科技部資訊安全技術研發專案計畫

『系統測試計畫書』

System Test Plan Document

雲端環境下之網路目標性攻擊、關連分析與多層次防禦技術研究

MOST 104-2221-E-006 -145 -MY3

楊竹星
國立成功大學 電腦與通信工程研究所

Department of Engineering and Applied Science
Ministry of Science and Technology, Taiwan

105/06/10

文件版本修正履歷表

編號： MOST 103-2221-E-006 -145 -MY3

名稱： 雲端環境下之網路目標性攻擊、關連分析與多層次防禦技術研究

修訂次序	核準日期	版本	修訂內容
1	104/03/25	1.00	發行初版
2	105/6/10	2.00	第二年

版本: 2.00

目錄

1. 簡介

本計畫「雲端環境下之網路目標性攻擊、關連分析與多層次防禦技術研究」主要目的為發展雲端環境下網路威脅資訊整合關連分析系統(ClouDefSys，CDS)，由總計畫及四個子計畫組成。主持人與相關計畫如表一所示。

表1 雲端環境下之網路目標性攻擊、關連分析與多層次防禦技術研究各計畫列表

計畫項目	主持人	計畫名稱	科技部編號
總計畫暨 子計畫四	楊竹星教授	雲端環境下之網路目標性攻擊、關連分析與多層次防禦技術研究	MOST 103-2221-E-006 -145 -MY3
子計畫一	陳嘉玫教授	雲端環境中持續且目標性攻擊偵測之研究	MOST 103-2221-E-110 -049 -MY3
子計畫二	李忠憲教授	雲端系統中分散式日誌蒐集、錯誤偵測、稽核及預警系統	MOST 103-2221-E-006 -146 -MY3
子計畫三	林輝堂教授	雲端環境中新型惡意網域偵測搜捕與分析之研究	MOST 103-2221-E-006-147-MY3

各子計畫簡介分別描述如下：

總計畫簡介

雲端運算環境日漸成熟，為傳統資訊基礎建設帶來革命性的改變，然而在新的環境 架構及科技的應用下，我們亦面臨著與以往全然不同之網路與資訊安全之威脅。基於現有 Testbed@TWISC 攻防測試平台，本整合型計畫將以利用以虛擬機器為基礎之測試平台，研發雲端平台上多層次防禦機制，與多元化攻擊之偵測技術。透過子計畫的分工合作，彙整研發成果，建立網路與雲端系統多層次防禦機制，可作為防禦網路與雲端攻擊之防線，提供高安全度的網路環境。

總計畫在本計畫中角色為一資料共享之平台，以建構多層次防禦機制為基礎，發展雲端網路活動日誌收集分析、異常雲端網路流量特徵分析、智慧型僵屍網路偵測、以及多階段目標攻擊之偵測與預測，進而建構多層次關聯分析雲端攻擊之防禦系統。

子計畫一簡介

子計畫一第一年的系統中，以電子郵件方式的社交工程攻擊手法為主之持續性滲透攻擊，收集電子郵件的記錄，追蹤後續階段性攻擊，採用隱藏馬可夫模型作為偵測模型，偵測低頻率持續性滲透攻擊。第二年，是利用貝氏網路的學習能力與架構圖表示出各階段事件或行為的發生機率，並結合以特徵值為基礎之風險評估預測入侵行為的發生，並預防未來可能發生之攻擊，達到協助 IPS 提高偵測率以及降低誤報率目標。

子計畫二簡介

子計畫二第一年之主要目的為透過雲端環境的日誌蒐集，提供雲端服務供應商瞭解系統與各設備的關係，並提供使用者資料傳輸軌跡的相關記錄，降低使用者對於使用雲端運算資源時的知覺風險。子計畫二第二年主要目的為透過蒐集雲端基礎設施的設定資訊，提供網路管理者診斷網路的工具，增加雲端運算資源的可靠度與可用性，避免人為造成的設定錯誤。最終目的為建置一「雲端系統中分散式日誌蒐集、錯誤偵測、稽核及預警系統」。

子計畫三簡介

子計畫三於第一年完成 DGA 型態殭屍網路偵測系統的初步建置，利用殭屍網路與控制中心通訊時因網域進行轉換而導致大量失效查詢之行為特徵來進行辨識受感染之殭屍主機。子計畫第二年提出一自適應式分群演算法，以針對殭屍網路模擬使用者行為規避偵查的行為進行更準確的分析，大幅提升殭屍網路辨識準確率，降低實體機器以及網域名稱伺服器被入侵或是濫用之可能，同時透過分析網域名稱流量紀錄以縮短偵測時間，可以有效降低殭屍網路利用偵測時間的空檔而到處散播繁殖所造成的傷害。

子計畫四簡介

子計畫四提出基於雲端環境的資訊安全防護架構，第一年的系統紀錄所有流量虛擬主機的流量，並利用 Netflow 系統進行分析。第二年則將雲端主機內部視為一區域網路，藉由收集虛擬機器在內部網路環境的封包並產生 Netflow 統計資料，以及分析封包中深層的內容以辨識出惡意流量或入侵行為，加以控管。

1.1 測試範圍

本文件主要是建置雲端環境下網路威脅資訊整合關連分析系統(ClouDefSys，CDS)。確認在系統整合前，必須先確認所有的設計模組皆可正確運行，並輸出

預期的成果，故本計畫著重於接受度測試(Acceptance Test)，待接受測試完成後方進行整合測試。本文件內容將依據系統需求規格書中所規範的系統規格進行相關的測試計畫。並希望透過此文件之描述與實踐，達到順利進行測試工作之目的。

1.2 接受準則

本測試計畫總計畫及各子計畫需要滿足的測試接受準則依計畫別分別詳述如下。且測試程序需要依照本測試計畫所訂定的程序進行，所有測試結果需要能符合預期測試結果方能接受。測試以測試案例為單位，當測試未通過時，則重新檢測系統設計並進行必要之修正後，再重新進行測試，至通過為止。

表2 接受測試需求項目表

測試需求編號	必要性	需求內容
CDS-TR-001	必要	測試避免 XSS 及 SQL Injection 之相關網站弱點
CDS-TR-002	必要	子計畫內容可互相分享
BNM-TR-001	必要	輸入資料格式須符合系統需求
BNM-TR-002	必要	確認資料輸出符合使用者輸入條件
CLS-TR-001	必要	溝通目標主機
CLS-TR-002	必要	讀取目標主機網路資訊
CLS-TR-003	必要	讀取目標資料庫內容
CLS-TR-004	必要	產生網路拓樸圖
CLS-TR-005	必要	錯誤偵測
MDD-TR-001	必要	溝通目標主機
MDD-TR-002	必要	讀取目標主機儲存之 DNS 流量資訊
MDD-TR-003	必要	過濾 DNS 流量資訊
MDD-TR-004	必要	產生網路拓樸圖
MDD-TR-005	必要	透過分群演算法產生分群結果
MDD-TR-006	必要	產生受感染主機黑名單
CNM-TR-001	必要	確認 Xen Server 是否能正確輸出 Netflow 資訊
CNM-TR-002	必要	確認原先架構之演算法能正常運行於雲端環境
CNM-TR-003	必要	確認 VM 內部與 VM 跟外部的異常行為皆能偵測
CNM-TR-004	必要	系統可調控性及適應性

表3 效能測試需求項目表

測試需求編號	必要性	需求內容
CDS-PR-001	必要	各子計畫相關之資料庫查詢，需於 10s 內完成
BNM-PR-001	必要	可以提供大量 log data 輸入
BNM-PR-002	必要	可以提供多人同時登入系統
CLS-PR-001	必要	在 0.5s 內讀取單一主機網路資訊
CLS-PR-002	必要	在 0.5s 內讀取單一資料庫內容
CLS-PR-003	必要	100 台虛擬主機迴圈偵測在 1 秒內
MDD-PR-001	必要	在 60m 內過濾完 100 萬筆以上的 DNS 查詢
MDD-PR-002	必要	系統需達到 90%以上的分群準確率
CNM-PR-001	必要	系統需能抓到 90%以上的入侵行為

2. 子系統模組、元件描述

子計畫一：

子計畫一會收集來自網路的警訊記錄、郵件伺服器中的可疑紀錄以及 Social Networking 行為記錄，全部整合前處理，並將 Social Networking 行為記錄進行社群網路分析，找出群組關係與核心目標。接著將 Mail 紀錄、網路的警訊記錄進行關聯分析，比對內外部之 C&C 連線的來源位址是否一致，並判斷是否為社交網路分析中的核心目標。最後使用貝氏網路結合特徵值的風險評估，根據本研究所定義的偵測目標式攻擊的攻擊流程，依其風險值偵測出目前受攻擊名單以及預測未來攻擊之目標。可分為以下四個模組：Log 整合模組(Log Aggregation Module, LAM)、Log 關聯模組(Log Correlation Module, LCM) 、貝氏網路與風險分析模組(Bayesian Network & Risk Assessment Module, BNRAM) 、偵測模組(Target Attack Detection Module, TADM)。

1. Log 整合模組(Log Aggregation Module, LAM)

該模組主要功能是分別收集來自入侵偵測系統的 Mail 紀錄、命令與控制伺服器異常連結警訊、網路流量警訊以及 Social Networking 行為記錄，刪除不必要雜訊與遺漏值，再全數存入 Database 中。

2. Log 關聯模組(Log Correlation Module, LCM)

將各主機 IP 之行為記錄整合並進行社交網路分析，利用 Gephi 找出紀錄中之來源端與目的端相互連結的關係，用以區別不同角色 IP 群組關係。主要就 Mail 紀錄、命令與控制伺服器異常連結紀錄與網路流量警訊記錄進行關聯分析，在這邊除了要比對判斷外部寄發給內網中的目的地位址與內網對外部進行 C&C 連線的來源位址是否一致之外，還要判斷此位址是否為社交網路分析中的核心目標。

3. 貝氏網路與風險分析模組(Bayesian Network & Risk Assessment Module, BNRAM)

使用貝氏網路架構圖表示出各類事件或行為的發生機率據以判斷入侵行為發生機率，結合各攻擊階段之特徵值經過觀察與分析，建立有效的風險評估。

4. 目標攻擊偵測模組(Target Attack Detection Module, TADM)

依據本研究所定義的目標式攻擊的攻擊流程進行關聯分析，找出潛在已受攻擊之目標 IP，並與 Bayesian Network & Risk Assessment 中之風險值綜合比對後，依其風險值找出目前受攻擊名單以及未來可能遭受威脅之目標。

子計畫二：

子計畫二為提升使用雲端基礎建設(IaaS)的可用性與可靠度，方便網路管理者在使用雲端基礎建設建立網路時診斷網路，提供錯誤安裝檢測警示管理者可能的網路問題，本計畫的系統主要包括以下三個模組：網路資料蒐集模組(Network Information Collector, NIC)、網路拓樸產生模組(Network Topology Generator, NTG)、錯誤安裝檢測模組(Misconfiguration Detection, MSD)，以下針對各模組說明：

1. 網路資料蒐集模組(Network Information Collector, NIC)

本模組主要為蒐集虛擬網路上各個網路節點的主機網路資訊與虛擬交換器資料庫資訊，主機資訊包括實體網路卡與主機名稱等，而虛擬交換器資料庫包括虛擬網橋、埠、介面的配置情形，將整個網路節點的資訊蒐集後傳至網路拓樸產生模組。

2. 網路拓樸產生模組(Network Topology Generator, NTG)

