無線網路下自動化入侵偵測系統設計與實作

李俊毅　　陳毓璋
術德科技大學資訊工程系
s94639101@mail.student.stu.edu.tw　sclass@ms1.hinet.net

摘要

現今每個人都享受著無線網路所帶來的便利性，但大多數的人都會忽略存在於無線網路上的威脅，由於無線網路屬於開放性的環境，若有攻擊者處於無線網路的涵蓋範圍下，就可以針對無線網路範圍下的任何主機進行攻擊行為。為了要早一步發現來自於網路上的惡意攻擊行為，進而發展出入侵偵測系統(Intrusion Detection System， IDS)，但 IDS 只能偵測到是否有惡意攻擊行為，卻無法針對此行為做隔離動作，這樣一來對於網路內部的主機造成的威脅性不減反增。本研究提供在無線及有線網路下的主動式入侵偵測系統，若偵測到有惡意攻擊行為系統可將此行為做阻隔動作，並記錄下此攻擊行為，作為往後偵測攻擊行為的依據，也可監控處在該網路底下的主機狀態。

關鍵詞：無線網路、開放性、攻擊者、入侵偵測系統。

Abstract

Everybody enjoys the wireless convenience brought of network now, but most people will neglect the threat of the existence in the wireless network, because the wireless network belongs to the open environment, if there are assailants under the range of containing of the wireless network, can carry on the attack to any host computer under the wireless network range . In order to want early step to find that come from the hostile attack on the network, and then development comes in and goes out and invades and detects and examines the system (Intrusion Detection System , IDS), but IDS can only detect and have a hostile attack to examine to , but unable to do movements of isolating to this behavior, do not reduce increasing to the threat that the host computer within the network causes instead in this case. The active invasion offered under the wireless and wired network in this research detects the system of examining, can do movements of separating of this behavior if detect and examine to and have hostile attack systems, and note this attack, as detecting the basis of examining the attack backward, can control and is in the host computer state under this network . This paragraph describes the major work in your paper.

Keywords: . wireless、opening、assailant、IDS

1. 前言

現今社會的資訊越來越發達，每個人對於網路的需求量也日益增加大，網路上所存在的危險性也逐漸增高。目前無線網路的興起，提供廣大使用者勤更方便的使用網路環境，目前的電腦已將無線網路列為必備內建功能，因此，隨時隨地上網的願景遂成為可能，但是對駭客而言，面對如此方便的無線網路，尤其在公共環境下，更將如魚得水。目前無線網路的安全性仍有許多值得加強之處，無線網路雖然帶來便利，但也可能形成企業資訊安全防護上的漏洞。無線區域網路所採用的開放式環境，讓擁有可自由存取無線網路的有心人士輕易擷取到傳遞中的任何訊息。

本研究主要讓管理者進行安全管理能力及分析行為，已達到流程自動化和提供即時反制能力，隔離不必要的危險行為，讓網路使用者能夠安心的存取有線及無線網路，並隔絕惡意人士進入網路。本子計劃系統目前實作於樹德科技大學的資訊工程研究所，重點在於可即時偵測、防範網路攻擊及入侵行為，在第一時間發現攻擊或入侵發生，系統即可立刻採取回應與隔絕措施，以確保網路使用者及重要主機的安全。

2. 參考文獻

現在網路的使用量逐漸增加，存在在網際網路下的威也日益增多，為了發現是否有惡意行為正在存取使用者的主機，進而發展出入侵偵測系統(Intrusion Detection System， IDS)，以下會對於 IDS 做個簡單的介紹。由於現在無線網路環境的發達，越來越多的使用者感受到無線網路環境所帶來的便利性。但無線網路環境雖然便利，可是在這其中所隱藏的危機卻不小，以下我們針對無線網路環境及一般網際網路上所存在的攻擊及危險詳細介紹。

2.1 入侵偵測系統

入侵偵測系統的功用為偵測出疑似入侵的行為，入侵行為包含了破解資訊資源的保密性、破壞修改原始資訊的完整性以及擅自使用系統資源等侵權之行為，而入侵偵測所偵測的對象則包含偵測

