# 基於多樣資訊發展之入侵偵測系統

**林佳憲**
**中國文化大學資訊管理研究所**
**lamb1@seed.net.tw**

**蔡敦仁**
**中國文化大學資訊管理研究所**
**drtt@mail.pccu.edu.tw**

## 摘要

目前的入侵偵測系統(Intrusion Detection System)發展都較偏向特徵型(Signature-based)的入侵偵測系統，特徵型的入侵偵測系統利用特徵比對的方式，當流量收集進入入侵偵測系統之後，透過特徵資料庫比對後，來確定流量是否為惡意的攻擊入侵的流量，還是正常的流量。

本研究透過以流量統計資訊、異質入侵偵測系統事件資訊與系統環境弱點知識庫，發展出一套基於多樣資訊之入侵偵測系統，並建立入侵偵測事件的分析機制，以提高偵測準確度與降低誤判率，並應用於實際的網路環境中收集網路存取資訊，期望能夠偵測出真正威脅網路的異常連線模式，並減輕對管理者的負擔。

**關鍵詞**：流量統計(Traffic Statistics)、特徵型入侵偵測系統(Signature-based Intrusion Detection System)、知識基礎(Knowledge-based)。

## 1. 前言

現今的網路安全防護方法，不外乎使用防火牆與入侵偵測系統來防禦與偵測來自外部或內部網路上的威脅。就防火牆系統而言，其特性就是有限度的開放網路服務，給予來自網路上的使用者使用，其缺點是入侵攻擊手法並非單純使用單一入侵攻擊手段，可能透過系統漏洞、電子郵件的收送管道植入木馬程式、甚至是暴力攻擊法等。因此攻擊方式已經由外部攻擊手法轉變成網路內部的攻擊手法。所以整體的資訊安全防禦措施必須搭配上入侵偵測系統協助，以增加整體的資訊安全防禦措施的可見度。

現有特徵型入侵偵測系統會有以下三種主要的缺點：

1. 新攻擊手法產生時，從發現新攻擊手法到特徵定義檔的開發完成，會有一段安全防禦的空窗期，在這段期間，特徵型入侵偵測系統無法抵抗未知的入侵攻擊，造成安全漏洞。

2. 特徵型入侵偵測系統採取特徵檔比對，來進行檢測，相對會有特徵資料庫儲存特徵定義檔資料，以進行比對。因此，每增加新入侵攻擊手法時，便會開發相對應特徵定義檔。然而，現今入侵攻擊發生期間短且多，因此特徵型入侵偵測系統的資料庫，會不斷增長，造成資料庫變龐大且複雜，比對效率變慢，因此入侵偵測系統無法有效消化所截取資料比對，形成部份資料容易被忽略，造成安全漏洞。

3. 特徵檔是固定格式的特徵，因此入侵者可利用相同弱點進行攻擊，將攻擊手法改變後便可迴避入侵偵測系統的偵測[12]，因此容易增加誤判率。

為了解決上述的問題，本研究利用不同資訊來描述網路或系統上正常與不正常的行為特徵，其中採取流量統計、異質入侵偵測系統、系統弱點知識庫來降低誤判率、增加對未知攻擊的偵測率以及對告警事件的準確度。

## 2. 研究模型

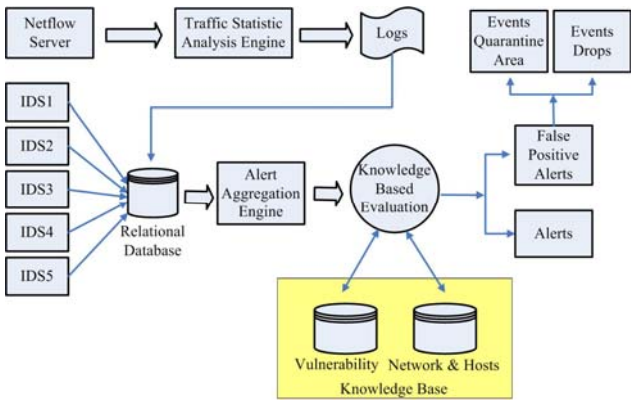


**圖 1 研究模型**

如圖 1 所示，整體模型分成三個主要元件：（1）流量統計引擎(Traffic Statistics Analysis Engine)（2）告警事件收斂引擎(Alert Aggregation Engine)（3）知識基礎評估引擎(Knowledge-based Evaluation Engine)。以下的章節將會對這些主要元件做詳細說明。