本模組主要為接收處理虛擬網路上網路節點的資訊，將其儲存並轉換格式後，可以產生網路拓樸顯示出虛擬網路上的連接情形並可以此為錯誤偵測的基礎。

3. 錯誤安裝檢測模組(Misconfiguration Detection, MSD)

本模組主要為檢測錯誤安裝的情形，藉由網路拓樸得到虛擬網路的連接狀態，可以檢測網路中迴圈發生的情形，當錯誤發生檢測出來時可以警示網路管理者發生問題的路徑以供修正。

子計畫三：

子計畫三所建置之新型態殭屍網路偵防系統，主要利用殭屍網路與控制中心間的通訊行為進行偵測與分析，並透過網域名稱系統的流量紀錄做特徵擷取，進而捕獲觀測網域中之受感染主機，以提供雲端服務使用者一安全的使用環境。本計畫系統主要包括三個模組：流量過濾模組 (Traffic Filtering Module, TFM)、模式分析模組 (Pattern Analysis Module, PAM) 與殭屍網路偵測模組 (Botnet Detection Module, BDM)，各模組說明如下:

1. 流量過濾模組 (Traffic Filtering Module, TFM)

本模組主要目的為過濾掉「正常」的失效查詢 (NXDomain)，此類正常流量主要包含第三方黑名單服務 (Third Party Blacklist)、應用程式與部分防毒軟體所產生。過濾後可大幅降低系統所需後續分析之資料量，並且提升系統之偵測準確率。

2. 模式分析模組 (Pattern Analysis Module, PAM)

本模組首先透過主機間的行為模式進行分析並繪製成關聯拓樸圖，接著利用本計畫所提出之自適應式分群演算法 Weighted Spectral Clustering Algorithm (WSCA) 針對拓樸進行分群，此演算法利用光譜分析尋找最適合的分群結果，不需要事先決定分群數量，可以根據群體結構自動決定是否需要繼續執行演算法。由於本計畫第一年的觀察，部分 DGA 型態殭屍網路有休眠的狀況以規避偵查，利用本計畫所提出之 WSCA 演算法可以準確的將受感

染主機與正常主機切割，最後將分群結果做為後續殭屍網路偵測的基礎。

3. 殭屍網路偵測模組 (Botnet Detection Module, BDM)

本模組主要目的為辨識出受感染之主機，透過第一年的變點偵測方式 (Change Point Detection) 以及第二年所提出之針對網域查詢的次數分布以及時間分布以進行辨識，此階段可偵測出受染感之群體以及其所屬的主機黑名單。

子計畫四：

子計畫四針對網路流量分別以封包和網路流(flow)為單位，進行巨觀和微觀的流量觀察，來達到惡意行為之偵測。以 flow 為單位可以從網路連線的變化偵測到異常行為，以封包為單位則直接根據封包內容之特徵字串來偵測惡意行為，個有優缺點並因此互相彌補其不足以達到區域聯防之功能。此系統可從雲端上的網路設施當作設定讓管理者可輕鬆觀察到無論 VM 之間的互動抑或是 VM 與外部網路的溝通。此系統主要有三個部分：

1. 流量輸出模組 (Netflow Exporter, NFE)

本模組主要是必須將 Xen Server 的網路模式從原本的橋接模式(Bridge Mode)更改為虛擬交換器模式(Open vSwitch Mode)，並讓此 Open vSwitch 作 Netflow 輸出，去解析封包的 Header 讓其能產生 Netflow 資訊供 Collector 收集與分析。

2. 流量收集與分析模組 (Netflow Collector & Analyzer, NCA)

此模組則是接收流量輸出模組(NFE)所輸出之雲端 Netflow 資料，並根據定義之演算法作惡意流量偵測。主要能從複雜之網路流量中解析出 5 個類型的攻擊行為，分別為 Flooding Flow、Horizontal Scan、Vertical Scan、Distributed Connection 和 Brute Force。

3. 事件呈現與設定模組 (Event Viewer & Configurer, EVC)

此模組主在將流量分析模組所解析出來的事件結果以網頁圖形介面的方式作呈現，並添加更多的元素比如 IP 地理資訊等方便使用者作進一步觀察與研究。

3. 需求規格

1.設計限制

CDS-DC-001	系統入口網站採用 LAMP 架構開發
BNM-DC-001	系統採 LAMP 架構開發
CLS-DC-001	採用 Open vSwitch
CLS-DC-002	於 Linux 作業系統下執行
MDD-DC-001	必須布建於擁有 DNS Server 之網路環境
CNM-DC-001	以 Netflow 資料為基礎

2.技術限制

CDS-TL-001	網頁分享架構採用 Code Ignite Framework
BNM-TL-001	記錄檔必須需符合輸入格式
CLS-TL-001	必須要有代理主機
CLS-TL-002	應用在 LAN Server 環境
CLS-TL-003	自行輸入實體交換器位址
MDD-TL-001	受測網域內主機必須使用網域內之 DNS Server
CNM-TL-001	流量需流經 Exporter

3.使用者介面需求

CDS-UR-001	管理者可新增帳號及修改使用者權限
CDS-UR-002	各子計畫擁有各自之頁面
BNM-UR-001	提供使用者匯入 Log 紀錄檔
CLS-UR-001	提供使用者輸入 Username/IP/Port
CNM-UR-001	可透過介面修改門檻值

4.外部介面需求

CDS-OR-001	一整合之可登入之網頁介面
BNM-OR-001	與其他主機的通訊進行加密
CLS-OR-001	外部元件透過 SSH 溝通目標主機
CLS-OR-002	外部元件透過 Socket 溝通目標主機
MDD-OR-001	外部元件透過 shell script 匯入資料
CNM-OR-001	外部元件透過 SSH 溝通目標主機

5.內部介面需求

CDS-IR-001	各子計畫可藉由資料庫(MYSQL)進行資訊交換之動作

BNM-IR-001	LAM 可將結果傳送至 LCM
BNM-IR-002	LCM 可央結果傳送至 BNM
CLS-IR-001	NIC 可以將得到網路資料送給 TPG
CLR-IR-002	TPG 可以將處理後的網路資料送給 MCD
MDD-IR-001	TFM 可以將過濾後的資料傳送給 PAM
CNM-IR-001	NCA 處理完的結果可寫進資料庫供 EVC 呈現

6.系統功能性需求

CDS-FR-001	可因應各子計畫之需求，開啟相對應之權限及頁面
BNM-FR-001	提供偵測結果報告
CLS-FR-001	能夠蒐集網路資訊
CLS-FR-002	提供網路拓樸圖
CLS-FR-003	提供迴圈發生路徑
MDD-FR-001	可將流量資訊寫入資料庫
MDD-FR-002	提供受感染主機黑名單
MDD-FR-003	提供受感染主機連線行為
CNM-FR-001	提供異常行為名單

7.效能需求

CDS-PR-003	各子計畫相關之資料庫查詢，需於 10 秒內完成
BNM-PR-001	可以提供大量 log data 輸入
BNM-PR-002	可以提供多人同時登入系統
CLS-PR-001	在 0.1ms 內讀取單一主機網路資訊
CLS-PR-002	在 0.1ms 內讀取單一資料庫內容
MDD-PR-001	在 60m 內過濾完 100 萬筆以上的 DNS 查詢
MDD-PR-002	系統需達到 90%以上的分群準確率
CNM-PR-001	需在 Netflow 資料輸出後的 1 分鐘內處理完畢

8.環境需求

CDS-ER-001	使用 Ubuntu 建構主系統，安裝 LAMP 及 Code Ignite
BNM-ER-001	使用 LAMP 架設系統
CLS-ER-001	需要預先設定 Port 供資料庫讀取
CLS-ER-002	需要提供目標主機 IP
CLS-ER-003	擁有目標主機密碼
MDD-ER-001	使用 Ubuntu 建構主系統
CNM-ER-001	Xen Server 5.6 版本以上

9.防護需求

CDS-DR-001	網頁需通過弱點掃描及可防範 XSS 及 SQL Injection
BNM-DR-001	系統輸入可過濾特殊字元以避免 SQL Injection
CLS-DR-001	避免資料庫開啟之 Port 遭其他連線存取
MDD-DR-001	資料庫僅允許特定 IP 連線
CNM-DR-001	資料庫僅允許特定 IP 連線

10.安全需求

CDS-DR-001	網頁需通過弱點掃描及可防範 XSS 及 SQL Injection
BNM-SR-001	使用者在短時間內登入錯誤次數過多時進行相關阻擋動作
CLS-SR-001	主機密碼以加密傳送
MDD-SR-001	資料庫連線行為需紀錄
CNM-SR-001	SSH 改掉預設 port

4. 測試環境

對於本系統總計畫及各子計畫進行系統測試的環境說明分別詳述如下：

子計畫一測試環境

首先將本研究所提出的目標式攻擊流程，轉化分為以下攻擊階段帶入貝氏網路模型當中，利用本研究定義的目標式攻擊的貝氏網路模型，以現有的資料進行各種風險評估，對於能受到攻擊的目標，能夠及時發出警報，並找出可疑的 IP，減少受到攻擊的機會，並在最短的時間做出應對措施，提早預防以達到將傷害減至最低的目標。

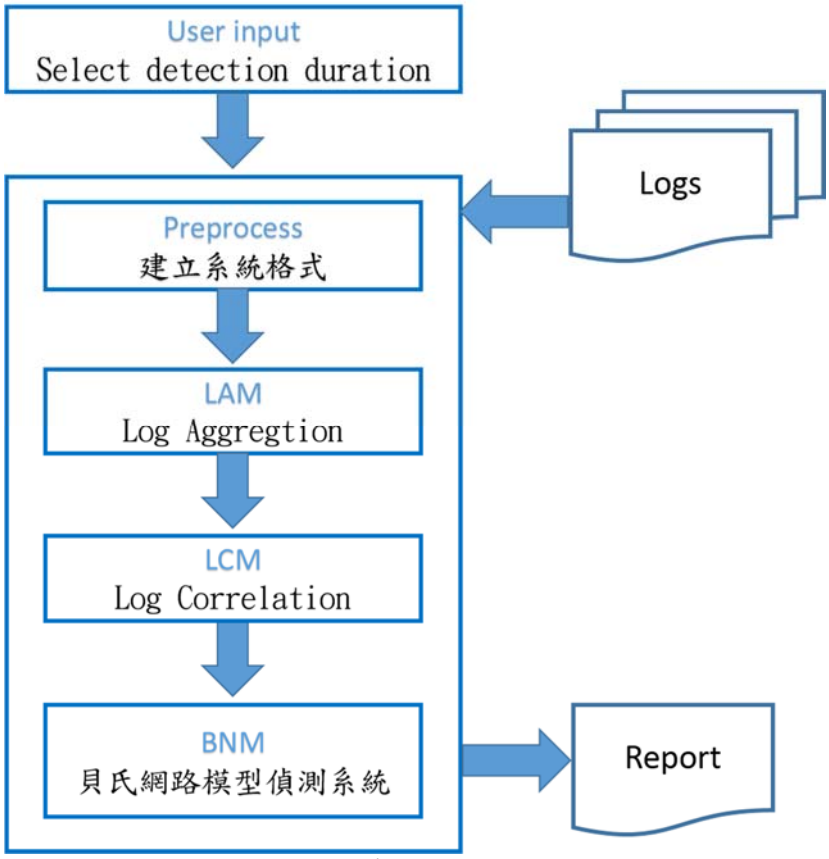


圖 1、子計畫一之測試環境圖

子計畫二測試環境

本計畫之重點為提升雲端基礎建設(IaaS)之可用性與可靠度，避免網路管理者在使用基礎建設創建虛擬網路時錯誤設定的發生，造成網路擁塞甚至無法使用，藉由讀取虛擬交換器的設定可以提供網路拓樸圖、錯誤檢測等功能，網路管理者可以藉由這些功能來診斷網路狀態。

