，這不一定是十分緊急的入侵事件。但有些警訊的發生，有可能造成後續的危害影響，例如 Port Scan，或是違法使用 P2P 軟體等。因此，第一階段我們可以藉由觀察事件次數的統計，讓網路管理者將觸發警訊次數過多的 IP 加入監測的名單。

圖 27　警訊事件次數超過 100 的 IP

IP 經過監測後，異常狀況若未改善，則封鎖 IP。，封鎖 IP 活動，有兩種方式。第一種是透過監測中 IP 列表，將欲封鎖的 IP 寫入防火牆規則，由防火牆將來自該 IP 的所有封包丟棄，禁止該 IP 任何的網路活動。

圖 28　封鎖 I P

封鎖 IP 活動的防火牆的規則如下：

DROP　　all　--　192.168.0.21　　anywhere

以上規則為將所有來自 192.168.0.21 的封包，不論是送往何處，都加以丟棄。

第二種方式，則是利用 Guardian，將欲防護的主機 IP，寫入 guardian.target 中，以達到主動封鎖的作用。當警訊發生時，其目的 IP 在 guardian.target 的防護主機列表中時，guardian 即主動呼叫防火牆將來源 IP 封鎖。

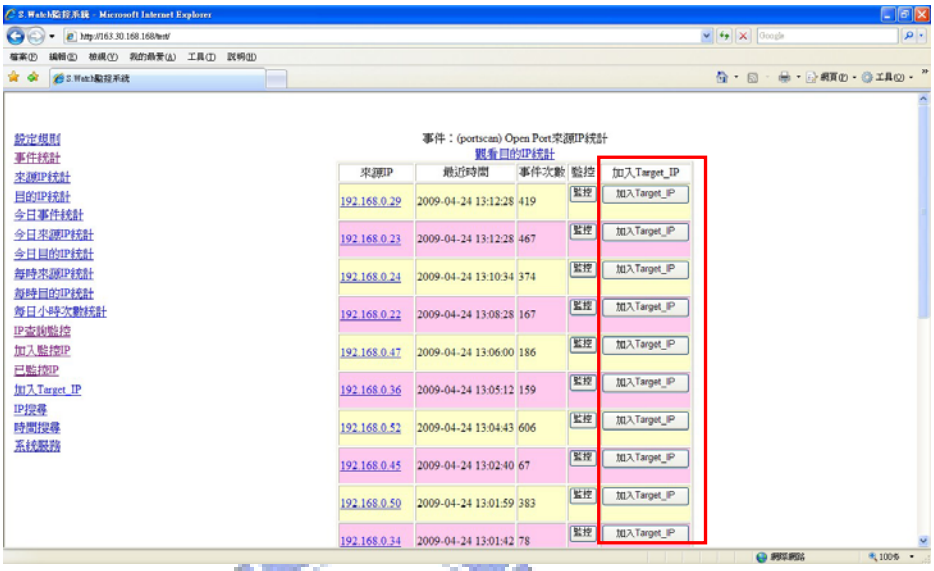

圖 29　加入 Target IP

4.2.4 搜尋模組

搜尋模組的功能主要分為 IP 搜索，與時間搜尋兩種。當想得知特定 IP 所發生的所有警告事件統計，可以透過 IP 搜索的功能來達成。IP 搜索可以顯示來源 IP 或是目的 IP 的事件統計總數，可查知可疑 IP 所引發的警示記錄，來提供網路管理人員做為判斷的依據。

