基於誘捕與弱點檢測技術建構高安全無線區域網路

曹偉駿*
大葉大學資訊管理學系

黃偉智
大葉大學資訊管理學系

蔡欣潔
大葉大學資訊管理學系

摘要

由於資訊的爆炸與科技的進步，網路的應用儼然與我們的生活產生了密不可分的關係，但是安全問題也隨之而起。雖然目前有許多的安全工具可以成功地偵測、攔截或者掃除某特定入侵行為，但卻少有工具可以在受到駭客未知型的攻擊入侵時，能及時做出適當的反應措施，其原因在於現行安全檢測工具大多採用資料庫特徵比對的方式進行檢測，所以才會造成無法及時偵測出未知型入侵攻擊的狀況，因此往往會錯失防護的時機與捕獲入侵者的機會。

有鑑於上述安全檢測方法之缺失，本研究首先建立一個高誘捕率的無線誘捕系統（Wireless Honeypot），進而加入鍵擊側錄與弱點檢測模組，以求更加詳盡的收集與分析入侵者惡意行為，如此一來不僅能夠大幅降低入侵偵測的誤判與增加 WLAN 的安全性，更能在受到未知型的駭客入侵前進行防護，把所有可能造成的損失降至最低。

關鍵詞：網路安全、無線區域網路、誘捕系統、弱點檢測

* 本文通訊作者。電子郵件信箱：wjtsaur@yahoo.com.tw
2010/12/30 投稿；2011/04/03 修訂；2011/06/24 接受

Constructing Highly Secure Wireless Local Area Networks Based on Honeypot and Vulnerability Scan Techniques

Woei-Jiunn Tsaur*
Department of Information Management, Da-Yeh University

Wei-Chih Huang
Department of Information Management, Da-Yeh University

Shin-Chieh Tsai
Department of Information Management, Da-Yeh University

Abstract

With the information explosion and technological progress, the applications of networks have already been bound up with our daily life. Meanwhile, security problems have arisen following this. Although there are many security tools that can successfully detect, intercept or remove certain kinds of intrusions, few tools can give response and find solutions promptly when the system is being attacked and intruded by unknown hackers. Current security detection tools execute the detection mostly via the method of signature comparison, so that unknown attacks and intrusions cannot be detected in time. Therefore, opportunities to defend the system and to capture the intruders are likely to slip.

In view of the defects of security detection tools mentioned above, this study will construct a wireless honeypot of high arrestment rate together with keyloggers and vulnerability scan modules in order to collect and analyze intruders' malicious behavior more exhaustively. In this way, the false positive rate of intrusion detection will be greatly reduced and the security of WLAN will be dramatically improved, and therefore the proposed protection mechanism can get underway before unknown hackers start to attack, by which potential losses will be minimized.

Keywords: Network Security, Wireless Local Area Networks, Honeypot, Vulnerability Scan

* Corresponding author. Email: wjtsaur@yahoo.com.tw
2010/12/30 received; 2011/04/3 revised; 2011/06/24 accepted

壹、緒論

隨著網際網路的迅速發展，使用人數與需求量也日益增加，尤其以無線網路最為熱門，其中無線區域網路（Wireless Local Area Networks; WLAN）更是受到使用者的歡迎，因為 WLAN 適合用來建構中小型的區域網路，例如家中、辦公室、圖書館等，與傳統有線網路相較之下節省了佈線的成本，且能更快速的架構網路環境。

由於 WLAN 的方便性，使用者容易在使用上忽略許多安全性的問題（Wang et al. 2003），造成入侵者能夠輕易存取 WLAN 上私人的訊息與資料，甚至利用使用者作為跳板進行攻擊，使其成為代罪羔羊，造成不堪設想的嚴重後果。

因此，擁有一套入侵偵測系統（Intrusion Detection Systems; IDS）作為 WLAN 防禦的工具（Kim et al. 2006; Lim et al. 2003; Potter 2004; Sobh 2006）是有其必要性，目前 IDS 就其整體架構而言可以分為主機型（Host Based Intrusion Detection System; HIDS）、網路型（Network Based Intrusion Detection System; NIDS）與分散式（Distributed Intrusion Detection System; DIDS）三種（Biermann et al. 2001; Denning 1987; Verwoerd & Hunt 2002; Yang et al. 2009），但無論是何種架構的 IDS 機制，皆必須等到網路遭受迫害時方能偵測出相關攻擊，所以 IDS 發展至今，依舊無法完全有效的抵擋各種類型之攻擊方式，追究其原因，可歸納出三點（Beheshti & Wasniowski 2007）：

1. 只能偵測已知型的攻擊：因為現行 IDS 大多使用特徵比對（Signature-based）的偵測方式，因此只能對應辨識出資料庫中所預先儲存的攻擊特徵與行為，但對於未知型的攻擊卻無法做出應有的反應。
2. 容易發生無效的偵測：現行的攻擊模式經由特徵比對的偵測後，常出現錯誤，也就是將正常的網路存取行為誤認為攻擊行為，或無法精確辨識出攻擊行為的種類。一旦經常發生無效的偵測，網路安全人員即必須花時間在系統維護上。
3. 不易查詢大量記錄檔：目前網際網路發展迅速，每日需面對數以萬計次的攻擊，因此產生龐大的攻擊記錄檔，在龐大的記錄檔中夾雜了準確及無效的偵測，故網路安全人員猶如大海撈針，以致無法即時做出對應的防護策略。

本研究為了提升 WLAN 之 IDS 偵測率，降低其誤報率、誤判率，以及提高記錄檔可閱讀性，將導入無線誘捕系統（Wireless Honeypot）的技術，並加入鍵擊側錄與資料分析模組，經由實驗證實能有效的阻止攻擊，進而預防系統受到入侵破壞，並減輕網路安全人員的負擔。

其餘章節架構分述如下，第貳節為相關文獻探討，第參節將建構高安全無線區域網路，第肆節則進行系統實作與測試，最後於第伍節作出結論與提出未來發展方向。

貳、相關文獻探討

在本節中，我們將對相關的文獻進行探討，首先介紹誘捕系統，針對其系統的缺點進行原因分析，並列出無線誘捕系統的相關技術。

一、誘捕系統的技術

長久以來我們很難知道駭客是如何入侵系統，他們是誰又是利用什麼工具，透過何種服務的漏洞，什麼時候進來，潛伏多久，系統又被竊取了什麼資料。有關駭客的動機與手法，一直是網路安全研究者想知道的。誘捕系統（Honeypot）的觀念首先被 Clifford Stoll（1990）與 Bill Cheswick（1991）提出，自此之後誘捕系統持續地被發展與研究，演變至今日成為強而有力的系統。Honeypot 是一個欺騙入侵者的環境，也是偵測攻擊的技術，亦或是設計來學習駭客的攻擊行為（Watson 2007）。以下我們將針對誘捕系統之互動方式與建置架構分別進行探討。

（一）互動方式

一般而言，誘捕系統互動方式可區分為低互動（Low-Interaction）與高互動（High-Interaction）兩種（Honeypots 2003; The Honeynet Project 2010），將詳細介紹如下。

1. 低互動誘捕系統：低互動的誘捕系統意指僅能進行有限的互動，一般僅能透過軟體所模擬的系統和服務與入侵者進行互動。其優點為易於建置與方便維護，缺點是所能夠收集的入侵者資料與互動比較少（Mukkamala et al. 2007），有經驗的入侵者透過連結服務時，主機回應（ICMP）的時間或下達進階指令（例如 FTP 下的 hash 指令），即可被偵測出來。Spitzner（2002）於 Honeypots: Tracking Hackers 一書提到，由 NielsProvos 所研發的低互動誘捕系統 Honeyd 最具有代表性。其特點在於監控整個區域網路，而並非監控單一主機，當發現入侵者嘗試攻擊不存在的機器，即轉由 Honeyd 接手與攻擊者進行互動，透過模擬作業系統配置與外掛服務腳本（Script），結合位置解析協定（Address Resolution Protocol; ARP）封包回應欺騙，以假亂真的欺騙入侵者。Honeyd 至今仍為 Lance Spitzner 所率領的誘捕技術團隊所推荐，其運作方式如圖 1 所示。