出擅用系統資源的入侵者或是誤用系統資源的合法使用者。若將各種入侵偵測的方法以及流程做有系統的統整，就成為了入侵偵測系統(Intrusion Detection System， IDS)。

IDS 在網路裡扮演著監控網路中各項活動的警衛，大部分的 IDS 都是以解讀各種封包內容、執行網路流量監測或是分析系統紀錄等方式來找尋可能入侵的行為，並且做出適當的反應。根據這種特性可以發現 IDS 需要一套規則來判定是否該行為已達到入侵的意圖，這些規則就是所謂的特徵(signatures)，符合特徵就可以判定為蓄意的入侵或有攻擊的意圖。若是特徵定得太鬆散便無法達到完全偵測的效果，失去使用的意義;若特徵訂得太嚴苛，就可能常發生誤判的情形，因此，IDS 最重要的部分就是在於特徵的訂定。

IDS 可分為三種類型，分別為 Network-Based IDS、Host-Based IDS 以及 Application-Based IDS，Network-Based IDS 主要是分析網路封包為主,可達到事先預警，而本系統架構接近於 Network-Based IDS，但不屬於上面幾種典型的 IDS 類型，典型的 IDS 是處理 OSI 第三層以上的資訊，僅處理第二層資料鏈結層部分，屬於非典型入侵偵測系統。入侵偵測系統有三項主要功能，分別為監視目前狀態、偵測處理以及反制方式，此三項功能為完整的入侵偵測流程，構成了入侵偵測的系統模型。

2.2 網路攻擊方式

目前網路的使用量大增，來自於網路上的惡意攻擊行為手法也日新月異。現在的攻擊方式大略可分為以下幾種：衝區溢位 (Buffer Overflow) 攻擊、通訊埠掃瞄 (Port Scan) 攻擊、木馬程式 (Trojan Horse) 攻擊、碎片封包 (IP Fragmentation) 攻擊及蠕蟲 (Worm) 攻擊等[3]，大多數的攻擊方式都是利用系統漏洞來進行攻擊行為，已達到竊取資料或癱瘓對方服務的目的。有些攻擊方式是使用程式語言上一些語法本身設計不嚴謹，讓使用者在執行程式造成錯誤進而引發系統錯誤。有不少的攻擊方式都是利用使用者自己的粗心大意，讓許多的惡意程式常駐在自己本身的主機裡，使得攻擊者可隨時進入到使用者的主機內竄改或竊取資料。現在大多的攻擊行為都不是以竄改竊取資料為目的，而是癱瘓對方所提供的服務為目的，像蠕蟲攻擊，利用蠕蟲可自行發佈的方式，將蠕蟲發佈到網路上所有的電腦，然後同一時間內引發，造成網路全部癱瘓。

2.3 無線網路中的威脅

目前線存在無線網路環境中的威脅有嵌入式攻擊、未經授權的無線傳輸攔截與監控、人為干擾、client-to-client 攻擊及無線存取點探測等[5][1]，無線網路與有限網路不同的地方，無線網路中只要有心的攻擊者需要在一個無線存取點的範圍之內(802.11b 大約是 300 英尺)對無線網路內的主機進行攻擊，而有線的攻擊者則是可以在任何與網路連接的地方對有線網路內的主機進行攻擊。阻絕服務攻擊也適用於無線網路，當非法傳輸的頻率覆蓋合法傳輸時，合法傳輸無法抵達 client 端或無線存取點。入侵者利用適當的設備和工具能夠輕易的使無線網路頻帶氾濫，破壞此信號直到無線網路結束運作為止。此外，無線電話、嬰兒監視器和其他運作於 2.4GHz 頻帶上的裝置，能夠中斷使用這個頻率的無線網路。服務阻絕可能源自無線存取點服務的工作範圍外，或者源自其他安裝在低於所有訊號網路範圍的 802.11b 裝置。無線網路為強調使用的簡易與快速的部署，許多無線存取點在不安全的架構中運輸。除非管理者瞭解無線安全風險並對每一個單元進行適當的部署，這些無線存取點將會置身於攻擊或誤用的高風險環境下。