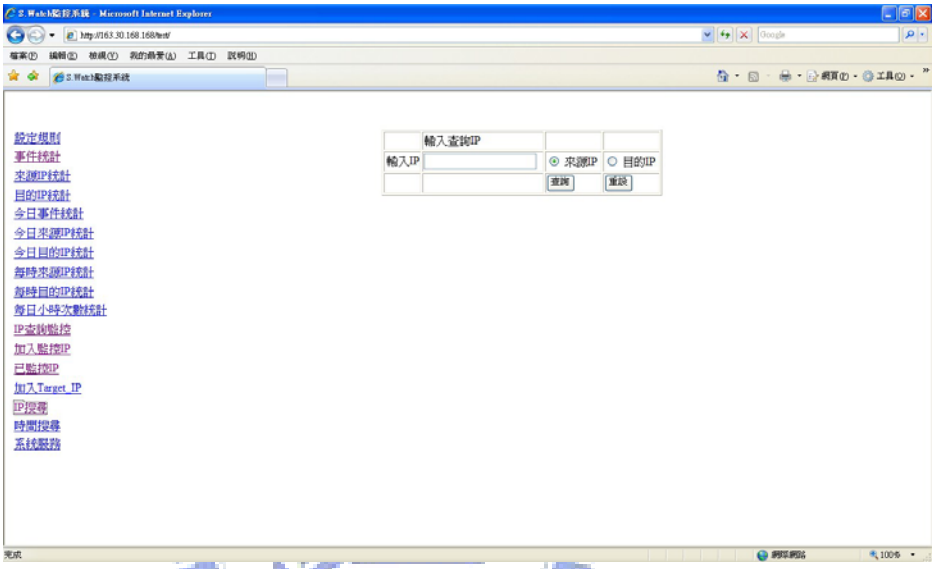

圖 30　IP 搜尋

圖 31　IP 搜尋結果

時間搜尋的功能透過時間區間的自由組合，可以得知過去及現在所記錄的歷史警警訊，配合每日小時統計，即可知道特定時段內所發生的警告訊息詳情。也可針對不同的需求，選擇對來源 IP、目的 IP 或事件作分析查詢。

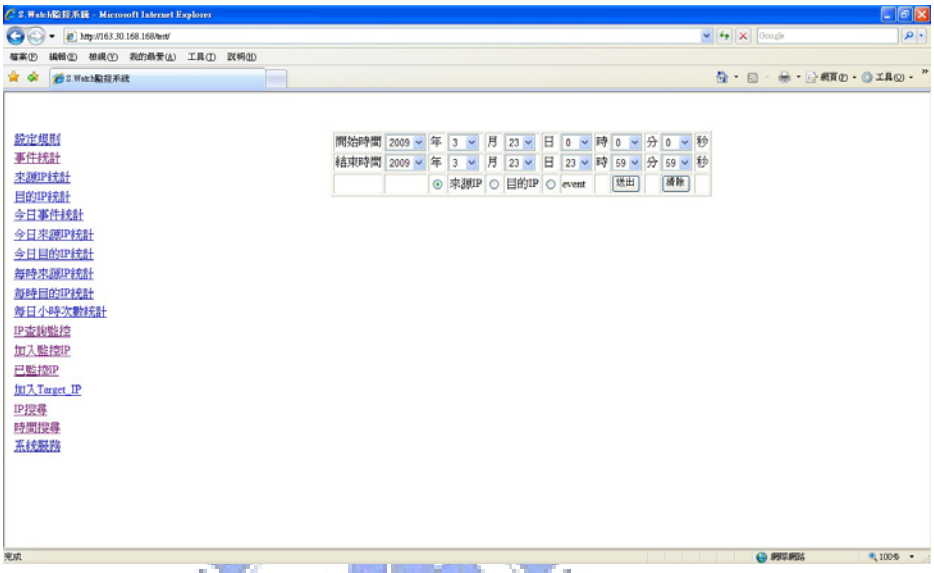

圖 32　時間搜尋

圖 33　時間搜尋結果

ABBA System 模組名稱與程式功能列表整理如下表：

表 3　ABBA System 功能與名稱列表

模組名稱	程式功能	程式列表
規則設定模組	設定規則	ruleset.php rule_in.php clean_rules.php service.php load.php data.rule
事件 IP 統計模組	事件統計	event.php sig_ip.php sig_no.php sig_no_ip.php
	來源 IP 統計	ip_src.php ip_search_show2.php sig_no_ip.php
	目的 IP 統計	ip_dst.php ip_search_show2.php sig_no_ip.php
	今日事件統計	event_today.php sig_no_today.php sig_ip_today.php sig_ip2_today.php sig_no_ip_today.php
	今日來源 IP 統計	ip_src_today.php ip_search_show2_today.php sig_no_ip_today.php
	今日目的 IP 統計	ip_dst_today.php ip_search_show2_today.php sig_no_ip_today.php
	每時來源 IP 統計	ip_src_hour.php ip_search_show2_hour.php sig_no_ip_hour.php
	每時目的 IP 統計	ip_dst_hour.php

		ip_search_show2_hour.php sig_no_ip_hour.php
	每日小時次數統計	day.php day_ps.php
監控／封鎖模組	IP 查詢監控	suspect_watch.php suspect_qry.php suspect_qry_ps.php suspect_ip_add.php
	加入監控 IP	suspect_add.php suspect_ip_add2.php
	已監控 IP	suspect_ip_show.php ip_search_show2_today.php suspect_del.php suspect_lock.php suspect_unlock.php
	加入 target_list	target_ip_add.php target_ip_del.php target_ip_list.php
搜尋模組	IP 搜尋	ip_search.php ip_search_show.php sig_no_ip.php
	時間搜尋	time_search.php search_ps.php time_ip_event.php time_event.php time_ip.php

ABBA System 所使用資料表格欄位如下：

表 4　acid_event 資料表欄位說明

欄位名稱	欄位型態	欄位說明
sid	int	警告 SID
cid	int	警告 CID

signature	int	警告
sig_name	varchar	警告名稱
sig_class_id	int	警告類別 ID
sig_priority	int	警告優先權
timestamp	datetime	日期時間
ip_src	int	來源 IP
ip_dst	int	目的 IP
ip_proto	int	IP Prototocal
layer4_sport	int	來源 PORT
layer4_dport	int	目的 PORT