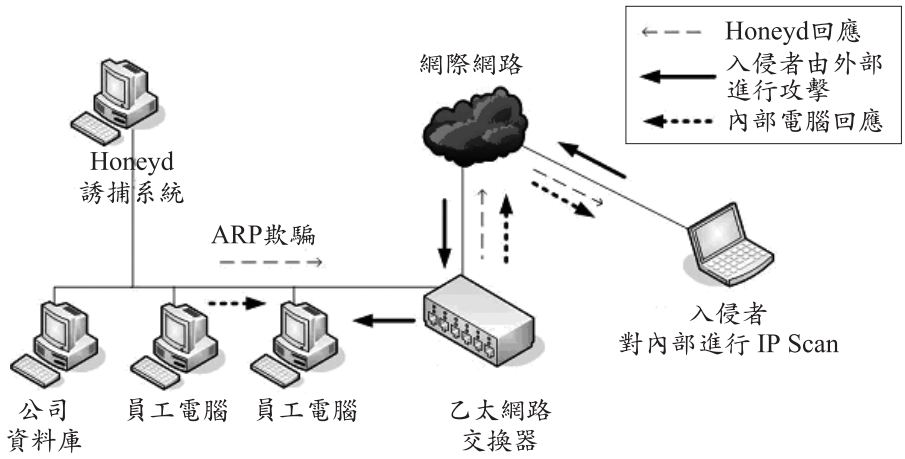


圖 1：Honeyd 低互動誘捕系統運作方式

於此假設一個情境，在一個企業的網路環境中，若內部現有 10 台主機，當入侵者由外部對內部進行 IP Scan（探測）時，則會有 10 次的回應。但是當一台 Honeyd 配置於網路環境中時，僅需依當時設定的數量回應，進而騙取入侵者與其連結，達到欺騙與拖延入侵者的目的，並且節省了大量監控的配置。

2. 高互動誘捕系統：高互動的誘捕系統完全是採用真實的作業系統和應用程式，非透過模擬的方式來提供完整的服務，其優點為可收集詳細的互動訊息與大量的攻擊樣本，缺點是可能會被利用為竊取內部資訊或當成跳板攻擊網路上其他系統。現今較具代表性的高互動誘捕系統為 Lance Spitzner 團隊所研發的誘捕防禦網路 Honeynet（Spitzner 2002），其系統之演變如表 1 所示。

表 1：誘捕防禦網路系統環境之演變

年份	演變	需求
1999 年	第一代	建立真實與自由進出的網路環境，並且可收及其攻擊行為與活動。
2003 年	第二代	變更為橋接（Bridge）模式，解決了第一帶在第三層運作，容易被偵測的問題，並針對封包流入與流出進行控管與數據的收集。
2005 年至今	第三代	導入分析模組，並結合 Keystrokes 技術，將入侵者從攻擊發起到入侵結束所下達的指令，傳送到後端的資料庫供管理者瞭解與分析其攻擊方式。

第三代 Honeynet（Watson 2007）環境最重要的核心就是在 Honeywall 的部份，透過架構上的三個網路介面 Eth0、Eth1、Eth2 進行資料連結。Eth0 連結外部網路環境，Eth1 連結內部誘捕系統環境 Eth2 提供分析系統連入與內部套件更新。使整個環境進一步達到資料控制（Data Control）、資料捕獲（Data Capture）和資料分析（Data Analysis）的目標，說明如下：

(1) 資料控制是針對入侵者所發起的攻擊進行控管之機制，降低誘捕系統攻擊傷害其他正在運作中主機。

(2) 資料捕獲是監控與收集流經 Honeywall 的資訊。

(3) 資料分析則為分析捕獲後的數據資料。

其運作模式如圖 2 所示。

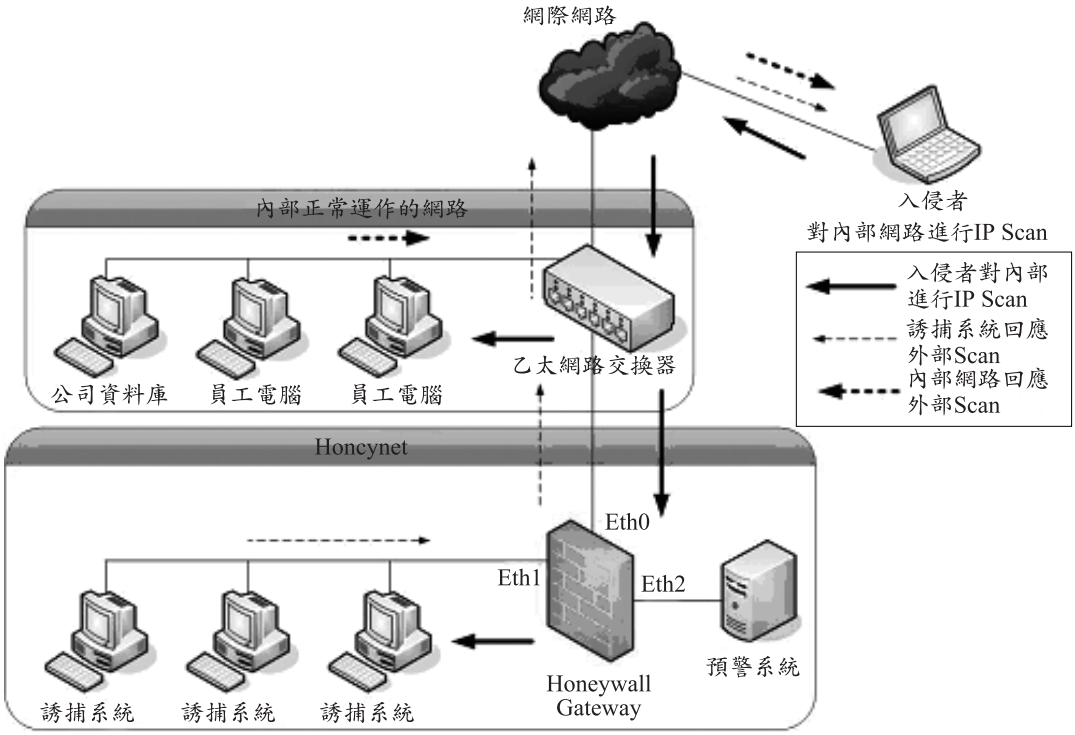


圖 2：Honeynet 誘捕網路系統運作方式

再假設一個情境，在一個企業的網路環境中，若內部現有 3 台運作中的主機與 3 台誘捕系統，當入侵者由外部對內部進行 IP Scan（探測）時，共計可獲得 6 個回應。但是流經 Honeywall 後端的 3 個要求與回應，則馬上被記錄下來並且送到後端資料庫存查。雖然透過高互動更能夠拖延入侵者與獲得更詳細的互動資訊，不過似乎無法有效率的捕獲入侵者的攻擊。

（二）建置架構

建置誘捕環境時必須依環境大小做為考量點，在建置上可分為實體誘捕系統與虛擬誘捕系統（Watson 2007），分別說明如下。

1. 實體誘捕系統（Physical Honeypot）：實體誘捕系統是存在於網路上的一台實體的機器，擁有一個實體的 IP 位置，並且安裝一些不正式對外開放的服務，建置者通常不會對其進行系統安全的更新，主機的配置一般都放在容易被攻擊的區域裡，極有可能被駭客當作跳板而攻擊其他使用中的主機。實體誘捕系統之配置如圖 3 所示。

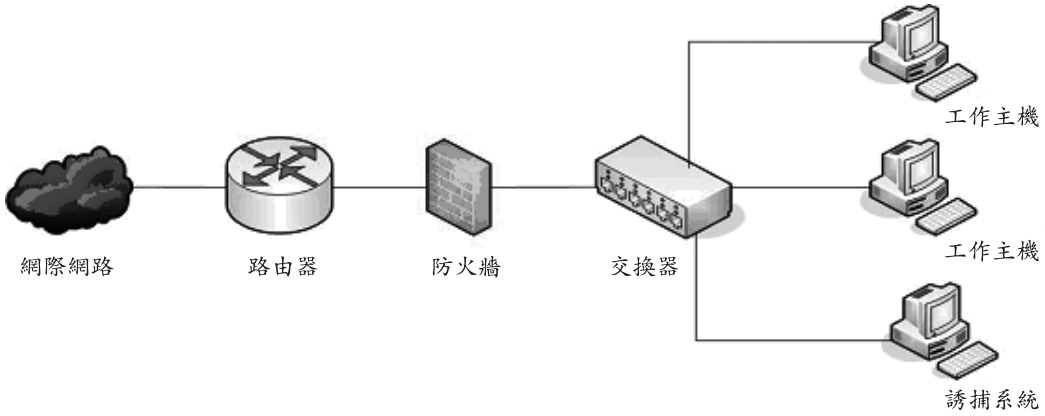


圖 3：實體誘捕系統之配置

2. 虛擬誘捕系統（Virtual Honeypot）：虛擬誘捕系統通常是安裝在主機作業系統上的一套軟體，利用它模擬建置而成的系統與服務，入侵者僅能透過模擬的環境或服務進行連結，因此僅能記錄一些簡單的互動資訊。虛擬誘捕系統之配置如圖 4 所示。

