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

106/06/12

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
3	106/6/12	3.00	變更為第三年資訊

版本: 3.00

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。

總計畫在第三年時所建立之資料共享之平台，以前兩年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

子計畫一第三年的系統中，結合電子郵件方式和社群網站兩種最典型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和網站瀏覽記錄，追蹤後續階段性攻擊，貝氏網路的學習能力模型作為偵測模型，並結合以特徵值為基礎之風險評估預測，偵測持續性滲透攻擊，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

隨著雲端運算技術的進步，許多企業組織會將資料儲存於雲端儲存空間中，然而，許多機敏資料可能會有遭受惡意使用者擷取、盜用的疑慮，而在網路安全領域中，不論對駭客或是網站管理員來說，日誌是相當重要的參考依據，所以本計畫「雲端系統中分散式日誌蒐集、錯誤偵測、稽核及預警系統」藉由蒐集系統日誌，透過存取網路儲存伺服器(NAS)與公有雲(Google Drive)的系統日誌，提供資料存取行為、傳輸軌跡以及異常行為預警機制。最終以提供一個具有正確組態，且可針對資料存取軌跡進行稽核、預警的雲端系統為主要目標。

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，當殭屍網路與控制中心通訊時，會因網域進行轉換而產生大量失效查詢之行為，利用此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，對於有規避偵查之行為的殭屍網路進行更準確的分析，並透過分析網域名稱流量紀錄以縮短偵測時間。子計畫第三年會針對受感染主機之行為特徵進行分析，受感染主機之特徵包含，定時查詢、固定間隔時間之查詢、產生網域之字元分布以及繪製關聯拓樸圖之結構差異，利用上述特徵來辨別受感染之主機以及正常主機之差異。

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。計畫第三年的目標為建置雲端資安防護管理系統，整合所收集的資訊與分析結果，並設置查詢 API 以便於系統設定與修改與資料查閱，並且在偵測出異常流量時能夠進行回報與處理。

1.2 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	測試須通過網站弱點檢測
CDS-TR-002	必要	子計畫之資訊可上傳至中控平台
CDS-TR-003	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	代理伺服器成功接收私有雲日誌資料。
CLS-TR-002	必要	代理伺服器成功接收公有雲日誌資料。
CLS-TR-003	必要	日誌資料透過資料庫整合於管理者介面。
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
MDD-TR-007	必要	產生受感染主機分析報告
CNM-TR-001	必要	系統可針對門檻值進行設定
CNM-TR-002	必要	系統可提供 GUI 介面進行查詢
CNM-TR-003	必要	系統可偵測內部網路威脅

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	各子計畫相關之查詢，需於10s內完成
BNM-PR-001	必要	各子計畫相關之資料庫查詢，結果正確且回應時間短，需於 10 秒內完成
BNM-PR-002	必要	可以提供多人同時登入系統
CLS-PR-001	必要	可持續於每 1 秒內處理 200 筆存取記錄
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	更改門檻值後，可於 30s 內反應至系統上

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社群網站瀏覽行為記錄，全部整合前處理，並將社群網站瀏覽行為記錄進行社群網路分析，找出群組關係與核心目標。接著將郵件紀錄、網路的警訊記錄進行關聯分析，比對內外部之命令與控制伺服器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郵件紀錄、命令與控制伺服器異常連結警訊、網路流量警訊以及社群網站瀏覽行為記錄，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)

將各主機之行為記錄整合並進行社交網路分析，利用視覺化之關連式圖表找出紀錄中之來源端與目的端之相互連結關係，並以顏色區別不同角色主機 IP 群組關係。主要就郵件紀錄、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命令與控制伺服器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：

本計畫提供管理者介面，蒐集系統日誌，呈現檔案資料存取情形，包括 I.私有雲日誌蒐集模組(Private Cloud Log Collection Module, RCM)、公有雲日誌蒐集模組(Public Cloud Log Collection Module, UCM)及資料存取稽核模組(Access log Auditing Module, AAM) ，各模組說明如下：

1. 私有雲日誌蒐集模組(PRivate Cloud log collection Module, RCM)

蒐集網路儲存伺服器傳送的系統日誌，透過儲存於資料庫伺服器進行歸類、分析，內容包括存取網路儲存伺服器系統日誌透過系統日誌伺服器存取群暉科技所提供的網路儲存伺服器(Synology NAS)輸出之系統日誌，並將系統日誌存入 MySQL 資料庫進行歸類。

2. 公有雲日誌蒐集模組(PUblic Cloud log collection Module, UCM)

蒐集公有雲系統日誌，並將之與私有雲日誌整合於管理者介面，內容包括存取公有雲 Google Drive 系統日誌，透過研究 Google API 日誌存取方式，將日誌存入 MySQL 資料庫內。

3. 資料存取稽核模組(Access log Auditing Module, AAM)

提供整合式管理者介面透過網頁呈現，從而達成資料存取行為、傳輸軌跡以及異常行為稽核機制。

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。本計畫系統主要包含三個模組：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：

4. 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)，此類正常流量之主要來源，包含應用程式、第三方黑名單服務 (Third Party Blacklist)與部分防毒軟體所產生。透過本模組之過濾，可大幅降低系統所需後續分析之資料量，以及提升偵測準確率。

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

本模組是透過主機之間的行為模式進行分析，並將其關聯繪製成拓樸圖，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。此演算法不需要事先決定分群數量，

利用光譜分析來尋找最適合的分群結果，依照群體結構自動決定是否需要繼續執行演算法。根據本計畫第一年的觀察，為了規避偵查，部分 DGA 型態殭屍網路會進行休眠的行為。而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。

6. 殭屍網路分析模組 (Botnet Analysis Module, BAM)

本模組主要目的為辨識出受感染之主機並且根據其行為特徵產生分析報告，透過第一年的變點偵測方式 (Change Point Detection)、第二年所提出之針對網域查詢的次數分布以及時間分布、以及第三年所提出之群體行為差異與網域字元分布等特徵以進行辨識，此階段可偵測出受感染主機黑名單以及分析出其與正常群體間之行為差異。

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)

在計畫前兩年此模組可以利用 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。在計畫的第三年則擴展到一般 Switch 之資訊亦可進行分析。

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)所輸出之雲端與一般 Switch 之 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 & Configureation, 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 IP 地理資訊等方便使用者作進一步觀察與研究。並於第三年時新增修改門檻值之功能，當系統被應用在不同環境下時，可根據情況進行門檻值修改以符合網路狀況。

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	系統建構在 Synology NAS 上
CLS-DC-002	系統搭配 Google G Suites 服務
MDD-DC-001	必須布建於擁有 DNS Server 之網路環境
CNM-DC-001	系統需可 Import Netflow 資料

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	日誌資料須符合特定格式
MDD-TL-001	受測網域內主機必須使用網域內之 DNS Server
CNM-TL-001	網路環境中需使用支援 Netflow 之網路設備

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	提供使用者稽核、管理整合式日誌資料
CNM-UR-001	提供管理者進行門檻值修改

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	提供整合式日誌介面
MDD-OR-001	外部元件透過 shell script 匯入資料
CNM-OR-001	可透過總計畫與其他子計畫進行資料分享

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 可將結果傳送至 BNM
CLS-IR-001	PCM 與 UCM 可將結果送至 AAM
MDD-IR-001	TFM 可以將過濾後的資料傳送給 PAM
CNM-IR-001	需可根據門檻值反應至系統上

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	提供資料存取稽核報告
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拓樸圖
MDD-FR-004	提供受感染主機行為分析報告
CNM-FR-001	需可找到潛藏在內部網路之異常主機

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	1秒內提供200筆存取紀錄
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	更改門檻值後，可於 30s 內反應至系統上

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	使用 Windows 架設系統
MDD-ER-001	使用 Ubuntu 建構主系統
CNM-ER-001	使用 Ubuntu 建構主系統

9.防護需求

CDS-DR-001	網頁需通過弱點掃描，並架設於防火牆後僅限特定 IP 進行連線
BNM-DR-001	系統輸入可過濾特殊字元以避免 SQL Injection
CLS-DR-001	日誌系統僅允許特定 IP 連線
MDD-DR-001	資料庫僅允許特定 IP 連線
CNM-DR-001	網頁主機、資料庫僅允許特定 IP 連線

10.安全需求

CDS-DR-001	當子計畫資料上傳之資料格式有誤或無法啟動時，不影響其他子計畫運作
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	日誌系統僅允許特定 IP 連線
MDD-SR-001	資料庫連線行為需紀錄
CNM-SR-001	網頁主機、資料庫僅允許特定 IP 連線