3. 系統設計

以下我們提出本系統的系統架構，來偵測目前網路上所存在的惡意攻擊及入侵行為，可自動阻擋惡意攻擊行為，進而紀錄攻擊者的行為模式作為後偵測的依據，並且管理監控內部區域網路的主機設備。

3.1 系統架構

本系統整體系統架構如圖一所示。Attacker A/B 負責扮演有線網路上的正當使用者及攻擊者，Attacker C 作為無線網路的正當使用者及攻擊者，用來驗證整個系統是否可正確判斷使用者的行為是否屬於正當或惡意。Wireless Authentication Server 主要用於驗證在無線網路上的使用者是否是屬於我們所認定的合法使用者，可直接過濾非法使用者。Target A/B 做為內部網路提供網際網路服務及存放重要資料的主機。IDS Server 負責檢查進入及出去的網路封包，偵測是否有惡意行為的封包，如果偵測到有惡意阻斷內部服務的行為(例如 DDOS 攻擊)，會此一攻擊行為導入 Honey pot Server，以便紀錄分析攻擊者的行為，或是自動告知 Switch 將通往內部網路的 Port 關閉，使攻擊者無法進入攻擊，並且會自行偵測對於在無線網路上可能存在著攻擊行為。L4 Switch 可直接監控網路第四層以上的資訊，並且可提供負載平衡，可分散底下主機所提供的服務，不會讓單一主機有過多服務要求，也可利用 L 4 swtich 直接針對網路連線 port 進行關閉開啟，對內部區域網路而言，本系統利用 L4 Switch 做 VLAN 的管理，提高內部主機的安全性。NMS 主要功用是做紀錄內部及外部網路流量，並且控管內部網路下的所有網路設備。本系統分成三個模組來來設計整個系統，分別為入侵偵測系統(IDS

server)、網管系統(WMS server)以及 Honey pot 系統。

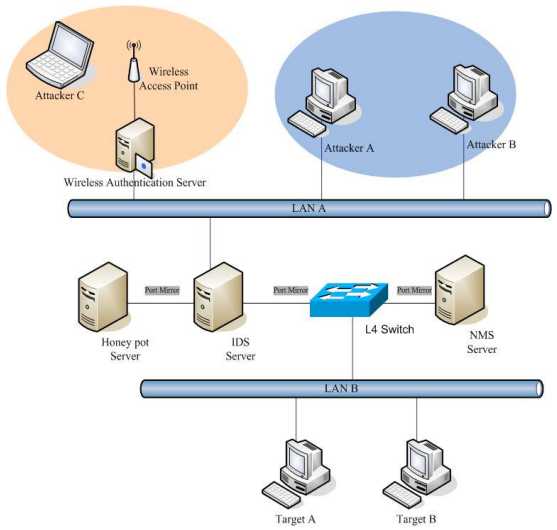

圖 1 系統架構圖

3.2 入侵偵測系統模組

本系統模組架構如圖二所示，使用 SNORT[6]作為入侵偵測的主要工具，並且連接 MySQL 可存放入侵偵設紀錄，可利用 XML 格式將攻擊訊息紀錄下來，再將攻擊訊息傳回網管系統模組，做進一步的阻絕攻擊動作，整個系統搭配 Apacha server 及 ACID[7]以 web 介面操作，讓管理者可利用 web 介面了解系統目前狀態與即時攻擊訊息。系統平台的作業系統採用 Red Hat Linux Fedora Core 3，提供管理者一個穩定及安全性高的管理環境

