結合入侵偵測和蜜罐之分散式預警系統的設計與實現

Design and Implementation of a Distributed Early Warning System Combined with Intrusion Detection System and Honeypot

黃培生
高雄師範大學資訊教育研究所
和平一路116號
高雄市802苓雅區
blhtw@hotmail.com

楊中皇
高雄師範大學資訊教育研究所
和平一路116號
高雄市802苓雅區
chyang@nknucc.nknu.edu.tw

摘要

網路世界的攻防是永無止境的戰爭。伴隨著網際網路的快速發展，網路攻擊也隨之增加且多樣化，面對不斷變種的惡意程式和推陳出新的攻擊手法，僅使用傳統防火牆和入侵偵測技術的系統已無法對應此一快速變化。爲因應此一趨勢，可藉蜜罐吸引惡意攻擊，並將攻擊過程記錄下來，藉蜜罐收集的資訊 (如：攻擊類型、惡意程式檔案、執行的程序和指令等)，分析惡意攻擊所使用的方法、工具及動機，以作爲預測或防治攻擊的參考資料。

本研究結合開放原始碼軟體建立一套分散式預警系統，收集大範圍的網路攻擊趨勢 (包含惡意程式活動和駭客攻擊行爲) 及警示訊息通知，藉由彙整過的資訊，讓資訊安全人員提前收到警訊通知，並瞭解目前網路攻擊的行爲與意圖，以擬定應變措施、確保網路安全。本系統結合 Snort、Nepenthes、Sebek 等入侵偵測及蜜罐工具，增加不同攻擊面向的記錄、分析能力。若發生攻擊行爲，管理者可收到正在進行的攻擊警告，並使用統計攻擊資訊，來瞭解攻擊行爲特性、推論發動攻擊的工具與方式。建置完成的分散式預警系統可安裝於 Live USB，藉由 Live USB 的高可攜性與隨插即用的特色，降低分散式預警系統部署的負擔。

關鍵詞: 防火牆、入侵偵測系統、蜜罐、惡意程式。

Abstract

Network attack and defense is a never-ending war. Along with the rapid development of the Internet, network attacks have increased and diversified. Use of traditional firewall and intrusion detection technologies cannot match to this rapid change. In response to this trend, we designed and implemented a distributed early warning system where several clients collected a wide range of network attack activities, such as malicious codes, sent attack activities back to a

central server, and provided warning messages to the network administrator. The proposed system consists of Snort intrusion detection system with Nepenthes/Sebek honeypot software. This combination comes with client and server architecture so that various aspects of attack-oriented records with analytical capabilities are provided. Network administrators will receive warning notices when the entire network under monitoring was attacking. To reduce the burden on the deployment of distributed early warning system, we also implemented the system on the live USB and our system can be easily installed with high portability and plug-and-play features.

Keywords: Firewall, Intrusion Detection System, Honeypot, Malware

一、前言

近年來網際網路的蓬勃進展，讓訊息得以快速傳遞、資訊能迅速流通，進而帶動了全球化網路和電子商務的發展熱潮；然而網際網路如此快速地發展，若未能同步重視網路安全基礎建置，將招致駭客利用惡意程式、系統漏洞和程式弱點等影響網路安全，進而入侵、破壞系統和竊取、竄改資料，使得個人、企業資料的外洩，造成侵犯他人隱私、引發財物損失等問題。

傳統防禦網路攻擊行爲是以防火牆搭配入侵偵測系統實行 [13]，但如此一來會造成二種問題 [6]：第一，攻擊者只要得知防火牆允許外界存取哪些服務，便可通過防火牆存取內部伺服器，進行下一步攻擊；第二，入侵偵測系統無法提供後續攻擊資訊來瞭解敵人，降低攻擊造成的損失。根據 CSI (Computer Security Institute) 2008年的電腦犯罪與安全性調查報告 [11]，綜合其中144家公司的各種損失 (包含病毒攻擊、未經授權的存取等)，約4,200萬美元。若再由521家公司回覆的資料來看，97%的公司擁有防毒軟體、94%的公司設置防火牆設備、69%的公司已有入侵偵測系統，說明擁有防毒軟體並使用傳統防火牆搭配入侵偵測的系統，已無法有效遏止網路攻擊的威脅。如果能在電腦遭受攻擊的第一時間，立即記錄攻擊事件的來源、手法，對其進行分析比對與推論後續可能的攻擊，並提供給資訊安全人員相關警示和資訊，藉以發佈安全警訊、研判攻擊型態、可能造成的危害、採用的方法或工具，對潛在的攻擊與損害預先掌握，能有效減緩並降低資訊安全風險。