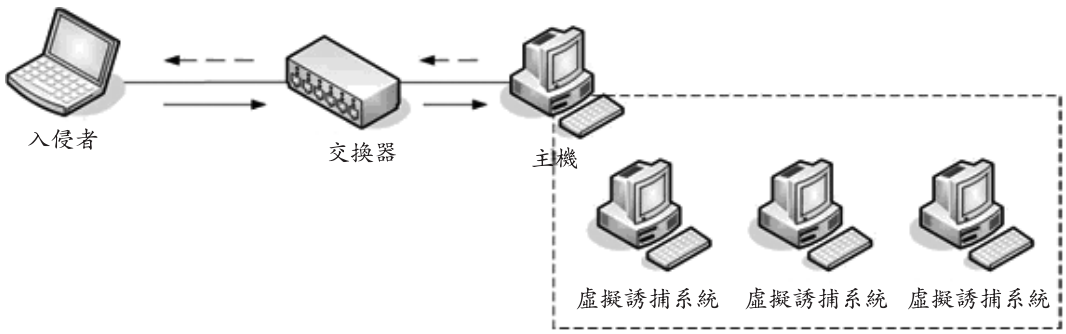


圖 4：虛擬誘捕系統之配置

由於在網路上建置實體誘捕系統非常昂貴，如果要建置一個 Class C 的環境則需要 255 台實體主機來達成目標，若改由用虛擬誘捕系統來建置，只需要一台即可達成。但是考量到系統的效能與增加擬真性，則必須建置一個混合式的監控環境（Artaila et al. 2006）。這個架構同時具有低互動的快速反應與偵測，高互動的擬真性與安全性。現有誘捕系統環境建置比較如表 2。

表 2：建置 Honeypot 環境的考量

互動方式	低互動	高互動	混合式
建置環境	通常為虛擬誘捕系統。	通常為實體誘捕系統。	結合虛擬與實體誘捕系統。
運作方式	通常透過 Guest OS 的方式，簡單安裝與設置即可完成。	於不同的主機上配置單一的作業系統與服務。	利用虛擬主機的方式將所偵測到的異常連線導入高互動誘捕偵測系統來增加真實性。
優點	低風險反應快，入侵者僅能連結該服務，卻無法對該服務進行更進一步的動作。	可記錄較詳實的入侵資料，包括木馬工具的安裝和入侵者所鍵擊與通訊的資訊。	節省誘捕系統配置的成本，並加快偵測與反應的時間。
缺點	僅能模擬簡單的動作，取得資訊有限，容易被入侵者識破。	高風險，可能被作為入侵者的攻擊跳板。	管理者本身需具備一定程度網路與作業系統管理知識。

此外，由於尚還欠缺入侵者的攻擊模式與步驟，且當入侵者進入系統取得權限後，採用了 SSH 與 SSL 等加密通道，利用入侵偵測無法辨視加密訊息的漏洞，達到保護入侵者所傳送的資料，因此更加深了監控的難度。為了要解決監控加密訊息的問題，Balas 在 2003 年研發出一個代號為「Sebek」的套件（Balas et al. 2006），其為一個 Kernel-based 的監控軟體，安裝在被監控的主機上。當 Sebek 執行後，系統有任何鍵擊的動作皆會被 Sebek 攔截並記錄，達到監控加密訊息的目的。而至 2006 年 Sebe 已經進化成特定工具，其被設計為記錄入侵者一連串的鍵擊和記錄加密通訊所開啟的各個子程序、通訊埠活動、檔案開啟與讀取活動，其運作原理如圖 5 所示。當使用者端送出標準函式庫至 Kernel 時，Sebek 模組攔截傳遞的資訊，並將資料側錄後再轉送到原先預設程序執行，達到突破加密通訊側錄之目的，使得整個誘捕系統架構更完整。

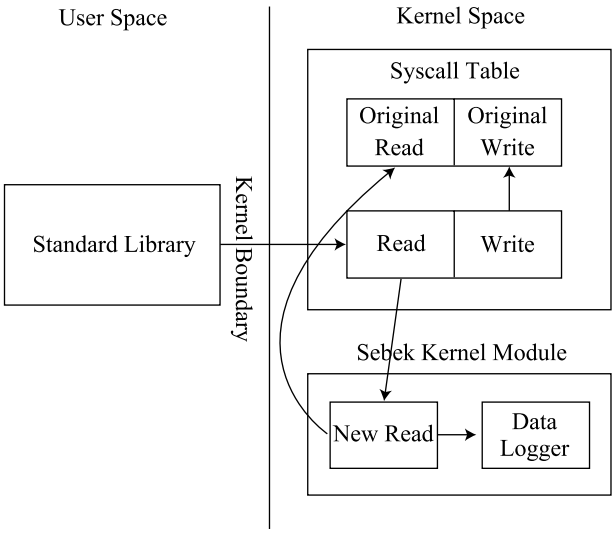


圖 5：Sebek 運作原理

二、無線誘捕系統的發展

在 2002 年學者 Hilley（2002）首先提出無線誘捕系統在未來的重要性，而學者 Yek（2003; 2004）也分別在 2003 及 2004 年發表無線誘捕系統的架構與應用。在學者 Yek 所提到的架構中，是以誘捕系統當作核心，第二層是利用 Honeyd 的技術，最外層則是應用 Fake AP 的架構以達到無線誘捕系統的建置，如圖 6 所示。但此架構並未對所收集到的資料進行深入探討與分析，因此在偵測率上勢必有所影響。

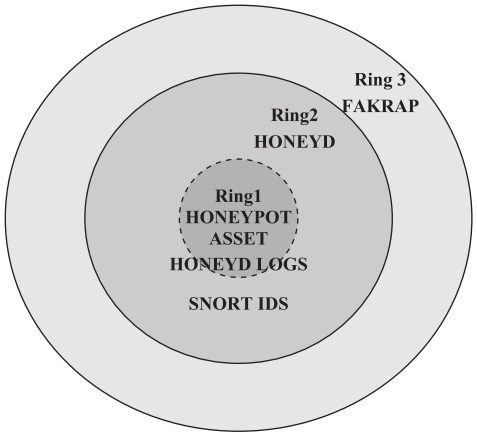


圖 6：應用無線誘捕系統深層欺騙

截至目前為止無線誘捕系統相關研究大部分還是只針對資料的收集，極少針

對資料分析部份做深入研究，而且許多文獻亦談到資料分析也是入侵偵測重要的環節之一。在誘捕系統中所收集到的記錄資料，主要是用來提供不同類型的網路活動報告，例如：

- 誘捕系統觸發的回應
- 嘗試的連線
- 對外的連線
- 誘捕系統上的 TCP 及 UDP 連接埠連線狀況
- 檔案修改

若使用者非相關研究人員，可能對於所產生的資訊將無法有效的利用或判讀，因此依照使用者需求或是程度，將誘捕系統所收集的資料做簡單化或是以量化的方式產生報表，將有利於組織未來的運用。

首先在無線誘捕系統中加入資料分析的概念是由 SHP（Siles 2007）所提出，如圖 7 所示。本概念主要是利用無線資料分析（WiFi data analysis; WDA）模組，分析誘捕系統所收集到的資料，進而產生圖形化報表及分析數據，因此經 WDA 模組分析比對後，除了可提高記錄檔可讀性以外，亦可因而提高偵測率並降低誤判率。雖然在架構上有線誘捕系統和無線誘捕系統相當類似，然而無線誘捕系統卻鮮少有人將系統實作，且 SHP 未能將其開發成實際的系統，是較令人惋惜的。因此，在本研究中我們整合 SHP 所提出資料分析模組至本研究建置的無線誘捕系統中，以期能進一步對入侵行為做較精準的研判。

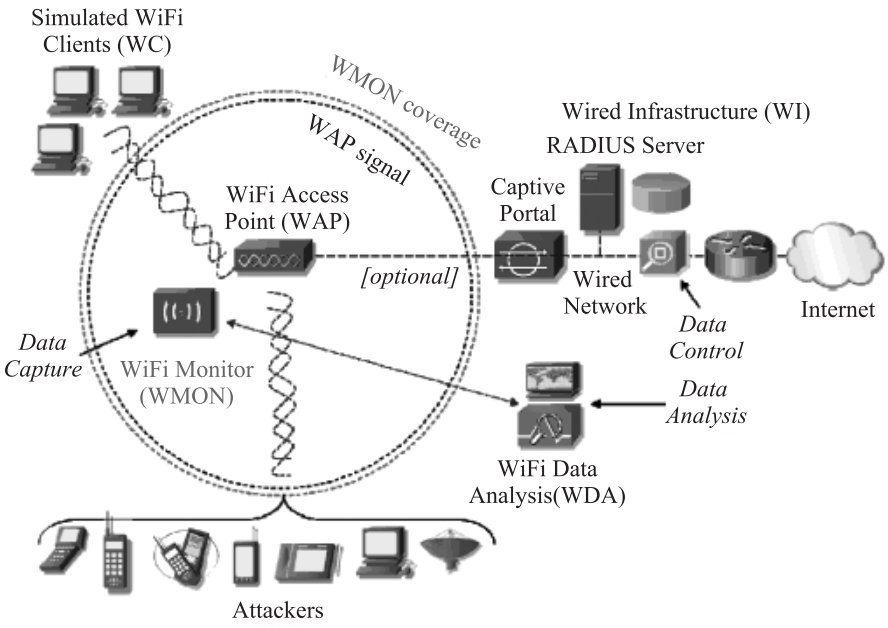


圖 7：SHP 所提出之無線誘捕系統架構

三、Nessus 弱點檢測系統

1998 年，Nessus 的創辦人 Renaud Deraison 展開了一項名為"Nessus"的計畫，其計畫目的是希望能為網際網路社群提供一個免費、威力強大、更新頻繁並簡易使用的遠端系統安全掃瞄程式。經過了數年發展，包括 CERT 與 SANS 等著名的網路安全相關機構皆認同此工具軟體的功能與可用性。