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：

總計畫測試環境

總計畫之主要目的為整合各子計畫之內容，進行資料呈現，故主要測試環境為可接收各子計畫上傳資訊之中央控管平台，如下圖 1 所示。

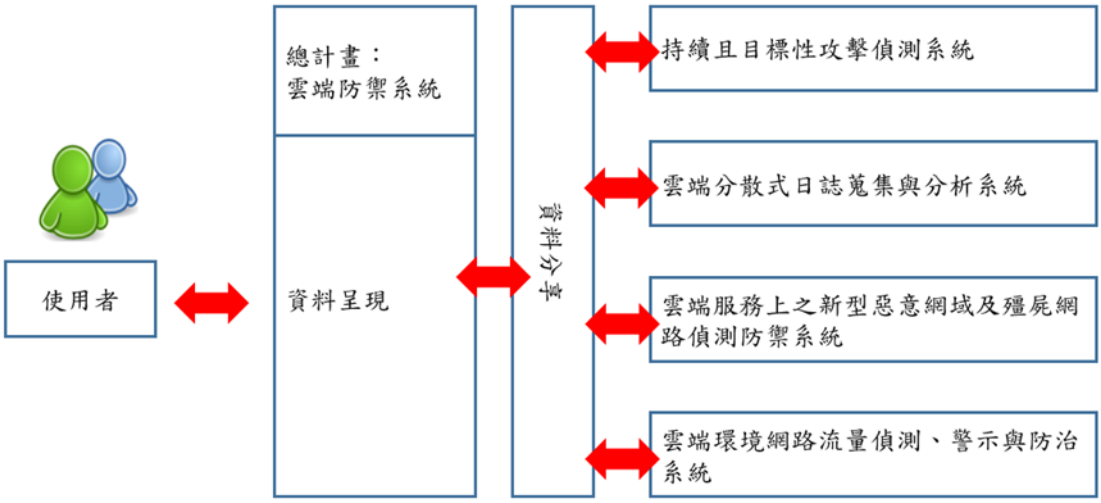


圖 1、總計畫測試環境

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。

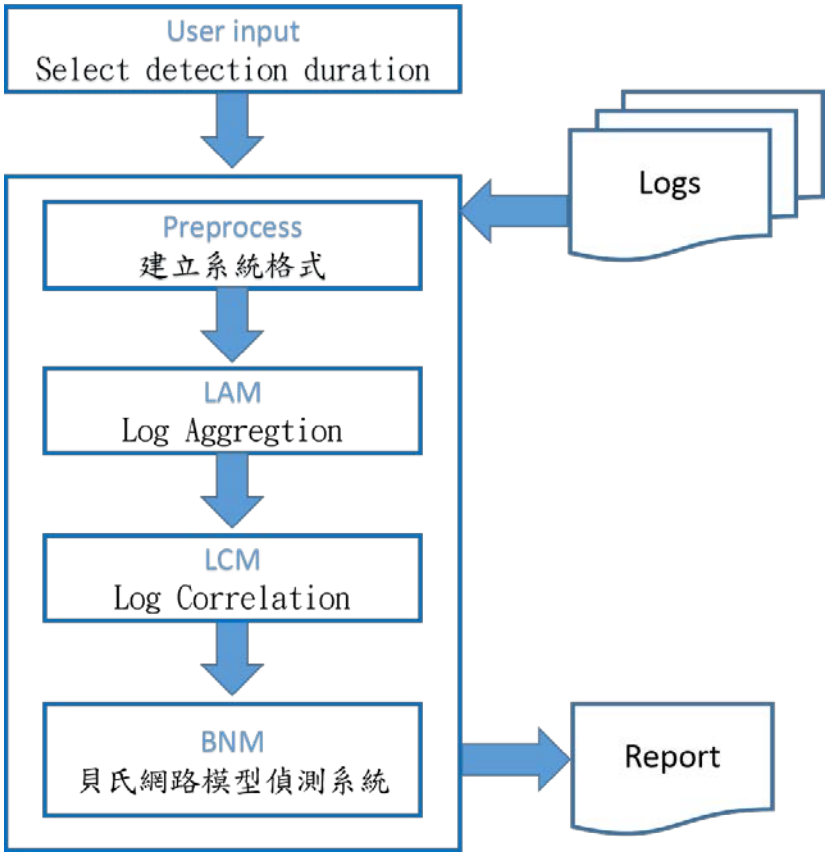


圖 2、子計畫一之測試環境圖

子計畫二測試環境

本階段針對雲端系統中分散式日誌蒐集、錯誤偵測、稽核及預警系統需求分析，建立代理伺服器蒐集私有雲(NAS)以及公有雲系統日誌，測試項目包括代理伺服器日誌資料的接收、彙整日誌資料至資料庫以及提供整合式使用者介面。

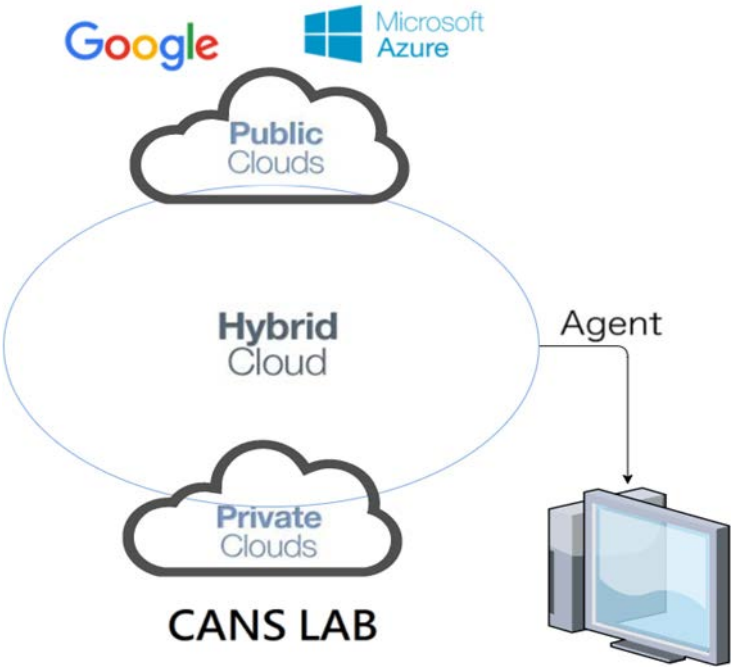


圖 3、雲端系統中分散式日誌蒐集、錯誤偵測、稽核及預警系統環境圖

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，利用殭屍網路與控制中心間的特定行為特徵，進行偵測與分析。在測試環境中，主要從主機與網域名稱系統 (Domain Name Server, DNS) 的流量紀錄執行特徵擷取，進而捕獲觀測網域中之受感染主機，並且對於其連線行為進行分析，標記出與正常群體間產生差異之行為特徵，以協助網路使用者免於殭屍網路之攻擊，提供一安全無虞的網路環境。

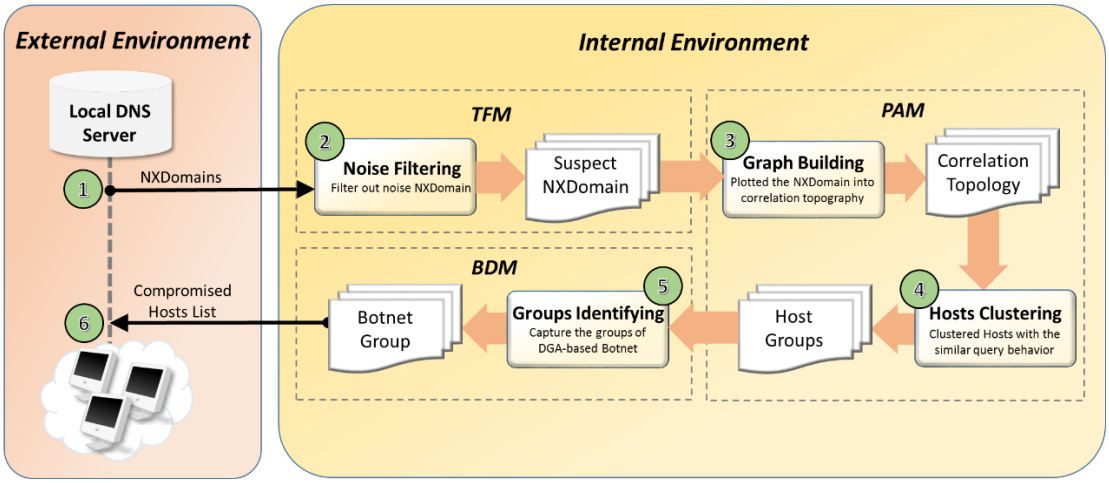


圖 4、子計畫三之測試環境圖

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。

此外由於私有雲之環境常會存在於其他網路區段中，第三年計畫導入同區網段底下之 Netflow 之資訊，透過擴大收集之範圍，找出潛藏在同區段底下之惡意主機。

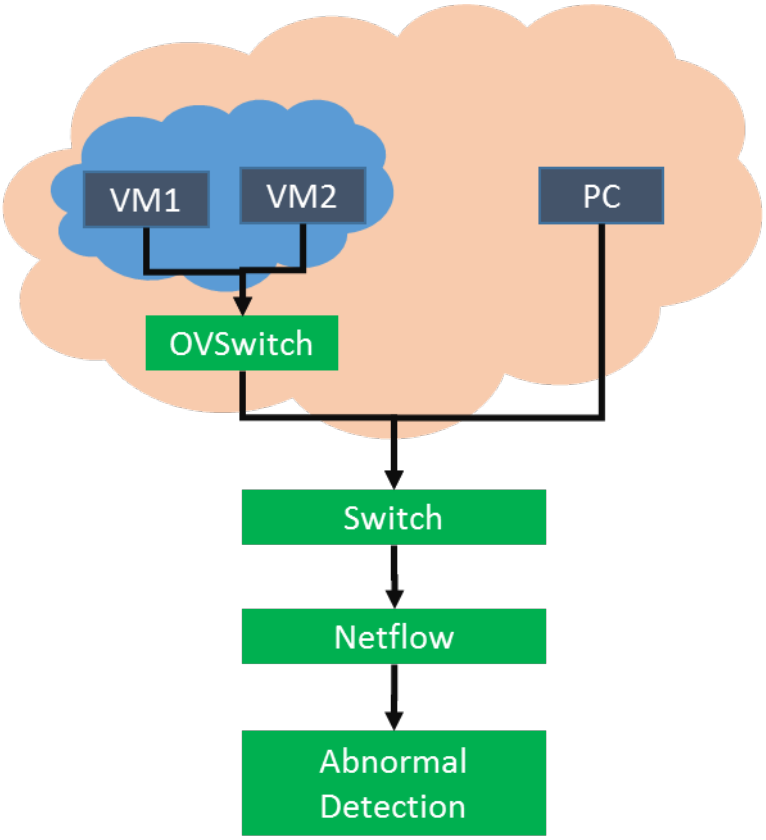


圖 5、子計畫四之測試環境圖

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
    - 計畫使用 Intel Xeon E5-2650
  - 2GB 以上的記憶體
    - 計畫使用 16G 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)
    - 計畫使用 1T 磁碟空間

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
  - 2GB 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 16.04 以上版本
  - 網頁伺服器：Apache 2.4.7(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 5.5 (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

- 雲端系統中分散式日誌蒐集、錯誤偵測、稽核及預警系統
  - 網頁伺服器: Apache Server
  - 資料庫管理系統: MySQL 5.0 (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 2.2.3 版本
- 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 工作日誌記錄資料，其資料包括分公司的所有進出的詳細工作日誌記錄，其中工作日誌記錄內容包含企業之電子郵件、所有訪問過的網址紀錄、防火牆紀錄以及系統內部資訊等等。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

- **日誌檔**

  本子計畫透過整合私有雲與公有雲所提供之日誌資料為主，其中私有雲使用市占率最高群暉科技所提供的網路儲存空間：Synology NAS ，而公有雲則使用 Google Drive。

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

- **Netflow 資料**

  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，此外並導入所處區段網路之資訊。

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 106/2/1 起，應於 106/2/28 完成)
2. 各子系統接受度測試(Acceptance Test) (自 106/3/31 起，應於 106/5/12 完成)

查核點

3. 系統整合與整合測試(106/5/13)
4. 系統測試完成(106/7/1)

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AppScan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。