傳統惡意程式 (Malicious Code/Malware) 之定義爲：任何惡意、未經授權存取、不符合預期的程式 [14]。比如電腦病毒 (Virus)、蠕蟲 (Worm)、木馬/後門程式 (Trojan/Backdoor Software)、危險程式 (Riskware) 等威脅程式皆爲惡意程式。根據賽門鐵克第十三期網路安全威脅研究報告 [7]，2007年偵測到71萬1912件全新威脅，較2006年增加468%；迄2007年底所偵測之惡意程式碼威脅總數已增至112萬2311件；而前50大惡意程式碼中68%會竊取機密資料，攻擊者可能會利用它們從事犯罪活動、侵犯隱私，造成個人、企業重大的財務損失。若能先瞭解目前網路上的惡意程式、特性及攻擊目標，可協助資訊安全人員進行惡意程式分析檢測，以作好網路安全防護。

蜜罐所收集到的資訊較精簡且能針對特定流量工作，提供其他工具所沒有的獨特資訊 [10][22]，因此得到的資訊價值也較高，若是搭配入侵偵測系統，可減少主動錯誤訊息 (False Positives) 和被動錯誤訊息 (False Negatives) 等問題 [25]。然而一般開放原始

碼蜜罐皆使用命令列的介面，使得一般使用者較不易進行廣泛設置，也導致收集之資訊有區域限制而不夠全面。對此，本研究建置結合入侵偵測和蜜罐之分散式預警系統，並開發友善的使用者介面，透過分散各網域運行各種應用程式的客戶端，收集大範圍的攻擊資訊及惡意程式進行資料彙整分析。讓資訊安全人員根據所分析的結果，觀察遭受攻擊的電腦及服務，瞭解目前攻擊型態及惡意程式與種類，以便推論其攻擊模式與意圖，及潛在風險與未來趨勢，以擬定應變措施、確保網路安全。。

二、文獻探討

本研究著重在網路攻擊行為之記錄與分析，茲依據研究所需之相關名詞進行文獻探討，並對本研究所使用的工具進行簡介：

1. 防火牆簡介

防火牆 [9] 對全部進出系統的資料執行存取控制，其安全管理機制為雙向的，透過事先設定的規則 (Rules)，阻擋外界惡意的入侵連線，並限制內部主機的對外通訊，不符合規則之封包是無法通過防火牆的，可保護網路內的機密資料，並防止駭客的破壞。但由於防火牆管制全部進出資料之關係，通常會影響到網路的傳輸效率；另外，若有未納入防火牆管制的情形 (如未設定規則的連線或使用者私設的通訊接點)，則使得入侵者可繞過防火牆進行攻擊，讓防火牆無法發揮其效果。

防火牆的型態 [2] 可分為封包過濾、應用層閘道以及電路層閘道等三種型態。

封包過濾器 (Packet Filter)：對每一個進出的 IP 資料封包檢查，若封包符合事先設定的規則就可通過，反之則否。由於封包過濾器是運作於網路層以下的網路，因此無法提供詳細的稽核能力；另外，若利用合法的通訊管道進行入侵 (如：使用 Http 協定、80 Port 的 CodeRedWorm)，封包過濾器也無法發揮效果。

應用層閘道器 (Application-Level Gateway)：使用事先設定的應用程式規則和組態設定，過濾及設定所連接的應用程式資訊，再透過存儲轉發 (Store-and-Forward) 的方式傳遞資訊。由於應用層閘道器接收與傳送資訊時使用不一樣的連接，可藉以隱藏並保護內部的網路。但其建置成本較高，且由於使用代理 (Proxy) 的方式無法相容某些應用程式。

電路層閘道器 (Circuit-Level Gateway)：同樣是透過代理的方式來進行安全存取控制，但於核可服務後會建立起一個交談 (Session)，結束即關閉其埠口；但由於無法針對每一個應用程式進行組態設定，使得其他的應用程式也能經過同一個交談管道進入到防火牆之內，有安全防護上的顧慮。

2. 入侵偵測系統簡介

入侵偵測系統，其定義為「偵測不適當、不正確或是異常的活動的技術」[20]，也就是解讀系統稽核檔 (Audit Record) 或網路活動， 偵測違反使用者定義安全規則的系統，並會在發生異常狀況時通知資訊安全人員以維護網路安全。依其應用環境的不同，入侵偵測系統可以歸類為兩種類型 [3][15]：主機型(Host Based) 與網路型(Network Based) 的入侵偵測系統。

主機型入侵偵測系統主要以電腦系統主機的稽核 (Audit) 資料或網路活動爲基礎 (如檔案、程序、日誌檔等) 作持續的監測，若有不正常的情形發生，系統就會發出被入侵的警告訊息，例如未授權的登入、非法程序的存取、異常的系統呼叫等任何可疑紀錄。缺點是資料量通常非常龐大，且其所紀錄的資訊若被竄改或者是刪除時，對於入侵行爲無從查起。

網路型入侵偵測系統則是直接擷取網路上傳送的封包爲依據，監測封包的檔頭以及內容部分，藉以判斷網路主機是否遭受攻擊者的攻擊或入侵。缺點是其所消耗的系統資源往往與網路封包的流量成正比，如果網路流量過大將會造成入侵偵測系統來不及處理，導致入侵偵測正確率的降低。