表 5　suspect_ip 資料表欄位及說明

欄位名稱	欄位型態	欄位說明
no	int	編號
ip_sup	int	可疑 IP
timestamp	datetime	日期時間
block	int	是否封鎖

利用 ABBA System 可以幫助校園內的網路管理人員，減少檢視 Snort 警示訊息的時間，可以快速的發現網路內可疑的入侵行為，並加以封鎖阻止。並透過統計的功能，可以知道發生警訊次數最多的事件，讓網路管理者可以亡羊補牢，做出防範，提高校園網路的安全性。

第五章　系統監測成果

本系統實際在國小電腦教室進行監測，從 2008 年 11 月到 2009 年 3 月 23 日止，實際以 Snort 紀錄網路使用狀況，並交由 ABBA System 來分析 Snort Log，並針對所發現的狀況進行封鎖，以提升校園網路安全。

5.1　監測環境

本研究所蒐集的資訊以國小電腦教室對外的網路連線為主，一間教室共有 40 台電腦可供教學及上網使用。由於國小經費有限，在不需要另外增加硬體支出及改變網路架構的情況下，本研究是以現有的 Nat 主機來建置系統。

系統的建置以自由軟體為主，作業系統使用的是 CentOS 5.1（Community ENTerpirse Operating System），是 Linux 的發行版之一，在做為伺服器用途的方面，具有穩定及安全的特性；在網頁程式開發上，選擇具有跨平台、內建多樣化函式庫等特性的 PHP5 來作為開發語言；資料庫則是以免費且穩定、效能優異的 MySQL 來儲存資料。本系統所採用的硬體及軟體套件版本詳列如下表：

表 6　系統硬體及軟體套件版本

用途	套件名稱及版本
硬體環境	Intel(R) Pentium(R) 4 CPU 3.40GHz
記憶體	620MB
作業系統	CentOS 5.1 (kernel-2.6.23.10)
資料庫	MySQL 5.0.45
開發網頁語言	PHP5.1.6
入侵偵測系統	Snort 2.8.2.1
輔助入侵偵測工具	Guardian 1.7

5.2 異常行為偵測

本研究將實際以系統蒐集到的電腦教室網路訊息，經由 ABBA System 分析後，將所監測到的異常狀況，分析如下：

（一）前十大警訊

本研究蒐集了從 2008 年 11 月 11 日到 2009 年 3 月 23 日之間所有發生的警告事件，所引發警告次數最多的前十大事件如下表。

表 7　前十大警訊事件排名

排名	警告名稱	警告次數	百分比
1	(portscan) Open Port	162539	49%
2	(http_inspect) OVERSIZE REQUEST-URI DIRECTORY	59105	18%
3	(http_inspect) IIS UNICODE CODEPOINT ENCODING	27591	8%
4	(http_inspect) BARE BYTE UNICODE ENCODING	9764	3%
5	P2P GNUTella client request	4926	2%
6	P2P Outbound GNUTella client request	4419	1%
7	P2P BitTorrent transfer	4250	1%
8	(http_inspect) DOUBLE DECODING ATTACK	3891	1%
9	POLICY Yahoo Webmail client chat applet	2683	1%
10	(http_inspect) OVERSIZE CHUNK ENCODING	2443	1%

從上表，可以發現網路警訊事件以(portscan)Open Port 所引發的事件佔大多數。由此可判斷，電腦教室內的電腦所可能因執行某些程式，而開啟某些 Port，而這些 Port 都有可能成為駭客入侵的主要途徑。且經統計發現，大多 portscan 的來源 IP 都是電腦教室內的 IP 位址，由此可推測，使用者在使用電腦期間，可能因下載及安裝不當軟體，而被植入某些程式而開啟 Port。

（二）異常傳輸的監測

從每日小時次數統計中，發現在 2009 年 3 月 16 日晚上 7 點到晚上 12 點間網路有發生異常傳輸的情形，有大量的警告訊息發生，經 ABBA Systme 查詢瞭解引起警訊的 IP 為 192.168.0.48 的電腦，所引起警訊的原因為 port scan。