## 2.1 流量統計引擎

路由器或核心交換器是網路封包的交換中心，網路上的訊息需靠路由器或核心交換器的傳送以達到目的地。因此，在適當的路由器或核心交換器上，我們可以有效的收集到網路上的流量資訊。依本研究而言，利用 Netflow[3]流量資訊收集架構如圖 2[1]所示。

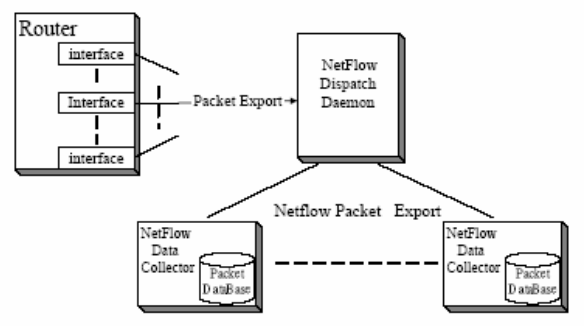


**圖 2 流量資訊收集架構**

## 2.2 流量資訊的格式

資料流是定義為單方向的封包資料流，這代表資料流產生是介於來源位置與目的位置之間。因此其中資料流包含了網路層的網路位置，與傳輸層的來源服務埠、目的服務埠等資料，所以具體來說一個資料流將包含七個主要的參數：

Source IP address
Destination IP address
Source port number
Destination port number
Layer 3 protocol type
ToS byte
Input logical interface (ifIndex)

Netflow 是由 Cisco 所提出的專屬技術規格，因而所傳送出來封包的內容也受到該規格的規範。本研究僅擷取了 Netflow 規格中的部分必要欄位，所抓取出來的資訊欄位如圖 3 所示。

| Source IP Address | Destination IP Address | Source Port | Destination Port | Protocol | ifIndex | Flag | Octets |
|---|---|---|---|---|---|---|---|

**圖 3 流量資訊收集架構**

Source IP Address：來源端 IP 位址。
Destination IP Address：接收端 IP 位址。
Source Port：發送端程式所使用的埠號。
Destination Port：接收端程式所使用的埠號。
Input：進入的網路介面。
Output：出去的網路介面。
Flag：TCP 旗標。
Octets：資訊流的大小。

透過 Netflow 規格中，我們截取了部份必要欄位後，運用這些必要欄位，交互運用，便可產生出 Netflow 特有的入侵偵測分析，在這裡稱為流量統計分析法，透過此分析法便可以針對特徵入侵偵測系統的弱點進行補強。

## 2.3 流量統計分析法

流量統計分析法中[13]，分成三大分析法分別為(1) Top N 與基準(Baseline) (2)IP 位址對應 (3)旗標分析法。

Top N 與 Baseline 分析，透過 Netflow 收集一段時間網路流量後，分析出 Top N Session 與 Data，定義正常狀態，此狀態就是所謂的 Baseline[2]，之後分析 Top N 與 Baseline 的關係，進而找出入侵攻擊的手法。

IP 位址對應分析[9]，其中不外乎是目的位置、來源位置、保留 IP 位置、網路介面、目的埠與來源埠等。透過這些資訊，分析出流量是否為合理、符合邏輯的，即可分析出攻擊模式。

旗標分析法，利用主動式的入侵攻擊特性，會在網路上尋找目標，因此不論是入侵攻擊者會利用三向交握訊息去試探攻擊目的電腦主機，或採取了 ICMP 的刺探方式，來找尋出攻擊目標主機，都可以利用旗標分析法，找出可疑的連線。

透過流量統計分析法，整個流量統計引擎實為提供現有的入侵偵測系統之補強，透過圖 4 可清楚瞭解，各種分析方法與可偵測的入侵種類。

| 分類 | 方法 | 假設說明 | 偵測入侵種類 |
|---|---|---|---|
| TopN & Baseline | Top N Session | 單一部主機對一或一群目的主機，產生大量的連線。 | DoS/DDoS、未知攻擊、網路掃瞄、網路資源濫用 |
| | Top N Data | 一段時間內大量網路資料傳輸到一或一群目的主機。 | 未知攻擊、網路資源濫用 |
| IP 位置對應 | Reserved addresses | IANA 保留部份的網路位置，是不被能路由。 | IP Spoofing |
| | A special IP or IP list | 考慮進出網路流量與特定位址。 | IP Spoofing |
| 線標分析法 | TCP SYN Scan | 入侵攻擊者利用三向交握訊息去試探攻擊目的電腦主機。 | 未知攻擊、網路掃瞄 |
| | UDP Detection Analysis | 採取了 ICMP 的刺探方式，來找尋出攻擊目標主機。 | 未知攻擊、網路掃瞄 |

