# 整合資安關聯警示以降低內部威脅之研究

空軍中校　周文祥　空軍中校　黃廉鈞


## 提　要

內部威脅是合法使用者因濫用所賦予的權限，進而可能造成單位資產的重大威脅。內部人員對組織而言，並非總是友善的，更可能是一個主要威脅來源。目前的資安技術大部分是針對外部攻擊的偵測與防禦，這樣的做法忽略了單位中內部人員所造成的威脅或是面臨的網路安全風險。

本研究提出以現有分散式入侵偵測系統為基礎，發展一個用來偵測暨評估內部威脅風險的概念架構及實現方法，著重於不應只考量傳統的攻擊優先等級，應量化其所造成的攻擊風險值。因此，本研究提出數個多面向的關鍵因素，如：人員角色、攻擊行為與資產資訊等因素，進行內部攻擊風險值評估與分類處置探討，以從傳統的大量攻擊警示中發現關鍵資訊，並正確辨識出單位內真正面臨高度風險主機或是具有惡意行為的內部人員，據以執行威脅分類與處置作為，進而提供各管理階層進行管理或決策參考依據。

因此本研究中，藉整合運用有效的資安關聯警示，期能在內部攻擊真正行實質破壞前，精準偵測暨評估出異常行為的徵兆與風險值，俾降低內部威脅程度，並可提供進階持續性滲透攻擊(APT)等先進手段一個初步防禦概念架構。。


**關鍵字**：內部威脅、資安防護監控、攻擊風險值、進階持續性滲透攻擊。

## 前　　言

### 一、研究背景與動機

隨著網際網路及資訊技術的快速發展，相對的網路攻擊其複雜度與規模皆日益增高，如進階持續性滲透攻擊(APT, Advanced Persistent Threat)等先進手段，致資訊安全與確保已成為企業生存與發展的重要議題。然而，對於重要的國防及基礎建設等資訊系統，「內部威脅」(Insider Threats)一直是重大威脅之一，亦即是經過授權且被信賴得以接觸或處理相關資訊人員的惡意行為所造成的威脅。根據美國2011年電子犯罪觀察調查(E-Crime Watch Survey)顯示，約有21%的電

子犯罪事件是因內部威脅所造成的，雖然案件的平均數量逐年遞減，但是對企業所造成的破壞與影響卻直逼外來攻擊的損失。[1]

當組織面對上述問題時，除制定相關的安全政策(Security Policy)外，亦會加強資安防護監控等技術，如防火牆(Firewall)、入侵偵測系統(IDS, Intrusion Detection System)等。然而Wang等人指出，目前的入侵偵測系統無法有效偵測內部攻擊，因授權的內部人員在掌握系統弱點後，可輕易地發動攻擊。[2]因此傳統的防制措施存在四個盲點：

1.由於內部威脅的來源通常是合法授權者，可能熟悉部分監控措施，進而規避或另尋攻擊途徑，以暗地進行非法行為，因此較難預測與防制。

2.傳統防禦主要是確保伺服器等重要主機安全，但忽略了於現實環境中，重要資料亦可能被存放在組織內部之重要職務人員電腦中。

3.多項來源警示紀錄繁多，如未與組織內系統弱點資訊與人員行為進行整合、關聯與分析，則不易有效挖掘有關內部威脅之異常徵兆。

4.無法針對已執行或預劃實施之防制措施，進行其對內部威脅防禦能力的預測與評估。

上述盲點亦說明了，相異的組織特性，先天上就有其不同的內部威脅問題。因此，內部威脅問題無法僅單獨依賴安全政策或先進架構與技術解決，必須考量相關政策、程序、技術等因素對內部威脅之影響。

上述盲點亦說明了，相異的組織特性，先天上就有其不同的內部威脅問題。因此，內部威脅問題無法僅單獨依賴安全政策或先進架構與技術解決，必須考量相關政策、程序、技術等因素對內部威脅之影響。[3]