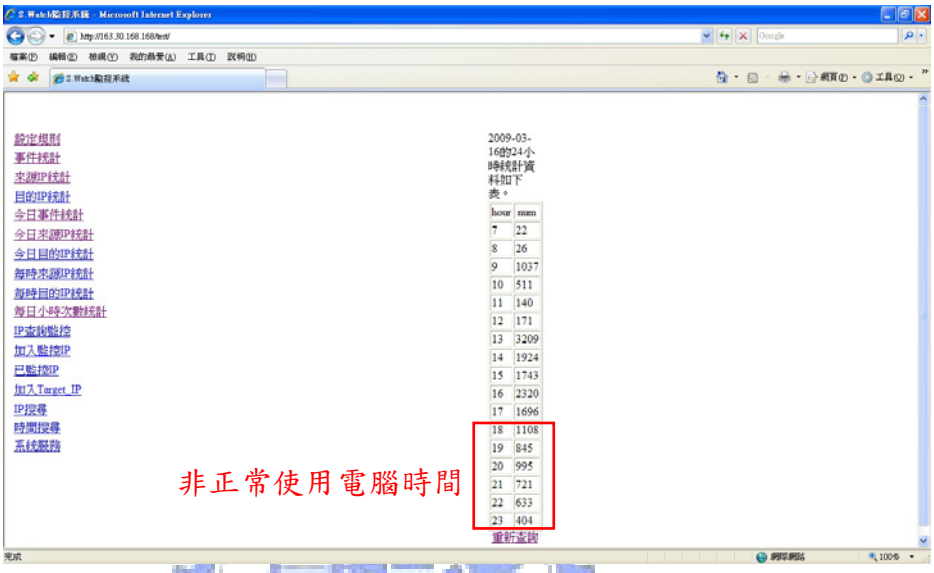

圖 34　異常傳輸情況

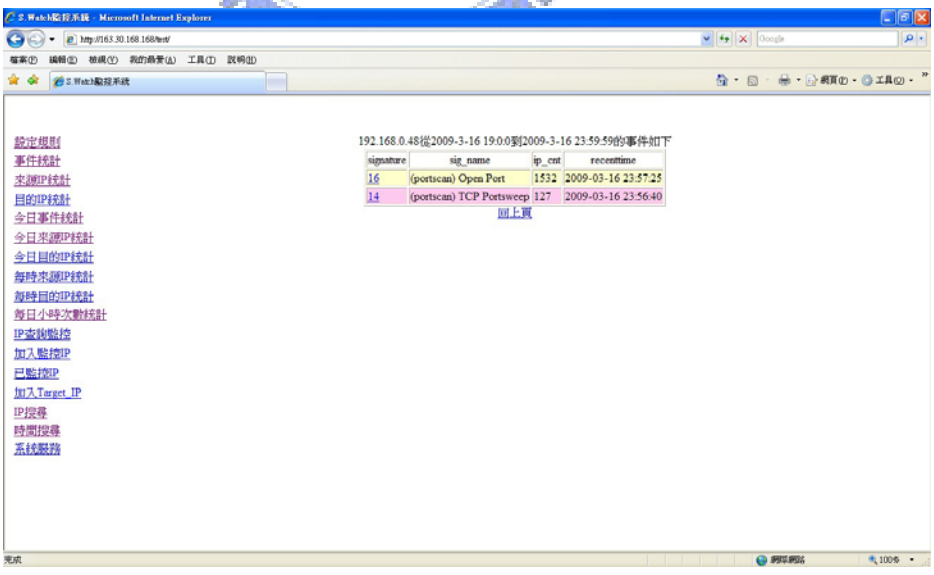

圖 35　觸發警訊的 IP 及事件

藉由每小時的次數統計，並與過去的紀錄作比較，可以得知網路目前使用的狀況是否有異常發生，以便網路管理者即時處理異常狀況。

（三）監測即時通訊的使用

即時通訊（Instant Messaging，簡稱 IM），是一種允許兩人或多人使用網路即時的傳遞文字訊息、檔案、語音與視迅交流的服務[31]。比較著名的即時通訊軟體有 Yahoo Message 及 MSN 等。即時通訊雖然方便，也帶來了不少病毒的威脅。許多入侵者利用即時通訊散播病毒連結，常使得使用者在不察的情況下點取連結，造成電腦中毒及資料外洩。由於學生普遍會使用即時通訊軟體來交談，因此在電腦教室若不加以控管，不僅影響學生學習，也很容易會成為散播病毒的媒介。