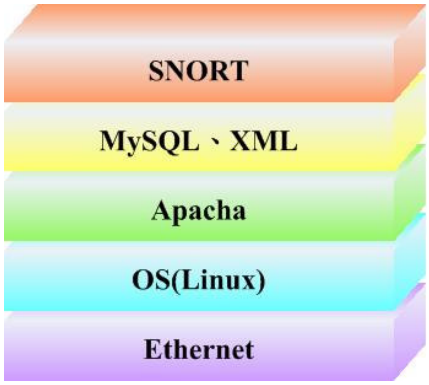

圖 2 入侵偵測系統模組架構圖

3.3 無線網路入侵偵測系統模組

圖三為「無線網路入侵偵測系統模組」之系統架構圖[2]。本模組能夠在異質的無線網路環境下，適時的偵測、防制無線網路中的入侵事件。其中，Packet Capture Module 負責監聽、儲存 WLAN 中的傳輸封包與流量資訊，提供網管人員作為平時稽核與網路犯罪蒐證之用；Intrusion Reaction Modules 則是負責偵測該無線區域網路中的入侵行為，並即時採取相對應之處理程序；此外，GSM 警示模組負責在偵測發現入侵行為時，發送簡訊給系統管理者。倘若攻擊者(Hacker)企圖攻擊 Access Point 範圍內之使用者，將會預先由「無線網路入侵偵測系統」所察覺並阻隔。

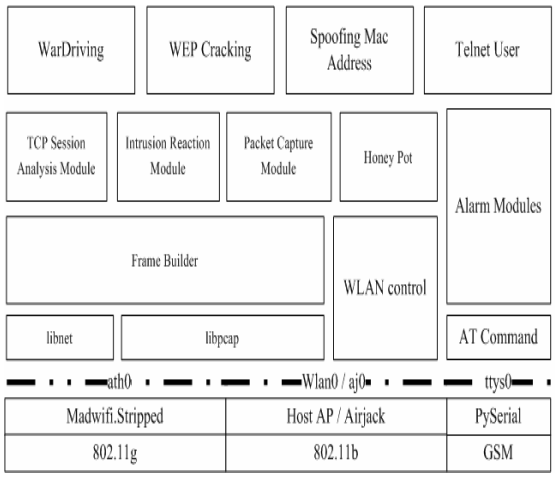

圖 3 無線網路入侵偵測系統架構圖

3.4 Honey pot 系統模組

Honey pot 系統架構圖如圖四所示，作業系統採用 Linux Red Hat 9.0，主要是提供系統一個較安全及穩定的環境。再利用 Sebek[4]架設整個 Honey pot 系統，Sebek 是用來記錄使用者操作行為的工具，主要是在記錄大多數入侵者在 honeypot 上的活動記錄；Sebek 是一種隱藏在系統核心裡面的一種捕獲工具，所以它不容易被入侵者發現，可以在入侵者完全不知情的情況下清楚記錄入侵者的一舉一動，以便提供管理者分析及修改 IDS 比對規則的依據，並且可以欺騙攻擊者延長攻擊 Honey server 的時間，提高內部主機的安全性及存活率，Sebek 的系統流程如圖五所示。

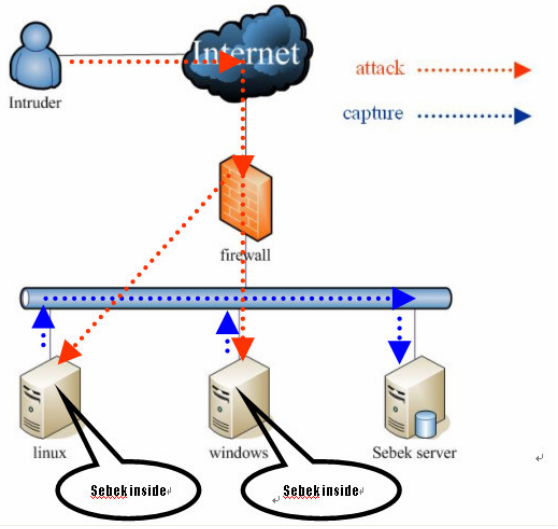

圖 5 Sebek 系統流程圖

3.5 網管系統模組

本網管系統模組架構圖如圖六所示，主要的管理介面由 PHP 撰寫而成，另外結合 Expect[8]語言，可背景式管理 L4 Switch 內部設定，並且可做到 Interactive Program 的操作自動化，所謂 Interactive Program（交談式程式）指的是設計來與真人互動的程式。在網路管理上，我們常要同時大量更改網路設備組態，這時用程式去把流程自動化是必要的，這樣一來可以減少管理者在管理上許多繁雜的工作。在整個網管系統上，我們利用 Apacha server 將系統以 Web 方式提供給管理者使用，這樣管理者可以利用遠端方式來管理網路設備。本系統模組的作業系統採用 Red Hat Linux Fedora Core 3，主要是提供給使用者有高穩定性的管理操作環境。Switch 的部分採用 Nortel Alteon Application Switch 2208[12]。