## 二、研究目的

依據前述背景與動機發現，傳統上對重要的資訊系統的內部威脅防制措施皆假設系統僅具有兩種邊際(Marginal)狀態，即完全失效或完全正常，然而在實務上絕大多數的系統皆是由完全正常的狀態逐漸進入完全失效的狀態，其異常的徵兆或許有時可經由先進的入侵偵測技術所發現。然而大部分的內部威脅通常是屬於具有合法授權且熟悉該系統人員之不當誤用或惡意行為，使得系統的表現有時仍然與正常完全一致，這類的威脅較難以防範。因此除了資訊系統的軟硬體及網路外，使用人員的特質與心理狀態亦會影響內部威脅的風險。因此，本研究以關聯資安警示為基礎之偵測暨評估模組進行驗證，其主要目的如下：

1.對內部威脅問題進行分析，運用分散式入侵偵測感應器(Sensors)所產生之警示，與系統弱點資訊及人員行為進行整合、關聯與分析，以找出單位中面臨高度風險系統或具有惡意的人員，提早預防可能的攻擊情境及降低遭到攻擊時所造成的損失。

2.回饋各管理階層改善管理或決策的參考依據。

## 三、研究方法與步驟

本研究以關聯資安警示分析為基礎，發展內部威脅偵測暨評估模組，將入侵偵測感應器分散部署於組織內重要任務電腦中，藉

由各感應器所產生的警示，自動和系統弱點資訊與人員行為，進行整合、關聯與分析，識別出攻擊者的異常行為、攻擊類別、受攻擊系統所受攻擊風險值與其他可觀察之潛在異常徵兆。資安人員經由被識別出之內部威脅徵兆，透過Web平台評估出須優先處置高度風險系統或具有惡意的人員，以提早預防可能的攻擊及降低遭到攻擊時所造成的損失，本研究將依下列步驟及方法進行內部威脅偵測暨評估模組的實現：

1.主機弱點評級與風險值探討；

2.攻擊與主機弱點資訊探討；

3.攻擊與人員行為等環境因素探討；

4.整合主機弱點資訊與人員行為等環境因素的攻擊風險值計算、評估；

5.系統建置與分析。

## 關聯資安警示為基礎之內部威脅偵測暨評估模組

### 一、傳統入侵偵測系統配置方式及其缺點

在傳統上無論網路型或是主機型的入侵偵測系統的配置方式，主要的目的都是在防止單位對外服務重要主機(如DNS Server、Mail Server、Database等)免於遭受來自於單位外部攻擊者的攻擊行為。

但是這樣的配置方式，對於組織中具有惡意的內部人員進行的攻擊行為並不易偵測，因為置於內部電腦並不是資訊安全管理人員眼中的重要主機。但是從現實的環境中來看，在這幾年由於個人電腦處理速度與儲存容量的增加，大部分的作業並非全在對外服務的伺服器上進行，而可能是放在個人電腦或內部重要主機當中。但是傳統入侵偵測系統的配置方式與防護對象，卻明顯忽略了內部電腦安全，讓資訊安全防護的架構出現漏洞。雖然陸續有許多商業化產品標榜「個人防火牆」或是「主機型入侵偵測系統」的功能，但是都受限於設定太過繁複或是缺乏集中管理的機制而無法發揮更大的功能。

### 二、分散式入侵偵測系統架構

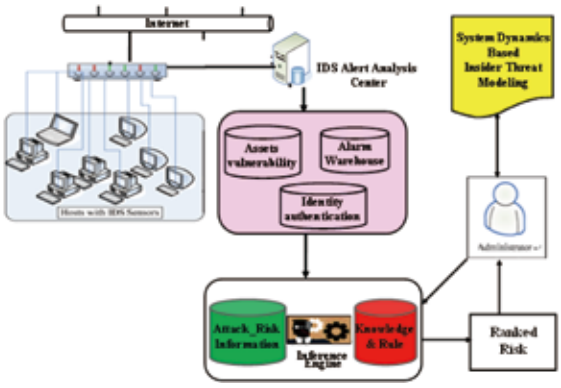
本研究希望能就技術層面提出一個解決方案，概念說明如下：將IDS(Snort)置於內部主機成為入侵偵測感應器，並且將偵測到異常狀況的警示傳送儲存至資料庫伺服器，並和組織環境因素等資料進行整合比對，最後透過統一的中央管理主機進行檢視。當然不可避免的會產生許多正確或是不正確的警示，因此如何定義出一種機制，能在大量警示中篩選或突顯出關鍵的資訊，節省管理所需花費的時間，成了本系統不可忽略的一個功能。[4]