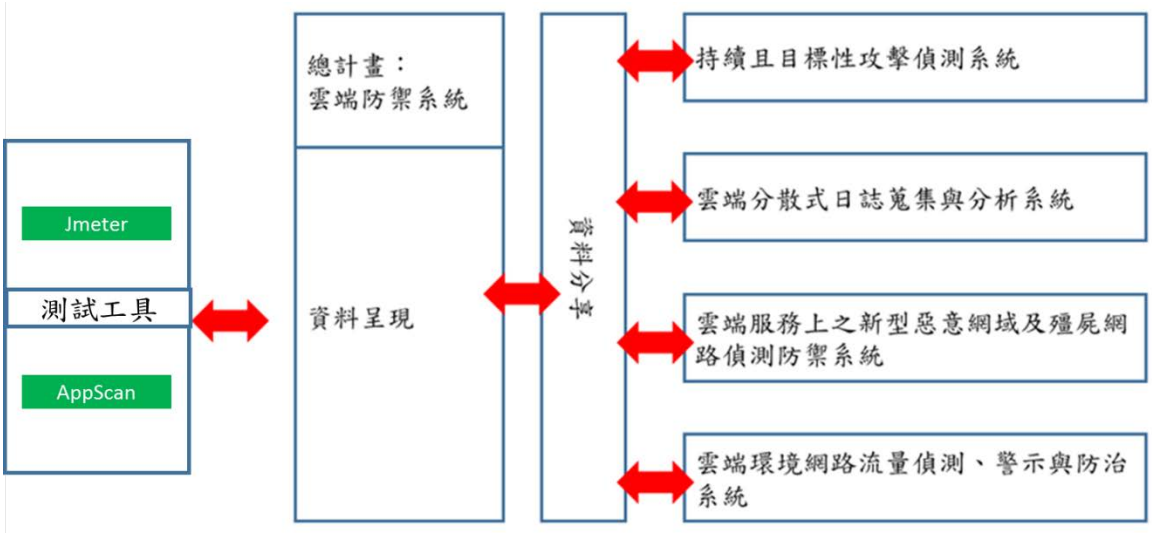


圖 6、總計畫測試架構

子計畫一接受測試程序

場景1：收集工作日誌記錄 並進行整合

從郵件記錄、社群網站瀏覽記錄與IDS警訊記錄中收集相關工作日誌記錄，進行擷取、整合並儲存到資料庫中，如下圖所示：

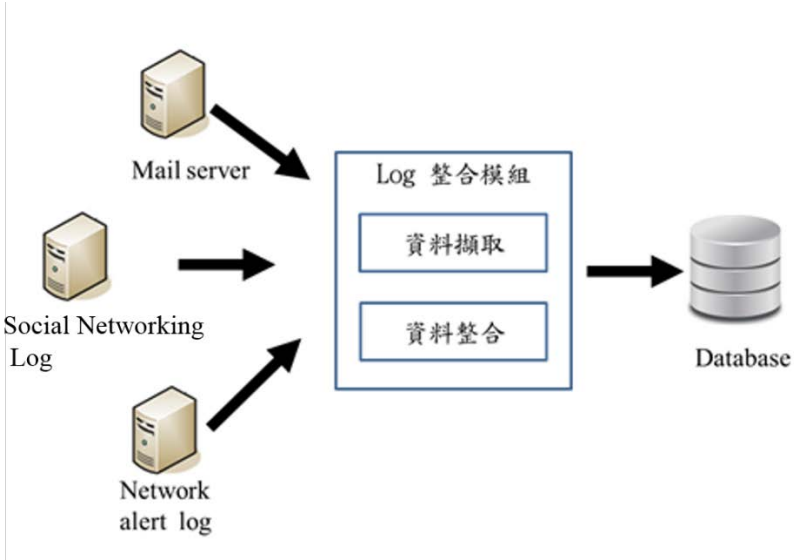


圖 7、資料整合模組

場景2：Log關聯模組

就郵件紀錄、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社群網站瀏覽分析：

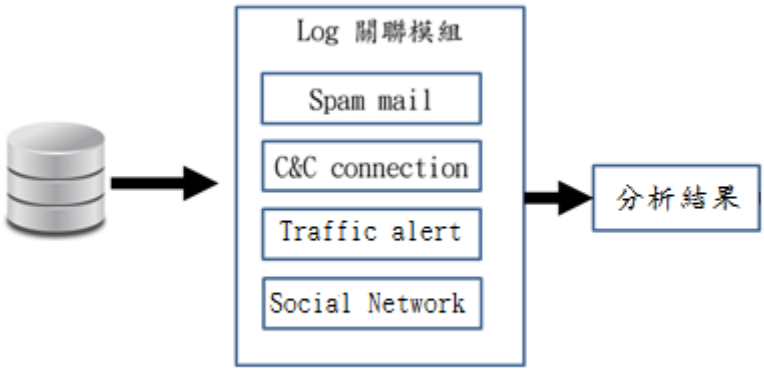


圖 8、 log 關聯模組

場景３：分析及目標攻擊偵測

運用偵測模型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 9、貝氏網路分析及系統偵測

子計畫二接受測試程序

場景 1: 代理伺服器蒐集 NAS 提供之日誌資料

RCM 模組透過 UDP 傳輸協定接收 NAS 提供之系統日誌。

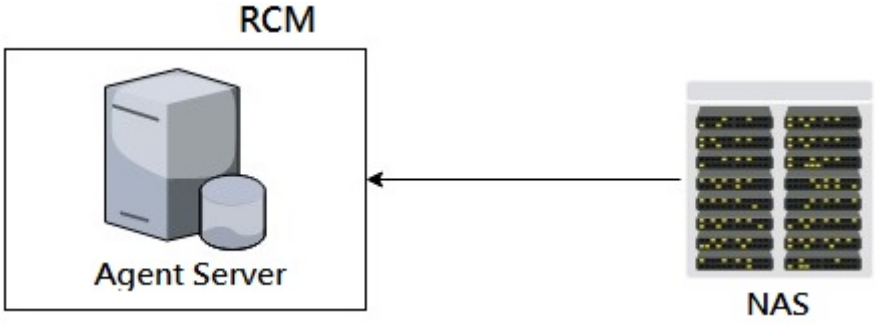


圖 10、代理伺服器接收私有雲日誌情形

場景 2: 代理伺服器蒐集公有雲日誌資料

UCM 模組接收公有雲 Google Drive 傳送之日誌資料。

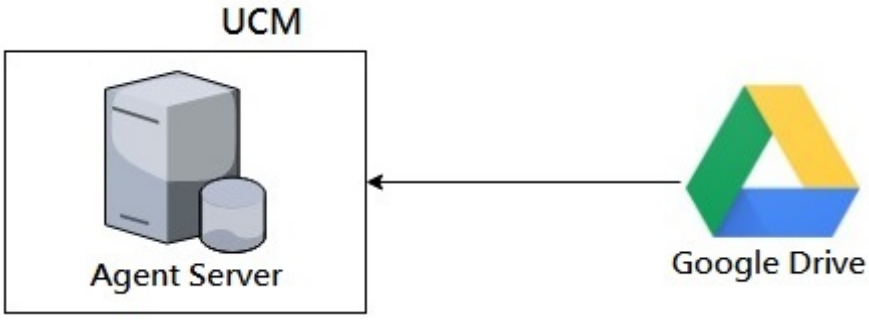


圖 11、代理伺服器接收公有雲日誌情形

場景 3:　管理者介面整合日誌資料

AAM 模組整合私有雲與公有雲日誌資料，提供存取資料稽核與預警服務。

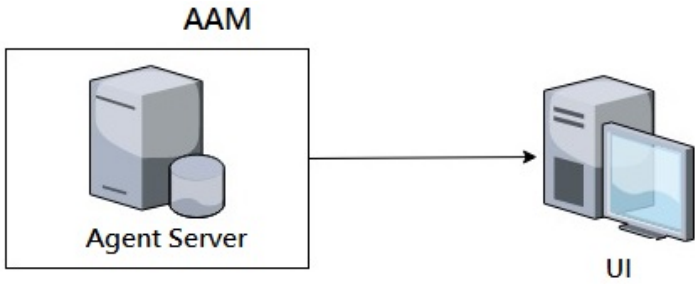


圖 12、整合日誌資料情形