Nessus 的特色（Benini & Sicari 2008）如下：

1. 提供完整的電腦弱點掃瞄服務，並隨時更新其弱點資料庫。
2. 不同於傳統的弱點掃瞄軟體，Nessus 可同時在本機或遠端上遙控，進行系統的弱點分析掃瞄。
3. 其運作效能隨著系統的資源而自行調整。如果將主機加入更多的資源（例如加快 CPU 速度或增加記憶體大小），其效率表現可因為豐富資源而提高。
4. 可自行定義外嵌（Plug-in）軟體
5. NASL（Nessus Attack Scripting Language）是由 Tenable 所開發出的語言，用來寫入 Nessus 的安全測試選項。
6. 完整支援 SSL（Secure Socket Layer）。
7. 自從 1998 年開發至今已逾十年，故為一架構成熟的軟體。

參、建構高安全無線區域網路

由於傳統誘捕系統的研究，多為分析所捕獲攻擊之記錄檔，輔助入侵偵測之不足。因此，本研究基於無線誘捕技術建立混合式誘捕環境，將誘捕系統所收集的攻擊記錄與弱點檢測系統之記錄經由交叉比對得到更精準的偵測結果，提供管理者了解入侵者的攻擊模式，進而保障網路主機安全。

一、研究流程

本研究採用「以一般無線區域網路節點的方式所建構的高互動性實體無線誘捕系統」，並加上 web 呈現的記錄檔分析模組和後端備份資料庫。其詳細研究流程如圖 8 所示。

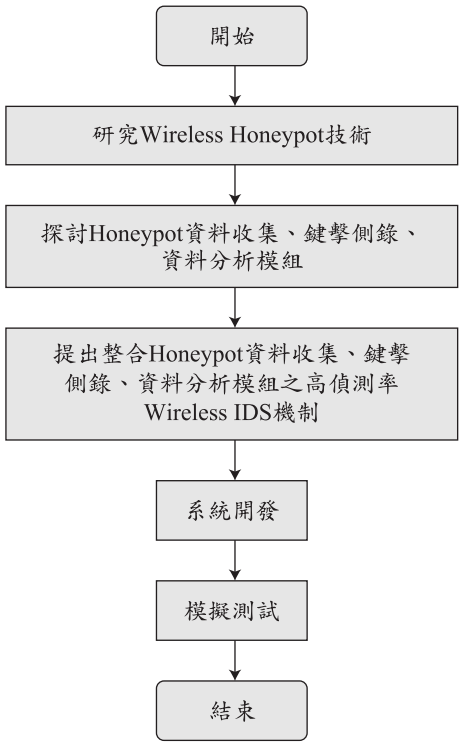


圖 8：研究流程

二、系統網路架構

本研究的目的是建構出利於收集真實的無線網路上入侵的行為，其網路架構如圖 9 所示。

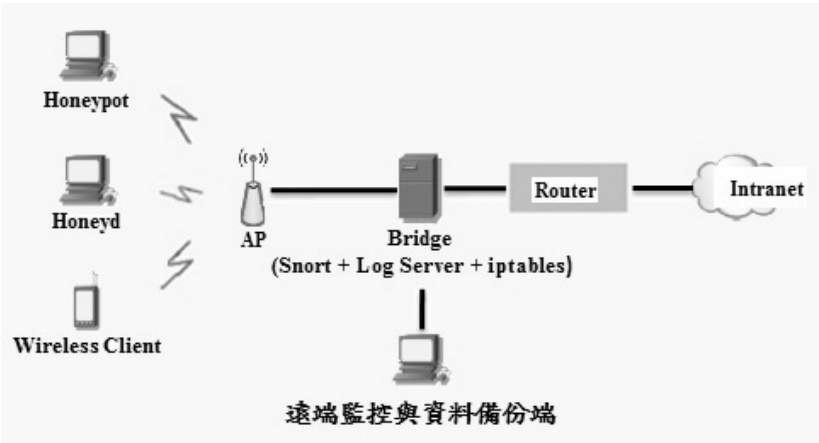


圖 9：系統網路架構

以下將對圖 9 的主要功能作一說明：

1. Bridge：snort＋Log Server＋iptables 在此架構中，Log Server、snort 和 Bridge 是同一台主機。其主要工作如下：
   (1) 此 Bridge 主機扮演防火牆、入侵偵測的任務，它有三張網路卡，分別連接網際網路、誘捕系統與遠端控制與資料備份端。首先它必須扮演和網際網路溝通的一個橋樑，偵測管制進入或是出去區域網路內部的封包，如果遇已知型惡意的封包要進入或是出去，snort_inline 將會予以記錄並允許通過，其目的是收集駭客所植入的惡意程式和其用來放置惡意程式原始碼的伺服器位置，但若剩下入侵偵測系統尚未發覺是否是惡意行為的封包要出入，則進入到誘捕系統收集行為（此收集到行為，不一定全部都是惡意行為，所以還需要未來進行分析與研究）。
   (2) 此 Bridge 主機是用來儲存由誘捕系統收集來的所有資料，它盡量放置在安全的區域網路之中，避免被攻擊者破壞，否則讓攻擊者發現，可能也遭受到攻擊或是發送無關緊要的訊息，導致未來分析時誤判。
2. 高互動 Honeypot 主機：它是用來偽裝伺服器主機，目的是收集攻擊者的行為方式，並且定時地將收集到資訊傳送到遠端 Log Server 儲存。它必須要有下列功能：
   (1) 模擬伺服器服務：像 FTP、HTTP、Telnet 等，一些存在標準伺服器的已知弱點和漏洞。
   (2) 記錄攻擊者行為。
   (3) 產生回應並通知管理人員。
   (4) 能檢查系統是否完整：如果被植入後門程式、被修改檔案或被利用，主機可以安全的回復。
3. 低互動 Honeyd 主機：為了節省架設多部實體誘捕系統龐大的成本開銷，本主機的用途是用於架設大量的虛擬誘捕系統，其目的在於收到連線要求後重導 Honeypot 主機，用以降低駭客的戒心。
4. 遠端監控與資料備份端：本主機的用途在於分析、備份誘捕系統收集的記錄檔，並將其記錄檔與本主機安裝的弱點檢測系統記錄檔交叉比對，用以分析出已知的攻擊手法與未知的入侵行為，是本研究的核心主機，安置在誘捕系統下的子網路來確保記錄檔的安全性，詳細功能條列如下：
   (1) 同步備份與更新傳送到 Bridge 主機的記錄檔。
   (2) 安裝弱點檢測軟體「Nessus」用以檢測 Honeypot 主機。
   (3) 將誘捕系統與弱點檢測兩者記錄檔進行交叉比對。
   (4) 提供多樣化的圖表模式與文字化的方法呈現交叉比對結果。
   (5) 實體無線網路存取點（Access Point; AP）：具有無線網路 Network