圖 36　使用 Yahoo Messager 的電腦 IP 列表

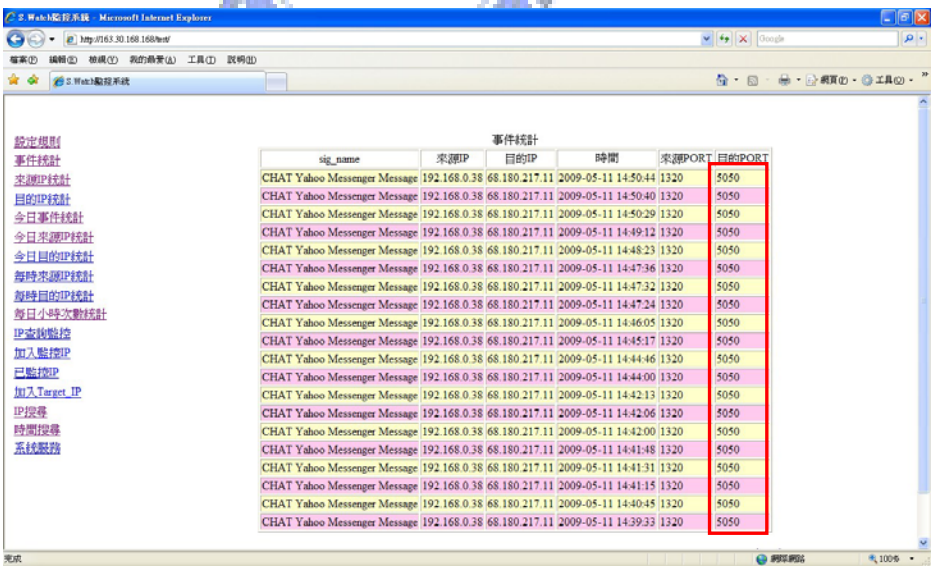

圖 37　CHAT Yahoo Messenger Message 警訊的目的 PORT

（四）使用 P2P 的偵測

點對點技術（Peer-to-Peer，簡稱 P2P），是一種網路新技術，具有相當多廣泛的用途。最常見也是最為人所熟知的用途是在檔案分享方面，如 eMule、eDonkey、BT、Foxy 等 P2P 檔案分享軟體。由於使用 P2P 軟體下載檔案時，會佔據大量的頻寬，且下載分享的檔案還涉及到著作權等法律問題，因此在校園中是禁止使用 P2P 軟體的。

Snort 規則中，設定針對 P2P 的封包傳送規則。透過 Snort 的偵測，可以即時的發現使用 P2P 傳輸檔案的訊息。如下圖。

圖 38　P2P 傳輸檔案警告訊息

圖 39　使用 P2P 傳輸的電腦 IP 位址

5.3 封鎖異常行為

本節針對監測環境中所偵測到的異常行為，即時通訊、P2P 及限制網站存取，如何以利用 ABBA System 進行封鎖做介紹。

（一）封鎖即時通訊

透過 ABBA System 的監測，我們發現當使用 Yahoo Messager 時，使用者會先連接到即時通訊 Server，以下載好友名單及狀態。如果在其連接即時通訊 Server 之前，將即時通訊程式的連接封包加以封鎖，使客戶端無法連接即時通訊 Server，即可封鎖住使用即時通訊的行為。以下為 Snort 偵測到 CHAT Yahoo Messenger Message 警告發生時，所連接的即時通訊 Server。

圖 40　即時通訊的 Server 列表

透過加入 Target_IP 將即時通訊 Server 寫入 guardian.target 中，當 Snort 偵測到有 CHAT Yahoo Messenger Message 警告發生時，即可透過 Guardain 呼叫防火牆阻擋封包的傳送，阻止使用者與即時通訊 Server 連接。且因為只會封鎖住即時通訊的 Server，因此並其他正常網路瀏覽，並不會因此而受到限制。

（二）封鎖 P2P

由於使用 P2P 會直接對於網路頻寬造成重大的影響，且藉由 P2P 下載檔案的同時，也同時分享本身電腦的檔案，容易造成個人資訊外洩及有侵犯著作權的問題。因此，當發現校園內電腦有使用 P2P 程式下載檔案時，應立即監控其所有 IP 活動，並加以封鎖。利用 ABBA System 的事件 IP 統計模組，直接將發現使用 P2P 軟體傳輸檔案的 IP 加加入監控，並由監測／封鎖模組直接封鎖 IP 活動。