整個系統的架構及流程，可以用圖一來表示，包含入侵偵測感應器、Snort資料庫、弱點資訊、主機資訊、內部人員資料表和中央管理主機等主要元件。

### 三、主機弱點資訊獲得

一個弱點資訊會因不同研究組織而有不同的命名方式，造成使用者查詢及判斷的困擾，因此可以參考MITRE組織所建立的統一弱點資訊命名(CVE, Common Vulnerabilities and Exposures)。[5]現今有很多自動化工具可幫助作資產的風險評估，即可經由量化的方式計算出風險值。[6]

本研究以Nessus掃瞄結果作為主機




圖一　本研究系統架構圖

弱點資訊紀錄表，格式如表一。[7]並結合美國NIST(National Institute of Standards and Technology)所維護的NVD(National Vulnerability Database )弱點資料庫資料表，格式如表二。[8]接著將主機弱點資訊紀錄表的CVE_id 欄位與弱點資料庫的name欄位作關聯後，即得到該弱點之CVSS Base Score評級值及威脅種類。以主機弱點評級及威脅種類表三為例，主機192.168.1.1經弱點掃描得知，共有3個弱點及其對應之服務通訊埠，經與NVD弱點資料庫關聯比對後，可得出各弱點之評級值及其威脅種類。

表一　主機弱點資訊紀錄表

| 欄位名稱 | 資料型態 | 長　度 | 備　　註　　說　　明 |
|---|---|---|---|
| host | varchar | 16 | 被掃瞄主機IP位置 |
| service | varchar | 60 | 服務類別／通訊埠 |
| CVE_id | varchar | 16 | 該弱點相對應之CVE編號<br>如：CVE-2004-0001 |
| plugin | varchar | 16 | Nessue用來掃描各類弱點的模組編號<br>如：34311為偵測ms-sq1其ms08-40弱點的模組編號 |

表二　弱點資料庫資料表

| 欄位名稱 | 資料型態 | 長度 | 備　　註　　說　　明 |
|---|---|---|---|
| name | vachar | 16 | 該弱點相應之CVE編號<br>如：CVE-2004-0001 |
| admin | int | 2 | 值為1時，表示可取得管理者權限 |
| user | int | 2 | 值為1時，表示可取得管理者權限 |
| other | int | 2 | 值為1時，表示可取得一般使用者權限 |
| local | int | 2 | 值為1時，表示可取得其他權限 |
| remote | int | 2 | 值為1時，表示於本機存取 |
| user_init | int | 2 | 值為1時，表示於遠端存取 |
| score | int | 2 | 值為1時，表示必須先是或具備目標主機之使用者權限 |
| | | 6 | CVSS Base Score |

表三　主機弱點評級及威脅種類表

| host | CVE_id | service | CVSS Base Score | Threat | Plugin |
|---|---|---|---|---|---|
| 192.168.1.1 | CVE-2000-1200 | Microsoft-ds(445/tcp) | 3.3 | 0 | 10398 |
| 192.168.1.1 | CVE-1999-0504 | Microsoft-ds(445/tcp) | 4.9 | 0 | 10394 |
| 192.168.1.1 | CVE-2004-0574 | nnfp(119/tcp) | 10 | RA | 15465 |

## 四、主機弱點風險值計算

計算主機弱點風險值，以考量資產、弱點及威脅等三項指標來衡量計算：

1.弱點方面：每一台主機經弱點掃描檢測出具那些弱點，根據這些弱點來對照CVSS之Base Score評級值，代表主機之弱點值。其考量原因是因為CVSS評級系統，是由資安組織及各軟體製造商來評估，對於弱點各項屬性及對系統的影響程度來分析，是較公信力的。[9]