**圖 4 分析比較圖**

流量統計引擎，透過 Netflow 資料流收集後，利用前述的各種分析法，將分析結果產生後，對有可疑之流量進行紀錄，這些可疑的紀錄需要將其格式正規化後，與其他資訊匯總後，再做進一步分析，圖 5 為流量統計引擎之流程圖。

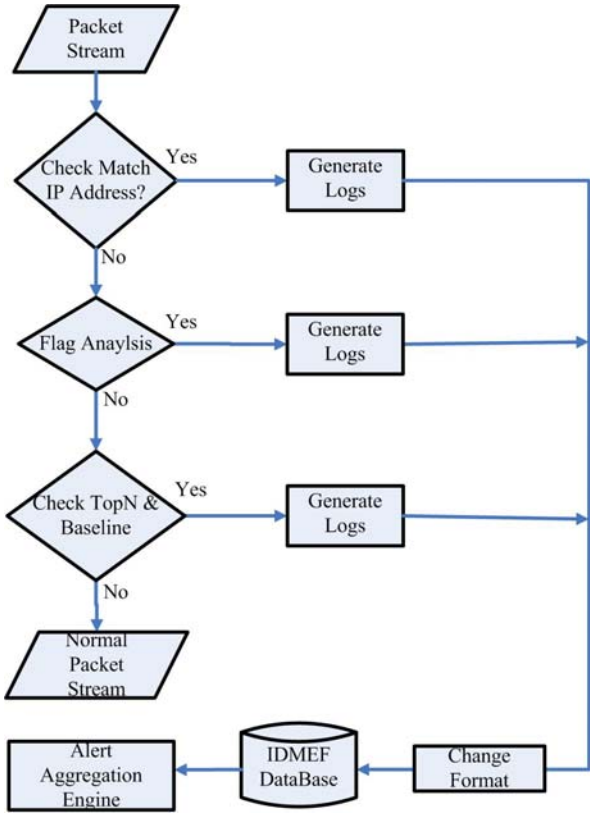


**圖 5 流量分析流程圖**

## 3. 告警事件收斂引擎

就現今來說，普遍存在各類型入侵偵測系統告警事件格式不統一的現象，因此在環境中有多種入侵偵測系統存在，無法有效讓異質入侵偵測系統協作。

本研究透過告警事件收斂引擎處理事件的匯總、統一事件格式與分類，也因此該元件提供（1）告警事件轉換(alert converting) （2）告警事件分群(alert grouping)（3）告警事件合併(alert merging)三種功能，透過三種功能運作之後，集中存放在關聯性資料庫中，如圖 6 所示。

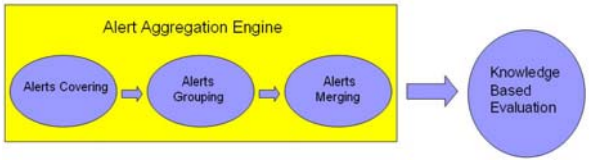


**圖 6 流程圖**

### 3.1 Alert Converting

透過不同格式的事件告警，讓異質的入侵偵測系統可以達到相互協作的目的，首先要將各種不同格式的告警事件轉變成統一標準的格式。本研究採用 Intrusion Detection Message Exchange Format（IDMEF）[8]，將告警事件標準化，再將標準化後的告警事件，儲存在關聯性資料庫。

### 3.2 Alert Grouping

根據發生時間、來源、目的、類型，將告警事件群組成一個事件叢集。每一個叢集會以一個代表告警事件來代表該事件叢集的特性，而群組化的目的是消除重覆的告警事件與入侵攻擊。

### 3.3 Alert Merging

此過程是將異質的入侵偵測系統告警事件，變成複合告警事件（Compound Alert）。在轉變的過程中，透過選舉機制，來消除入侵偵測系統的衝突。選舉機制說明如下

所有入侵偵測系統都有偵測到入侵告警事件：產生一個新的告警事件，刪除所有個別入侵偵測系統告警事件。

部份入侵偵測系統偵測到入侵告警事件：(1)以表決法決定，有告警事件入侵偵測系統數量大於無告警事件入侵偵測系統數量，產生一個新的告警事件，刪除所有個別入侵偵測系統告警事件。(2)有告警事件入侵偵測系統數量小於無告警事件入侵偵測系統數量，刪除所有個別入侵偵測系統告警事件。