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

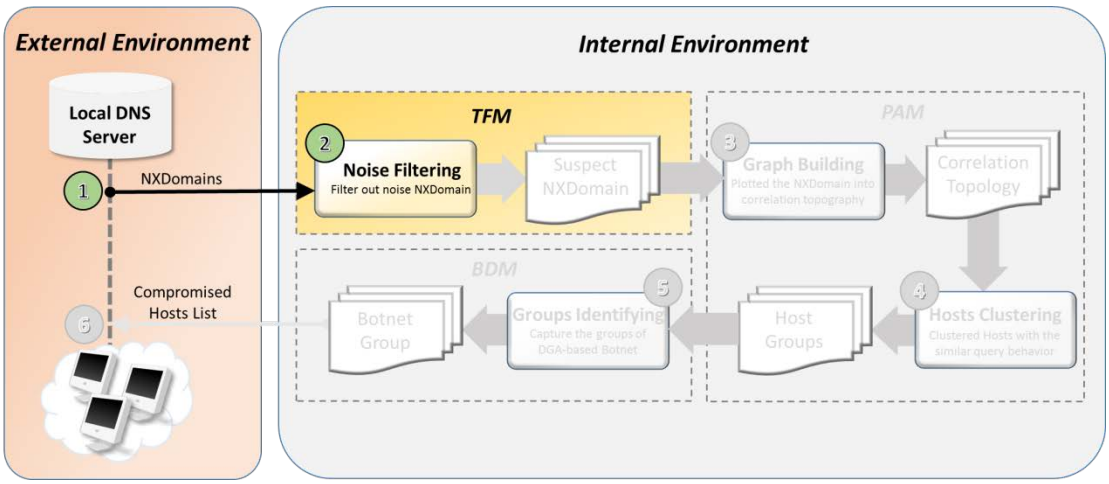


圖 13、殭屍網路偵測系統取得失效查詢流量

場景 2: 過濾失效查詢流量

透過 TFM 模組過濾流量，將正常的失效查詢去除，剩餘之疑似惡意失效查詢部分匯入 PAM 模組。

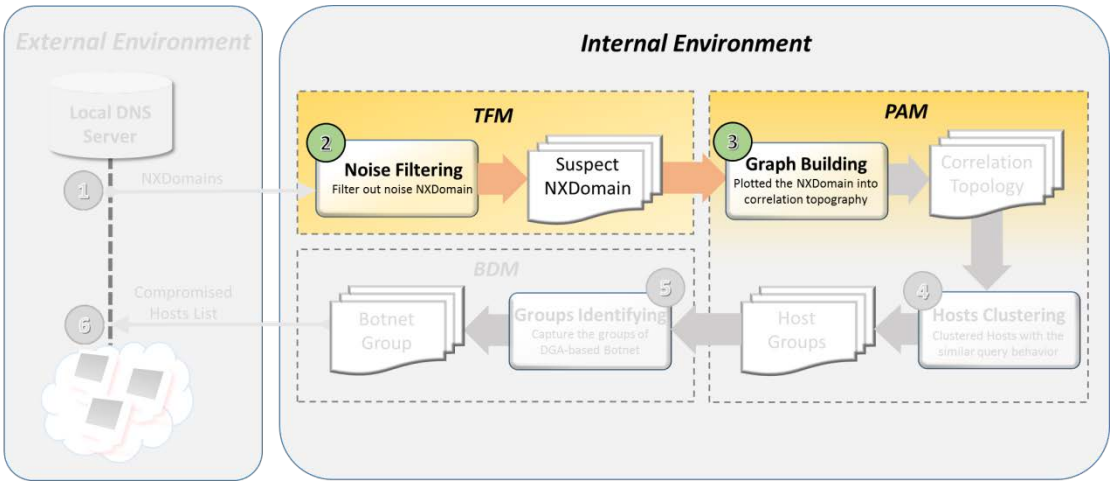


圖 14、殭屍網路偵測系統之 TFM 模組進行流量過濾

場景 3: 繪製關聯拓樸圖

透過 PAM 模組將過濾後之失效查詢，依據主機之間的行為特徵，來繪製成關聯拓樸圖。

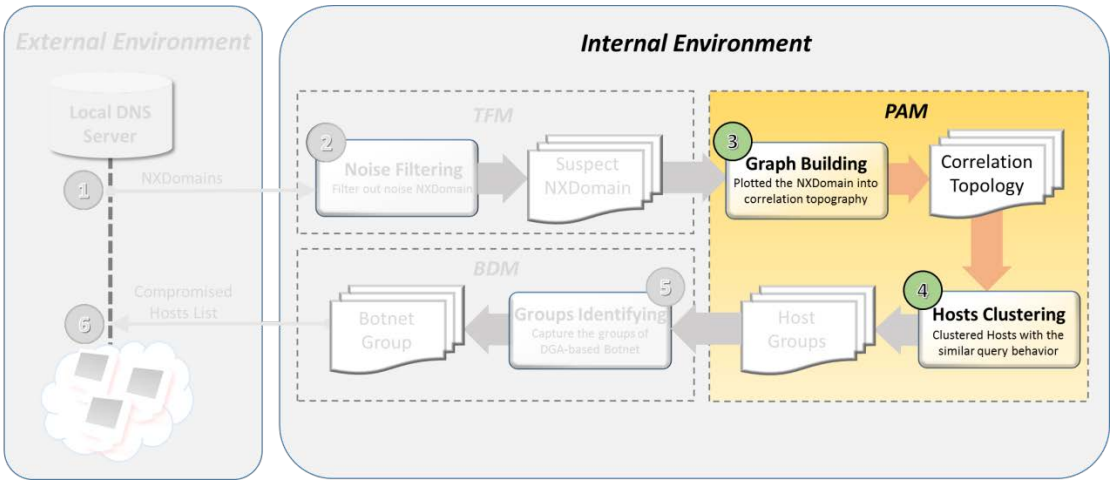


圖 15、殭屍網路偵測系統之 PAM 模組產生主機關聯圖

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 BAM 模組。

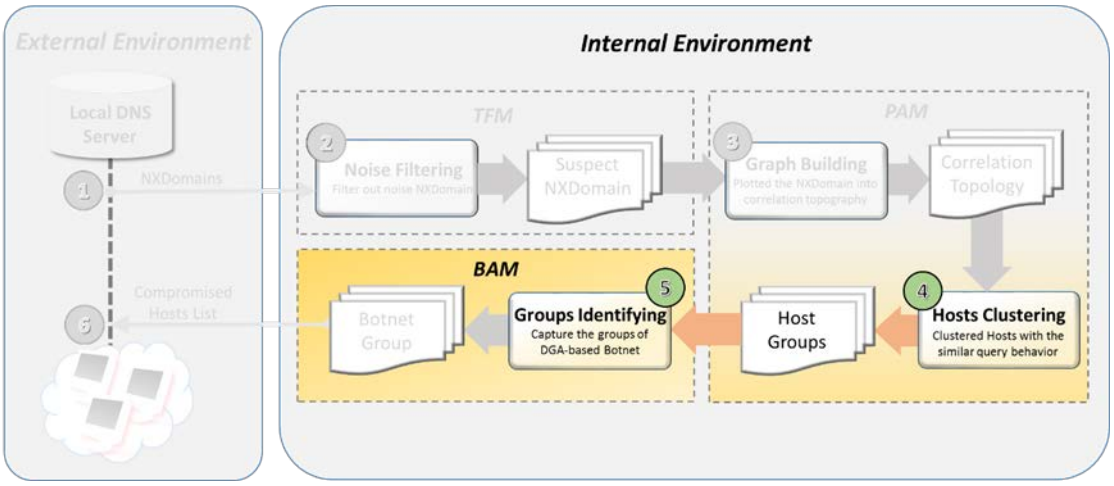


圖 16、殭屍網路偵測系統之 PAM 模組產生分群結果

場景 5: 產生辨識結果

BAM 模組利用群體內的失效查詢進行偵測，透過群體行為差異與網域字元分布等特徵以進行辨識，此階段可偵測出受感染主機黑名單以及分析出其與正常群體間之行為差異，最後產生殭屍網路辨識結果與分析報告。

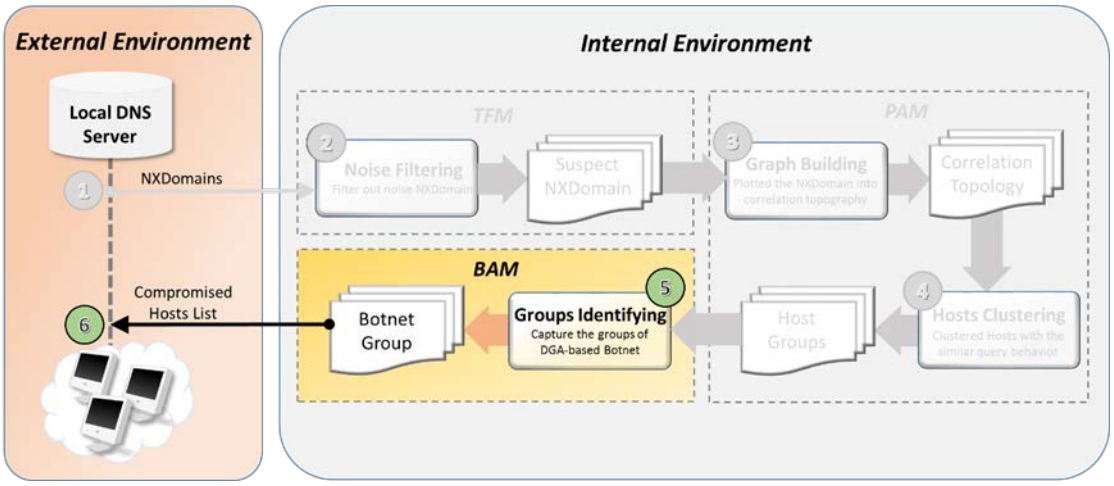


圖 17、殭屍網路偵測系統之 BDM 模組產生殭屍網路辨識結果

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。在雲端內部及區域網路製造流量，於 Collector 端驗證是否的確出現該流量。