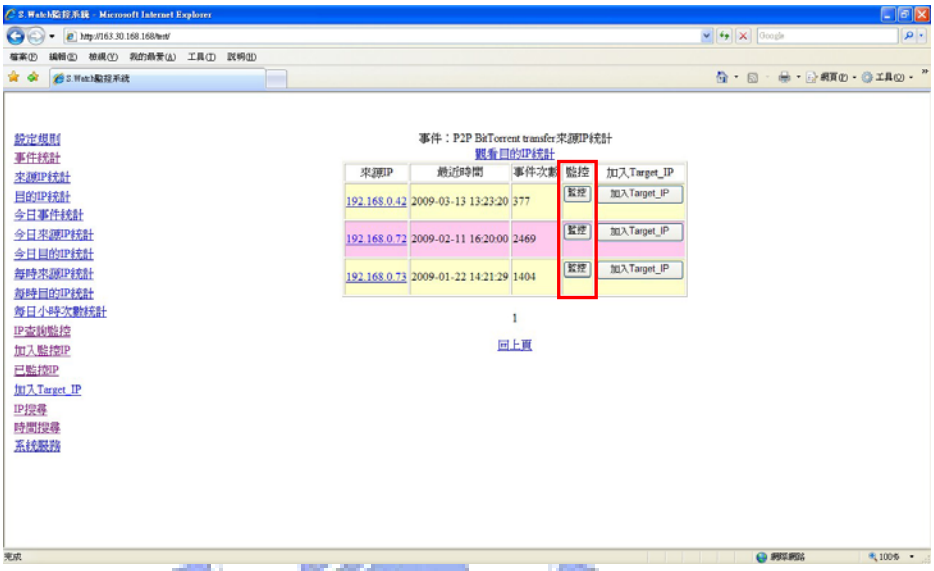

圖 41　加入監測 IP

圖 42　封鎖使用 P2P 軟體的 IP

由於 P2P 所連結下載檔案的電腦太多，因此直接將使用 P2P 傳輸檔案的電腦 IP 位址封鎖其所有封包，停止其所有網路活動，自然可阻止該 IP 與外部 IP 進行連結下載檔案。

（三）限制網站的存取

從 ABBA System 的事件 IP 統計模組中觀察，發現引發事件警訊的目的 IP，大部分都是瀏覽網站所留下的紀錄。因此藉由引發警訊的事件 IP，我們可以藉由查詢得知使用者瀏覽哪些網站。

在 2009 年 3 月 23 日，Snort 從 61.57.152.165 這個 IP 位址，偵測到了異常的 ICMP 封包發送。經過查詢，發現此 IP 為一線上遊戲網站所使用。將該 IP 加入監測名單，並透過 ABBA System 的監測封鎖模組，封鎖該 IP 網站的封包進入，以限制該網站的存取。

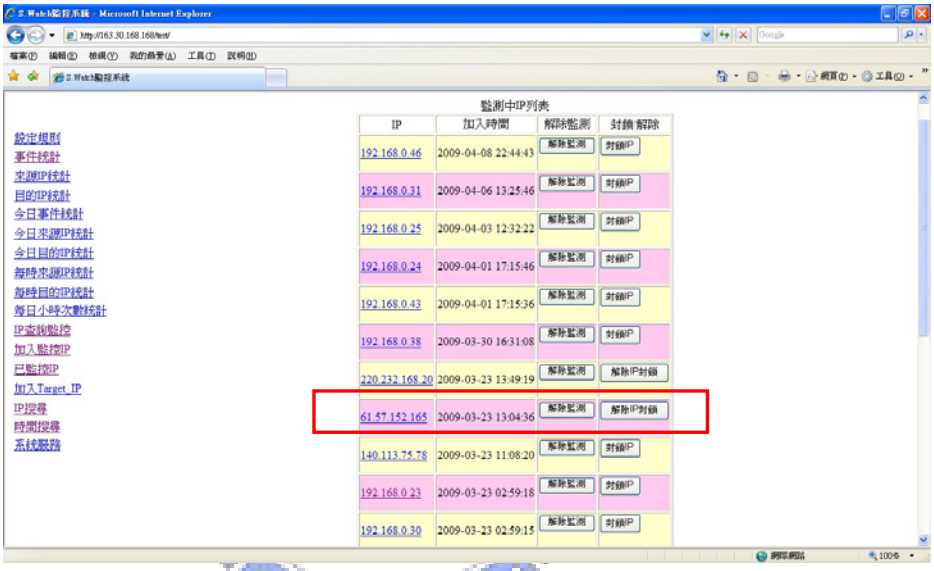

圖 43　限制網站的存取

透過監控／封鎖模組限制遊戲網站的存取，可以避免學生因沈迷遊戲網站而荒廢上課的學習，也可避免因安裝遊戲，連帶的也將後門程式一起安裝入電腦中，減少電腦遭受入侵的機會。

第六章　結論

網路的發展越興盛，政府或企業利用網路來提供服務的頻率也越來越高。各級教育單位也伴隨著這股科技趨勢，開始提供各式各樣的多元網路服務。隨著各項資料的 E 化，如電子公文及學生成績的資訊化，雖帶來了不少便利，但也伴隨著各種危機。如駭客的入侵，導致學生資料外洩或成績遭到竄改等。本論文的主要研究目的即在於提升校園網路的安全性，預防入侵，以防護重要資料的安全。

6.1　結論

本研究實際在國小電腦教室中蒐集 Snort 所產生的警訊，並利用 ABBA System 進行統計分析，經由分析的結果，讓網路管理人員瞭解目前網路的異常狀況，且藉此擬定因應的措施，以達到提升校園網路安全的目的，獲得良好的效果。實際經由 ABBA System 分析 Snort Log，發現的確可以幫助網路管理人員省下許多察看 Log 的時間，而且藉由觀察可以得知異常狀況，並藉由 ABBA System 的監控／封鎖模組加以封鎖阻止，以免危害擴大，造成更大的損失。