2.資產方面：這裡係考量主機所提供的服務。主機於弱點檢測後，考量多項弱點使用同一通訊服務埠，與單一弱點使用唯一通訊服務埠，對該服務埠而言，其風險值是不相同的。因此，針對多項弱點存在於同一服務埠其風險值越高，權重計算相對高。

3.威脅方面：在結合NVD弱點資料庫的過程中，除可獲知弱點之CVSS之Base Score評級值外，亦已針對弱點之威脅類別進行分類，共8類。因本研究主要偵測內部威脅的可能途徑及存取方式，應以近端取得使用者權限為較大威脅，權重計算相對高。

4.主機弱點風險值計算：根據Yazar所提風險值計算(Risk Value)方式，以上述三項指標(弱點值、資產值、威脅值)來計算主機弱點風險值。[10]各運算元、符號及計算公式(1)所示，表四為弱點風險值計算結果。

$$(Host)_i = \left(\sum_j V_{ij} \times T_{ij}\right) \times A_{ij} \quad (1)$$

j：主機弱點別。

i：依據 j 得知存有弱點通訊服務埠。

V：弱點值，代表弱點 j 之CVSS Base Score評級值。

T：威脅值，代表弱點j之威脅代表值。

A：資產值，代表通訊服務埠 i 上，j 的個數經比例換算後的對應值。

## 五、攻擊警示說明與對弱點資訊影響

(一)攻擊警示紀錄說明

表四　弱點風險值計算表

| Host | CVE_id | Service | V | T | V*T | 小計 | A | V*T*A |
|---|---|---|---|---|---|---|---|---|
| 192.168.1.1 | CVE-2000-1200 | Microsoft-ds(445/tcp) | 3.3 | 1.1 | 3.63 | | | |
| 192.168.1.1 | CVE-1999-0504 | Microsoft-ds(445/tcp) | 4.9 | 1.1 | 5.39 | 9.02 | 1.21 | 10.91 |
| 192.168.1.1 | CVE-2004-0574 | nnfp(119/tcp) | 10 | 1.43 | 14.3 | 14.3 | 1.1 | 15.73 |
| $(192.168.1.1)_{445}$=10.91，$(192.168.1.1)_{119}$=15.73 | | | | | | | | |

在IDS(Snort)單一筆偵測警示紀錄中，可得知攻擊行為的攻擊類別(Classification)、優先權(Priority)、攻擊的時間(Timestamp)、弱點種類、攻擊來源IP 與目標IP等資訊，故透過以下警示可掌握每次網路攻擊事件的資訊：

1.攻擊類別(Classification)：用以判斷攻擊手法與可能結果。

2.弱點種類：利用何種系統弱點或服務進行攻擊。

3.優先權(Priority)：得知該攻擊行為本身的破壞性。

4.時間戳記(Timestamp)：得知攻擊行為警示發生時段(尖峰、離峰)。

5.目標主機(Dst_ip)：得知內部或外部目標主機遭受攻擊。

6.來源主機(Src_ip)：得知攻擊來源為內部或外部主機。

然而，僅從警示中雖可了解各種攻擊行為本身資訊，但難以顯示出內部攻擊的一些特徵，如：何種權限或職務人員發動攻擊、目標主機之重要等級、目標主機弱點資訊、潛藏異常行為與動態風險值等，因此我們認為，為了有效降低內部威脅，不只是要偵測找出有哪些攻擊行為，更要結合人員、行為與環境等組織內在因素，辨識出可疑與有效徵兆，以有效評估出組織內部之整體風險值，以見微知著，優先處置高度風險系統或具有惡意的人員，降低遭到攻擊時所造成的損失。

(二)攻擊警示對弱點資訊影響

我們以Snort偵測警示紀錄為依據，自動連結查詢前述主機弱點評級與威脅種類表，以判定此目標主機是否存在相對應之弱點資訊。如圖二表示當Snort 偵測到利用CVE-2001-0144弱點攻擊畫面時，假若目標主機本身並無此弱點，則此攻擊之影響應較小；相反的，主機如已存在此弱點，其攻擊影響應較大。