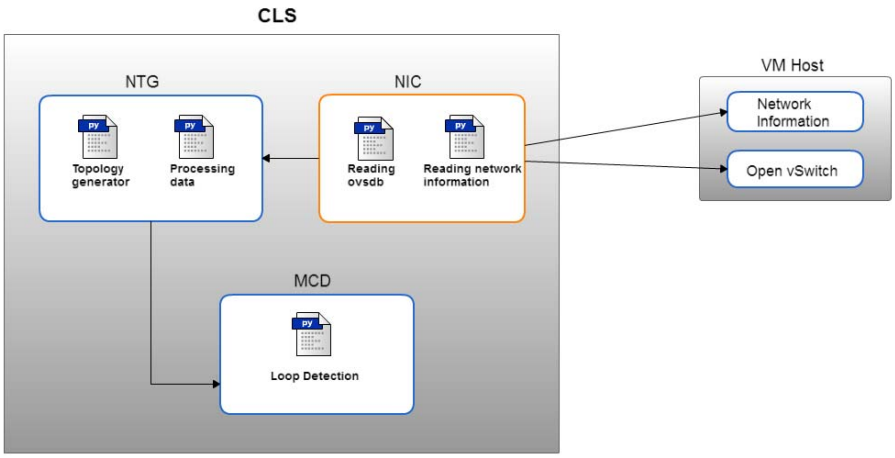


圖 2、子計畫二之測試環境圖

子計畫三測試環境

本計畫之目的為建置一新型態殭屍網路偵防系統，主要針對殭屍網路與控制中心間的行為特徵進行偵測與分析，因此在測試環境中主要透過主機與網域名稱系統 (Domain Name Server, DNS) 的流量紀錄做特徵擷取，進而捕獲觀測網域中之受感染主機，以提供雲端服務使用者安全無虞的使用環境。

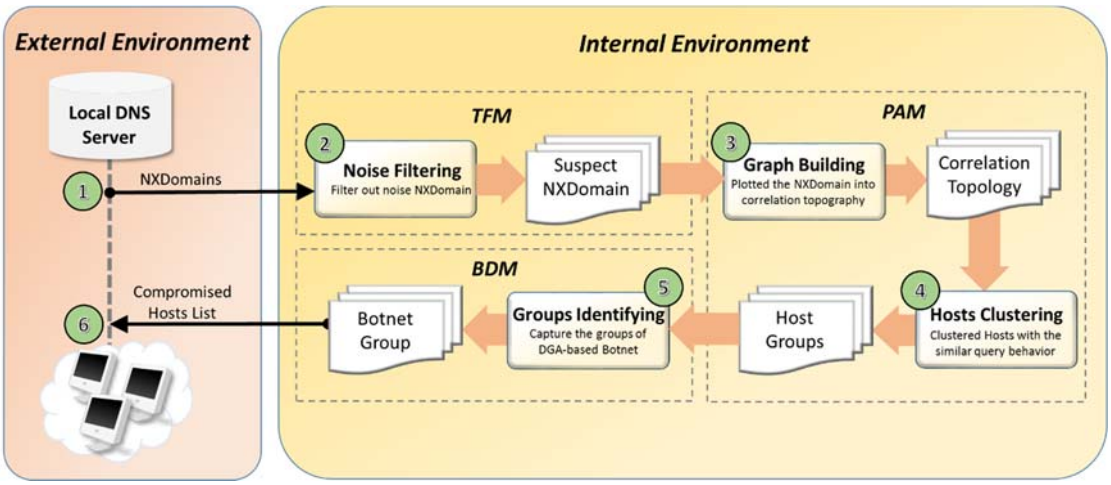


圖 3、子計畫三之測試環境圖

子計畫四測試環境

本計畫在雲端環境下檢查網路流量以監控異常行為的發生，結合 XenServer 的 Open vSwitch，不僅可以設定其作 Netflow 輸出，亦可作 Port Mirror 將流量複製給 Deep Packet Inspector 作分析，此系統不會因為 OS 版本或是硬體型號的不同而無法作處理，相容性高，移植容易且方便。本計畫於 Xen Server 6.5 上作測試，使用其內建之 Open vSwitch 2.1.3 作此區域網路之虛擬交換器，並透過此虛擬設備作資料匯出點。

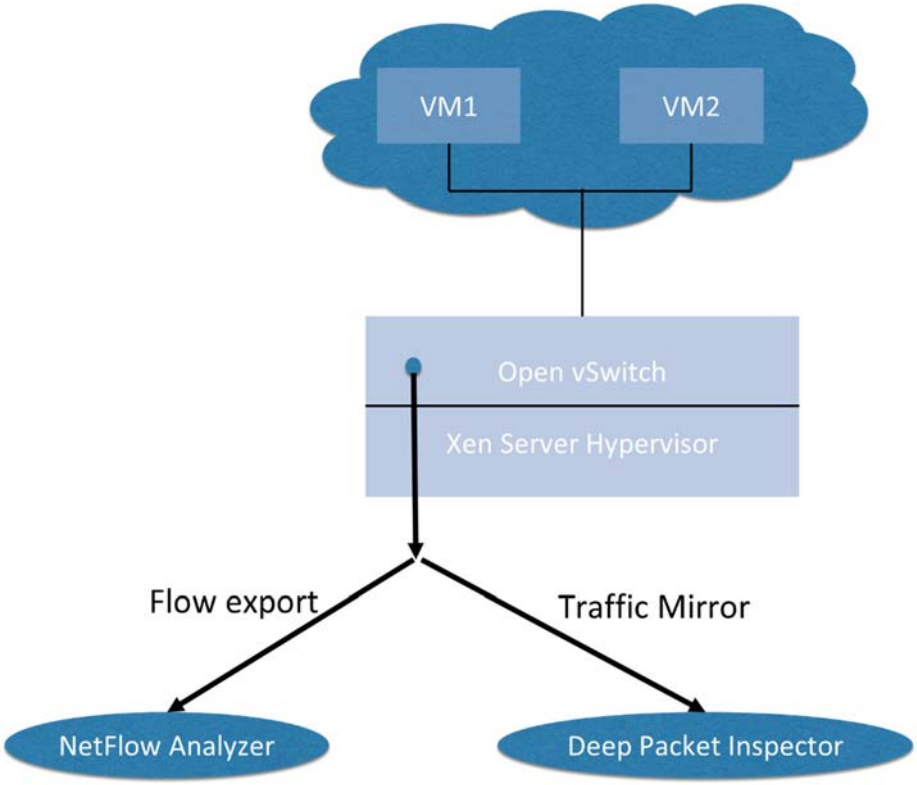


圖 4、子計畫四之測試環境圖

3.1 硬體規格

本系統總計畫及各子計畫關於測試環境所需的硬體規格說明，如下列所示：

總計劃硬體規格

- 雲端防禦系統
  - Intel Core2Duo 1.6GHz 或以上相容處理器
  - 1GB 以上的記憶體
  - 1GB 以上剩餘磁碟空間(網頁及相關關聯分析程式)
  - 10GB 以上剩餘磁碟空間(視資料庫內容增加)

子計畫一硬體規格

- 持續且目標性攻擊偵測系統
  - Intel Core2Duo 2.0GHz 或以上相容處理器
  - 2GB 以上的記憶體
  - 1GB 以上剩餘磁碟空間(系統程式本身)
  - 5GB 以上剩餘磁碟空間(視樣本數量增加)

子計畫二硬體規格

- 雲端分散式錯誤偵測系統
  - Intel Core2Duo 1.6GHz 或以上相容處理器
  - 512 MB 以上的記憶體
  - 100MB 以上剩餘磁碟空間

子計畫三硬體規格

- 雲端服務上之新型惡意網域及殭屍網路偵測防禦系統
  - Intel Core2Duo 1.6GHz 或以上相容處理器
  - 4 GB 以上的記憶體
  - 100 MB 以上剩餘磁碟空間 (系統程式本身)
  - 50 GB 以上剩餘磁碟空間 (存放網路流量資料)

子計畫四硬體規格

- 雲端環境網路流量偵測、警示與防治系統

- Intel Core2Duo 1.6GHz 或以上相容處理器
- 2GB 以上的記憶體
- 100 MB 以上剩餘磁碟空間 (系統程式本身)
- 100 GB 以上剩餘磁碟空間 (存放網路流量資料)

3.2 軟體規格

總計畫軟體規格

- 雲端防禦系統
  - ◆ 作業系統：Ubuntu 14.04 以上版本
  - ◆ 網頁伺服器：Apache 2.0(或以上版本)
  - ◆ 其他軟體元件：PHP 5.5.0(或以上版本)
  - ◆ 資料庫管理系統: MySQL 5.0 (或以上版本)

子計畫一軟體規格

- 持續且目標性攻擊偵測系統
  - 作業系統：Ubuntu 10.04 (或以上版本)
  - 網頁伺服器：Apache 2.0(或以上版本)
  - 其他軟體元件：PHP 5.5.0(或以上版本)
  - 資料庫管理系統: MySQL 5.0 (或以上版本)

子計畫二軟體規格

- 雲端分散式錯誤偵測系統
  - 虛擬交換器:Open vSwitch2.4.0(或以上版本)
  - 其他軟體元件:Python 2.7.9 (或以上版本), matplotlib 1.5.1(或以上版本), networkx 1.11(或以上版本)

子計畫三軟體規格

- 雲端服務上之新型惡意網域及殭屍網路偵測防禦系統
  - ■ 其他軟體元件: Dev C++ 或 visual studio2010

子計畫四軟體規格

- 雲端環境網路流量偵測、警示與防治系統
  - 作業系統：Linux 3.12.4 版本
  - 網頁伺服器：Apache Server
  - 程式：Python 2.7 以上
  - Xen Server：6.5

2.3 測試資料來源

本系統總計畫及各子計畫關於測試期間所需的測試資料來源及數量，說明如下：

子計畫一測試資料來源

本研究資料來源是利用真實企業建置多個 IDS 系統的 log 資料，其資料包括分公司的所有進出的詳細 log。透過真實企業組織中不同入侵偵測系統的警訊紀錄收集相關資料，分析企業網路中的重要伺服器，偵測目標性攻擊，以確實偵測到進階持續性滲透攻擊。

子計畫二測試資料來源

關於測試期間所需的測試資料來源及數量，主要為由說明如下：

- **雲端組態設定檔**

  1. 在實驗室伺服器所提供之雲端測試環境，讀取環境中虛擬交換器的設定組態。

子計畫三測試資料來源

- **DNS 紀錄檔**

  由總計畫私有雲蒐集網路流量資料，從而解析出所需之 DNS 流量資料以進行使用。

子計畫四測試資料來源

實驗室自架私有雲及網路安全測試平台，設定其中虛擬交換器將其轄內之網路流量以 Netflow 資料之型式予以分析器。

3. 測試時程、程序

3.1 測試時程

測試時程及查核點為總計畫訂定時間由各子計畫協助完成測試。

時程

1. 各子系統單元測試 (Unit Test) (自 105/2/1 起，應於 105/2/28 完成)
2. 各子系統接受度測試(Acceptance Test) (自 105/3/31 起，應於 105/5/12 完成)

查核點

3. 系統整合與整合測試(105/5/13)
4. 系統測試完成(105/7/1)