國小教師由於編制的原因，資訊組長往往都由教師兼任。在班級數比較多的大型學校，資訊組長可以由教師專任，專門負責處理校園網路及電腦維護的事務。但在班級數比較少的學校，往往都由帶班的導師兼任資訊組長。且在師資培育過程中，並非所有的老師都具有資訊專長，或是對網路有充分的瞭解與認識。往往是接任資訊組長職務之後，才開始接觸有關網路的知識。在人力資源不足的情況下，單靠資訊組長一人來負責整個校園網路安全是不夠的。如果能夠有一個可以方便快速掌握網路狀況的資訊系統，來協助網路管理者，降低網路管理的工作負擔，是每個網路管理者所期望的。

雖然大部分的校園網路，通常都會架構防火牆作為防止駭客入侵的第一道防線，但駭客的攻擊方式與手法也隨著網路的發展越來越成熟且多樣化。尤其現在資訊發達，在網路上很容易便搜尋到入侵方式的教學，以及相關入侵攻擊的軟體與程式，使得網路入侵事件有逐年增加的趨勢。面對層出不窮且變化多端的網路入侵攻擊，單靠防火牆的防禦是不夠的。本研究以入侵偵測系統 Snort 及防火牆 Iptables 為基礎，搭配 PHP 開發出 ABBA System，協助網路管理人員有效的從眾多的警示訊息中分析出可疑的入侵行為，並透過防火牆加以封鎖。

本研究透過結合入侵偵測系統(Snort)與防火牆(Iptables)的實作，搭配 ABBA System 的分析，確信可以達到以下目的：

1.不需額外經費支出下，建構更安全的網路環境。

Snort、Guardian、Iptables、 ABBA System 所開發使用的語言（PHP）及資料庫（MySQL），都是屬於自由軟體，可以免費使用，不需另外花錢購買。

2.不需改變現有網路架構，提升校園網路安全。

本研究所使用的 Snort 系統屬於網路型偵測系統（NIDS），具有架設成本低，且不需改變網路架構，只需增加偵測主機等優點。

3.有效減輕網路管理者負擔，增加工作效率。

透過 ABBA System 可以快速掌握並處理 Snort 所偵測到的警示訊息，減少狀況判斷的時間。

4.能有效封鎖網路異常行為。

透過 ABBA System 的監測封鎖模組，可以達到主動防禦及監測可疑 IP 的能力，並藉由防火牆加以封鎖異常行為。

5.能洞燭機先，防範未然。

藉由 Snort 入侵偵測及 ABBA System 統計分析，能夠使網路管理者有充分的時間與資訊來處理網路異常行為，而能避免因時間延宕而造成網路或系統的破壞，以致設備的維修經費支出及重建系統的時間浪費。

6.2 校園網路安全建議措施

從網際網路各項服務的發達以及越來越大的網路頻寬來看，顯而可見未來網路的應用將越來越普及在校園生活中。而校園網路的入侵威脅更是一刻也未曾停止過。因此對網路管理者提出未來校園網路安全及防護措施建議如下：

1.隨時更新系統修正程式

大部分校園電腦的作業系統都是屬於 Windows 作業系統，也是駭客及病毒最容易攻擊入侵的對象，因此網路管理人員一定要隨時注意系統漏洞與弱點的修補，安裝最新的修正程式。

2.時常檢視防火牆規則與入侵偵測系統紀錄

透過紀錄的分析，可以瞭解網路狀況或發現已發生的攻擊行為，可以即時修補漏洞，更新防火牆規則。

3.入侵偵測系統的調校與規則更新

根據實際的網路狀況及架構，進行調整，以減少入侵偵測系統的誤判（False Positive）及漏判（False Negative）；並注意規則的更新以偵測新的威脅。

4.防範後門程式及病毒

經實際的紀錄分析，發現有不少主機開啟不明的 Port，因此要注意後門程式及病毒入侵的可能性。

5.使用者資訊安全素養的提升

教導使用者有「正確使用電腦」的觀念：不下載、安裝不明程式；不瀏覽可疑或非法網站；避免轉寄來歷不明的電子郵件，避免病毒感染。

6.3 未來研究方向

未來後續研究方向可朝下列方向進行：

1.分析機制的自動化

目前 ABBA System 的分析是以紀錄行為特徵次數，交由人工來判斷是否有可疑的入侵行為，未來可以研究類神經網路技術來進行自我學習及分析的方式，達到自動分析的結果。

2.簡訊即時回報模組

由於手機的便利與普及，未來可在系統加入簡訊通知模組，在系統偵測到有特定事件(如：P2P 傳輸)發生時，即時以簡訊通知網路管理人員進行封鎖及處理。

3.主機紀錄的交叉比對

結合主機上的各種服務所產生的日誌檔，如 syslog、messages、httpd log 等，做全面的比對分析，針對異常行為作更完善的分析，以期更能夠完全掌握入侵行動。