address translation 的功能。

三、建構無線誘捕系統

為了能夠有效地捕獲入侵者的攻擊與取得鍵擊側錄資訊，本研究所提之監控環境如圖 10 所示。其中相關之運作說明如下：

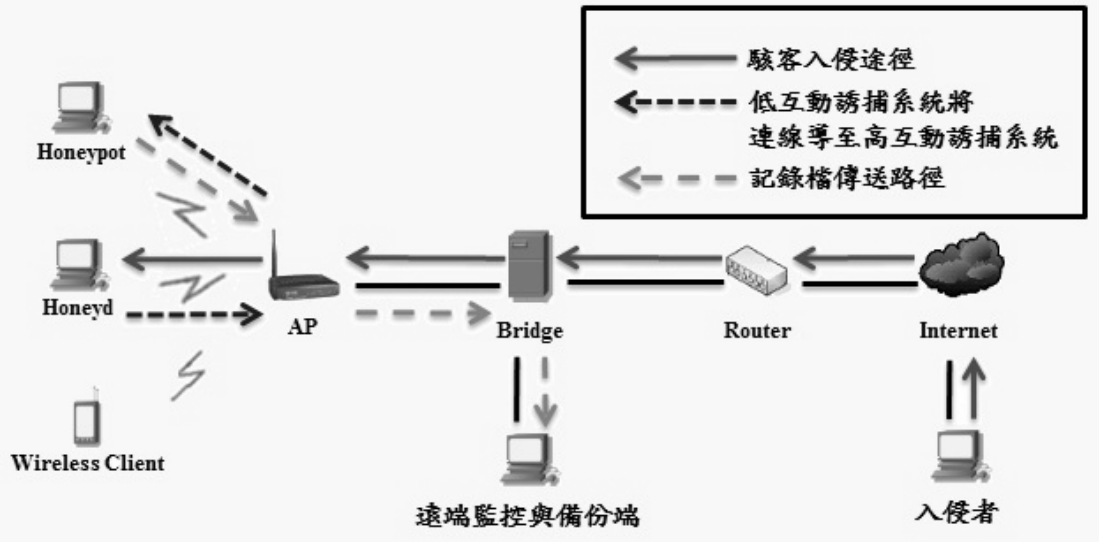


圖 10：本研究之誘捕系統運作模式

1. 當入侵者對內部網路環境進行 IP 與通訊埠（Port）掃描時，首先會取得內部網路 IP 的相關資訊。
2. Honeyd 監控網路封包，當發現設定的誘捕區域有入侵者進行刺探，就代為回應欺騙入侵者使其以為真的有這台設備，誘騙入侵者進而發動攻擊。
3. 當入侵者嘗試發動攻擊時，Honeyd 主機將連線依類型導入高互動誘捕系統與入侵者進行互動。為了能增加環境真實性，依照不同的服務需求導入不同的誘捕環境，如：SSH 連線導入 Linux Server 高互動誘捕系統。
4. 當入侵者對高互動誘捕系統進行攻擊時，Sebek 套件會開始記錄入侵者的入侵歷程，並將鍵擊資訊傳送到監控主機進行儲存。
5. 將誘捕系統收集到的攻擊資料與弱點掃描結果透過前置處理進行比對，另外收集入侵者鍵擊指令以供管理者之後的歷程查閱。詳細流程如圖 11 所示。在圖 11 中，其誘捕系統採混合式建構，若有攻擊行為則先透過低互動誘捕系統再重導連線至高互動誘捕系統，此時高互動誘捕系統將進行連

線控管、封包比對與鍵擊側錄等三項工作，之後再記錄入侵者攻擊特徵。另一方面，弱點檢測模組將可收集到內部弱點資料，接著分別將內部弱點資料與上述攻擊特徵資料先進行前置處理以獲得相同資料格式，之後再將兩者進行攻擊字串之比對，若為同字串則以圖形化呈現比對結果，反之則不予理會。其中攻擊字串之比對（即資料分析模組）的作法說明如圖 12 所示。

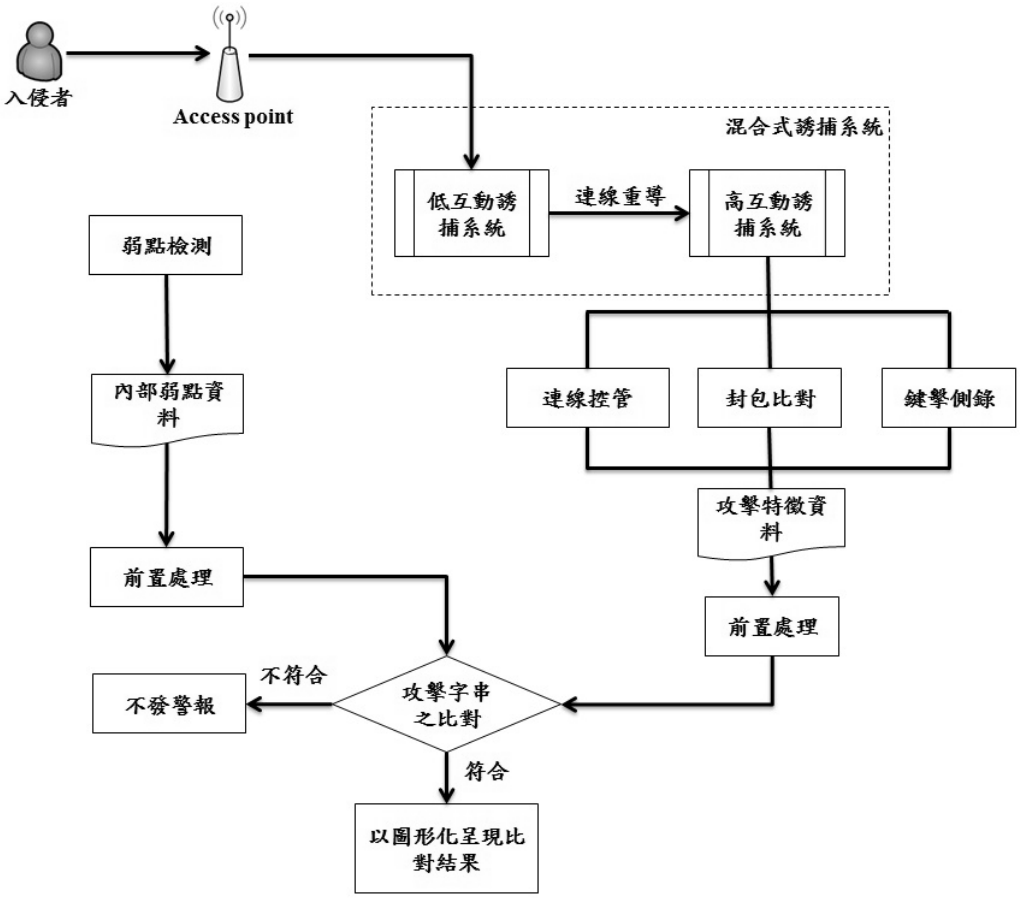


圖 11：誘捕記錄與弱點資訊比對偵測流程

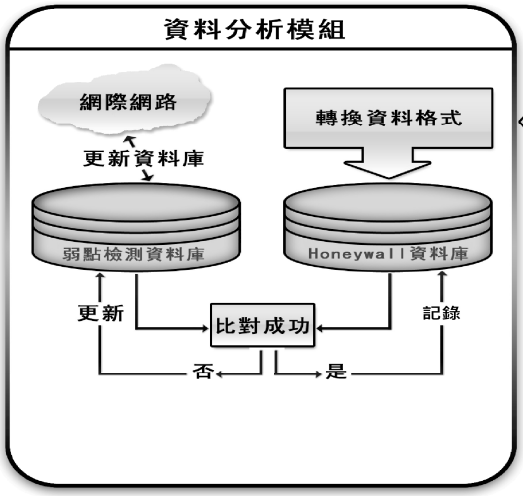


圖 12：資料分析模組

以下針對圖 12 的所呈現的功能作一說明：

1. 轉換資料格式：在此階段中，先將此系統記錄檔中的資料格式轉換成為 Honeywall 資料庫的資料格式。
2. 弱點檢測資料庫（Malware Database）：我們將參照 Honeynet 所提供的資料庫，定期更新此弱點檢測資料庫，以達到比對的完整性。
3. 資料比對：在此比對過程中，主要以攻擊來源 IP、入侵行為與攻擊連接埠這三項進行比對。若攻擊手法與弱點檢測資料庫中相符，則顯示為可辨認之攻擊行為，若比對不成功則將此筆攻擊的來源 IP 與攻擊連接埠做記錄，代表為未知型的攻擊，比對資料庫表單設計如表 3 與表 4 所示。

表 3：Honeywall 資料庫表單

Remote system	date	port	commands	intention
213.135.2.227	27/Feb 14:13:38	20520	cd /tmp; wget www.shady.go.ro/aw.tgz; tar zxf aw.tgz; rm -f aw.tgz; cd .aw; ./inetd; pstree;	Download and install Energy Mech 2.8.5 IRC bot

表 4：弱點檢測資料庫表單範例

id	date	attack_ip	attack_type	attack_port	commands

在比對過程中，若弱點檢測資料庫中的 port 與 Honeywall 資料庫中的 attack_port 相符，且 commands 亦相符，則將 Honeywall 表單中的 attack_type 設定為弱點檢測資料庫中的 intention。此外，若出現無法成功比對，則將 attack_type 的表單設定為 null（無法判別），這表示這筆入侵資訊可能為一個新型態的攻擊手法，故判定為未知型的攻擊。另外，再將此筆無法判別之資料寫入弱點檢測資料庫中作更新，做為日後比對的依據。相較於入侵偵測系統以誤用的方式來比對，本研究更能記錄未知型的攻擊手法。