3.2 接受測試程序

基於本計畫系統需求規格書內容，本系統須達成以下使用操作場景的需求。各子系統的元件測試,由各子系統的開發負責人執行，待各子系統整合完成後，由全體人員協同執行整體計畫的整合測試。

總計畫接受測試程序

場景 1：進行網頁弱點掃描及壓力測試

由外部主機對網頁主機進行弱點掃描及壓力測試。使用者利用弱點掃描系統進行主機及 Web Application 之弱點掃描；使用者利用 Jmeter 於測試平台 100 台主機模擬 100 人同時連線之系統效能。如圖所示。

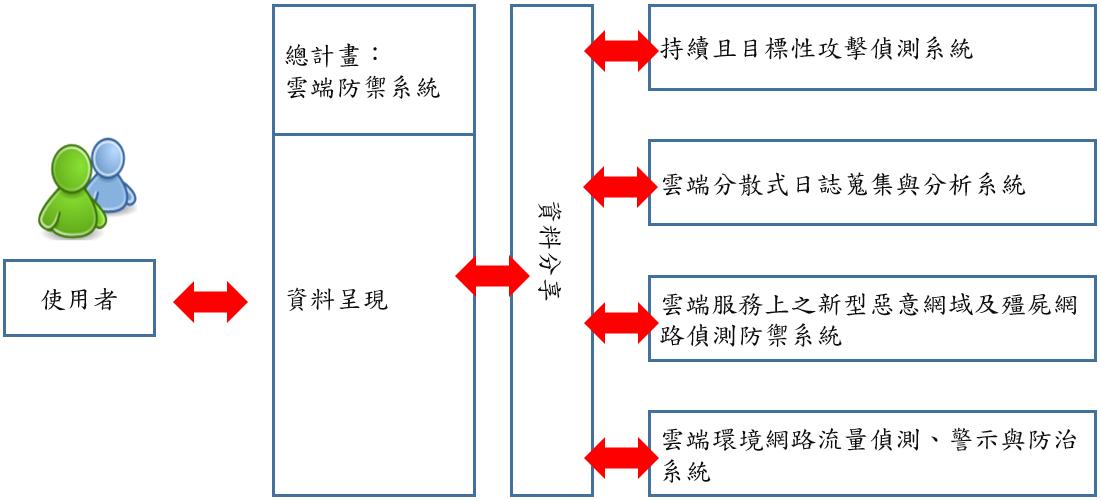


圖 5、總計畫測試架構

子計畫一接受測試程序

場景 1：**收集 log 並進行整合**

從 Mail server、Social Networking Log 與 Network Alert log 中收集相關 log，進行擷取、整合並儲存到資料庫中，如下圖所示：