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 22 (msg:"EXPLOIT ssh
CRC32 overflow NOOP"; flow:to_server,established; content:"|90 90 90 90 90 90
90 90 90 90 90 90 90 90 90 90|";
reference:bugtraq,2347; reference:cve,CVE-2001-0144;
classtype:shellcode-detect; sid:1326;  rev:3;)
```

圖二　Snort偵測到CVE-2001-0144攻擊

## 六、建構關聯資安警示為基礎之內部威脅偵測暨評估模組

(一)組織內在/攻擊行為因素分析

以性質、特性來分析內部威脅評估因素，其分析結果如下：

1.攻擊行為因素之性質：

攻擊行為類別、優先等級等資訊可從入侵偵測系統警示中得知；然而每筆警示的性質未必都相同，故攻擊行為因素的性質是變動的。

2.組織內在因素之性質：

僅有在人員、程序與環境等設定有異動後才會有變化，故組織內在因素其性質是相對較固定的、不易更動的。我們可以建立一個屬於組織有關的知識庫(Knowledge Base)，以彈性調整與更新。

(二)內部威脅評估模組設計

根據上述因素分析結果，我們採用「基底」、「指數」與「加權」的形式來反映出攻擊行為與組織內在因素的關係。實際作法是，以組織內在因素為「基底」與「加權」，再搭配上變動性較大的攻擊行為因素為「指數」來設計我們的內部威脅評估模組，以計算出整體攻擊風險值。藉由變動的指數，可針對攻擊重要主機、攻擊人員權限、弱點資訊的攻擊行為反應在整體攻擊風險值上，其風險值變化上將有明顯的差異存在，且數值範圍也容易控制。

當內部攻擊行為發生時，要突顯該行為的特性則需依其參數將警示量化，且相同種別的攻擊行為發生在不同環境因素下時，其整體風險值應有所差異。在風險值的算式中，用來作為輸入的變數為前述幾個風險評估因素，其中Am 為主機重要性指數，Ua 為攻擊人員權限指數，Pri 代表攻擊行為優先等級，Srv代表服務重要性權重，Cv代表CVSS base score，Vr 代表弱點風險值，則各主機遭受攻擊風險值如表五。

主機K遭受攻擊風險值：

$$Risk\_Hit_k = F(Am, Ua, Pri, Srv, Max(Cv), Vr) \quad (2)$$

表五　各情況下，主機遭受攻擊風險值公式

| | | |
|---|---|---|
| 無啓動服務 | $Risk\_Hit_k = Am \times Ua \times Pri$ | (3) |
| 無弱點服務 | $Risk\_Hit_k = Am \times Ua \times Pri \times Srv$ | (4) |
| 服務的非弱點 | $Risk\_Hit_k = Am \times Ua \times Pri \times Srv \times Max(Cv)$ | (5) |
| 服務的弱點 | $Risk\_Hit_k = Am \times Ua \times Srv \times (Vr)^{Pri}$ | (6) |

## 結果與分析

### 一、系統測試情境與流程

本研究測試流程如圖三。


圖三　本研究測試流程圖

### 二、系統測試環境

為了能讓系統測試順利進行，依據本研究的系統架構在實驗室中建立系統測試環境，在系統測試環境中，可以分為入侵偵測感應器、Snort資料庫與中央管理主機三個組成元件，本節僅就這三個元件在系統測試環境中的軟硬體設備與相關設定做說明：

(一)入侵偵測感應器

在系統測試環境中，3部電腦均安裝Snort2.8.0版入侵偵測軟體；這3部電腦軟體配置如表六。

本研究中根據內部人員在單位內的職務或從事的工作來定義內部人員的機密等級，資訊安全管理人員可以藉由這項指標，迅速得知單位內涉及機密業務的內部人員電腦的安全狀態，以區別出不同的機密等級(如表七)。

表六　入侵偵測器軟硬體環境與網路設定

| 編號 | 機器 | 作業系統 | 軟體 |
|---|---|---|---|
| 1 | H00001 | Windows 2000 Server | Metasploit 3.1<br>Snort 2.8.0<br>MS SQL 2000 |