肆、系統實作與測試

在本節中我們將基於第參節所提出的系統架構與網路規劃方式來實際建構無線區域網路誘捕系統。以下各節將分別介紹該系統之建置、測試與所獲致成果。

一、系統建置

本研究之誘捕系統網路架構建置將依據第參節之圖 10 所示，其所使用電腦設備規格與軟體配備分別描述於表 5 與表 6 中。

表 5：所需之電腦設備

主機名稱	配備	
Bridge 主機	CPU	AMD-K6-400 MHz
	RAM	512 MB
	HD	20 GB
	O.S.	CentOS 5 Kemel2.4.20-8
	NIC IP	eth0: 接無線基地台 eth1: 接路由器 eth2: 61.59.193.157
Honeypot 主機	CPU	Pentium-III-667-MHz
	RAM	128 MB
	HD	20 GB
	O.S.	Radhat Linux 9 Kemel2.4.20-31.9 smp (i386)

主機名稱	配備	
	網路卡	無線網路卡：802.11g D-LINK 120
	NIC IP	eth0: 192.168.2.5
遠端監控與資料備份之主機	CPU	Pentium-4-800-2 GHz
	RAM	512 MB
	HD	80 GB
	O.S.	Windows XP SP3
	NIC IP	eth0: 192.168.3.6
Honeyd 主機	CPU	Pentium-4-800-2 GHz
	RAM	256 MB
	HD	40 GB
	O.S.	Fedora 6
	NIC IP	192.168.2.6~9

表 6：所需之軟體配備

主機名稱	主要使用軟體
Bridge 主機	Rc.Firewall, Snort_inline , Snort
Honypot 主機	Sebek
Honeyd 主機	Honeyd
遠端監控與資料備份端之主機	PHP, PHP/SWF, Nessus

二、系統測試

以下我們將說明本系統測試流程，其運作流程主要分為三階段，分別為系統前置作業、弱點掃瞄與攻擊封包發送與測試誘捕系統，將分別說明如下。

1. 系統前置作業階段：本階段主要動作是利用 Honeyd 建立虛擬的作業系統，以及利用一台電腦建立真實的誘捕系統。首先我們設定虛擬主機作為誘捕系統，供駭客入侵，如表 7 所示。

表 7：虛擬主機設定範例

create default set default personality "Microsoft Windows XP Home Edition" set default default tcp action reset set default default udp action reset set default default icmp action open add default tcp port 80 "sh scripts/misc/test.sh" add default tcp port 21 open add default tcp port 23 open add default udp port	create default1 set default personality "Microsoft Windows NT" set default default tcp action reset set default default udp action reset set default default icmp action open add default tcp port 80 "sh scripts/misc/test.sh" add default tcp port 21 open add default tcp port 23 open add default udp port 25 open

完成之後，我們利用系統內建的遠端遙控功能來確定誘捕系統是否已經架設成功，如圖 13 所示。

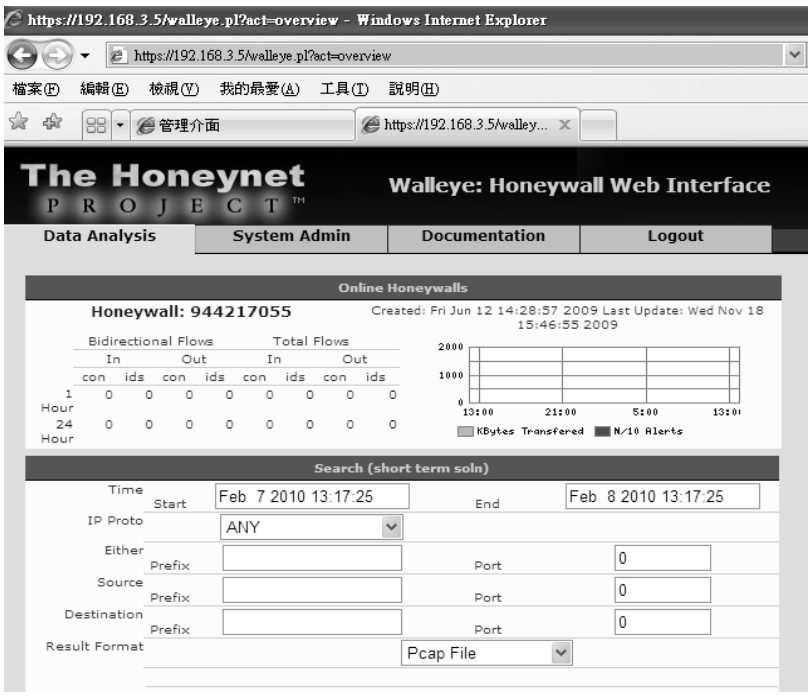


圖 13：Walleye 運作

2. 弱點掃瞄與攻擊封包發送之階段：本階段主要使用 Nessus 對誘捕系統進行攻擊封包的發送，如圖 14 與 15。封包發送完成後，便可得到目前誘捕系統上的弱點檢測報告，如圖 16 所示。

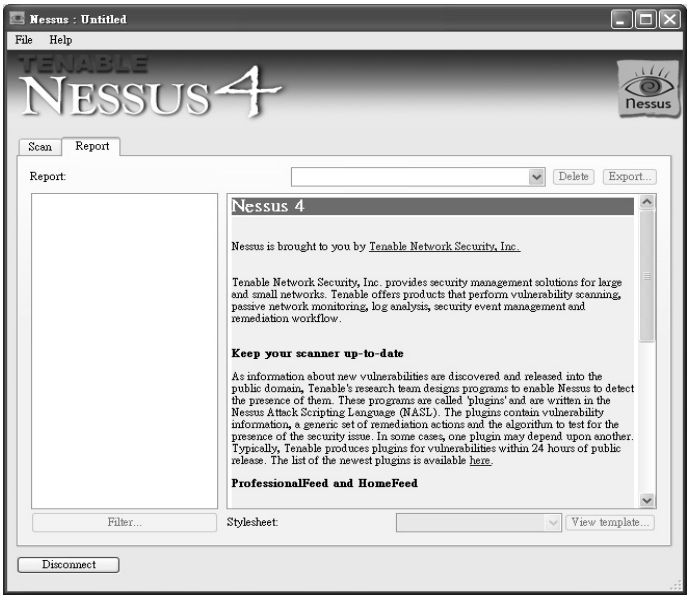


圖 14：Nessus 載入畫面

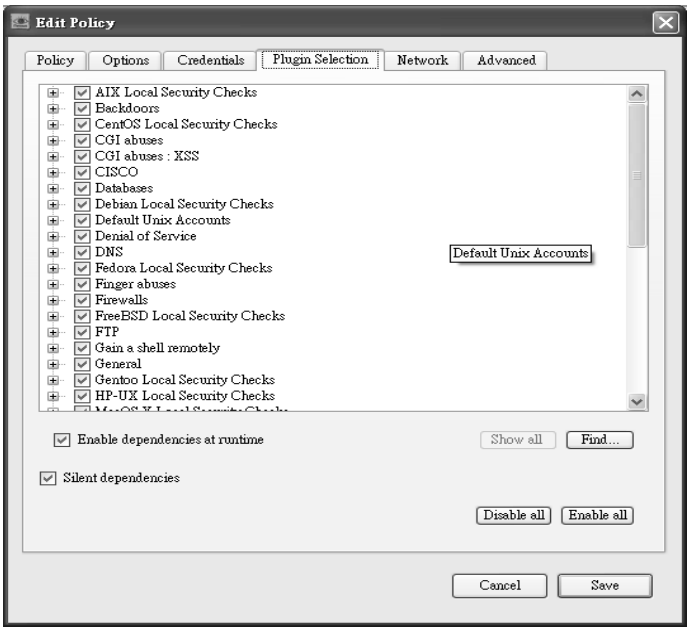
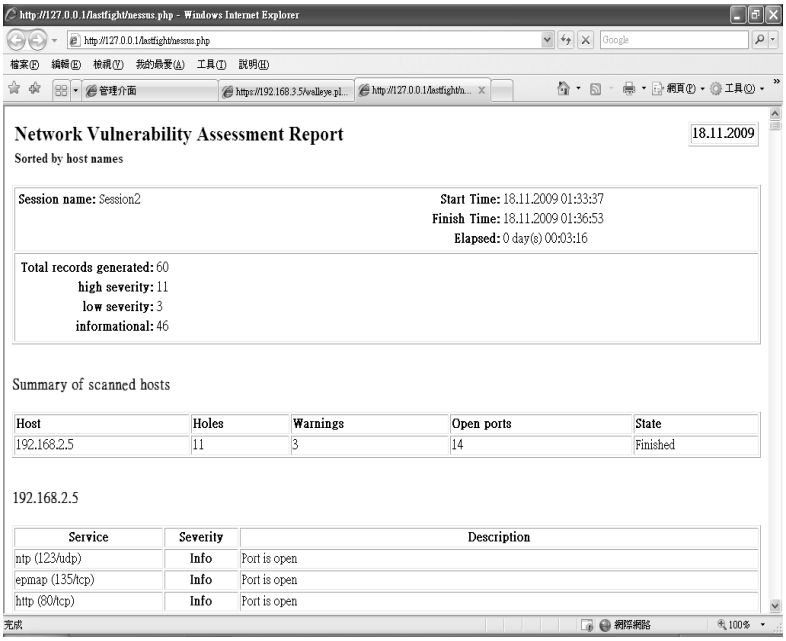