參考文獻

[1] Jay Beale, James C. Foster, Jeffrey Posluns, Ryna Russell, and Brian Caswell. Snort 2.0 Intrusion Detection. Syngress, 2003。

[2] 沈文吉（2001）。網路安全監控與攻擊行為之分析與實作。國立台灣大學資訊管理研究所碩士論文，未出版，台北市。

[3] 莊振宏（2003）。針對網路銀行之異常偵測模組研究。長庚大學資訊管理研究所碩士論文，未出版，桃園縣。

[4] 蘇俊維（2003）。網路安全威脅分析與防制策略。東海大學資訊工程與科學研究所碩士論文，未出版，台中市。

[5] 陳永烈（2004）。以入侵偵測系統為基礎之主動式網頁過濾及阻擋機制。逢甲大學資訊工程學系研究所碩士論文，未出版，台中市。

[6] 林仁傑（2004）。自動排序入侵偵測。逢甲大學資訊工程學系碩士論文，未出版，台中市。

[7] 李為漢（2005）。網際網路惡意程式之活動調查—以某企業對外網路連線為例。國立中央大學資訊管理研究所碩士論文，未出版，桃園縣。

[8] 劉博瑋（2006）。使用入侵偵測系統與流量控制模組減緩分散式阻斷服務攻擊。逢甲大學資訊工程學系研究所碩士論文，未出版，台中市。

[9] 陳美君（2007）。運用線上分析處理與資料探勘於網路流量分析。國立交通大學管理學院（資訊管理學程）碩士論文，未出版，新竹市。

[10] 教育部（2001）。中小學資訊教育總藍圖。

[11] 盧盈如。主機弱點檢測及網路入侵偵測系統在校園網路中的應用。中正學報第七期，141, 142。

[12] 蕭漢威、楊錦生、魏志平、馬淑貞。以網路流量資料探勘進行阻斷服務攻擊偵測之研究。資訊管理學報，第十四卷，第二期，5。

[13] 蘇建郡、方鵬喜。Snort 於網站管理之應用。第三屆離島資訊技術與應用研討會，2003 年 6 月。

[14] 陳炳彰、張耀生。具有可追蹤攻擊者的網路式入侵偵測系統。2008 數位科技與創新管理研討會，2008 年。

[15] 薛宇盛。網路入侵偵測系統實務 WinSnord for Wireless 加強版。台灣：松崗電腦圖書有限公司，2008 年。

[16] 資安專家：校園電腦恐成駭客殭師大軍。2009 年 1 月 12 日，取自 http://www.zdnet.com.tw/news/comm/0,2000085675,20115706,00.htm。

[17] 提升校園資訊安全服務計畫。2009 年 1 月 12 日，取自 http://cissnet.edu.tw/case_school_01.aspx。

[18] DDOS 阻斷服務攻擊。2008 年 8 月 12 日，取自 http://netflow.tceb.edu.tw/virus/DDOS.html。

[19] ICMP DoS(Denial of Service)阻絕服務攻擊之防禦方法。2009 年 1 月 13 日，取自 http://www.iii.org.tw/adc/papers/thesis/00B02.htm。

[20]DDoS 攻擊的趨勢與防禦策略。2008 年 8 月 12 日，取自 http://www.cert.org.tw/document/column/show.php?key=73。

[21]何謂電腦病毒。2008 年 8 月 13 日，取自 http://www.microsoft.com/taiwan/athome/security/viruses/intro_viruses_what.mspx。

[22]如何協助電腦對抗病毒。2009 年 1 月 14 日，取自 http://www.microsoft.com/taiwan/athome/security/viruses/intro_viruses_protect.mspx。

[23]蠕蟲病毒－維基百科。2008 年 8 月 13 日，取自 http://zh.wikipedia.org/wiki/%E9%9B%BB%E8%85%A6%E8%A0%95%E8%9F%B2。

[24]防毒入門。2008 年 8 月 13 日，取自 http://www.hkedcity.net/article/edmall_feature/trendmicro1/。

[25]病毒、蠕蟲及特洛伊木馬程式簡介。2008 年 8 月 13 日，取自 http://www.microsoft.com/taiwan/security/articles/virus101.mspx。

[26]網路駭客攻擊－分散式阻斷服務（DDoS）攻擊。2008 年 8 月 13 日，取自 http://www.ascc.sinica.edu.tw/n1/89/1620/02.txt。

[27]入侵偵測系統－降低網路安全風險。2008 年 8 月 26 日，取自 http://www.symantec.com/region/tw/enterprise/article/intrusion_detection.html。

[28]http://www.snort.org。

[29]賴溪松，“網路安全基礎概念”，http://crypto.ee.ncku.edu.tw/class/network_security/93/Ch1.pdf.

[30]http://www.chaotic.org/guardian/。

[31]http://zh.wikipedia.org/