| 2 | H00002 | Windows 2003 Server | Metasploit 3.1<br>Snort 2.8.0<br>Nessus 3.0<br>IIS 6.6 |
| 3 | H00003 | Windows XP | Metasploit3.1<br>Snort2.8.0 |

表七　人員、主機在Snort資料庫手動建立

| 項次 | 主機 | 任務類別 | 使用人員 | 網址 | 重要等級 |
|---|---|---|---|---|---|
| 1 | H00001 | iAssemble主機 | 業務主管 | XX.52.9 | 機敏 |
| 2 | H00002 | 測式主機1 | 系統管理員 | XX.52.10 | 重要 |
| 3 | H00003 | 測式主機2 | 一般人員 | XX.52.15 | 一般 |

(二)中央管理主機

在本研究中，中央管理主機可以是一部單獨的機器，但是由於測試環境較為單純，因此並未單獨設置中央管理主機，而是將中央管理主機與Snort資料庫安裝於同一部電腦當中，這部電腦當中安裝了IIS6.0網頁伺服器與ACID0.9.6版。

### 三、系統測試時使用的攻擊方式

攻擊行為的偵測率與所使用的入侵偵測系統種類息息相關，在本研究的系統測試架構中的入侵偵測感應器，是直接使用Snort入侵偵測軟體為偵測核心，因此對於各種網路攻擊行為的偵測率，並不在研究的系統測

試範圍內。本研究在測試過程中，模擬內部攻擊者對入侵偵測感應器發動攻擊，讓入侵偵測感應器能偵測到這些不同類別的攻擊行為，產生警告訊息傳送儲存至Snort資料庫，並產生攻擊風險值。

本研究測試環境皆為Windows作業系統，因此僅選擇針對此作業系統或應用程式漏洞行測試。另外由於內部攻擊大都以少量攻擊、針對性攻擊為主，故本研究使用的攻擊軟體Metasploit3.2，包含了許多針對性弱點的攻擊程式。[11]

## 四、建立主機弱點資訊、評級與風險值

我們用Nessus3.0進行弱點掃描，以產生各弱點之CVE編號，並查詢NVD資料庫，據以產生對應之CVSS base score、威脅種類等資訊，最後依公式(1)計算出各弱點之風險值，結果如表八，並儲存於Snort資料庫自行建立的資料表中。

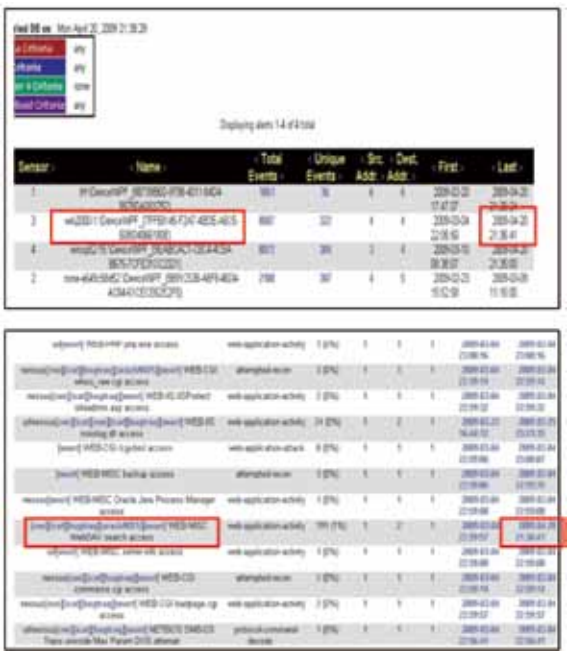
表八　主機權重、弱點資訊與風險值在Snort資料庫中自動產生

| 主機 | 主機權重 | 執行服務 | 服務權重 | 存在弱點 | 弱點Plugin ID (弱點風險值) |
|---|---|---|---|---|---|
| H00001 | 0.9 | IIS | 1.54 | V | 10526(7.26)<br>11213(1.91) |
| | | Ms-sql | 1.65 | V | 11214(124.26)<br>11067(10.98) |
| | | FTP | 1.1 | X | NA |
| | | SMB | 1.21 | V | 19408(16.94)<br>22182(16.94)<br>10860(7.26) |
| | | SMTP | 1.21 | X | NA |
| H00002 | 0.5 | IIS | 1.46 | V | 11664(20.95) |
| | | Ms-sql | 1.32 | V | 34311(61.48) |
| | | Decrpc | 1.65 | V | 11790(66.79) |
| | | SMB | 1.1 | V | 34477(16.94) |
| H00003 | 0.3 | IIS | 1.43 | X | NA |
| | | FTP | 1.32 | V | 10079(6.05) |
| | | Decrpe | 1.65 | V | 11790(61.22) |
| | | SMB | 1.1 | V | 22536(56.91)<br>34477(23.72)<br>11921(8.89) |

## 五、 系統偵測暨評估結果

在實際測試中，內部人員以Metasploit3.2軟體進行攻擊，此時經分散式Snort系統偵測，將所有警示集中彙集於中央管理主機，並經ACID介面呈現相關的警示內容與細節。因Snort內建偵測功能並無法於ACID介面立即將攻擊者身分等級、受攻擊主機重要性與弱點資訊進行關聯、過濾與分析，導致大量警示淹沒了管理者第一時間察覺異常行為的機會。