圖 15：Nessus 選擇攻擊封包種類



Network Vulnerability Assessment Report 18.11.2009

Sorted by host names

Session name: Session2
Start Time: 18.11.2009 01:33:37
Finish Time: 18.11.2009 01:36:53
Elapsed: 0 day(s) 00:03:16

Total records generated: 60
high severity: 11
low severity: 3
informational: 46

Summary of scanned hosts

Host	Holes	Warnings	Open ports	State
192.168.2.5	11	3	14	Finished

192.168.2.5

Service	Severity	Description
ntp (123/udp)	Info	Port is open
epmap (135/tcp)	Info	Port is open
http (80/tcp)	Info	Port is open

圖 16：Nessus 檢測報告

3. 測試誘捕系統階段：此階段將確認誘捕系統是否有正確捕獲攻擊封包，如圖 17 所示。

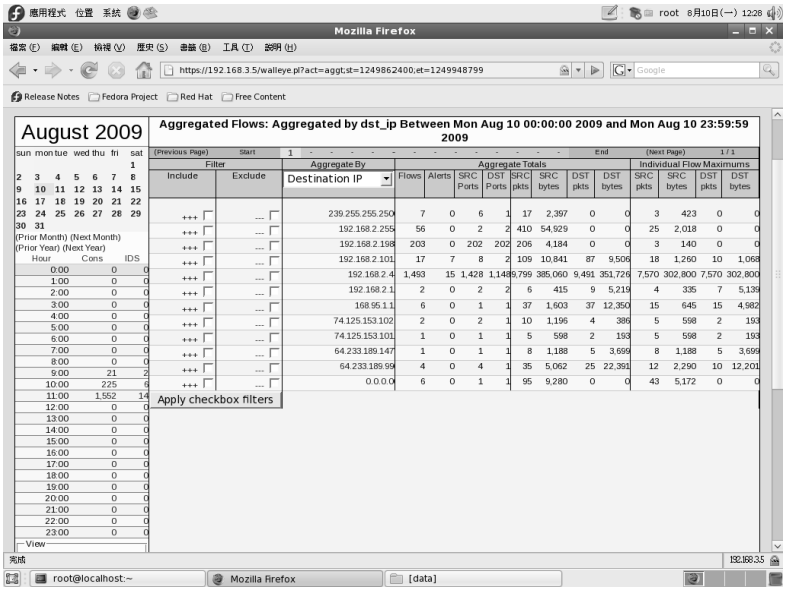


圖 17：誘捕系統捕獲攻擊封包

誘捕系統記錄檔在未加入資料分析模組（WiFi data analysis; WDA）前，要檢視其入侵資訊是相當複雜的，若資料量過多，則難以在短時間內快速判別入侵資訊。而導入分析模組後，我們發現以 web 介面呈現的方式要比未導入資料分析模組精簡，也較能馬上判別入侵資訊，因此，本研究提供文字與圖表兩種模式供管理者參考，如圖 18，並做出最精確的判斷。

圖 18：記錄檔分析模式選擇

在文字模式中，可由設定搜尋條件的方式來過濾資料，我們提供了來源 IP、目標 IP、目標連接埠、通訊協定與風險等級數種條件供選擇，讓管理者可將這些資訊作最有效的應用，如圖 19 與 20 所示。

圖 19：文字分析模式選擇畫面

事件編號	來源IP	目標IP	來源Port	目標Port	Protocol	事件發生時間	事件結束時間
9523	192.168.2.110	192.168.2.5	47828	445	TCP	01:55 Monday 21 Sep '09	01:55 Monday 21 Sep '09
9550	192.168.2.110	192.168.2.5	47828	3389	TCP	01:55 Monday 21 Sep '09	01:55 Monday 21 Sep '09
10685	192.168.2.110	192.168.2.5	47828	445	UDP	01:55 Monday 21 Sep '09	01:55 Monday 21 Sep '09
10804	192.168.2.110	192.168.2.5	47829	445	UDP	01:55 Monday 21 Sep '09	01:55 Monday 21 Sep '09
10979	192.168.2.110	192.168.2.5	47828	3389	UDP	01:55 Monday 21 Sep '09	01:55 Monday 21 Sep '09
11534	192.168.2.110	192.168.2.5	4577	445	TCP	01:55 Monday 21 Sep '09	01:55 Monday 21 Sep '09
11539	192.168.2.110	192.168.2.5	4581	445	UDP	01:55 Monday 21 Sep '09	01:56 Monday 21 Sep '09
11571	192.168.2.110	192.168.2.5	4594	445	TCP	01:56 Monday 21 Sep '09	01:56 Monday 21 Sep '09
11573	192.168.2.110	192.168.2.5	4596	445	TCP	01:56 Monday 21 Sep '09	01:56 Monday 21 Sep '09
11575	192.168.2.110	192.168.2.5	4598	445	TCP	01:56 Monday 21 Sep '09	01:56 Monday 21 Sep '09
11577	192.168.2.110	192.168.2.5	4600	445	TCP	01:56 Monday 21 Sep '09	01:56 Monday 21 Sep '09
11579	192.168.2.110	192.168.2.5	4602	445	TCP	01:56 Monday 21 Sep '09	01:56 Monday 21 Sep '09
11581	192.168.2.110	192.168.2.5	4604	445	TCP	01:56 Monday 21 Sep '09	01:56 Monday 21 Sep '09
11583	192.168.2.110	192.168.2.5	4606	445	TCP	01:56 Monday 21 Sep '09	01:57 Monday 21 Sep '09
11589	192.168.2.110	192.168.2.5	4645	445	TCP	01:58 Monday 21 Sep '09	01:58 Monday 21 Sep '09
11590	192.168.2.110	192.168.2.5	4647	445	TCP	01:58 Monday 21 Sep '09	01:58 Monday 21 Sep '09
11592	192.168.2.110	192.168.2.5	4648	445	TCP	01:58 Monday 21 Sep '09	01:58 Monday 21 Sep '09
11593	192.168.2.110	192.168.2.5	4649	445	TCP	01:58 Monday 21 Sep '09	01:58 Monday 21 Sep '09
11594	192.168.2.110	192.168.2.5	4650	445	TCP	01:58 Monday 21 Sep '09	01:58 Monday 21 Sep '09

圖 20：文字分析模式結果

同時，我們也提供將系統記錄檔用圖表方式呈現的方法，我們提供了如文字模式的五種搜尋方法加上七種圖表種類供管理者瀏覽，如圖 21 與 22 所示。

圖 21：圖表分析模式選擇畫面

圖 22：圖表模式分析結果

三、系統成果效益

實際架設 Honeynet 時必須注意，首先要盡可能地收集入侵者的有意義資料，其次是資料必須被收集儲存在安全的地方，再者，必須將收集到的龐大記錄檔做最有效的分析與整理，最後用最言簡意賅的方式呈現分析的結果。在本次研究中，我們使用高互動方式架設誘捕系統，並加以改良，且架設記錄檔備份伺服器，記錄檔的備份與分析工作都在此台伺服器進行，以達到保護記錄檔的功用。此外，我們使用了親和力極高的 web 介面和直覺式的條件查詢來輔助管理者進行管理，再結合「charts」這套統計圖表套件來幫助我們有效呈現本研究的誘捕與弱點檢測系統記錄檔之交叉比對成果。亦即，本研究整合混合式 Honeypot 與弱點檢測系統來輔助記錄檔分析，並加上圖表化之呈現方式，且藉由結合弱點檢測系統與圖表化分析模組，大幅地提昇記錄檔的可讀性。Honeywall 記錄檔與 Nessus 弱點檢測記錄檔之比對的實驗結果如表 8 所示。

表 8：Honeywall 與 Nessus 記錄檔之比對

	1	2	3	4	5
Honeywall 記錄檔筆數	10357	13548	8269	12405	15403
Nessus 記錄檔筆數	2058	1726	1069	2347	1583
Honeywall 與 Nessus 記錄檔比對後相同的記錄檔筆數	5814	6729	4251	5147	7159
Honeywall 記錄檔筆數精簡率	56.14%	49.67%	51.41%	41.49%	46.48%
平均記錄檔精簡率	49.04%				