半數數量入侵偵測系統偵測到入侵告警事件：原先的嚴重性(Severity)分成 info、low、medium、high 四等級，依照告警事件等級降一個等級，產生一個新的告警事件，刪除所有個別入侵偵測系統告警事件。

## 4. 知識基礎評估引擎

入侵偵測系統一般只對於自身所偵測的網路流量去做分析是否符合入侵偵測系統所認知的入侵事件，缺乏對於周遭系統環境的整合監控與察覺。入侵偵測系統與系統環境無法有效整合，產生許多系統環境因系統修補或弱點修復後已經免疫的無效入侵偵測告警事件，增加入侵偵測系統的誤判率。

舉例來說，入侵偵測系統發出告警事件，偵測到一種對有 Linux 系統環境損害性極大的攻擊入侵事件，結果在系統環境中並無任何 Linux 系統存在，因此系統安全管理員會耗費時間在處理這類不可能攻擊成功的告警事件，大量的誤判告警事件將使系統安全管理人員無法清楚尋找到真正惡意的攻擊告警事件。

目前許多入侵偵測系統，如 Snort、Cisco IDS，它們的特徵定義檔的制作會參考 CERT[5]或 CVE[6]等。CERT 與 CVE 會詳細列出所有的系統環境的弱點以及入侵攻擊會影響那些應用程式的資訊。

因此透過此類資訊，便可評估入侵攻擊成功機率與否。在此，本研究透過知識基礎評估引擎去排除這類已經免疫的系統環境，讓系統安全管理人員有能力去專注真正的威脅入侵攻擊。

知識基礎評估引擎是整合網路架構、系統環境、應用程式的資訊組合而成，結合弱點資訊做為威脅管理評估，如圖 1 所示，知識庫內儲存著所有系統弱點以及目前網路或系統環境的相關資訊，如系統啟動何種服務、使用何種應用程式、修復何種弱點等。因此，知識基礎評估引擎就像告警事件過濾器，透過評估處理過後，過濾掉誤判告警事件。

舉例說明，如圖 7，當入侵偵測系統或流量統計分析引擎產生告警事件後，透過事件正規化產生出相關資訊，透過相關資訊與知識基礎評估引擎的弱點知識庫比較，如果產生的告警事件中所敘述的弱點是弱點知識庫中沒有的，將會把此事件歸類等級為嚴重性事件。反之，評估進入網路與主機知識庫比對，此告警事件的目的設備是否有這類弱點？或者是有這類弱點，但已經弱點修復？如果無這類弱點或已經修復這類弱點，此時此告警事件便為誤判或無效的入侵攻擊。反之，此告警事件就為真正有威脅性的攻擊入侵事件。

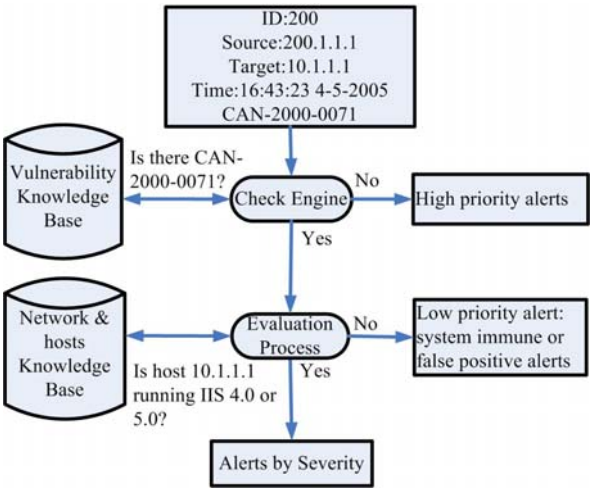


**圖 7 知識基礎評估引擎流程範例**

## 5.模型實驗

本研究分別以 Snort 與 Cisco IDS 做為兩種異質網路型入侵偵測實驗系統，監控一個網段，而此網段為有許多不同平台的系統環境，包含 Windows 與 Linux 的系統環境。另外，主要網路設備啟動 Netflow 功能，透過 Netflow 伺服器收集有關網路流量統計的資料，如圖 8 所示。