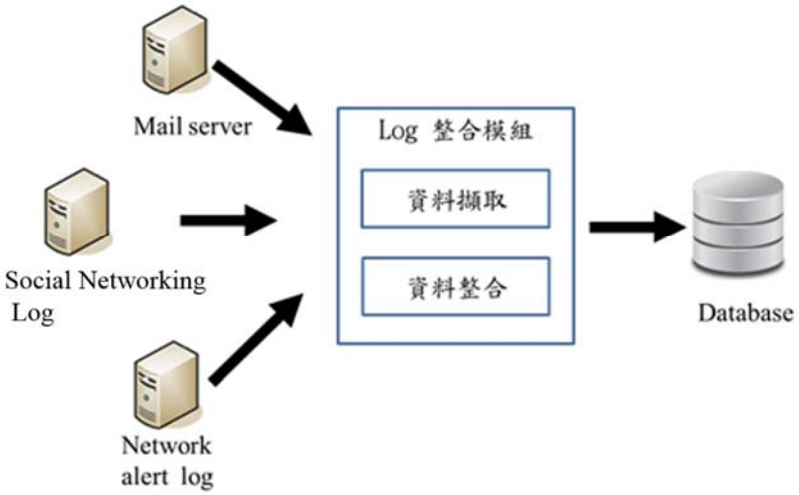


圖 6、資料整合模組

場景 2：**Log 關聯模組**

就 Mail 紀錄、命令與控制伺服器異常連結紀錄與網路流量警訊記錄進行關聯分析及 Social Network 的分析：

圖 7、 log 關聯模組

場景 3：貝氏網路分析及目標攻擊偵測

運用貝氏網路進行風險值計算之後帶入目標攻擊偵測模組，最後產出結果：

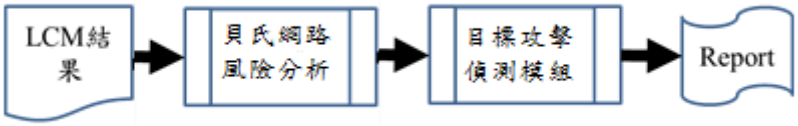


圖 8、貝氏網路分析及系統偵測

子計畫二接受測試程序

場景 1: 利用 SSH 蒐集目標主機網路資訊

NIC 模組藉由 SSH 連線取得目標主機實體網路卡以及主機名稱等資訊並回傳。

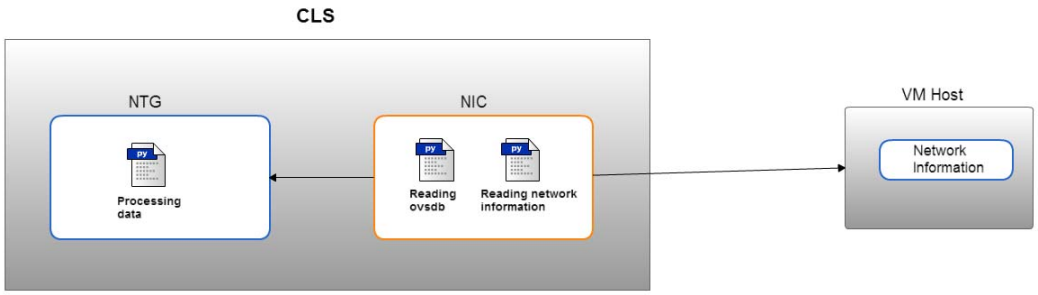


圖 9、利用 SSH 蒐集目標主機網路資訊

場景 2: 利用 Socket 蒐集資料庫資訊

NIC 模組藉由 socket 與目標主機上的虛擬交換器資料庫(ovsdb)溝通，讀取虛擬網橋、虛擬連接埠、虛擬介面資訊並回傳。

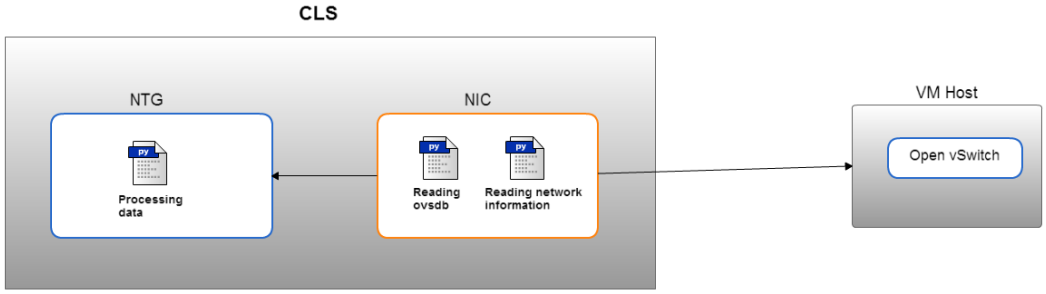


圖 10、利用 Socket 蒐集目標資料庫資訊

場景 3:　雲端分散式錯誤偵測系統產生網路拓樸圖

NTG 模組會收到 NIC 模組的回傳訊息，將蒐集後的資訊儲存並處理完之後，通過 NTG 即能夠生成虛擬網路拓樸圖，並顯示網路資訊。

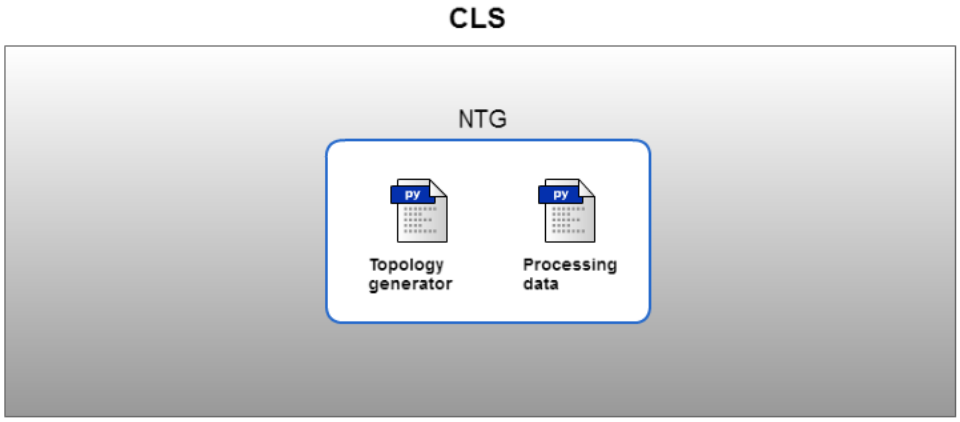


圖 11、雲端分散式錯誤偵測系統產生網路拓樸圖

場景 4:　雲端分散式錯誤偵測系統之錯誤組態設定偵測

藉由網路拓樸圖，得知網路節點的連線情況，雲端分散式錯誤偵測系統能夠使用 MCD 的迴圈偵測演算法偵測錯誤設定導致的迴圈問題。

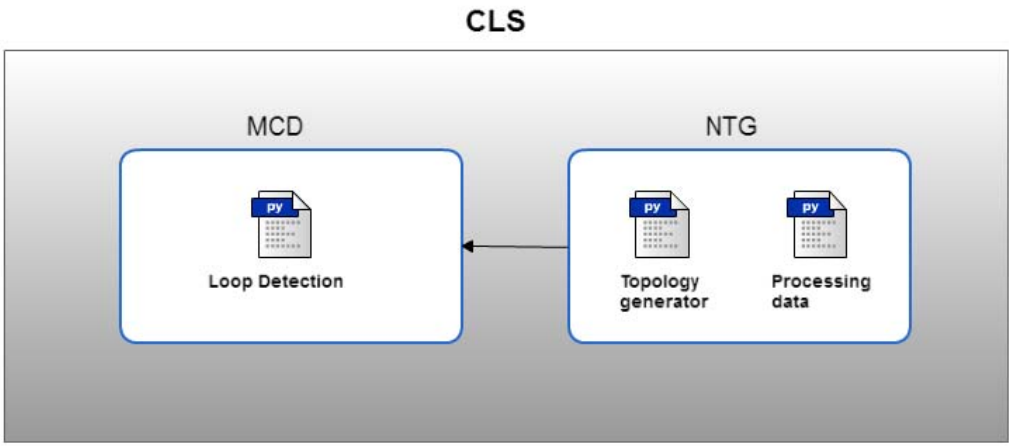


圖 12、雲端分散式錯誤偵測系統之錯誤組態設定偵測

子計畫三接受測試程序

場景 1: 取得失效查詢流量

從網路流量中過濾取得 DNS 流量中的失效查詢部分並匯入 TFM 模組

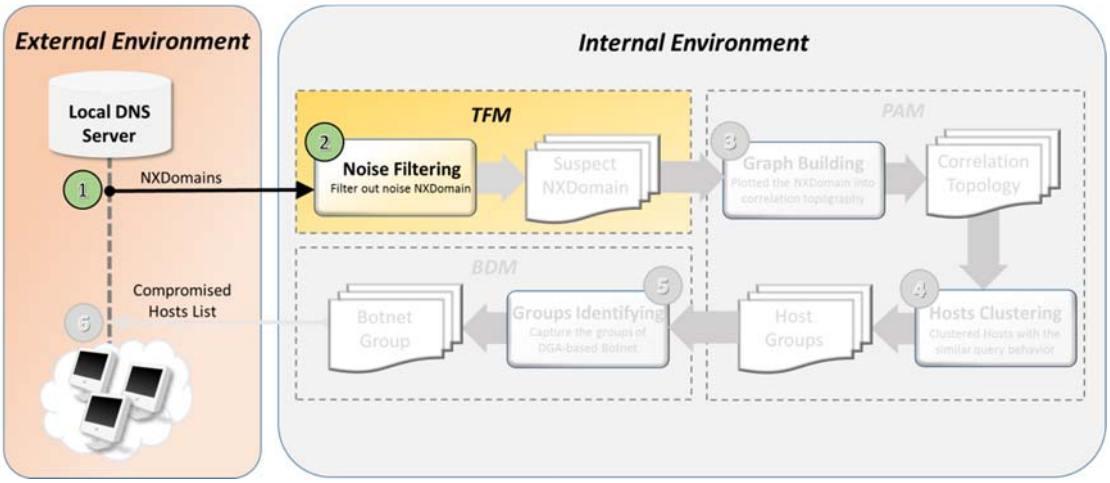


圖 13、殭屍網路偵測系統取得失效查詢流量

場景 2: 過濾失效查詢流量

透過 TFM 模組過濾流量中正常的失效查詢，濾除後剩餘疑似惡意失效查詢部分匯入 PAM 模組。

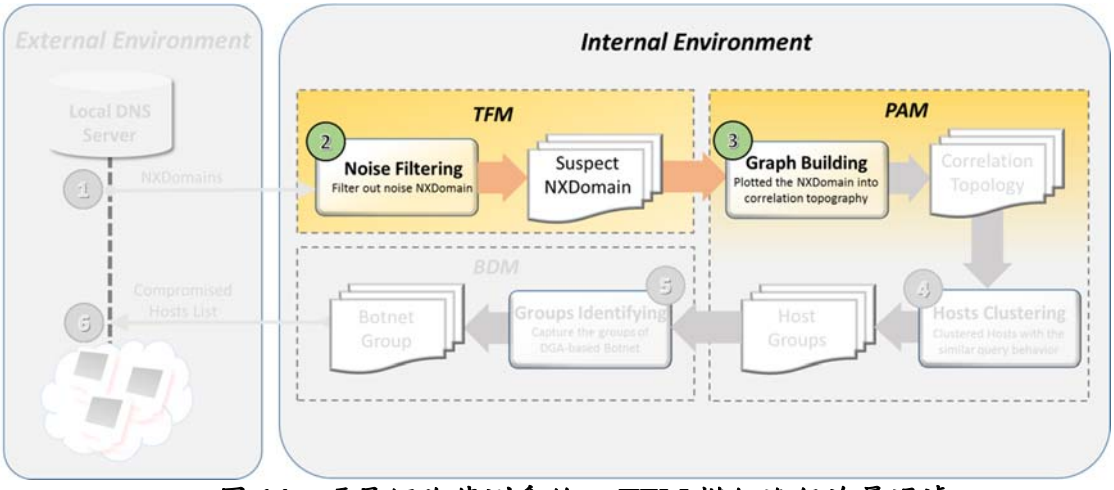


圖 14、殭屍網路偵測系統之 TFM 模組進行流量過濾

場景 3: 繪製關聯拓樸圖

透過 PAM 模組將過濾後之失效查詢根據主機間之行為特徵繪製成關聯拓樸圖。

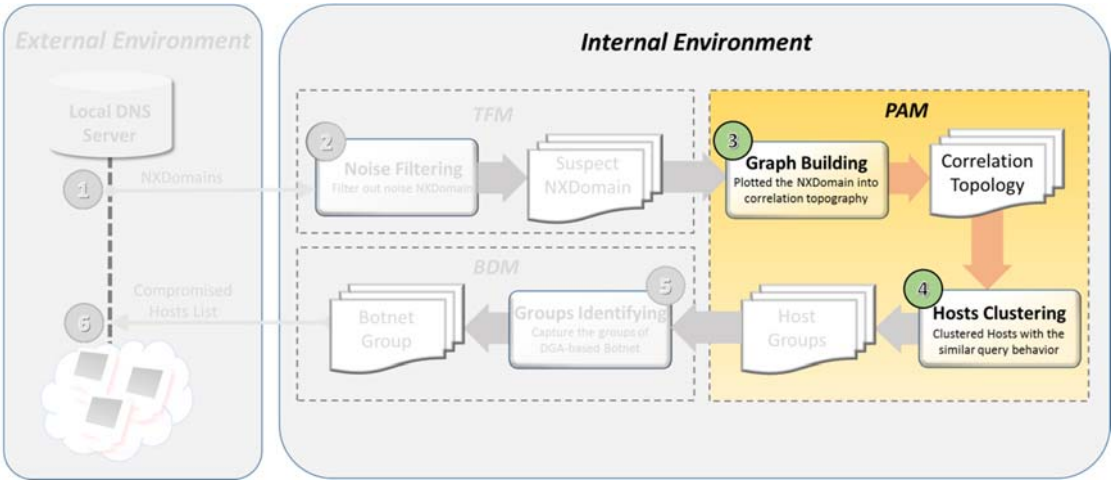


圖 15、殭屍網路偵測系統之 PAM 模組產生主機關聯圖

場景 4: 產生分群結果

PAM 模組利用本子計畫所提出之 WSCA 分群演算法產生分群結果並匯入 BDM 模組。

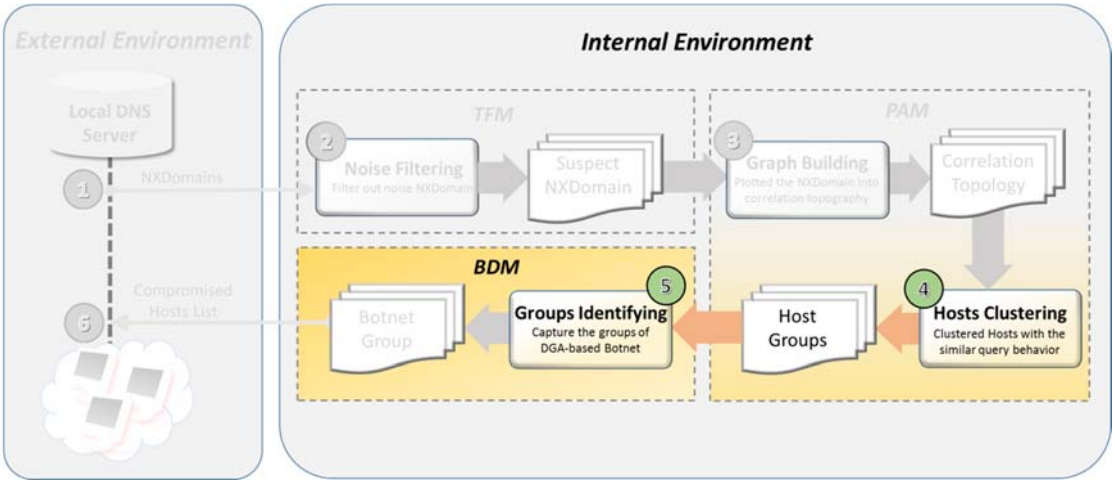


圖 16、殭屍網路偵測系統之 PAM 模組產生分群結果

場景 5: 產生辨識結果

BDM 模組利用群體內的失效查詢進行偵測，透過變點偵測、數量分布以及時間分布針對各群體進行辨識，最後產生殭屍網路辨識結果。

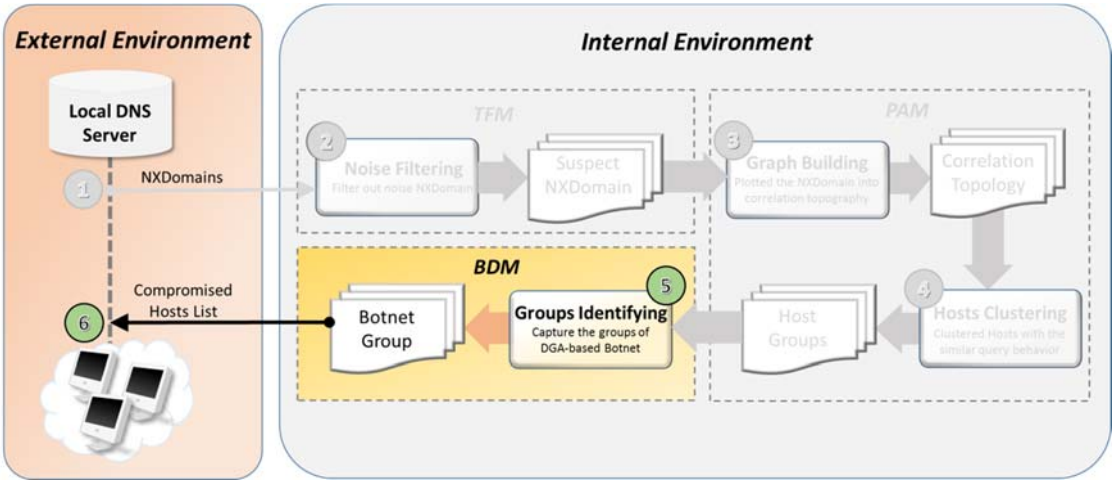


圖 17、殭屍網路偵測系統之 BDM 模組產生殭屍網路辨識結果

子計畫四接受測試程序

場景 1: 測試虛擬交換機是否正確輸出 Netflow 資料

虛擬交換器必須正確設定至能夠將通過此交換器之流量以 Netflow 格式輸出至指定之 Collector。在雲端內部刻意製造流量，於 Collector 端驗證是否的確出現該流量。