表 8 為本研究從 2010 年 2 月至 2010 年 6 月共 5 個月所收集到的 Honeywall 與 Nessus 記錄檔筆數，本研究以每月之前三個星期為一個次別，當月最後一星期則用來分析與整理記錄檔。由表 8 可得知，在未整合 Nessus 弱點檢測功能之純粹 Honeywall 系統中，其記錄檔筆數相當龐大，但於 Honeywall 記錄檔與 Nessus 記錄檔進行交叉比對後，Honeywall 將大幅去除比對未相符的記錄，僅保留比對相符的記錄檔內容，從中可較精準地找出攻擊行為，因而有助於降低誤判率及提高偵測率。本研究所提出之整合式系統平均可達到 49.04%的記錄檔精簡率。

四、比較與討論

本研究在導入誘捕系統與弱點檢測之資料分析模組後，其在提昇無線網路安全方面，與其它相關研究之比較結果如表 9 所示。

表 9：本研究與現存相關機制之功能比較

機制 / 項目	SHP	Walleye	Yek's scheme	本研究
系統實作	無	有	無	有
資料分析模組	有（僅為概念）	有	無	有
系統更新功能	無	無	無	有
報表呈現	無	無	無	有
使用者自訂性	無	低	無	高
圖表化功能	無	無	無	有

由於 Yek（2003; 2004）機制與 SHP（Siles 2007）在無線誘捕系統皆未能有實際系統的開發，因此本研究在系統實作、資料分析模組、系統更新功能與使用者自訂性上皆優於 Yek's scheme 與 SHP。此外，根據學者 Viecco（2007）的研究，其提出了 Walleye 的二項缺失，亦即缺乏使用上的彈性以及無法擴充其它功能。這是由於 Walleye 無法讓使用者自行修改程式碼，所以也導致在使用上的不便。除了無法更新系統功能之外，使用者較難依照自己的需求對系統進行修改，而本研究是以 PHP 為開發環境，除了因為 PHP 是目前較廣為使用外，另外 PHP 在網路上亦擁有許多已開發的套件，使用者只要根據資料庫的表單做相對的修改便能使用，因此本研究具有較高彈性的使用者自訂性。而本研究帶來另一主要的效益為報表的呈現，這是為了減少使用者在判別入侵訊息的困難，另一方面也可讓管理人員清楚了解系統存在的問題，做為日後系統更新上的依據。

伍、結論與未來研究方向

經由上述章節對研究成果的分析與探討後，在本節中將作出總結與提出未來可行的研究方向。

一、結論

我們設計與實作了本機制之後，應用了多種資料收集與分析模組，能詳盡的擷取、記錄與分析入侵者的惡意行為。簡言之，本研究所獲得的成果如下：

1. 經由本研究將弱點檢測資料庫及 Honeywall 資料庫進行交叉比對，可得到更精準及有效的偵測結果。
2. 從本研究可發現，記錄檔經由系統化分析和圖表化的呈現之後，大大地提

昇記錄檔的可讀性，管理者可更輕鬆的瞭解目前的網路安全狀況，並做出最有效率的決策。

二、未來研究方向

以下列出未來的研究方向：

1. 有關於誘捕系統的系統回復性方面，本研究著重於入侵資料的收集與分析，對於遭入侵後的系統如何快速的恢復與重置，本研究未探討此部份，未來的研究方向可朝向系統快速的回復，用以增加駭客的鑑別度與系統的真實度。
2. 本研究僅將記錄檔進行詳細的收集與分析，但並無對管理者即時發送電子郵件或即時訊息的功能，未來可朝向即時發出訊息通知管理者，加強與管理者的聯繫。

誌謝

本研究接受國科會研究計畫案 NSC 100-2219-E-212-001、NSC 99-2622-E-212-010-CC3 經費補助，特此致謝。

參考文獻

Artaila, H., Safab, H., Sraja, M., Kuwatlya, I. and Al-Masria, Z. (2006), 'A hybrid Honeypot framework for improving intrusion detection systems in protecting organizational networks', *Computers & Security*, Vol. 25, No. 4, pp. 274-288.

Balas, E., Travis, G. and Viecco, C. (2006), 'A dynamic filtering technique for Sebek system monitoring', *Proceedings of the Information Assurance Workshop,* West Point, NY, USA, Jane 21-23, pp. 275-282.

Beheshti M. and Wasniowski R. (2007), 'Data fusion support for intrusion detection and prevention', *Proceedings of Fourth International Conference on Information Technology*, Las Vegas, Nevada, USA, April 2-4, pp. 966.

Benini, M. and Sicari, S. (2008), 'Risk assessment in practice: a real case study', *Computer Communications*, Vol. 31, No. 15, pp. 3691-3699.

Biermann, E., Cloete, E. and Venter, L.M. (2001), 'A comparison of intrusion detection system', *Computers & Security*, Vol. 20, No. 8, pp. 676-683.

Cheswick, B. (1991), 'An evening with berferd', *Proceedings of USENIX*, San Francisco, CA, USA, January 7, pp. 1-11.

Denning, D.E. (1987), 'An intrusion detection model', *IEEE Transactions on Software Engineering*, Vol. 13, No. 2, pp. 222-232.

Hilley, S. (2002), 'At last, a Wireless Honeypot', *Network Security*, Vol. 8, pp. 1-2.

Honeypots: Definitions and Value of Honeypots (2003), available at http://www.tracking-hackers.com/papers/honeypots.html (accessed 20 December. 2010).

Kim, D., Koh, S. and Kim, S. (2006), 'An integrated scheme for intrusion detection in WLAN', *Proceedings of International Conference on Information Networking, Advances in Data Communications and Wireless Networks*, January 16-19, Sendai, Japan, pp. 723-732.

Lim, Y., Schmoyer, T., Levine J. and Owen, H. (2003), 'Wireless intrusion detection and response', *Proceedings of the IEEE Workshop on Information Assurance*, June, West Point, NY, USA, pp. 68-75.

Mukkamala, S., Yendrapalli, K., Basnet, R., Shankarapani, M.K. and Sung, A.H. (2007), 'Detection of virtual environments and low interaction Honeypots', *Proceedings of the Information Assurance and Security Workshop,* June 20-22, West Point, NY, USA, pp. 92-98.

Potter, B. (2004), 'Wireless Intrusion Detection', *Network Security*, Vol. 2004, No. 4, pp. 4-5.

Siles, R. (2007), *HoneySpot: the Wireless Honeypot*, Spanish Honeynet Project.

Sobh, T. (2006), 'Wired and wireless intrusion detection system: classifications, good characteristics and state-of-the-art', *Computer standards & interfaces*, Vol. 28, No. 6, pp. 670-694.

Spitzner, L. (2002), *Honeypot*: *Tracking Hackers*, Addison Wesley, Boston, MA, USA.

Stoll, C. (1990), *The Cuckoo's Egg*：*Tracking a Spy through the Maze of Computer Espionage*, Pocket Books, New York.

The Honeynet Project (2010), available at http://www.honeynet.org (accessed 10 December 2010).

Verwoerd, T. and Hunt, R. (2002), 'Intrusion detection techniques and approaches', *Computer Communications*, Vol. 25, No. 15, pp. 1356-1365.

Viecco, C. (2007), 'Improving Honeynet data analysis', *Proceedings of the IEEE Workshop on Information Assurance and Security*, June 20-22, West Point, NY, USA, pp. 99-106.

Wang, S., Tao, R., Wang, Y. and Zhang, J. (2003), 'WLAN and it's security problems', *Proceedings of the Fourth International Conference on Parallel and Distributed*

Computing, Applications and Technologies, August 27-29, Chengdu, China, pp. 241- 244.

Watson, D. (2007), 'Honeynets: a tool for counterintelligence in online security', *Network Security*, Vol. 2007, No. 1, pp. 4-8.

Yang, L., Wang, J.L., Tian, Z.H., Lu, T.B. and Chen, Y. (2009), 'Building lightweight intrusion detection system using wrapper-based feature selection mechanisms', *Computers & Security*, Vol. 28, No. 6, pp. 466-475.

Yek, S. (2003), 'Measuring the effectiveness of deception in a wireless Honeypot', *Proceedings of the 1st Australian Computer, Network & Information Forensics Conference,* November 25, Perth, WA, Australia, pp. 1-10.

Yek, S. (2004), 'Implementing network defense using deception in a wireless Honeypot', *Proceedings of the 2nd Australian Computer, Network & Information Forensics Conference,* November 25-26. Perth, WA, Australia, pp. 4-15.