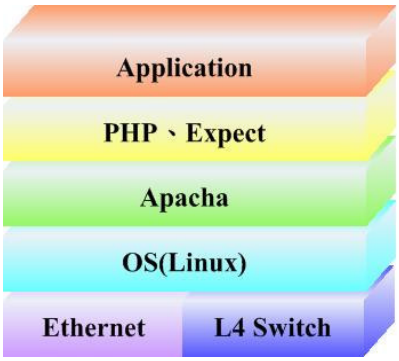

圖 6 網管系統模組架構圖

4. 實作成果

我們依照所規劃的系統架構實做系統，從圖七及圖八所示可以看到我們利用 Snort 搭配 ACID 的入侵偵測系統畫面，圖上可以看到在比對出有入侵攻擊封包的時候能將比對出的訊息顯示在畫面上，讓管理者清楚知道入侵者的行為，以便管理者做相關的處裡。並且搭配 web 介面，管理者只要透過網路環境就可以隨時利用 web 介面使用系統。

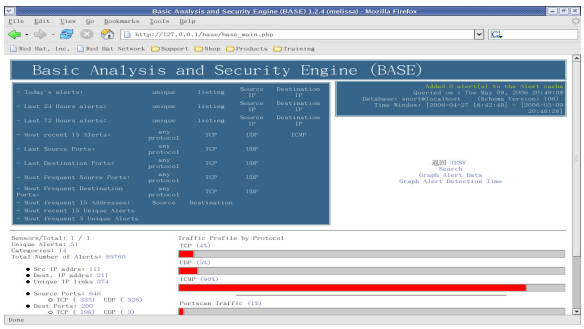

圖 7 入侵偵測系統畫面

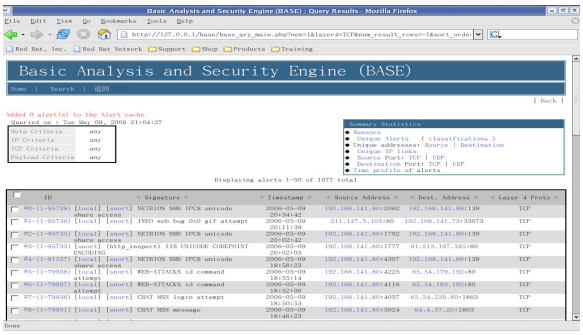

圖 8 入侵偵測系統畫面

當系統偵測到有入侵攻擊行為封包的時候，會依照系統所設定的危險層級作相關的處裡，並且將攻擊行為封包導向至 Honey pots server，將攻擊者的行為特徵紀錄分係，作為日後再偵測攻擊行為的依據比對，這樣一來可提高系統在偵測攻擊行為時的準確度，如圖九及圖十所示。