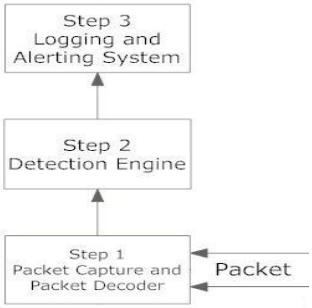
依其使用偵測模式的不同，入侵偵測系統可以分爲三種類型 [1][12]：不當行爲偵測 (Misuse Detection)、異常行爲偵測 (Anomaly Detection) 與混和模式偵測 (Mixed and Hybrid Mode Detection)。

不當行爲偵測：將駭客攻擊的特徵收集起來並彙整儲存爲一大型的攻擊知識庫，然後再利用此知識庫比對所有流入的網路封包，若有封包內的特徵跟攻擊知識庫內所儲存的特徵相符合，系統則判斷其爲危險的行爲並發出警報。但當駭客利用新的手法攻擊時，入侵偵測系統會因攻擊知識庫內並沒有此種攻擊的特徵而未產生警報，使其偵測率較低。

異常行爲偵測：先統計出正常使用者或應用程式的行爲模式，若有不同於此行爲方法所規定的行爲時，則判斷爲不正常的使用並發出警報。但其缺點是可能會產生出誤判的結果，即使用者不同於以往的行爲並非是攻擊行爲，但被入侵偵測系統判定爲攻擊並發出警報。而駭客也有可能在一連串正常行爲之後，逐步改變攻擊行爲，使得入侵偵測系統應該要產生警報但是卻未產生。

混和模式偵測：混合運用不當行爲偵測和異常行爲偵測兩種方式，發揮截長補短的作用，以達到高偵測率與低誤判率的目的。

Snort [4][21] 爲1998年 Marty Roesch 發展出的一套開放原始碼 (Open Source) 的網路入侵偵測軟體 (IDS)。Snort 使用模組化架構和規則驅動 (Rule-Driven) 語言的設計，結合異常行爲、偵測簽章 (Signature-Based) 與通訊協定的偵測方法，爲一套功能強大的網路入侵偵測系統。其架構如圖一。



圖一: Snort 架構圖

3. 蜜罐簡介

蜜罐 (Honeypot) [23] 是一種資訊系統資源，其價值在於被未經授權者或非法者所使用 (A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource)，可部署在開放網路中幫助我們收集並瞭解人侵者行爲的系統，由於

蜜罐所使用的都是未使用的位址，因此流入的連線均可視爲異常連線，故辨別異常連線的正確性較入侵偵測系統高，藉由資料採礦技術的運用與網路封包內容的分析，讓資訊安全人員可更明確分析攻擊發生的原因與未知的攻擊型態，並經由分析得知惡意攻擊所使用的方法、工具及動機。

蜜罐依其設立目的可以分爲兩種類型 [5]：產品型蜜罐 (Production Honeypot) 與研究型蜜罐 (Research Honeypot)。

產品型蜜罐：主要用於保護組織內部網路，偵測並分散來自外部的攻擊拖延攻擊者對真正目標的攻擊，降低資訊安全風險。

研究型蜜罐：主要藉獲取入侵者攻擊的資訊，以認識新的攻擊手法和工具，並瞭解組織系統潛在的資訊風險和漏洞。

依其與入侵者互動的程度，又可分爲三種類型：低互動蜜罐 (Low-Interaction Honeypot)、中互動蜜罐 (Medium-Interaction Honeypot) 與高互動蜜罐 (High-Interaction Honeypot)。

低互動蜜罐：此類型蜜罐一般以模擬的系統和服務來實作，入侵者無法在其上執行任何程序，也因此可獲取的入侵者攻擊資訊較少且不詳細。

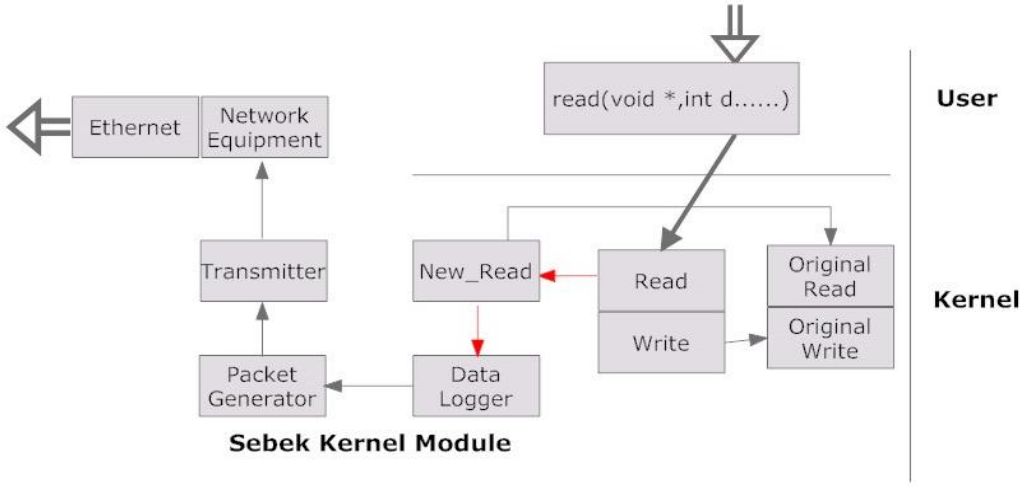
中互動蜜罐：同樣是以模擬的系統和服務實作，但允許入侵者執行部分程序，與低互動蜜罐相比面臨的資訊風險較大。