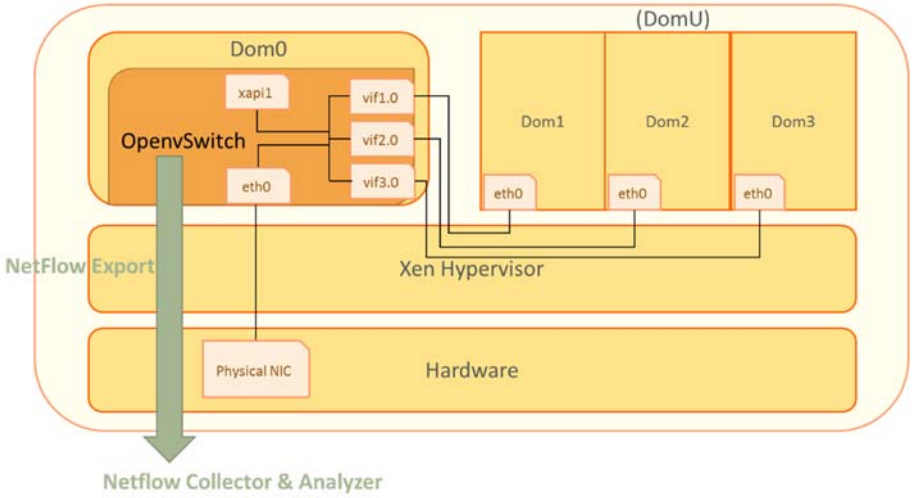


圖 18、利用 XenServer 之 Open vSwitch 產生 Netflow

場景 2: 測試異常行為是否能被發現

在正常流量中穿插異常行為產生，觀察分析系統是否能夠偵測並透過網頁圖形介面呈現事件。

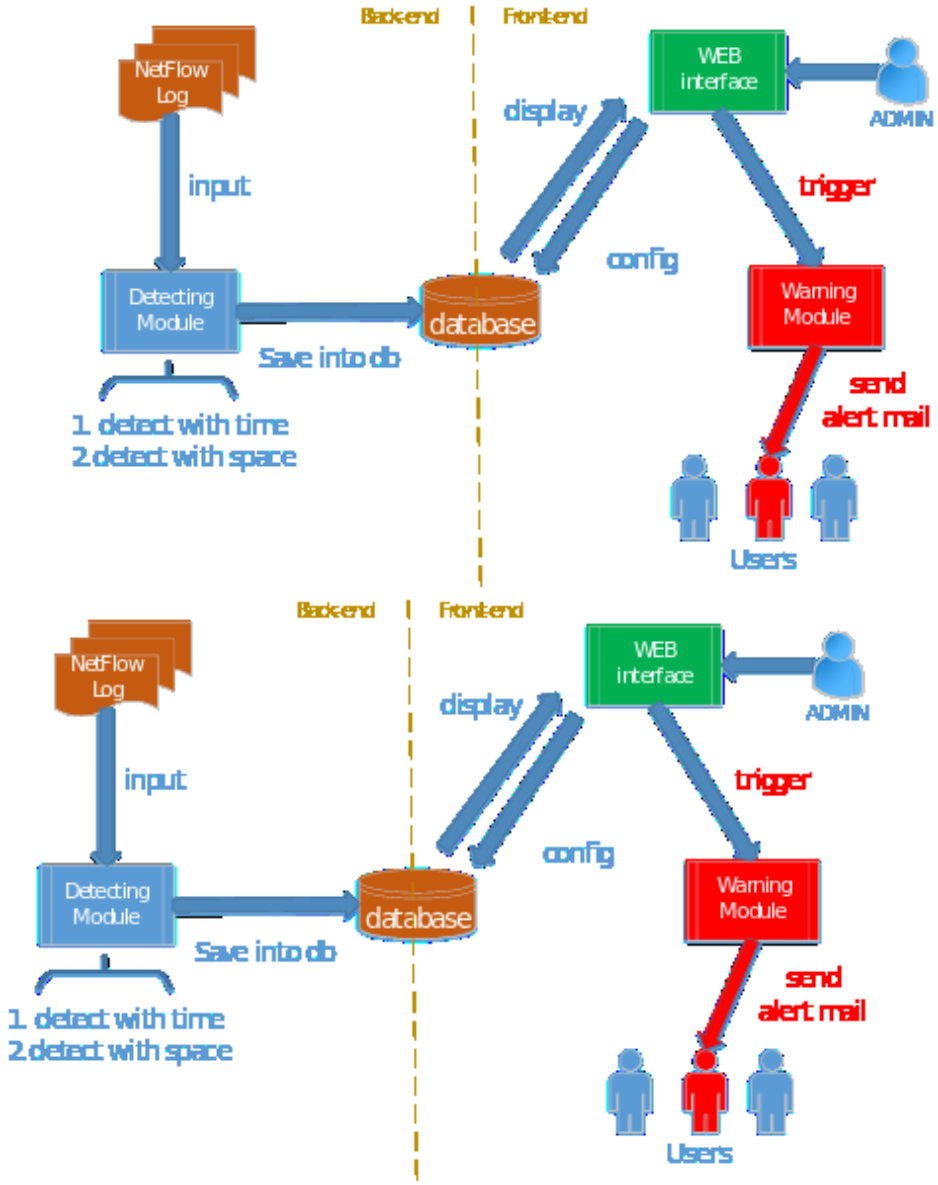


圖 19、偵測異常事件並以網頁介面呈現

場景 3: 測試系統的靈活性

透過網頁介面去調整門檻值，並測試調整後系統是否仍能運作以及根據新門檻值對惡意行為進行偵測

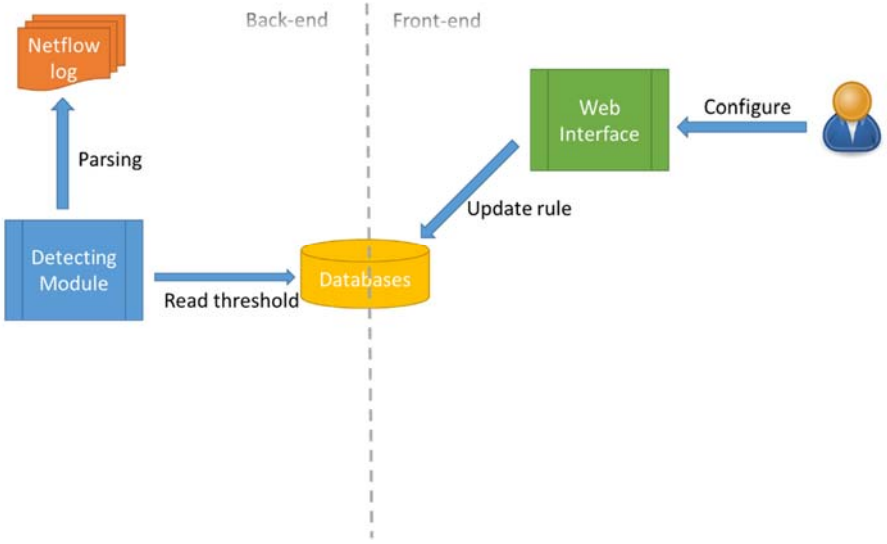


圖 20、調整門檻值進行偵測

3.3 整合測試

本計畫為整合型之計畫，各子計畫之開發成果可互享，需於測試中加入整合測試以驗證系統之可行性。測試之內容為各子計畫間分享資料流及資料呈現。

3.4 壓力測試

計畫為提供網路管理人員使用之工具，在查詢目標主機已獲得網路設定資料，測試查詢時間，其測試場景如接受測試之場景，並於接受測試時一併進行壓力測試。

4. 測試案例

計畫測試案例

CDS-AT-001 Case Test

目的:

- 為了確保各子計畫所上傳之內容已可紀錄於資料庫，互相分享，且不會有 XSS 及 SQL Injection 之情況發生。

✧ 操作說明:

表 4: CDS-AT-001 Case Test

Identification	CDS-AT-001	
Name	正確建立資料庫，各子計畫可分享內容。	
Test Target	資料庫結果正常呈現。	
Requirements	CDS-TR-001、CDS-TR-002、CDS-FR-001、 CDS-DR-001	
Severity	1(Critical)	
Instructions	Actor Actions	Instructions
	1.各子計畫上傳內容及輸入特殊字串，避免安全疑慮	
		2.資料顯示於資料庫中
Expected Result	實驗過程中，各子計畫之資料庫皆可正常匯入及分享。	
Cleanup	無	

總計畫測試案例

CDS-AT-002 Case Test

目的:

- 為了確保同時多人上限可正常呈現，利用測試平台之主機對系統進行多人同時上線之壓力測試。

✧ 操作說明:

表 5: CDS-AT-002 Case Test

Identification	CDS-AT-002	
Name	主系統壓力測試。	
Test Target	於多人連線時可正常回應。	
Requirements	CDS-PR-001	
Severity	1(Critical)	
Instructions	Actor Actions	Instructions
	1.同時多人連線	
		2.網頁與資料庫可正常回應
Expected Result	實驗過程中，網頁與資料庫皆能正常回應。	
Cleanup	無	

子計畫一測試案例

BNM-AT-001 Case Test

目的:

為了確保偵測結果有效性，必須能讓多人同時登入系統，並容許大量的資料匯入，且要求格式設定符合系統需求。利用 LAM 收集相關 log，進行擷取、整合並儲存到資料庫中。

表 6: BNM-AT-001 Case Test

Identification	BNM-AT-001	
Name	正確建立偵測系統的資料庫。	
Test Target	確保偵測結果有效性。	
Requirements	BNM-TR-001，BNM-TR-002，BNM-DC-001，BNM-TL-001，BNM-UR-001，BNM-IR-001，BNM-PR-001，BNM-PR-002，BNM-DR-001， BNM-SR-001。	
Severity	1(Critical)	
Instructions	Actor Actions	Instructions
	將所有系統的 log 整合	正確的建立規格
Expected Result	實驗過程中，本研究正確建立規格，整合多個 IDS 的 log 資料，以利 log 資料輸入正確並快速辨識。	
Cleanup	無	

BNM-AT-002 Case Test

目的:

驗證系統中的 LCM 的有效性，就 Mail 紀錄、命令與控制伺服器異常連結紀錄與網路流量警訊記錄進行關聯分析。比對內外網對 C&C 連線的來源位址是否一致，再判斷此位址是否為社交網路分析中的核心目標。

表 7: BNM-AT-002 Case Test

Identification	BNM-AT-002	
Name	log 資料進行關聯分析。	
Test Target	將資料進行關聯，判斷社交網路分析中的核心目標。	
Requirements	BNM-TR-002，BNM-DC-001，BNM-TL-001，BNM-UR-001，BNM-OR-001，BNM-IR-002，BNM-PR-002，BNM-DR-001，BNM-SR-001。	
Severity	1(Critical)	
Instructions	Actor Actions	Instructions
	將所有系統的 log 進行關聯	建立偵測系統的步驟
Expected Result	實驗過程中，本研究將所有 IDS log 進行關聯分析，得到社交網路分析中的核心目標。	

Cleanup	無

BNM-AT-003 Case Test

目的:

為了確保偵測結果有效性，使用貝氏網路架構圖表示出各類事件或行為的發生機率據以判斷入侵行為發生機率，結合各攻擊階段之特徵值經過觀察與分析，建立有效的風險評估。

表 8: BNM-AT-003 Case Test

Identification	BNM-AT-003	
Name	進行分析及風險評估。	
Test Target	在 BNM 中建立有效的風險評估，以利後續偵測。	
Requirements	BNM-TR-002，BNM-PR-002，BNM-DR-001。	
Severity	1(Critical)	
Instructions	Actor Actions	Instructions
	所有資料進行風險評估	建構 BNM 偵測系統
Expected Result	實驗過程中，經由 BNM 的評估，以利後續偵測。	
Cleanup	無	

BNM-AT-004 Case Test

目的:

為了確保偵測結果有效性，依據本研究所定義的目標式攻擊的攻擊流程進行關聯分析，找出潛在已受攻擊之目標 IP，並與 BNM 中之風險值綜合比對後，依其風險值找出目前受攻擊名單以及未來可能遭受威脅之目標。

表 9: BNM-AT-004 Case Test

Identification	BNM-AT-004	
Name	產出結果報告。	
Test Target	偵測受攻擊名單及可能遭受威脅之目標。	
Requirements	BNM-TR-002 ， BNM-OR-001 ， BNM-FR-001 ， BNM-PR-002，BNM-DR-001	
Severity	1(Critical)	
Instructions	Actor Actions	Instructions
	根據比對找到受攻擊名單	產出有效結果報告
Expected Result	實驗過程中，本研究依 BNM 之風險評估進行比對，找到受攻擊名單，及未來可能遭受威脅之目標。	
Cleanup	無	

子計畫二測試案例

CLS-AT-001 Test Case

目的:

- 利用 SSH 溝通目標主機，讀取主機網路資訊後並回傳資訊

表 10:CLS-AT-001 Case Test

Identification	AGN-AT-001	
Name	SSH 溝通目標主機	
Test Target	得到目標主機網路資訊	
Requirements	CLS-DC-002, CLS-FR-001, CLS-ER-003, CLS-OR-0(CLS-SR-001	
Severity	1(Critical)	
Instructions	Actor Actions	System response
	1.利用 SSH 溝通目標主機	
		2.回傳網路卡資訊與主機名稱
Expected Result	Agent 收到目標主機網路資訊	
Cleanup	無	