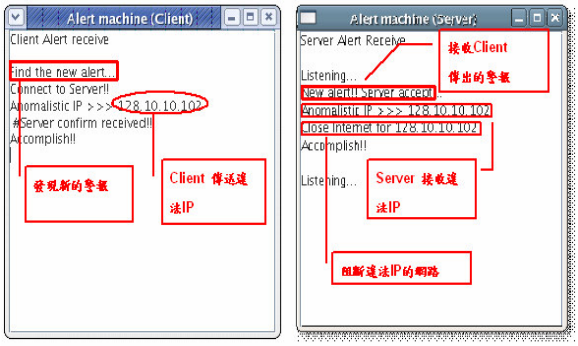

圖 9 入侵攻擊行為通告

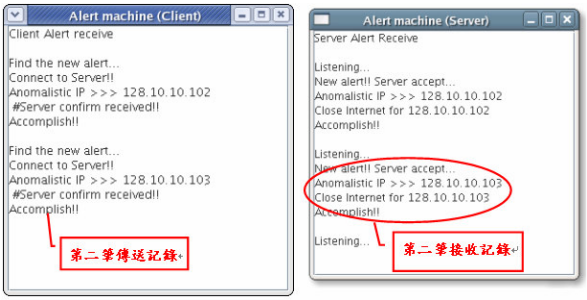

圖 10 入侵攻擊行為通告

IDS Server 不斷接收來自 Layer 4 Switch Mirror Port 的 Traffic package，經由 Snort Rules 與 Preprocessor 檢測所有封包流量內容，並判斷是否有入侵或不法的網路行為，如果有則產生警報並透過 Syslog 通訊方式轉送異常資訊給 WANMS 的 Syslog Host；而 WANMS 會於每分鐘會檢查一次新收到的 Syslog Message，如果發現異常，將依該 Syslog Message 內容檢查對應的網路流量及設備 Alarm，並確認是否也有異常之處，若依據的規則成立，則觸發執行 Expect Script，登入 Layer 4 Switch 修改 Routing Table，將異常之封包流量依警報類別進行將可疑流量重新導向至誘捕系統或直接將此攻擊

流量封包丟棄。

IDS server 動作流程如圖十一所示，一開始會擷取網路封包，在利用目前已知的攻擊行為規則做比對，如果是比對出此一封包為惡意的封包，會將此一資訊儲存於資料庫，並且產生 Log 檔以便管理者做分析之用途，系統會依照產生出來的 Log 檔擷取出目的 IP 及行為並且傳送至 Server 進行阻斷及導向的動作，也會同時通知管理人員，讓後端管理人員更清楚知道現在所正在發生的事件。

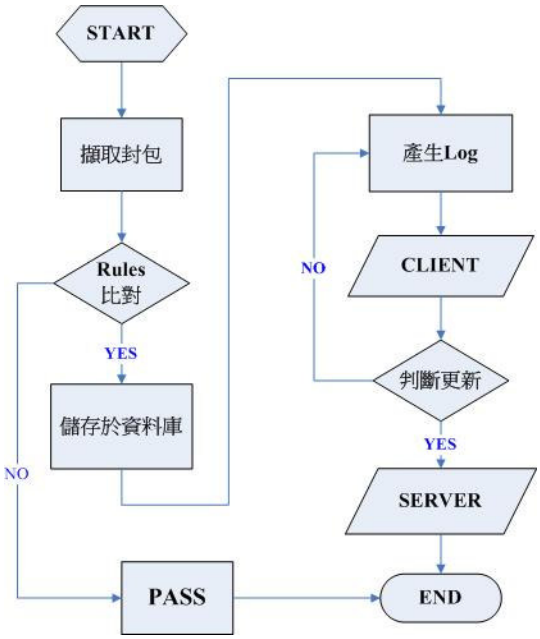

圖 11 IDS server 系統動作流程圖

圖十二為 Honey pot server 監視畫面，在畫面上可以看到我們成功的記錄下攻擊者的行為，管理者可以利用此紀錄分析攻擊者的行為，來新增 IDS server 的入侵攻擊比對規則，並且可以欺騙攻擊者，讓攻擊者以為自己已達成目的，確保內部網路上重要主機的安全性。

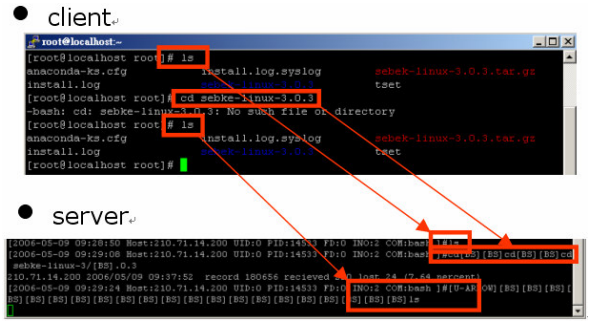

圖 12 Honey pot server 監視畫面

另外管理者可以利用本系統所提供的網管系統模組，可透過網路使用系統模組所提供的 web 介面隨時隨地的監控內部主機的情形，如果內部主機有異常行為發生的時候，管理者可透過系統內的監控功能，直接管理內部主機，如圖十三及圖十四所示。