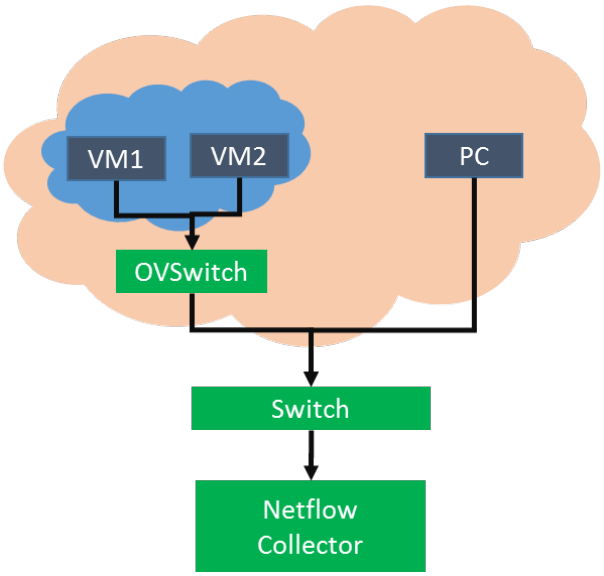


圖 18、產生雲端及區域網路之 Netflow 資料

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。

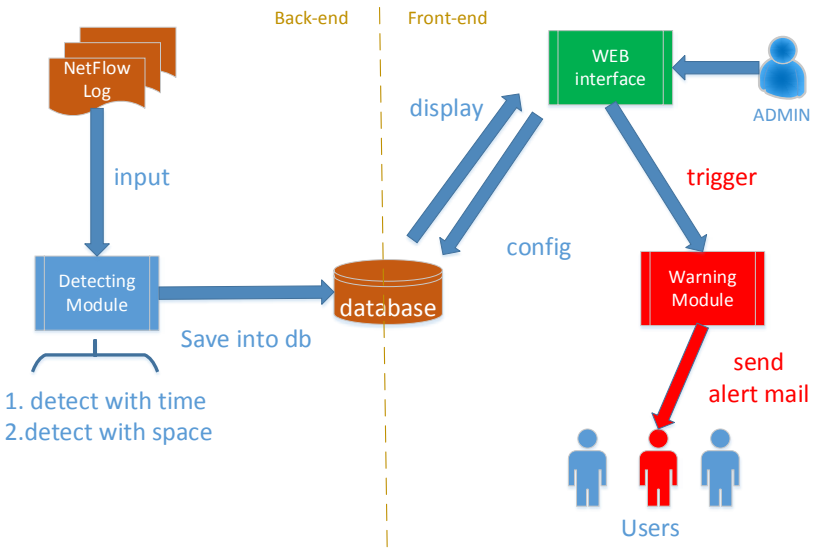


圖 19、偵測異常事件並以網頁介面呈現

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

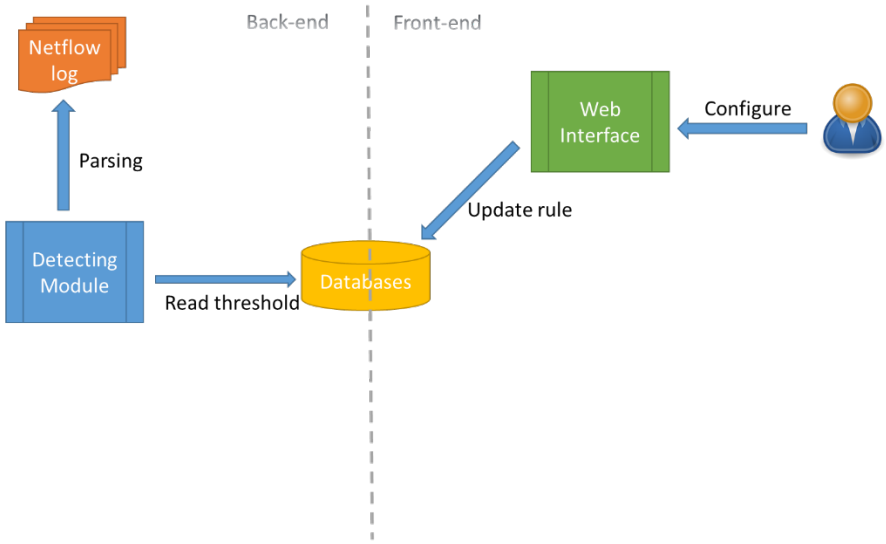


圖 20、調整門檻值進行偵測

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。

實驗場景為模擬企業遭到 APT 攻擊之情形，進行概念驗證。測試環境如下圖所示，將於可合法進行攻擊之平台上驗證。

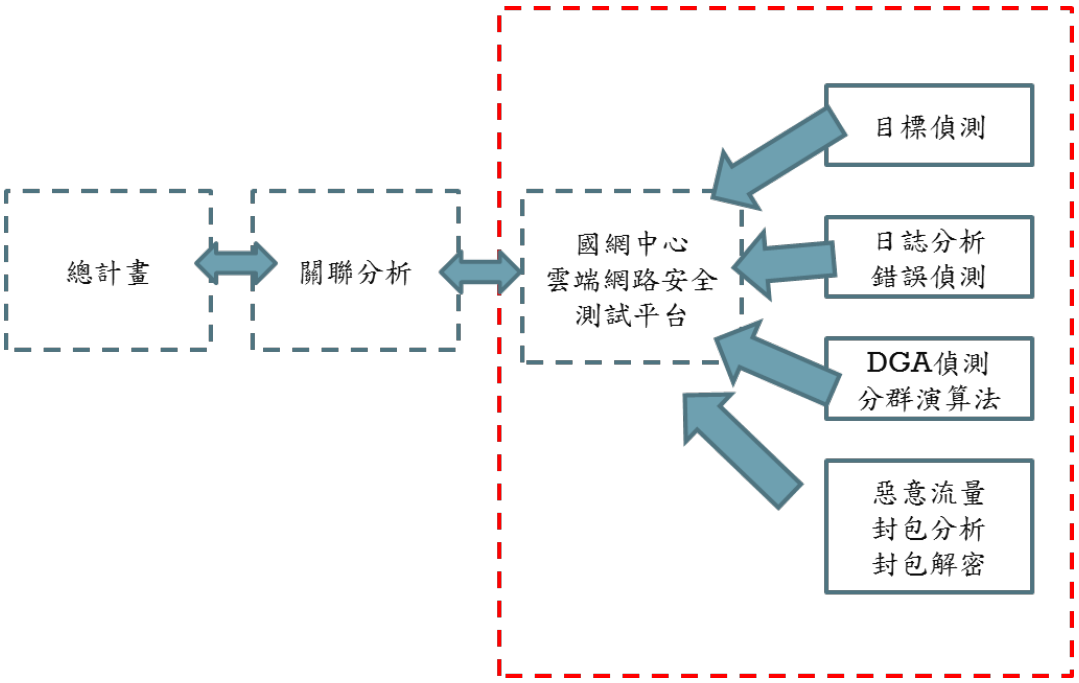


圖 21、整合測試場景

主要步驟有(1) 駭客會透過社交工程，將惡意程式植入在一般員工所使用的電腦中、(2)內部系統間橫向移動、(3)植入 DGA Bot

場景 1:社交工程攻擊

於外部網路建立惡意網址，透過社交工程方式傳送給使用者，使用者(192.168.6.151)點擊相關網址。

Source	Destination	Product	Application / Site	Application Risk
192.168.6.151	210.17.38.59	Application Control	Sina Services	Low
192.168.6.151	31.13.87.1	Application Control	Facebook	Low
192.168.6.151	74.120.121.34	Application Control	Plurk	Low
192.168.6.151	68.232.44.241	Application Control	Zemanta	Low
192.168.6.151	199.59.150.7			
192.168.6.151	199.16.156.102			
192.168.6.151	199.16.156.102			
192.168.6.151	199.16.156.102	Application Control	Twitter	Low
192.168.6.151	23.48.130.110	Application Control	Facebook	Low

Threat/Content Type	Source address	Destination address	Threat/Content Name
vulnerability	192.168.6.151	23.48.130.110	Snort URIContent Rules Detection Vulnerability(33334)

圖 22、偵測社交網路攻擊

場景 2: 橫向移動

攻擊者取得主機權限後，進行內部掃描及檔案上傳

event_type	src_ip	src_port	dst_ip	dst_port	attack_count
Flooding Flow	192.168.6.10	X	192.168.6.20	56902	2871
Flooding Flow	192.168.6.10	X	192.168.6.20	56902	2823
Flooding Flow	192.168.6.10	X	192.168.6.30	56902	2819
Brute Force	192.168.6.151	X	192.168.6.150	22	135

圖 23、偵測網路暴力破解密碼攻擊

場景 3:感染主機

IP	Frquency	Domain Detail
192.168.6.151	562	detail
192.168.6.89	562	detail

mt.liebiao.800fy.com
sr.liebiao.800fy.com
ed.liebiao.800fy.com
ep.liebiao.800fy.com
sn.www.uc088.com
wz.www.uc088.com
of.www.uc088.com
qj.www.uc088.com
gb.www.uc088.com

圖 24、偵測 DGA Botnet

3.4 壓力測試

其測試場景如總計畫接受測試之場景，並於接受測試時一併進行壓力測試。壓力測試結果顯示於 25 台節點模擬 250 人同時使用時，系統可在 0.4s 秒內回應。相關壓力測試結果如附錄 C 所示。

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-TR-003、 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 收集相關工作日誌記錄，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
	將所有系統的工作日誌記錄整合	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 的工作日誌記錄資料，以利工作日誌記錄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，就郵件紀錄、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。比對內外網對命令與控制伺服器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	工作日誌記錄資料進行關聯分析。	
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

	將所有系統的工作日誌記錄進行關聯	建立偵測系統的步驟
Expected Result	實驗過程中，本研究將所有 IDS 工作日誌記錄 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:

- 確認代理者 Agent (系統日誌伺服器)是否成功接收私有雲日誌。

表 10:CLS-AT-001 Case Test

Identification	CLS-AT-001	
Name	私有雲日誌接收確認	
Test Target	與網路儲存伺服器(NAS)連線	
Requirements	CLS-DC-002, CLS-FR-001, CLS-ER-003, CLS-OR-001, CLS-SR-001	
Severity	1(Critical)	
Instructions	Actor Actions	System response
	1.NAS 輸出測試日誌	
		2.成功接收後，Agent 會顯示該測試日誌訊息。
Expected Result	成功接收私有雲日誌	
Cleanup	無	

CLS-AT-002 Test Case

目的:

- 確認代理者 Agent (系統日誌伺服器)是否成功接收公有雲日誌。

表 11:CLS-AT-002 Case Test

Identification	CLS-AT-002	
Name	公有雲日誌接收確認	
Test Target	透過 Google API 與 Google Drive 進行連線	
Requirements	CLS-DC-001~002, CLS-FR-001, CLS-ER-001~002, CLS-OR-002	
Severity	1(Critical)	
Instructions	Actor Actions	System response
	1.Google API 輸出日誌	
		2. 成功接收後,Agent 會顯示該測試日誌訊息。
Expected Result	得到虛擬網橋、埠、介面資訊	
Cleanup	無	

CLS-AT-003 Test Case

目的:

- 建立存取整合式日誌的資料庫，並彙整於管理者介面。

表 12:CLS-AT-003 Case Test

Identification	CLS-AT-003	
Name	整合式管理者介面建立	
Test Target	確認代理者與日誌資料庫連線	
Requirements	CLS-FR-001~002, CLS-TL-001, CLS-IR-001	
Severity	1(Critical)	
Instructions	Actor Actions	System response
	1.日誌統整於資料庫	
		2.管理者介面顯示整合日誌資料
Expected Result	產生網路拓樸圖	
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 13: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-OR-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 14: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
	1. 取得失效查詢流量與白名單	
		2. 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 15: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 BAM 模組。

表 16: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-IR-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:

- BAM 模組利用群體內的失效查詢進行偵測，透過變點偵測、數量分布和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 17: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，進而產生殭屍網路辨識果。	
Requirements	MDD-AT-001~004, MDD-TR-006, MDD-TR-007, 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 18: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與一般交換器之流量	
		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 19: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 20: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 21、總計畫測試結果

Test Case #	Results(PASS/FAIL)	Comment
CDS-AT-001	PASS	相關掃描結果如圖所示。僅有低風險存在。相關檢測報告如附件。
CDS-AT-002	PASS	相關壓測結果如圖所示。相關檢測報告如附件。

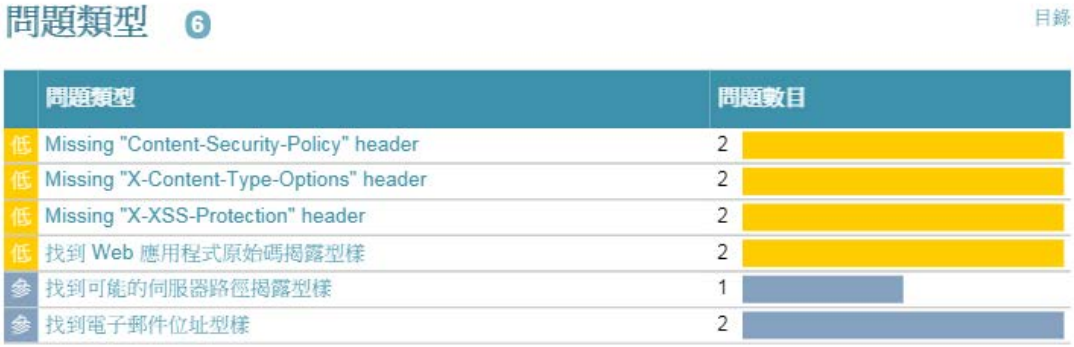


圖 25、弱點掃描結果

圖 26、壓力測試結果

子計畫一

表 22、子計畫一測試結果

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	**PASS**	功能正常

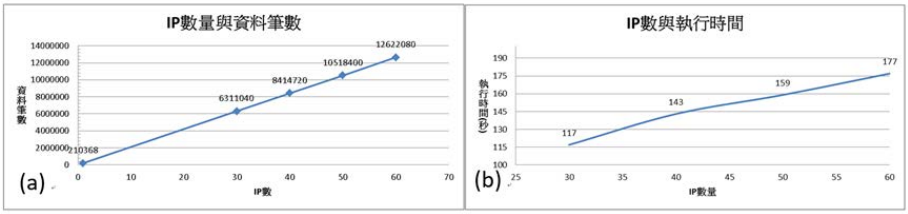


圖 27、BNM-AT-002

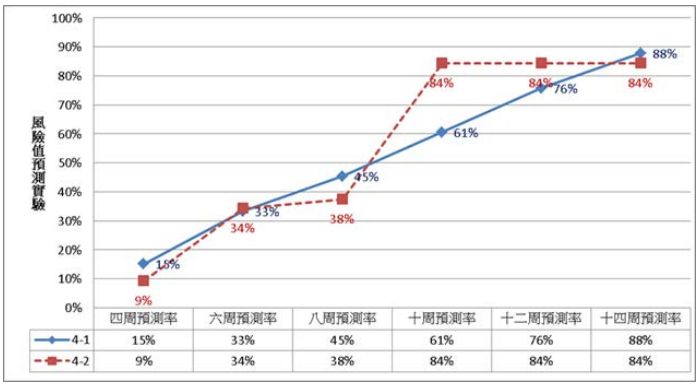


圖 28、BNM-AT-003

圖 29、BNM-AT-004

子計畫二

表 23、子計畫二測試結果

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

date	time	event	path	file	size	user	ip
Jun 13	16:45:11	rename	/homes/admin/test12.txt -> /homes/admin/test112.txt	File	0 Bytes	admin	192.168.163.137
Jun 13	16:45:18	create	/homes/admin/???????????????.txt	File	0 Bytes	admin	192.168.163.137
Jun 13	16:45:21	rename	/homes/admin/???????????????.txt -> /homes/admin/22.txt	File	0 Bytes	admin	192.168.163.137
Jun 13	16:45:29	delete	/homes/admin/test123.txt	File	0 Bytes	admin	192.168.163.137