攻擊主機透過 Nessus[10]弱點掃瞄與滲透測試工具，對目標主機與網段發動攻擊。攻擊期間，為了達到產生誤判告警事件的效果，本研究以 IIS buffer overflow 入侵手法，攻擊 Linux 主機與對已經修復 IIS 的弱點的 Windows 主機。最後，攻擊主機會啟動合法正常的資料流量存取網路上的資源，以求達更符合真實網路使用環境。

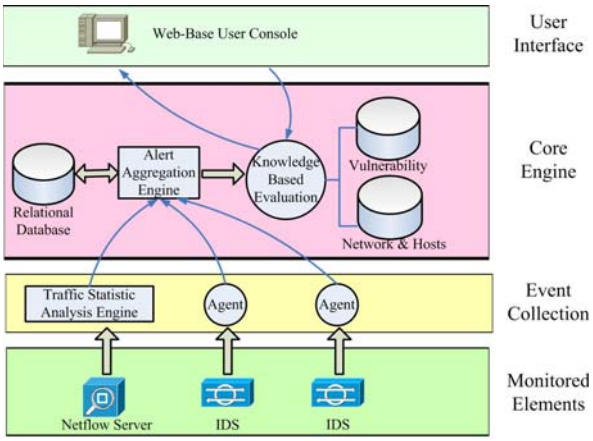


**圖 8 實驗模型**

就另一研究目的而言，要測試透過流量統計技術可以偵測到未知的入侵攻擊，因此將此兩部入侵偵測系統，採取使用較舊的特徵檔資料庫，以期讓兩部入侵偵測系統無法偵測到入侵攻擊，但可透過流量統計技術，偵測出入侵攻擊。

在實驗測試期間，採取約 30 種不同的入侵攻擊，Snort 產生了 458 個告警事件，而 Cisco IDS 產生了 384 個告警事件。利用多樣資訊的入侵偵測系統產生 246 個告警事件，如圖 9 所示。因此透過收斂、群組化事件，加上知識基礎評估引擎，可以比較有效的降低告警事件的數量，以及增加準確率。

| 危機等級 | Snort | Cisco IDS | Multi-info IDS |
|---|---|---|---|
| 警告(Info) | 67 | 51 | 34 |
| 低危險(Low) | 286 | 238 | 153 |
| 中危險 (Medium) | 74 | 69 | 43 |
| 高危險 (High) | 31 | 26 | 16 |

**圖 9 偵測事件數據**

## 6. 結論

多樣資訊的優點可以有效增加入侵偵測系統的準確度，避免不必要的告警事件，降低管理人員的負擔。另外，對網路上的未知的入侵攻擊手法，因攻擊方式有軌跡可依循，便可採取流量統計技術，輔以入侵偵測系統偵測未知入侵攻擊的能力。

本研究中所建立的研究模型，是根據流量統計、異質入侵偵測系統與知識基礎三種資訊來做研究，這樣的作法多少會因資料的多寡來影響精準度。所以如何決定再增加更多樣化的資訊，如防火牆與系統日誌檔，網路設備設定檔等資訊，將是一個有待後續實驗的重要問題。

## 參考文獻


[1] 林鳳銘、吳守豪、李蔡彥， “Intrusion Detection: a Network View”, in Proceeding s of TANet 2001 Conference, pp. 34-48, 2001

[2] Ophir Rachman,”Baseline Analysis of Security Data”,Securimine Software Inc ,Feb 2005

[3] Cisco’s NetFlow Feature, http://www.cisco.com/warp/public/732/netflow/

[4] Cisco’s IDS Overview http://www.cisco.com/en/US/products/sw/securs-w/ps2113/index.html

[5] CERT, http://www.cert.org

[6] CVE,http://www.cve.mitre.org

[7] F. Cuppens, “Managing alerts in a multi-intrusion detection environment”, 17th Annual Computer Security Applications Conference (ACSAC). New-Orleans, December 2001.

[8] H. Debar , D. Curry and B. Feinstein ,”Intrusion Detection Message Exchange Format”, http://www.ietf.org/internet-drafts/draft-ietf-idwg-idmef-xml-14.txt ,Jan 2005

[9] IANA,"Special-Use IPv4 Addresses",RFC 3330,September 2002

[10] Nwssus,http://www.nessus.org/

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

[12] Thomas H. Ptacek and Timothy N. Newsham, “Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection”,Secure Networks, Inc., January, 1998.

[13] Yiming Gong ,“Detecting Worms and Abnormal Activities with NetFlow”, http://www.securityfocus.com/infocus/1796, Aug 2004