高互動蜜罐：一般是以真正的系統和服務運行，允許入侵者自由地存取各種資訊資源，可獲取的攻擊資訊最爲詳細，而其所承受之風險爲最高的，因此需要較高的知識來發展與維護此類型蜜罐，以免蜜罐被人侵者控制當作攻擊組織內部其他電腦的跳板。

Nepenthes [16] 爲使用模組化架構的低互動蜜罐，可模擬一般伺服器提供的服務與常見的漏洞，藉以騙取攻擊並下載惡意程式，再將其壓縮成 MD5 檔名的 UPX 檔，便於後續資料分析及管理。圖二爲目前 Nepenthes 所具有的模組。

圖二: Nepenthes 模組

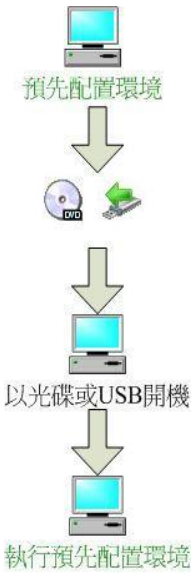
Sebek [19] 主要用來記錄蜜罐裡入侵者行爲的工具，可分爲客戶端和伺服器端。客戶端藉著精巧地設計隱藏於蜜罐核心 (Kernel) 之中，暗中蒐集蜜罐上的攻擊行爲資料 (執行程序、對外連線、存取系統資源等)，再將蒐集到的資料傳送至伺服器端進行資料記錄。其架構如圖三。



圖三: Sebek 架構圖

4. Live CD/USB簡介

Live CD [17] 爲包含預先配置軟體的可開機光碟，讓使用者可以在不需使用硬碟的情況下 (除非使用者想要儲存資料)，經由光碟開機使用，而不需更動現有系統。Live USB 爲 Live CD 的觀念延伸，可滿足使用者儲存資料的需求，並解決先前 CD 唯讀不可更動的限制，提供更快的存取速度，配合依照使用者需求建置的系統，讓 Live CD 的應用更加多元化，成爲可移動之系統平台。其基本原理如圖四。



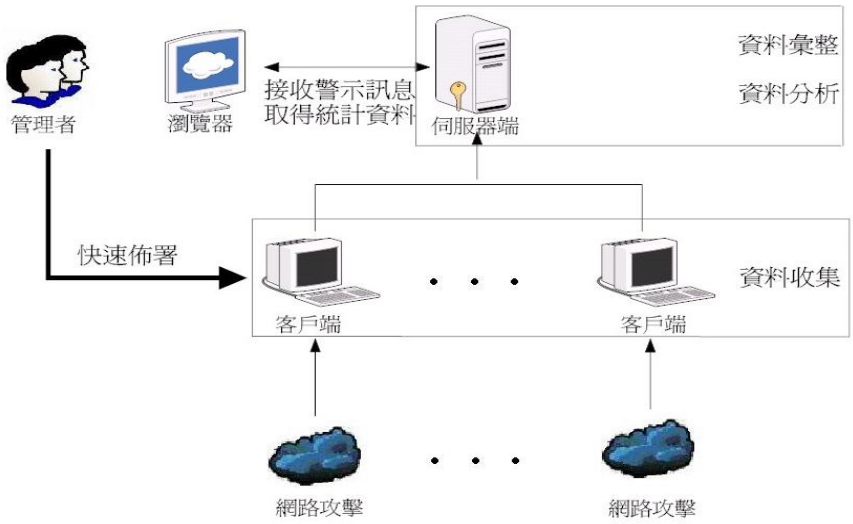
圖四: Live CD/USB 基本原理

三、結合 IDS 與 Honeypot 之分散式架構設計

本研究以收集大範圍網路攻擊資訊及警示訊息發報爲目的，建構一個可快速部署的分散式預警系統，以減少資訊安全人員分散式系統建置和大範圍資料收集的負擔。研究實際結合 Snort、Nepenthes、Sebek 等入侵偵測與蜜罐工具，彙整不同格式資料，對大範圍網路攻擊和警示訊息進行集中分析和發報，再利用網頁介面顯示經分析後的彙整資訊，讓管理者能迅速對攻擊事件做出因應行動。