圖 30、CLS-AT-001 測試結果

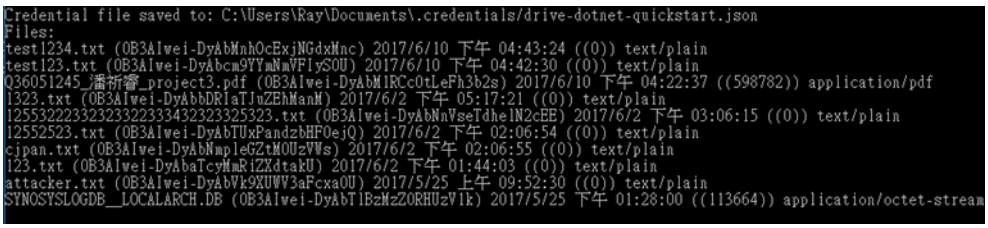


圖 31、CLS-AT-002 測試結果

子計畫三

表 24、子計畫三測試結果

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 所示
MDD -AT-005	PASS	可產生受駭主機清單與分析報告，如下圖 XXX 所示

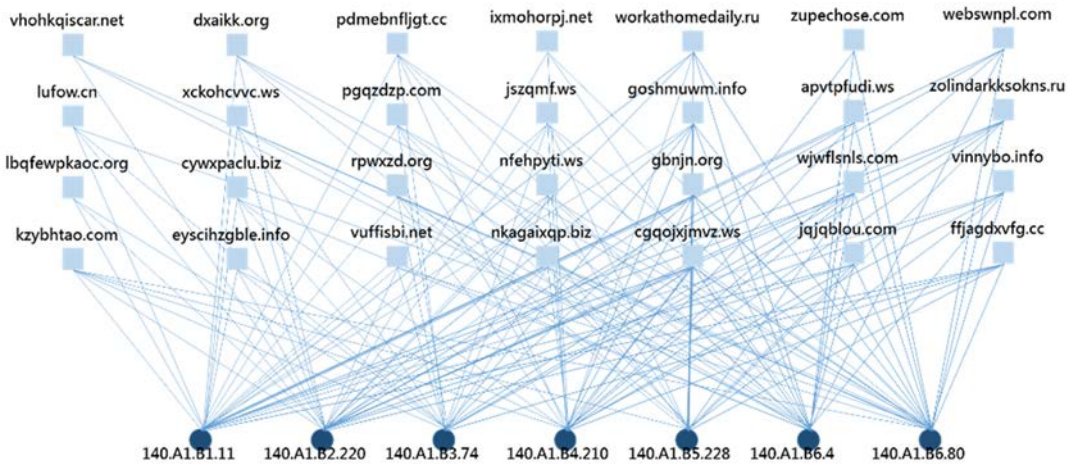
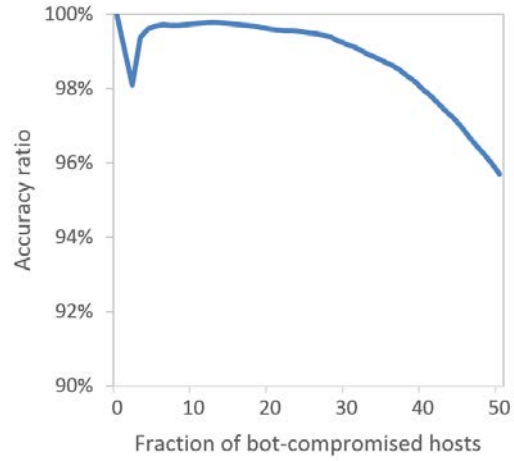
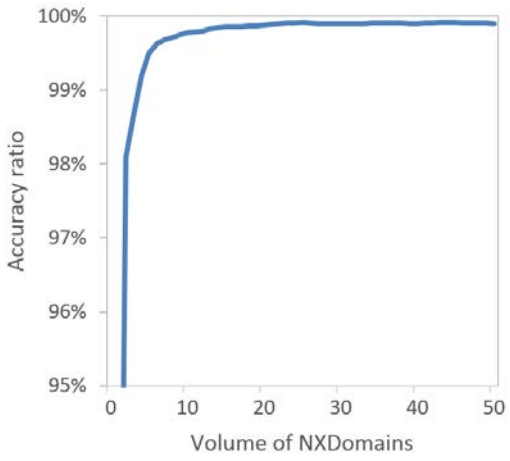


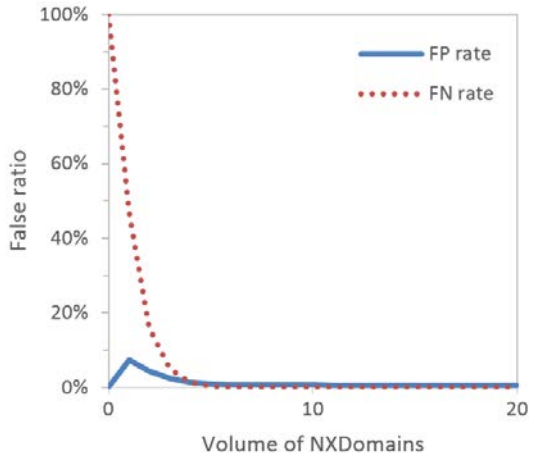
圖 32、MDD-AT-003



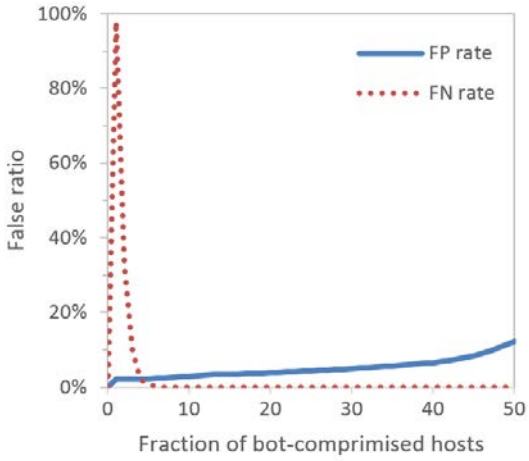
(a)



(b)

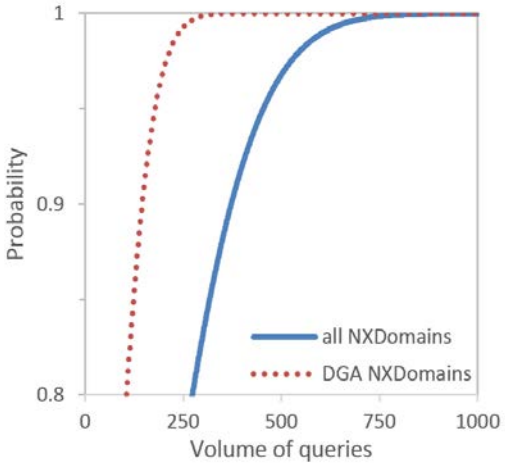


(c)

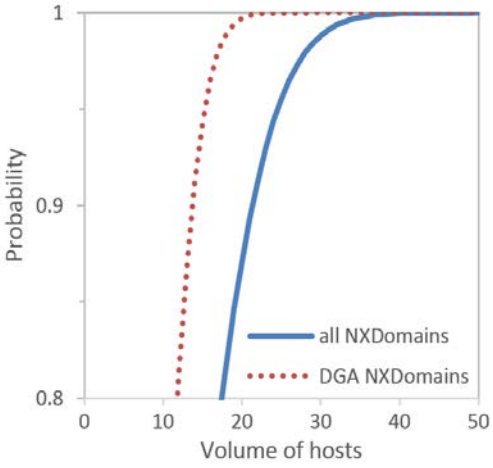


(d)

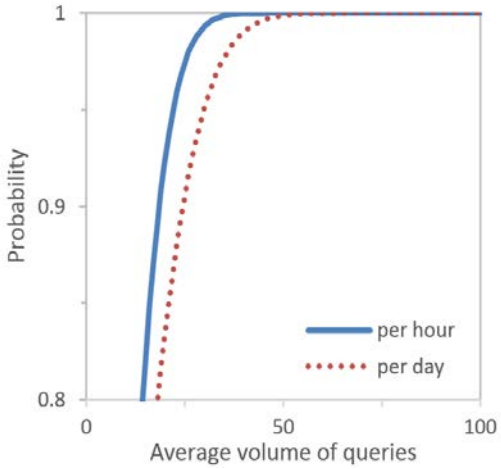
圖 33、MDD-AT-004


1
0.9
0.8
Probability
0
250
500
750
1000
Volume of queries
all NXDomains
DGA NXDomains

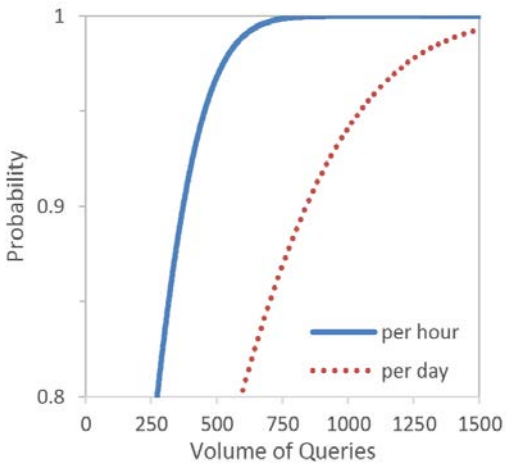
(a)


1
0.9
0.8
Probability
0
10
20
30
40
50
Volume of hosts
all NXDomains
DGA NXDomains

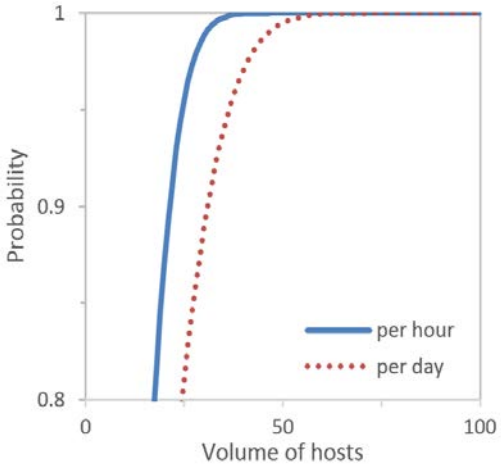
(b)