為驗證本研究正確性，我們以Exploit-IIS-ms03_007_ntdl_webdav弱點攻擊碼對主機H00001進行攻擊，並比對ACID(圖四)與本研究所產生的結果。因本研究結果儲存於Snort資料庫中，故本研究運用ASP程式進行Web-based程式撰寫，以即時顯示攻擊風險值等量化警示畫面(圖五)。



圖四　ACID警示圖

圖五　本研究內部偵測暨評估模組畫面

從圖五看出本研究內部威脅偵測暨評估模組可立即、無誤的將組織內受攻擊的重要主機、內部攻擊者身分、攻擊特徵、弱點攻擊資訊與攻擊風險值呈現出來，避免重要攻擊警示遭淹沒，供及時處置。

**六、結果分析**

當內部攻擊行為發生時，相同種別的攻擊發生在不同環境因素時，要突顯該行為的特性則需要依其參數將警示量化。本研究採用「基底」、「加權」與「指數」的形式反映出攻擊行為，其攻擊風險值應有所差異(彙整如表九)。

表九　內部攻擊風險值及分類處置表

| 攻擊者 | 目標主機 | 攻擊手段（服務/埠） | ITDAM 攻擊風險值（環境因素） | ACID 攻擊優先權（無環境因素） | 威脅分類與處置 |
|---|---|---|---|---|---|
| 系統管理者 | H00001（重要） | ms03_026_dcom (Dcerpc/135) | 2.43 | 攻擊 1 | Ignorance List |
| | | FTP_wuftp 2MD6 (FTP/21) | 2.67 | 風險 1 | Watch List |
| | | ms06_035_mailist (SMB/445) | 8.9 | 值遞 3 | Suspicious List |
| | | ms02_039_slammer (Ms-sql/1434) | 166.07 | 漸增 3 | Malicious List |
| 系統管理者 | H00003（測試） | ms03_026_dcom (Dcerpc/135) | 102218.07 | 高 1 | Malicious List |
| | | FTP_wuftp 2MD6 (FTP/21) | 5.791 | 1 | Suspicious List |
| | | ms06_035_mailist (SMB/445) | 16.90 | 3 | Malicious List |
| | | ms02_039_slammer (Ms-sql/1434) | 0.27 | 3 | Ignorance List |
| 一般使用者 | H00001（重要） | ms03_026_dcom (Dcerpc/135) | 0.81 | 1 | Ignorance List |
| | | FTP_wuftp 2MD6 (FTP/21) | 0.89 | 1 | Watch List |
| | | ms06_035_mailist (SMB/445) | 2.97 | 3 | Suspicious List |
| | | ms02_039_slammer (Ms-sql/1434) | 55.35 | 3 | Malicious List |
| 一般使用者 | H0003（測試） | ms03_026_dcom (Dcerpc/135) | 34072.69 | 1 | Malicious List |
| | | FTP_wuftp 2MD6 (FTP/21) | 1.93 | 1 | Suspicious List |
| | | ms06_035_mailist (SMB/445) | 5.63 | 3 | Malicious List |
| | | ms02_039_slammer (Ms-sql/1434) | 0.09 | 3 | Ignorance List |

## 結論與建議

**一、結論**

本研究重點於目前的網路安全防護機制，較少將內部人員所造成的威脅與風險納入考量，這種情形造成整體安全防護漏洞，甚至可能使得單位投資的網路安全設備成本都付之一炬。為彌補這樣的缺陷，本研究先對內部威脅問題加以探究，以關聯資安警示分析為基礎，發展內部威脅偵測暨評估模組，不僅找出有哪些攻擊行為，更結合人員、行為與環境等組織內在因素，量化攻擊風險值，以從傳統的大量攻擊警示中發現關鍵資訊，並正確辨識出單位內真正面臨高度風險主機或是具有惡意行為的內部人員，據以執行威脅分類與處置作為，進而提供各管理階層進行管理或決策參考依據。