CLS-AT-002 Test Case

目的:

- 利用 socket 溝通目標主機資料庫，得到虛擬網橋、埠、介面資訊，並回傳資訊

表 11:CLS-AT-002 Case Test

Identification	AGN-AT-002	
Name	Socket 溝通目標主機資料庫	
Test Target	得到虛擬網橋、埠、介面資訊	
Requirements	CLS-DC-001~002, CLS-FR-001, CLS-ER-001~002, CLS-O 002	
Severity	1(Critical)	
Instructions	Actor Actions	System response
	1. 利用 socket 溝通目標主機資料庫	
		2. 回傳虛擬網橋、埠、介面資訊
Expected Result	得到虛擬網橋、埠、介面資訊	
Cleanup	無	

CLS-AT-003 Test Case

目的:

- 將蒐集到的資訊整理並且產生網路拓樸圖。

表 12:CLS-AT-003 Case Test

Identification	CLS-AT-003	
Name	整理資訊並產生網路拓樸圖	
Test Target	產生網路拓樸圖	
Requirements	CLS-FR-001~002, CLS-TL-001, CLS-IR-001	
Severity	1(Critical)	
Instructions	Actor Actions	System response
	1.傳入網路資訊	
		2.網路拓樸圖
Expected Result	產生網路拓樸圖	
Cleanup	無	

CLS-AT-004 Test Case

目的:

- 藉由網路拓樸圖偵測錯誤組態，若遇到錯誤給予錯誤訊息

表 13:CLS-AT-004 Case Test

Identification	CLS-AT-004	
Name	偵測錯誤安裝組態	
Test Target	偵測錯誤安裝組態發生的情形，並且回傳錯誤發生路徑	
Requirements	CLS-FR-001, CLS-FR-003, CLS-IR-002, CLS-PR-003	
Severity	1(Critical)	
Instructions	Actor Actions	System response
	1.給予網路拓樸圖	
		2.有錯誤回傳錯誤發生路徑，沒有則回傳正確訊息
Expected Result	偵測錯誤組態發生的情形，並且回傳錯誤發生路徑	
Cleanup	無	

子計畫三測試案例

MDD-AT-001 Test Case

目的:

- 從網路流量中過濾取得 DNS 流量中的失效查詢部分並匯入 TFM 模組

表 14:MDD-AT-001 Case Test

Identification	MDD-AT-001	
Name	取得失效查詢流量	
Test Target	取得受測網域內 DNS 主機之失效查詢流量	
Requirements	MDD-TR-001~002, MDD-DC-001, MDD-TL-001, MDD-O 001, MDD-FR-001,MDD-ER-001, MDD-DR-001, MDD-SR-001	
Severity	1(Critical)	
Instructions	Actor Actions	System response
	1.溝通目標主機	
		2.回傳失效查詢流量
Expected Result	資料庫取得受測網域內之失效查詢流量	
Cleanup	無	

MDD-AT-002 Test Case

目的:

- 透過 TFM 模組過濾掉失效查詢流量中的正常失效查詢

表 15:MDD-AT-002 Case Test

Identification	MDD-AT-002	
Name	過濾失效查詢流量	
Test Target	過濾流量中正常的失效查詢	
Requirements	MDD-AT-001, MDD-TR-003, MDD-PR-001, MDD-IR-001	
Severity	1(Critical)	
Instructions	Actor Actions	System response
	3. 取得失效查詢流量與白名單	
		4. 回傳過濾後之失效查詢流量
Expected Result	得到疑似受感染主機所產生之失效查詢流量	
Cleanup	無	

MDD-AT-003 Test Case

目的:

- 透過 PAM 模組將過濾後之失效查詢根據主機間之行為特徵繪製成關聯拓樸圖。

表 16:MDD-AT-003 Case Test

Identification	MDD-AT-003	
Name	繪製拓樸圖	
Test Target	將主機間之行為特徵繪製成關聯拓樸圖。	
Requirements	MDD-AT-001~002, MDD-TR-004,	
Severity	1(Critical)	
Instructions	Actor Actions	System response
	1.傳入過濾後之失效查詢流量	
		2.產生關連拓樸圖
Expected Result	產生拓樸圖	
Cleanup	無	

MDD -AT-004 Test Case

目的:

- PAM 模組利用本子計畫所提出之 WSCA 分群演算法產生分群結果並匯入 BDM 模組。

表 17:MDD-AT-004 Case Test

Identification	MDD-AT-004	
Name	產生分群結果	
Test Target	利用 WSCA 分群演算法針對主機產生分群結果	
Requirements	MDD-AT-001~003, MDD-TR-005, MDD-PR-002, MDD-I 002	
Severity	1(Critical)	
Instructions	Actor Actions	System response
	1.傳入關聯拓樸圖	
		2.產生分群結果
Expected Result	根據主機關聯產生分群結果	
Cleanup	無	

MDD -AT-005 Test Case

目的:

- BDM 模組利用群體內的失效查詢進行偵測，透過變點偵測、數量分布以及時間分布針對各群體進行辨識，最後產生殭屍網路辨識結果。

表 18:MDD-AT-005 Case Test

Identification	MDD-AT-005	
Name	產生辨識結果	
Test Target	利用群體內的失效查詢行為進行偵測，進而產生殭屍網路識結果。	
Requirements	MDD-AT-001~004, MDD-TR-006, MDD-FR-002~003,	
Severity	1(Critical)	
Instructions	Actor Actions	System response
	1.傳入分群結果與失效查詢流量	
		2.辨識群體內主機是否為殭屍網路
Expected Result	產生受感染主機黑名單	
Cleanup	無	

子計畫四測試案例

CNM -AT-001 Test Case

目的:

- 虛擬交換器必須正確設定至能夠將通過此交換器之流量以 Netflow 格式輸出至指定之 Collector。在雲端內部刻意製造流量，於 Collector 端驗證是否的確出現該流量。

表 19:CNM-AT-001 Case Test

Identification	CNM-AT-001	
Name	測試虛擬交換機是否正確輸出 Netflow 資料	
Test Target	確保 Netflow 資料的來源與傳送過程無誤	
Requirements	CNM-TR-001, CNM-TL-001, CNM-ER-001	
Severity	1(Critical)	
Instructions	Actor Actions	System response
	1.製造會流經虛擬交換器之流量	
		2.Netflow 資料記錄此筆流量
Expected Result	與刻意製造之流量相對應之 Netflow 格式資料	
Cleanup	無	

CNM -AT-002 Test Case

目的:

- 在正常流量中穿插異常行為產生，觀察分析系統是否能夠偵測並透過網頁圖形介面呈現事件。

表 20:CNM-AT-002 Case Test

Identification	CNM-AT-002	
Name	測試異常行為是否能被發現並記錄	
Test Target	異常行為之偵測與呈現	
Requirements	CNM-TR-002, CNM-TR-003, CNM-PR-001, CNM-IR-001	
Severity	1(Critical)	
Instructions	Actor Actions	System response
	1.產生惡意流量	
		2.偵測並寫進資料庫
Expected Result	網頁圖形介面呈現該筆事件以及相關流量資料	
Cleanup	無	

CNM -AT-003 Test Case

目的:

- 透過網頁介面去調整門檻值，並測試調整後系統是否仍能運作以及根據新門檻值對惡意行為進行偵測

表 21:CNM-AT-003 Case Test

Identification	CNM-AT-003	
Name	測試系統的靈活性	
Test Target	透過網頁介面設定門檻值並成功運作	
Requirements	CNM-TR-004, CNM-UR-001	
Severity	1(Critical)	
Instructions	Actor Actions	System response
	1.透過網頁設定新門檻	
		2.系統正常運作
Expected Result	偵測模組根據新門檻解析 Netflow 資料	
Cleanup	無	

5. 測試結果與分析

總計畫

表 22、總計畫測試結果

Test Case #	Results(PASS/FAIL)	Comment
CDS-AT-001	待測中	整合測試中，目前相關掃描結果如圖所示。
		待整合測試結束後進

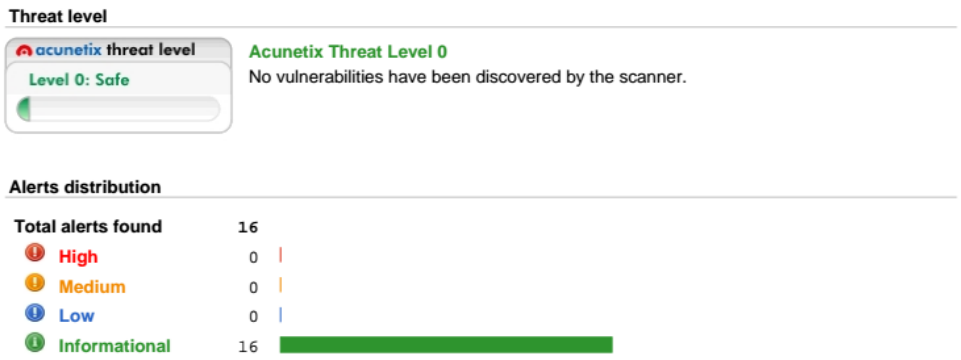


圖 21、弱點掃描結果

子計畫一

Test Case #	Results(PASS/FAIL)	Comment
BNM-AT-001	**PASS**	功能正常
BNM-AT-002	**PASS**	功能正常
BNM-AT-003	**PASS**	功能正常
BNM-AT-004	**待測中**	

表 23、子計畫一測試結果

子計畫二

表 24、子計畫二測試結果

Test Case #	Results(PASS/FAIL)	Comment
CLS-AT-001	PASS	回應時間測試 30 次平均約為 0.4 毫秒
CLS-AT-002	PASS	回應時間測試 30 次平均約為 0.05 毫秒
CLS-AT-003	PASS	拓樸正常產生
CLS-AT-004	PASS	執行時間測試 30 次平均