1
0.9
0.8
Probability
0
50
100
Average volume of queries
per hour
per day

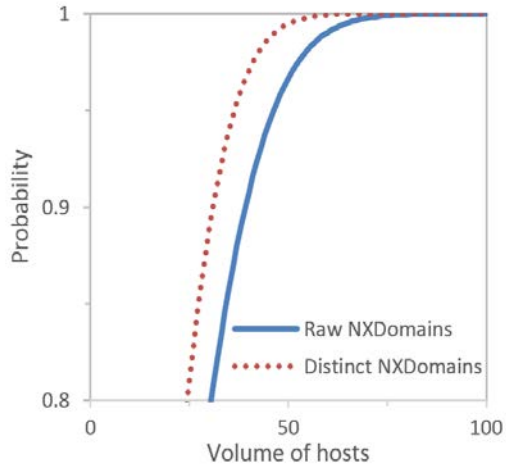
(c)


1
0.9
0.8
Probability
0
250
500
750
1000
1250
1500
Volume of Queries
per hour
per day

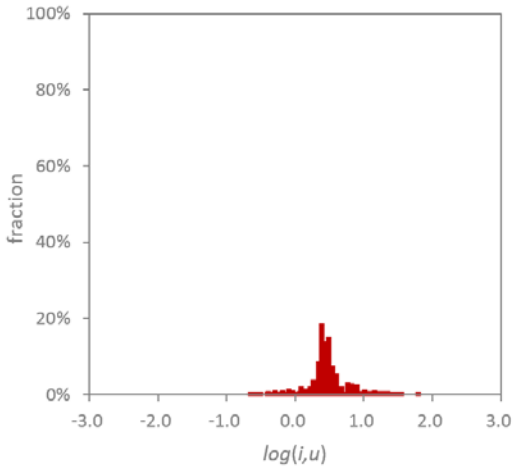
(d)


1
0.9
0.8
Probability
0
50
100
Volume of hosts
per hour
per day

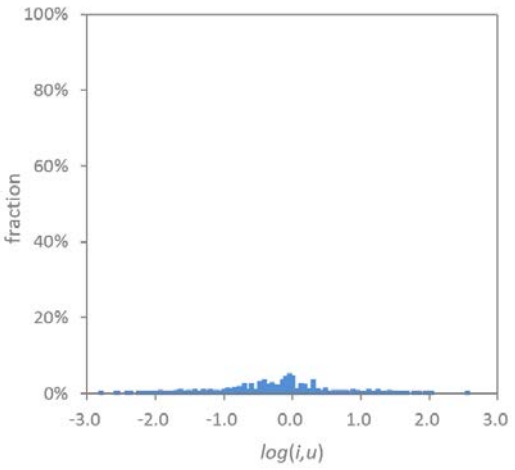
(e)


1
0.9
0.8
Probability
0
50
100
Volume of hosts
Raw NXDomains
Distinct NXDomains

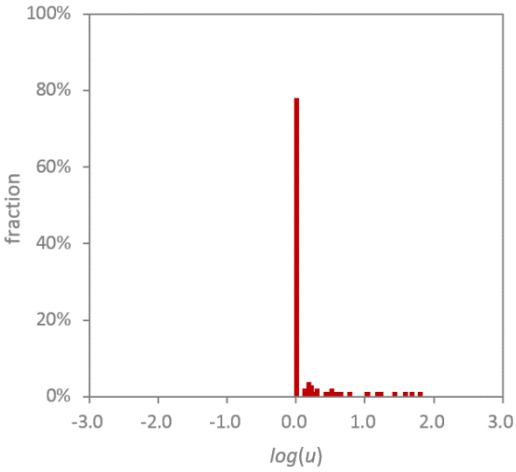
(f)



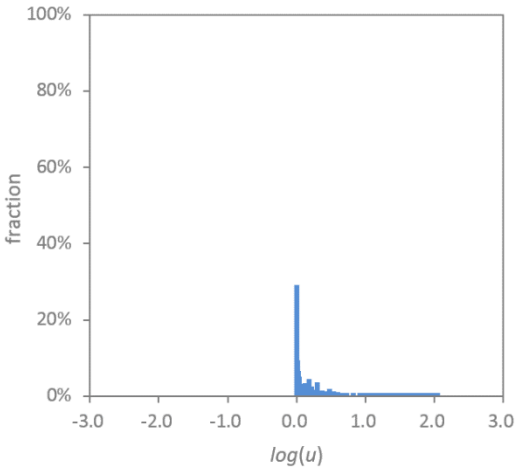
(g)



(h)



(i)



(j)

圖 34、MDD-AT-005

子計畫四

表 25、子計畫四測試結果

Test Case #	Results(PASS/FAIL)	Comment
CNM-AT-001	**PASS**	如下圖 CNM-AT-001 所示
CNM-AT-002	**PASS**	如下圖 CNM-AT-002 所示
CNM-AT-003	**PASS**	如下圖 CNM-AT-003 所示

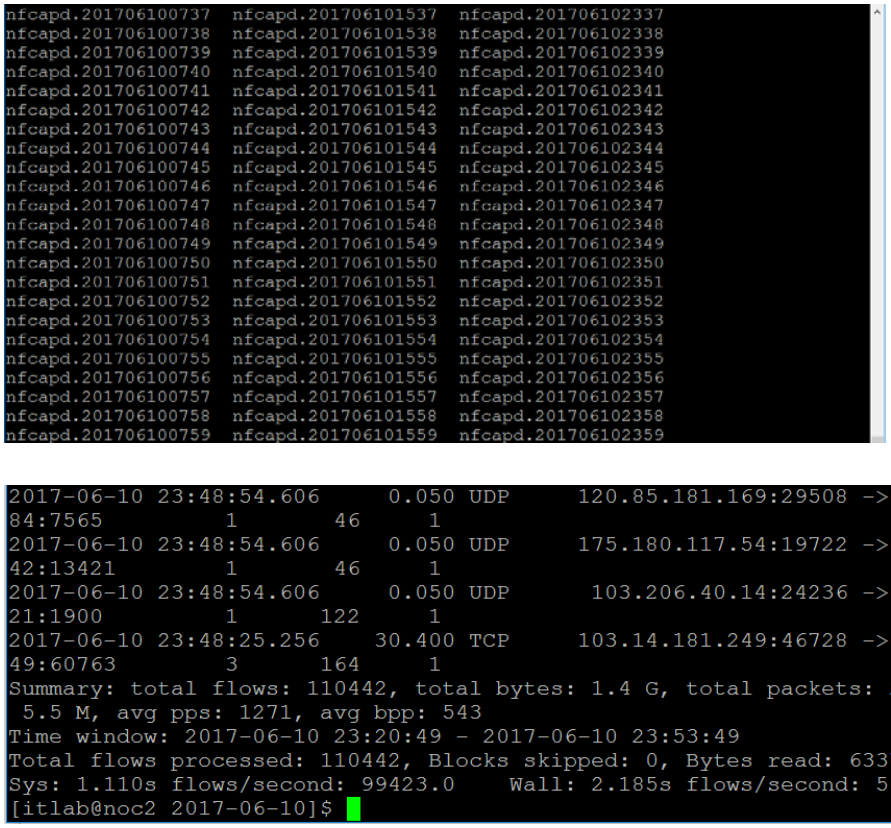


圖 35、CNM-AT-001

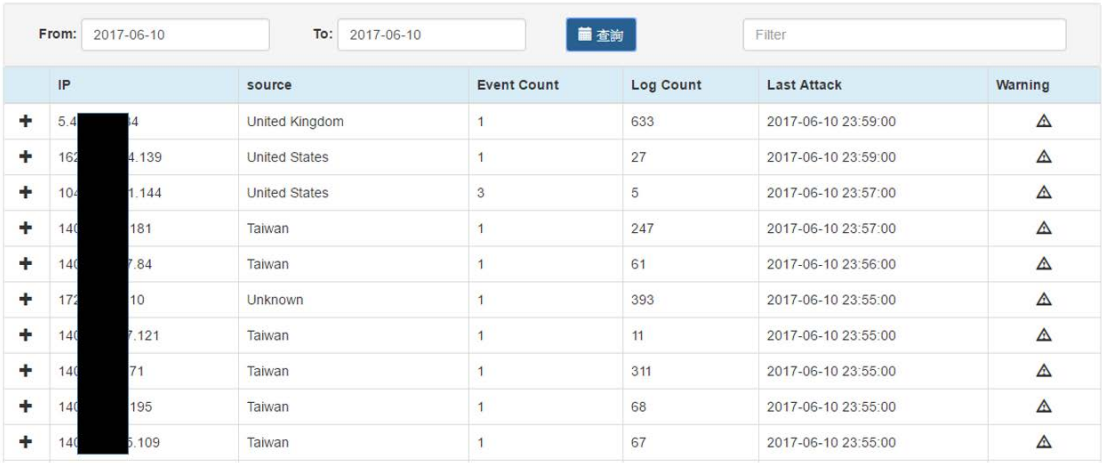


圖 36、CNM-AT-002

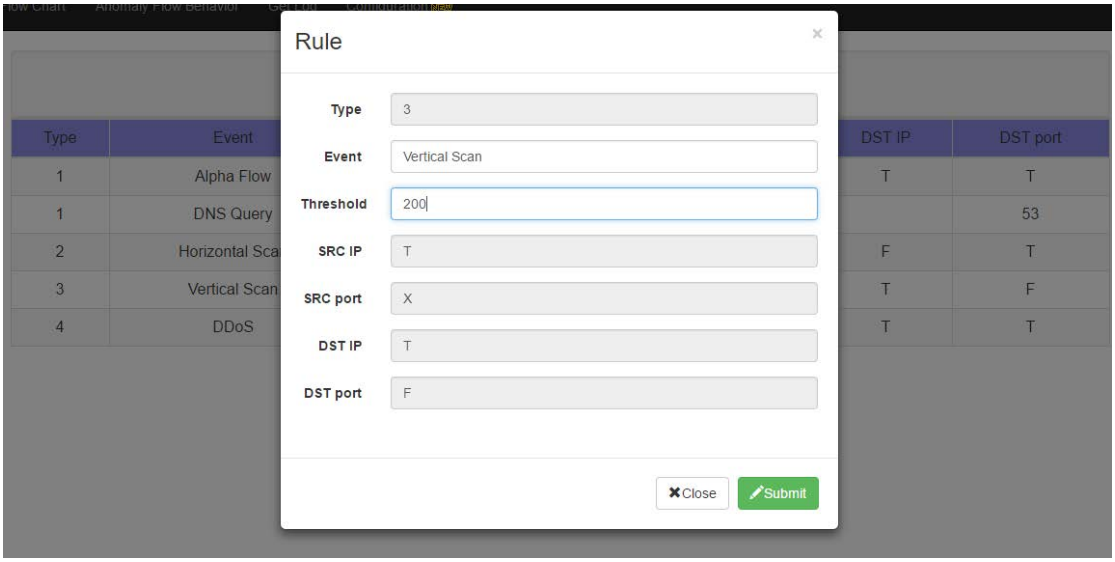


圖 37、CNM-AT-003

附錄 A 追朔表

總計畫追溯表

表 26、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 27、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-TR-003
CDS-AT-001	V	V	V
CDS-AT-002	V		