1. 系統架構介紹

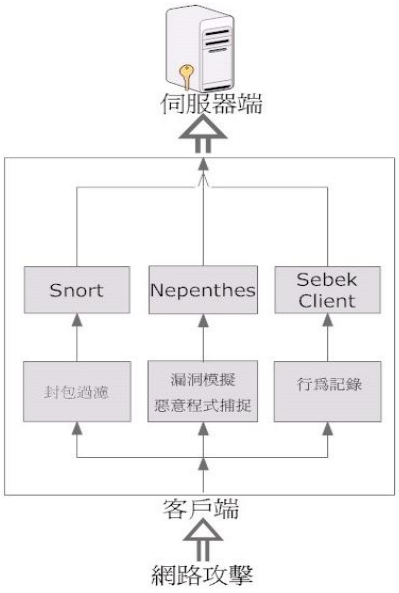
分散式預警系統是由客戶端 (Client) 與伺服器端 (Server) 二部分所組成的，系統架構如圖五所示。客戶端將遭受攻擊的資料與捕獲的惡意程式回傳給伺服器端，由伺服器端進行攻擊記錄與分析、入侵通報，再以網頁的方式呈現彙整後的資訊，利用伺服器端和多個客戶端之間的連結，達到分散資訊集中管控的效果，建構起一個完整的預警網絡。以下將對這些元件作比較深入的介紹。



圖五: 系統架構圖

2. 客戶端

客戶端安置於網域中負起蒐集入侵者攻擊行爲的任務，其架構如圖六所示。以下說明各個元件的功能：



圖六: 客戶端架構圖

Nepenthes：模擬常見服務漏洞引誘入侵者發動攻擊，並捕捉惡意程式樣本，再將其傳回伺服器端，便於進行後續分析。

Snort：監聽並過濾封包來偵測可能的入侵或網路攻擊，辨識其攻擊型態等資訊，再將警告訊息傳回伺服器端。

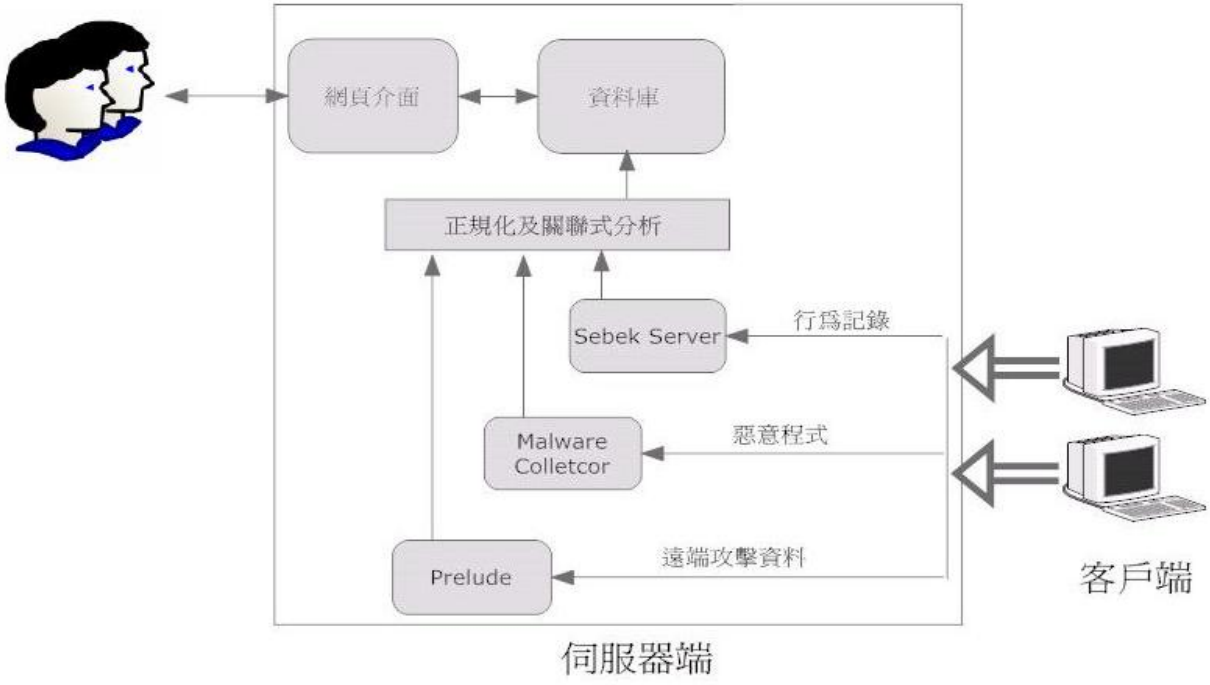
Sebek Client：記錄入侵者在蜜罐上的行爲 (如：執行程序、對外連線、存取系統資源、輸入的指令等資料)，再將資料傳回伺服器端。

網路管理人員可依所在網路環境的不同，利用可攜式 Live USB 進行客戶端快速部署 (如圖七)，並使用操作介面 (如圖八) 進行客戶端設置。當網路攻擊發生時，依其攻擊類型的不同，會觸發不同的系統元件進行資料的收集，最後傳遞到伺服器端進行後續處理。

圖七: 客戶端開機畫面

圖八: 客戶端操作介面

3. 伺服器端



圖九: 伺服器端架構圖

由圖九中我們可以觀察到，伺服器端可以同時連接多個客戶端並接收到所有客戶端傳遞的訊息，由各個不同的元件進行過濾分析後儲存於資料庫，若這些訊息都有相關性，則可能有入侵者針對網域內的電腦作大範圍的攻擊或掃描。以下說明各個元件的功能：