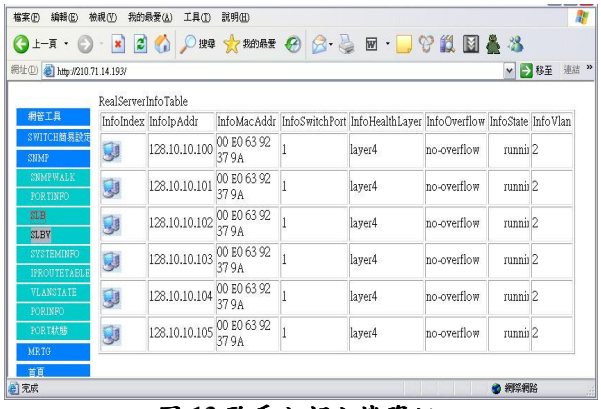

圖 13 監看內部主機資訊

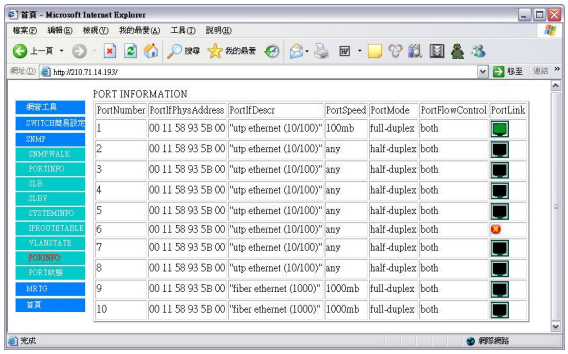

圖 14　Switch port 狀態

管理者可利用網管系統模組產生系統報表，報表上可記錄某一段時間內有多少惡意行為封包進入或內部往勒的設備異常，可作為往後調整系統的依據，管理者也可依照報表內容分析攻擊者的行為，可作為修改入侵偵測比對規則的依據。在網管系統模組下也提供訊息通知功能，系統在偵測到有異常行為的時候，可依照管理者事前所設定的訊息通知方式來告知管理者，讓管理者可以第一時間內得知異常行為的警報。

5. 結論

從系統實作結果看到本系統入侵偵測系統模組可在第一時間內發現惡意行為封包時，可發送訊息告知網管系統模組，網管系統在依照告知訊息內容對於惡意行為封包自行做隔離或導向的動作，與以往由人員自行做隔離或導向的動作不同，可提高整理效率，並且利用 Honey pot server 欺騙攻擊者及收集新的攻擊方式，提高系統對於入侵攻擊行為的辨識率。之後將整合身分驗證功能來提高整體系統安全性，並且增加反向追蹤功能，可針對惡意封包做反向追蹤，以降低入侵攻擊行為的發生，並且可在無線網路環境上有反向追蹤的能力。可利用所偵測到的攻擊行為來更新系統內的入侵偵測比對規則，這樣一來可以提高整體系統在比對惡意攻擊盈為的準確度及效率。

參考文獻

[1] 施威銘研究室,「無線網路架設實務」,旗標出版股份有限公司,2002 年。

[2] 謝文川、李境豈、陳毓璋 : 異質無線網路入侵偵測系統之研製.

[3] 賴溪松 : 網路攻擊模式分析

[4] D. Burroughs, L. Wilson and G. Cybenko. Analysis of Distributed Intrusion

[5] http://documents.iss.net/whitepapers/wireless_LAN_security.pdf

[6] http://acidlab.sourceforge.net/

[7] http://expect.nist.gov/

[8] http://www.costcentral.com/proddetail/Nortel_Alteon_Application_Switch_2208/EB1412010/E81663/