子計畫一追溯表

表 28、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 29、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 30:子計畫二 子系統 vs. 測試案例 追溯表

Sub System / Test Cases	RCM	UCM	AAM
CLS-TR-001	V		
CLS-TR-002		V	
CLS-TR-003			V

表 31: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-AT-001	V		
CLS-AT-002		V	
CLS-AT-003			V

子計畫三追溯表

表 32、子計畫三 子系統 vs. 測試案例 追溯表

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

表 33、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-TR-006
MDD-AT-001	V	V					
MDD-AT-002			V				
MDD-AT-003				V			
MDD-AT-004					V		
MDD-AT-005						V	V

子計畫四追溯表

表 34、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 35、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

附錄 B 總計畫弱點掃瞄報告

附錄 C 總計畫壓力測試報告

網頁伺服器效能評估報告

成大資通安全研究與教學中心

中華民國 106 年 6 月

目　次

檢測方式

本次測試為使用 Apache JMeter 工具軟體對受測單位提供的網址進行測試及效能評估。檢測方式是以腳本控制多台客戶端主機對網頁伺服器進行存取，測試方式如下：

測試方式

項目	內容
1.1	撰寫行為腳本，在客戶端主機上運行 Apache JMeter 進行模擬網頁存取之行為。

1. 客戶端主機使用 Public IP。
2. 客戶端主機作業系統為 Ubuntu 16.04 with kernel 2.6.18-194
3. Apache JMeter 版本為 2.12

本報告中的內容為本單位於 106 年 6 月 12 日對受測單位指定網址進行檢測的結果，僅供參考，不代表伺服器之實際運作狀況。

測試結果

Apache JMeter 測試結果

10 連線數測試 (HTTP)

節點模擬同時間共 50 個 http 連線數對網頁伺服器運行腳本，每個客戶端同一時間有 2 個連線數，測試腳本包含以下的 URL：

測試時間

2017 年 6 月 12 日 09:14 ~ 10:03

測試結果

URL	Average time (ms)	Error Rate	錯誤發生原因
http://140.116.221.14:5601	120	0.00%	
http://140.116.221.14:5601/app/kibana	103	0.00%	
http://140.116.221.14:5601/app/kibana#/discover	99	0.00%	
http://140.116.221.14:5601/elasticsearch/.kibana/_mapping/*/field/_source	171	0.00%	
http://140.116.221.14:5601/app/kibana#/visualize	98	0.00%	
http://140.116.221.14:5601/app/kibana#/visualize/step/1	111	0.00%	
http://140.116.221.14:5601/app/kibana#/visualize/edit/%E5%85%B1%E5%90%8C%E6%83%85%E8%B3%87%E5%88%86%E6%9E%90-Top-20%E6%94%BB%E6%93%8A%E4	103	0.00%	

%BA%8B%E4%BB%B6			
http://140.116.221.14:5601/app/kibana#/visualize/edit/%E5%85%B1%E5%90%8C%E6%83%85%E8%B3%87-(Trojan.Ransom)%E7%B6%B2%E5%9F%9F%E9%BB%91%E5%90%8D%E5%96%AE	78	0.00%	
Average	110.375	0.00%	

20 **連線數測試 (HTTP)**

節點模擬同時間共 100 個 https 連線數對網頁伺服器運行腳本，每個客戶端同一時間有 4 個連線數，測試腳本包含以下的 URL：

測試時間

2017 年 6 月 12 日 10:10 ~ 10:13

測試結果

URL	Average time (ms)	Error Rate	錯誤發生原因
http://140.116.221.14:5601	159	0.00%	
http://140.116.221.14:5601/app/kibana	256	0.00%	
http://140.116.221.14:5601/app/kibana#/discover	199	0.00%	
http://140.116.221.14:5601/elasticsearch/.kibana/_mapping/*/field/_source	246	0.00%	
http://140.116.221.14:5601/app/kibana#/visualize	120	0.00%	
http://140.116.221.14:5601/app/kibana#/visualize/step/1	91	0.00%	
http://140.116.221.14:5601/app/kibana#/visualize/edit/%E5%85%B1%E5%90%8C%E6%83%85%E8%B3%87%E5%88%86%E6%9E%90-Top-20%E6%94%BB%E6%93%8A%E4%BA%8B%E4%BB%B6	63	0.00%	
http://140.116.221.14:5601/app/kiban	53	0.00%	

a#/visualize/edit/%E5%85%B1%E5%90%8C%E6%83%85%E8%B3%87-(Trojan.Ransom)%E7%B6%B2%E5%9F%9F%E9%BB%91%E5%90%8D%E5%96%AE			
Average	148.375	0.00%	

40 **連線數測試 (HTTP)**

節點模擬同時間共 150 個 http 連線數對網頁伺服器運行腳本,每個客戶端同一時間有 6 個連線數，測試腳本包含以下的 URL：

測試時間

2017 年 6 月 12 日 10:20 ~ 10:23

測試結果

URL	Average time (ms)	Error Rate	錯誤發生原因
http://140.116.221.14:5601	211	0.00%	
http://140.116.221.14:5601/app/kibana	278	0.00%	
http://140.116.221.14:5601/app/kibana#/discover	386	0.00%	
http://140.116.221.14:5601/elasticsearch/.kibana/_mapping/*/field/_source	76	0.00%	
http://140.116.221.14:5601/app/kibana#/visualize	264	0.00%	
http://140.116.221.14:5601/app/kibana#/visualize/step/1	296	0.00%	
http://140.116.221.14:5601/app/kibana#/visualize/edit/%E5%85%B1%E5%90%8C%E6%83%85%E8%B3%87%E5%88%86%E6%9E%90-Top-20%E6%94%BB%E6%93%8A%E4%BA%8B%E4%BB%B6	204	0.00%	

http://140.116.221.14:5601/app/kibana#/visualize/edit/%E5%85%B1%E5%90%8C%E6%83%85%E8%B3%87-(Trojan.Ransom)%E7%B6%B2%E5%9F%9F%E9%BB%91%E5%90%8D%E5%96%AE	191	0.00%	
Average	238.25	0.00%	

60 **連線數測試 (HTTP)**

節點模擬同時間共 200 個 http 連線數對網頁伺服器運行腳本,每個客戶端同一時間有 8 個連線數，測試腳本包含以下的 URL：

測試時間

2017 年 6 月 12 日 10:30 ~ 10:33

測試結果

URL	Average time (ms)	Error Rate	錯誤發生原因
http://140.116.221.14:5601	309	0.00%	
http://140.116.221.14:5601/app/kibana	516	0.00%	
http://140.116.221.14:5601/app/kibana#/discover	398	0.00%	
http://140.116.221.14:5601/elasticsearch/.kibana/_mapping/*/field/_source	312	0.00%	
http://140.116.221.14:5601/app/kibana#/visualize	226	0.00%	
http://140.116.221.14:5601/app/kibana#/visualize/step/1	464	0.00%	
http://140.116.221.14:5601/app/kibana#/visualize/edit/%E5%85%B1%E5%90%8C%E6%83%85%E8%B3%87%E5%88%86%E6%9E%90-Top-20%E6%94%BB%E6%93%8A%E4%BA%8B%E4%BB%B6	355	0.00%	
http://140.116.221.14:5601/app/kiban	197	0.00%	

a#/visualize/edit/%E5%85%B1%E5%90%8C%E6%83%85%E8%B3%87-(Trojan.Ransom)%E7%B6%B2%E5%9F%9F%E9%BB%91%E5%90%8D%E5%96%AE			
Average	347.125	0.00%	

80 **連線數測試 (HTTP)**

節點模擬同時間共 250 個 http 連線數對網頁伺服器運行腳本，每個客戶端同一時間有 10 個連線數，測試腳本包含以下的 URL：

測試時間

2017 年 6 月 12 日 10:40 ~ 10:43

測試結果

URL	Average time (ms)	Error Rate	錯誤發生原因
http://140.116.221.14:5601	284	0.00%	
http://140.116.221.14:5601/app/kibana	528	0.00%	
http://140.116.221.14:5601/app/kibana#/discover	622	0.00%	
http://140.116.221.14:5601/elasticsearch/.kibana/_mapping/*/field/_source	527	0.00%	
http://140.116.221.14:5601/app/kibana#/visualize	250	0.00%	
http://140.116.221.14:5601/app/kibana#/visualize/step/1	271	0.00%	
http://140.116.221.14:5601/app/kibana#/visualize/edit/%E5%85%B1%E5%90%8C%E6%83%85%E8%B3%87%E5%88%86%E6%9E%90-Top-20%E6%94%BB%E6%93%8A%E4%BA%8B%E4%BB%B6	251	0.00%	

http://140.116.221.14:5601/app/kibana#/visualize/edit/%E5%85%B1%E5%90%8C%E6%83%85%E8%B3%87-(Trojan.Ransom)%E7%B6%B2%E5%9F%9F%E9%BB%91%E5%90%8D%E5%96%AE	140	0.00%	
Average	359.125	0.00%	

100 **連線數測試 (HTTP)**

節點模擬同時間共 250 個 http 連線數對網頁伺服器運行腳本,每個客戶端同一時間有 10 個連線數，測試腳本包含以下的 URL：

測試時間

2017 年 6 月 12 日 10:51 ~ 10:53

測試結果

URL	Average time (ms)	Error Rate	錯誤發生原因
http://140.116.221.14:5601	360	0.00%	
http://140.116.221.14:5601/app/kibana	818	0.00%	
http://140.116.221.14:5601/app/kibana#/discover	651	0.00%	
http://140.116.221.14:5601/elasticsearch/.kibana/_mapping/*/field/_source	243	0.00%	
http://140.116.221.14:5601/app/kibana#/visualize	210	0.00%	
http://140.116.221.14:5601/app/kibana#/visualize/step/1	426	0.00%	
http://140.116.221.14:5601/app/kibana#/visualize/edit/%E5%85%B1%E5%90%8C%E6%83%85%E8%B3%87%E5%88%86%E6%9E%90-Top-20%E6%94%BB%E6%93%8A%E4%BA%8B%E4%BB%B6	177	0.00%	
http://140.116.221.14:5601/app/kiban	82	0.00%	

a#/visualize/edit/%E5%85%B1%E5%90%8C%E6%83%85%E8%B3%87-(Trojan.Ransom)%E7%B6%B2%E5%9F%9F%E9%BB%91%E5%90%8D%E5%96%AE			
Average	370.875	0.00%	