Sebek Server：接收多個客戶端傳回的指令或連線資料進行過濾，再將其存入資料庫。

Malware Collector：接收 Nepenthes 傳回的惡意程式樣本，並儲存記錄於資料庫中。

Prelude [18]：模組化設計的開放原始碼混合型入侵偵測系統 (Hybrid IDS)，使用標準 IDMEF 格式進行通訊，從設計的方式來看定位於適應大型網絡的需求，可接收來自多個客戶端的資料，統整不同的資料格式，再儲存於資料庫。

資料庫：儲存經正規化後的網路攻擊相關資訊。

網頁介面：分析由資料庫中取得的攻擊資訊，再以網頁的方式進行呈現，同時監控網路攻擊情況，若是有異常情形發生，會對這些訊息進行標記並依管理者設定的方式進行通知或是輸出報表等相關事務。另外，管理者也可從遠端進行資訊查詢或惡意軟體樣本下載。

四、系統開發與實驗測試分析

1. 開發工具與環境

本研究之軟硬體環境如表一所示。

表一: 開發工具與環境

系統硬體	Intel Core2Duo P8600 2.4GHz 4GB 之PC相容電腦
系統軟體	(一)xUbuntu 8.04 (二)Snort 2.8.3.2 (三)Nepenthes 0.2.2 (四)Sebek 3 (五)Apache 2.2.8 (六)MySQL 5.0.5 (七)VMware 6.5.1
程式語言 及工具	(一)PHP 5.2.4 (二)QT4