**二、建議**

國軍歷經「精實案」、「精進案」及「精粹案」等三階段組織人員裁減及國防預算逐年遞減的情形，現有的資訊(安)人力仍須例行執行日益增多的資訊管理、資安監控作業及其他戰備整備任務，如何在現有資安防護監控系統或未來雲端資安規劃架構下，提升「機動、快速、精準」的資安防禦戰

力，已是刻不容緩的議題。本研究概念架構確實可實現驗證，建議整合本軍現行的「資訊資產管理系統」、「資安區域聯防系統AFIS」、「漏洞掃描系統」及「ISO27005資安風險評鑑」知識庫，即時產出精準關聯分析與應處建議，俾各級決策、管理及作業人員作出更正確的判斷；並研究如何回饋至「國軍營區網路管理系統」及本軍「端點網路存取控制政策」，及時防堵內部人員進一步的破壞機會。另針對進階持續性滲透攻擊(APT)等先進手段，本研究概念架構亦可提供異於一般傳統攻擊的偵測分析，並適切搭配先進的動態引擎(Sandbox)行為分析及資料外洩預防(DLP)等防禦技術，對於鎖定特定目標、低調緩慢及客製化惡意病毒等攻擊特徵，皆可達成初步的防禦任務。

## 參考文獻


1. CSO Magazine, United States Secret Service, and CERT Coordination Center, "2011 E-Crime Watch Survey," CXO Media, Framingham, MA, pp. 1-8, 2011.
2. Wang, H., Liu, S., and Zhang, X., "A Prediction Model of Insider Threat Based on Multi-agent," 2006 1st International Synposium on Pervasive Computing and Applications, Beijing, China, pp. 273-278, 2006.
3. Keeney, M.M., Kowalski, E.F., Cappelli, D.M., Moore, A.P., Shimeall, T.J., and Rogers, S.N., "Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors," Joint SEI and U.S. Secret Service Report, Pittsburgh, PA, pp. 1-45, 2005.
4. ＜Snort 官方網頁＞，2013/6，http://www.snort.org/。
5. ＜Common Vulnerabilities and Exposures 官方網頁＞，2013/6，http://cve.mitre.org/。
6. ＜CVE 各國適用版本＞，http://cve.mitre.org/compatible/country.html。
7. ＜Nessus 官方網頁＞，2013/6，http://www.tenable.com/products/nessus。
8. ＜National Vulnerability Database 官方網頁＞，2013/6，http:// nvd.nist.gov/。
9. ＜A Complete Guide to the Common Vulnerability Scoring System＞，『CVSS評級系統報告』，http://www.first.org/cvss/cvss-guide.pdf。
10. Yazar, Z., "A qualitative risk analysis and management tool," SANS Institute, 2002.
11. ＜Metasploit 滲透測試官方網頁＞，2013/6，http:// www.metasploit.com /。



**作者簡介**

周文祥中校，中正理工84年班、國防大學理工學院資訊科學所98年班，曾任網路官、程設官、資督官、通信官、科長，現任空軍航空技術學院軍學部資電組中校主任教官。

黃廉鈞中校，國防管理學院87年班、國立中正大學資管碩士班，曾任網路官、程設官、資督官、通安官，現任空軍司令部通資處資戰組中校通安官。