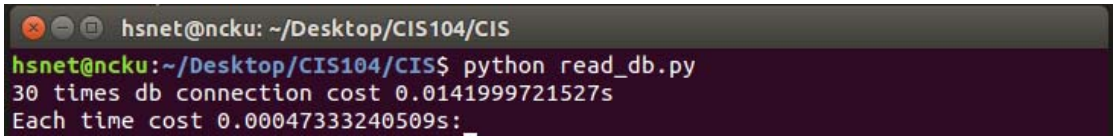


圖 22、CLS-AT-001 測試結果

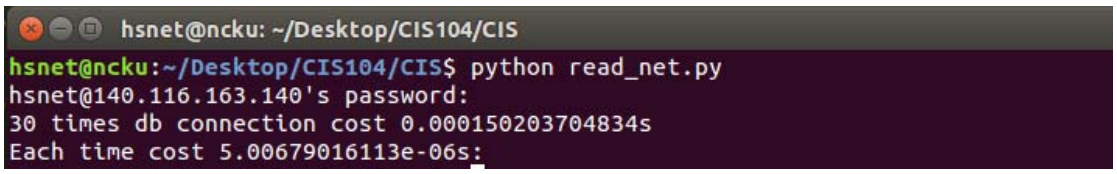


圖 23、CLS-AT-002 測試結果

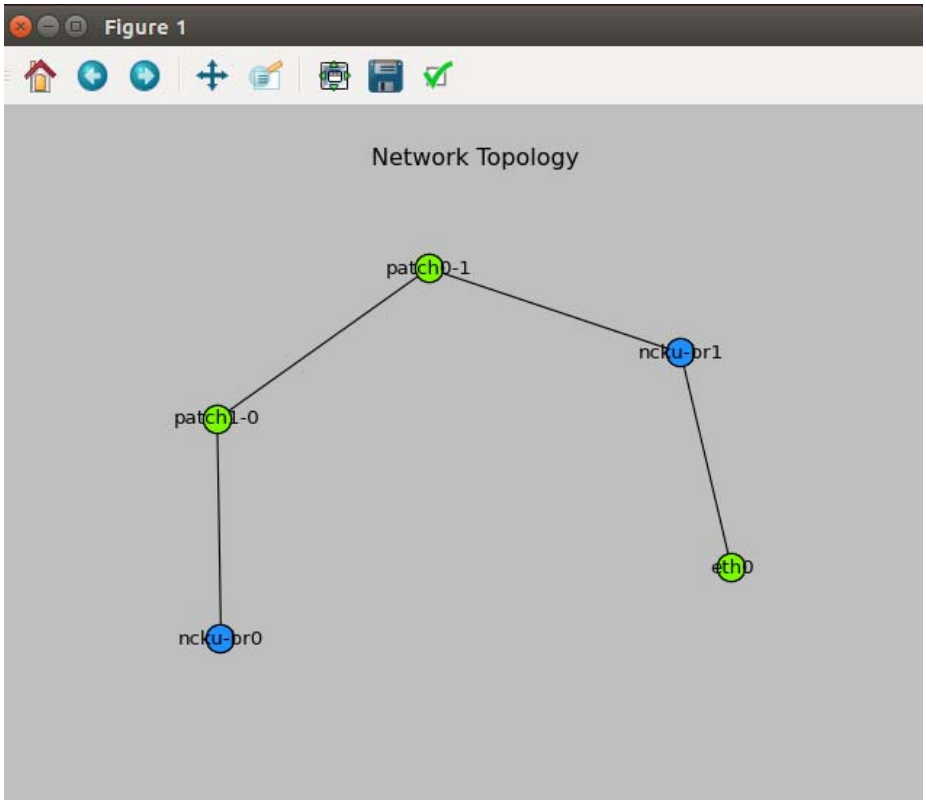


圖 24、CLS-AT-003 測試結果

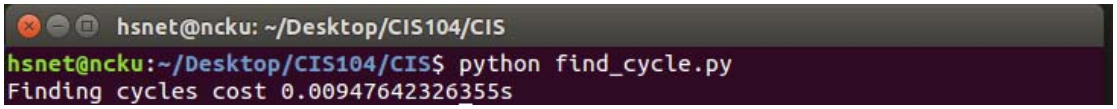


圖 25、CLS-AT-004 測試結果

子計畫三

Test Case #	Results(PASS/FAIL)	Comment
MDD-AT-001	PASS	可取得網路流量，如下圖 26 所示
MDD -AT-002	PASS	測試結果平均每秒可進行 300 筆以上查詢過濾
MDD -AT-003	PASS	可產生關連拓樸圖
MDD -AT-004	PASS	測試結果平均分群準確率可達 95%，如下圖 27

表 26、子計畫三測試結果

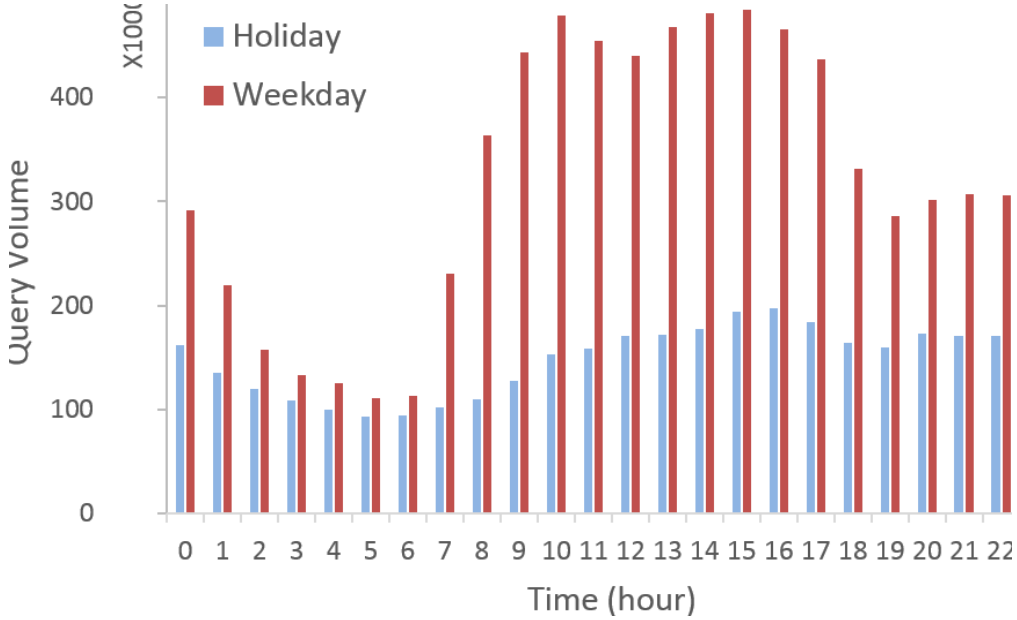
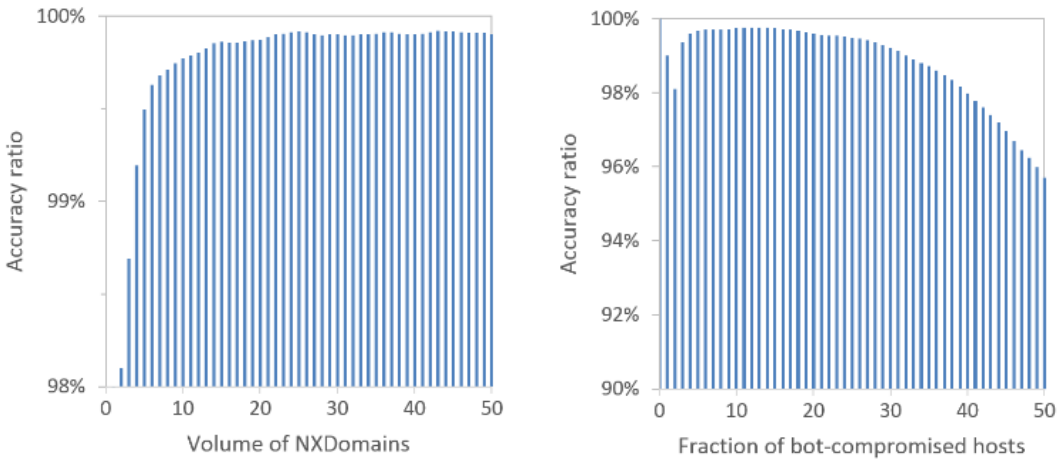


圖 26、MDD-AT-001



(a) (b)

圖 27、MDD-AT-004

子計畫四

Test Case #	Results(PASS/FAIL)	Comment
CNM-AT-001	**PASS**	如下圖 AT-001 所示
CNM-AT-002	**PASS**	如下圖 AT-002 所示
CNM-AT-003	**PASS**	系統正確讀進新門檻

表 26、子計畫四測試結果

```
root@ubuntu:/nfs/netflow# nfdump -R 2016-02-16 | grep ICMP
2016-02-16 15:23:10.659     3.002 ICMP      192.168.5.10:0     ->     192.168.5.20:0.0     4     392     1
2016-02-16 15:23:11.659     2.002 ICMP      192.168.5.20:0     ->     192.168.5.10:8.0     3     294     1
2016-02-16 15:23:39.451     0.000 ICMP      192.168.5.10:0     ->        8.8.8.8:8.0       1      98     1
2016-02-16 15:23:32.141     4.000 ICMP      192.168.5.20:0     ->     192.168.5.10:0.0     5     490     1
2016-02-16 15:23:32.141     4.000 ICMP      192.168.5.10:0     ->     192.168.5.20:8.0     5     490     1
2016-02-16 15:23:40.453     2.001 ICMP      192.168.5.10:0     ->        8.8.8.8:8.0       3     294     1
2016-02-16 15:23:39.462     3.004 ICMP         8.8.8.8:0       ->     192.168.5.10:0.0     4     392     1
```

圖 28、AT-001

start_time	stop_time	event_type	src_ip	src_port	dst_ip	dst_port	attack_count
2016-03-29 11:36:00	2016-03-29 11:37:00	Horizontal Scan	192.168.5.10	X	F	53	798
2016-03-29 11:35:00	2016-03-29 11:36:00	Vertical Scan	192.168.5.10	X	192.168.5.20	F	255
2016-03-29 11:35:00	2016-03-29 11:36:00	Brute Force	192.168.5.10	X	192.168.5.30	3389	24

圖 29、T-002

附錄 A 追朔表

總計畫追溯表

表 27、總計畫 子系統 vs. 測試案例追溯表

Sub System Test Cases	BNM	CLS	MDD	CNM
CDS-AT-001	V	V	V	V
CDS-AT-002	V	V	V	V

表 28、總計畫 系統需求 vs. 測試案例追溯表

Sub System Test Cases	CDS-TR-001	CDS-TR-002
CDS-AT-001	V	V
CDS-AT-002	V	

子計畫一追溯表

表 29、計畫一 子系統 vs. 測試案例追溯表

Sub System Test Cases	LAM	LCM	BNRAM	TADM
BNM-AT-001	V	V		
BNM -AT-002		V	V	
BNM -AT-003			V	V
BNM -AT-004			V	V

表 30、子計畫一 系統需求 vs. 測試案例追溯表

Sub System Test Cases	BNM-TR-001	BNM-TR-002
BNM-AT-001	V	V
BNM-AT-002	V	
BNM-AT-003	V	V

子計畫二追溯表

表 31:子計畫二 子系統 vs. 測試案例 追溯表

Sub System Test Cases	NIC	NTG	MSD
CLS-TR-001	V		
CLS-TR-002	V		
CLS-TR-003	V		
CLS-TR-004		V	
CLS-TR-005			V

表 32:子計畫二 系統需求 vs. 測試案例 追溯表

Test Req. Test Cases	CLS-TR-001	CLS-TR-002	CLS-TR-003	CLS-TR-004	CLS-TR-005
CLS-AT-001	V	V			
CLS-AT-002		V	V		
CLS-AT-003				V	
CLS-AT-004					V

子計畫三追溯表

表 33、子計畫三 子系統 vs. 測試案例 追溯表

Sub System Test Cases	TFM	PAM	BDM
MDD-AT-001	V		
MDD-AT-002	V	V	
MDD-AT-003		V	
MDD-AT-004		V	V
MDD-AT-005			V

表 34、子計畫三 系統需求 vs. 測試案例 追溯表

Test Req. Test Cases	MDD-TR-001	MDD-TR-002	MDD-TR-003	MDD-TR-004	MDD-TR-005	MDD-TR-006
MDD-AT-001	V	V				
MDD-AT-002			V			
MDD-AT-003				V		
MDD-AT-004					V	
MDD-AT-005						V

子計畫四追溯表

表 35、子計畫四 子系統 vs. 測試案例追溯表

Sub System Test Cases	NFE	NCA	EVC
CNM-AT-001	V	V	
CNM-AT-002		V	V
CNM-AT-003		V	V

表 36、子計畫四 系統需求 vs. 測試案例追溯表

Test Req. Test Cases	CNM-TR-001	CNM-TR-002	CNM-TR-003	CNM-TR-004
CNM-AT-001	V			
CNM-AT-002		V	V	
CNM-AT-003				V