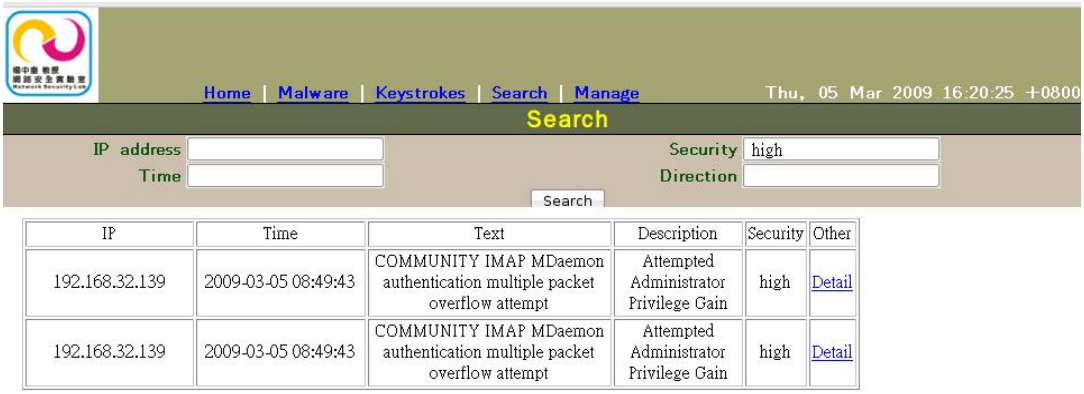
2. 系統測試

爲了測試能否收集到網路攻擊記錄和惡意軟體樣本，本研究使用攻擊軟體於實際發動攻擊。

攻擊一：遠端針對被攻擊主機進行緩衝區溢位攻擊。

攻擊主機: 192.168.32.139。

被攻擊節點: 192.168.32.137。

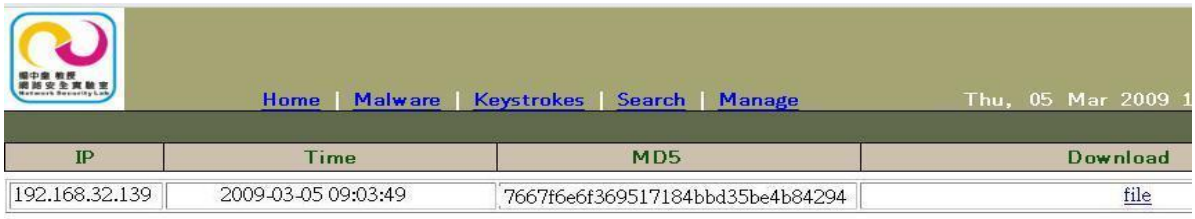


圖十: 顯示攻擊一之偵測結果

攻擊二: 利用 Nepenthes 所模擬的漏洞上傳惡意程式。

攻擊主機: 192.168.1.139

被攻擊節點: 192.168.1.137

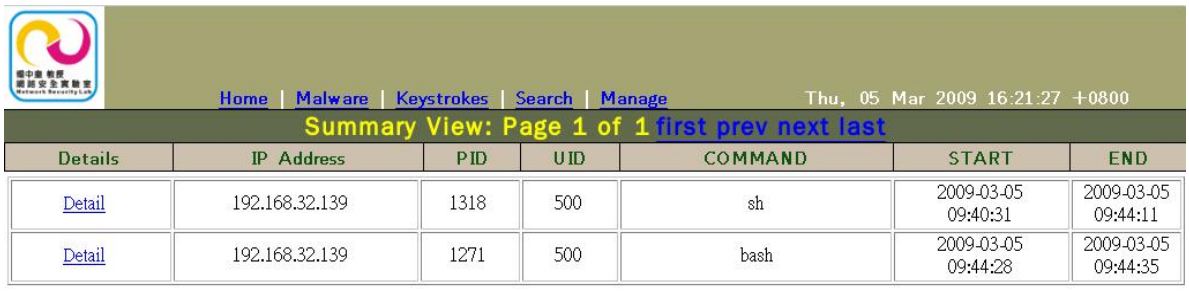


圖十一: 顯示攻擊二之偵測結果

攻擊三: 假設駭客利用未知漏洞取得執行權限，並執行程序。

攻擊主機: 192.168.1.139

被攻擊節點: 192.168.1.137



圖十二: 顯示攻擊三之偵測結果

3. 實驗分析

將開發完成的系統實際部署於校園網路環境和私人企業，經過一個月(2009/2/25~2009/3/25)的資料收集，客戶端總共遭受到2571次攻擊，依 Snort 分類其風險等級 (如表二)，並針對遭受攻擊的埠列出前10名排行榜 (如表三)，其中模擬 Windows 系統 TCP 埠139及445的次數明顯較高，說明其仍是蠕蟲或入侵的攻擊目標。

表二: 風險等級

等級	次數
低	782
中	1028
高	761

表三: 遭受攻擊的埠

排名	埠	次數
1	445	2554
2	139	2199
3	80	595
4	NULL	294
5	135	207
6	1434	97
7	25	93
8	443	34
9	5000	32
10	10407	30

再列出來自校內 (如表四) 和校外 IP (如表五) 的攻擊次數，以及相關攻擊型態統計 (如表六)，並將收集到的惡意程式上傳至 VirusTotal [24] 進行分析，列出惡意程式的統計資訊 (如表七)，可檢視出內部和外部網路的異常情形，預測可能的危害，據以進行後續處理和防範。

表四: 來自校內攻擊的 IP

排名	IP	次數
1	140.127.38.43	267
2	140.127.38.13	237
3	140.127.38.51	90
4	140.127.47.45	78
5	140.127.38.50	68

表五: 來自校外攻擊的 IP

IP	國家	次數
87.55.74.160	Denmark	729
220.129.76.130	Taiwan	209
218.169.81.216	Taiwan	130
87.220.66.176	Spain	128
220.129.124.28	Taiwan	90
220.129.86.92	Taiwan	80
220.143.12.75	Taiwan	78
220.129.114.197	Taiwan	63
220.129.43.143	Taiwan	60
220.129.146.157	Taiwan	59

表六: 攻擊型態統計

攻擊型態統計	次數
ATTACK-RESPONSES Microsoft cmd.exe banner	222
Shellcode detected: execute::cmd	168
Exploit attempt: NETDDEDialogue	146
Malware submitted	117
(portscan) TCP Portsweep	85
WEB-IIS view source via translate header	82
Exploit attempt: LSASSDialogue	60
NETBIOS SMB-DS lsass DsRolerUpgradeDownlevelServer unicode little endian overflow attempt	59
Shellcode detected: url::anyurl	53
ICMP PING speedera	31

表七: 惡意軟體統計

MD5	次數	偵測率
1a6c7da5357152ef34cadf2a5bd17bfa	28	82.05%
8128405d8c32a75bab02a1f0d125d11c	25	90%
3490e2ea159616cc59e5ad904ca11857	22	58.97%
ead12a6c0224703ebc41a7121513a348	6	100%
986b59708d2ca33f4c1ad682a5d7a673	4	94.87%
93dcd8587f65259b8b784b9176252080	4	75%
7d99b0e9108065ad5700a899a1fe3441	4	94.87%
9bb68450cdaad8713b49ce7204512bdc	3	97.22%
34c33016095ceff453e5bb2d45f188c5	2	84.62%
b5b793a6018dfe1b6763444ae20b75ab	1	94.87%

4. 本研究與相關研究之比較

Hybrid Honeypot Framework [8] 爲利用 Honeyd、Honeywall 及 Snort 等工具所建置的混合式蜜罐系統，其概念與本研究相似，均爲結合多種蜜罐工具之系統，可用以偵測入侵攻擊，並分析駭客行爲與攻擊的系統。以下是本研究系統與 Hybrid Honeypot Framework 系統的比較 (如表七)：

表八: 本研究與相關研究比較

分析項目	Artail et al., 2006	本研究
分散式部署	◯	◯
網路型入侵偵測	◯	◯
異常行爲偵測	◯	◯
低誤報率	◯	◯
可擴充性	◯	◯
及時偵測	◯	◯

本研究與 Hybrid Honeypot Framework 系統比較不同的是，本研究除了以 Snort 來識別攻擊的類型，並結合了 Nepenthes 的模擬服務與惡意程式收集，再以 Sebek 記錄利用弱點並迴避人侵偵測系統於客戶端操作之行爲，最後藉由匯集的警訊與惡意程式，對駭客的攻擊行爲作更進一步的分析。

五、結論與未來發展

本研究所開發之分散式預警系統，結合入侵偵測系統 Snort 和蜜罐工具 Nepenthes、Sebek，吸引惡意攻擊並收集相關攻擊資訊，並對不同格式及分散資訊進行關聯性分析，再利用網頁介面顯示彙整資訊，以減輕資訊人員資料收集的負擔，並致力於推論可能攻擊、預測未來趨勢。最後將分散式預警系統建置於 Live USB，並透過友善的使用者介面，進行快速的平台建置與部署。

在未來發展方面，可加強本系統的傳輸安全性及運作隱密性，來減低被偵測的風險；或考慮再加入網頁型蜜罐，收集網頁攻擊的相關資訊，以檢測潛藏的網頁漏洞、提升偵測網路攻擊的廣度，使其能更全面的瞭解駭客攻擊的趨勢與變化，並協助資訊安全人員作好網路防護工作。

參考文獻

[1] 李駿偉、田筱榮、黃世昆，“入侵偵測分析方法評估與比較”，*資訊安全通訊*，第八卷，第二期，2002：頁38~61。

[2] 張思源，“揭開防火牆的神祕面紗”，*網路通訊雜誌*，第七十五期，1998：頁107~109。

[3] 黃家楷、邱國政、黃盈源、馮立琪，“一個可動態調控的元件化網路式入侵偵測系統”，*第十三屆全國資訊安全會議*，2003：頁333～340。

[4] 楊中皇，網路安全：理論與實務，台北：學貫行銷股份有限公司，2008，第十三章。

[5] 賴明豐，“蜜罐技術的分析與應用”，*資通安全分析專論*，T9603，2007，http://ics.stpi.org.tw/Treatise/doc/46.pdf

[6] 賽門鐵克公司，入侵偵測系統：誘捕式網路防禦技術的演進，http://www.symantec.com/region/tw/enterprise/article/mantrap.html

[7] 賽門鐵克公司，第十三期網路安全威脅研究報告，http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf

[8] Artail, H., Safa, H., Sraj, M., Kuwatly, I. and Al-Masri, Z., “A Hybrid Honeypot Framework for Improving Intrusion Detection Systems in Protecting Organizational Networks,” *Computers & Security* (25:4), 2006: pp. 274-288.

[9] Bellovin, S. M. and Cheswick, W. R., “Network Firewalls,” *IEEE Communications Magazine* (32:9), 1994: pp. 50-57.

[10] Chuvakin, A., “Honeynets: High Value Security Data: Analysis of Real Attacks Launched at a Honeypot,” *Network Security* (2003:8), 2003: pp. 11-15.

[11] Computer Security Institute, CSI computer crime and security survey, http://www.gocsi.com/forms/csi_survey.jhtml

[12] Cuppens, F. and Miège, A., “Alert Correlation in a Cooperative Intrusion Detection Framework,” *IEEE Symposium on Research in Security and Privacy*, 2002: pp. 202-215.

[13] Levine, J.G., Grizzard, J.B. and Owen, H.L., “Using Honeynets to Protect Large Enterprise Networks,” *IEEE Security & Privacy* (2:6), 2004: pp. 56-58.

[14] McGraw, G. and Morrisett, G., “Attacking Malicious Code: a Report to the Infosec Research Council,” *IEEE Software* (17:5), 2000: pp. 33-41.

[15] McHugh, J., Christie, A. and Allen, J., “Defending Yourself: The Role of Intrusion Detection Systems,” *IEEE Software* (17:5), 2000: pp. 42–51.

[16] Nepenthes, http://nepenthes.mwcollect.org/

[17] Pillay, H., “The Magic of Live CDs,” *Free Software Magazine*, http://www.freesoftwaremagazine.com/node/1103/pdf

[18] Prelude, http://www.prelude-ids.com/

[19] Sebek, http://www.honeynet.org/tools/sebek/

[20] Singh, S. and Kaur, G., “Unsupervised Anomaly Detection In Network Intrusion Detection Using Clusters,” *Proceedings of National Conference on Challenges & Opportunities in Information Technology*, 2007: pp. 107-110.

[21] Snort, http://www.snort.org/

[22] Spitzner, L., “Honeypots: Simple, Cost-Effective Detection,” Securityfocus, 2003, http://www.securityfocus.com/infocus/1690

[23] Spitzner, L., “Honeytokens: The Other Honeypot,” Securityfocus, 2003, http://www.securityfocus.com/infocus/1713

[24] VirusTotal，http://www.virustotal.com/zh-tw/

[25] Zhang, F., Zhou, S., Qin, Z. and Liu, J., “Honeypot: a Supplemented Active Defense System for Network Security,” *Proceedings of Fourth International Conference on Parallel & Distributed Computing Applications and Technologies*, 2003: pp. 231-235.