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

**基於Hadoop平台之APT攻擊大數據分析研究**

**MOST 105-2221-E-261-003-MY2**

**賴谷鑫**

**臺灣警察專科學校 科技偵查科**

Department of Technology Crime Investigation

Ministry of Science and Technology, Taiwan

107/05/14

# 文件版本修正履歷表

|  |  |  |  |
| --- | --- | --- | --- |
| 編號： | MOST 105-2221-E-261-003-MY2 | | |
| 名稱： | 基於Hadoop平台之APT攻擊大數據分析研究 | | |
|  | | | |
| **修訂次序** | **核準日期** | **版本** | **修訂內容** |
| 1 | 107/05/14 | 1.00 | 發行初版 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**版本: 1.00**

# 目錄

[文件版本修正履歷表 2](#_Toc485221060)

[目錄 3](#_Toc485221061)

[1 簡介 4](#_Toc485221062)

[1.1 測試範圍 4](#_Toc485221063)

[1.2 接受準則 4](#_Toc485221064)

[2 測試環境 5](#_Toc485221065)

[2.1 硬體規格 7](#_Toc485221066)

[2.2 軟體規格 7](#_Toc485221067)

[2.3 測試資料來源 8](#_Toc485221068)

[3 測試時程、程序 8](#_Toc485221069)

[3.1 測試時程 8](#_Toc485221070)

[3.2 接受測試程序 8](#_Toc485221071)

[4 測試案例 10](#_Toc485221072)

[5 測試結果與分析 13](#_Toc485221073)

[6 追朔表 13](#_Toc485221074)

# 簡介

本研究以雲端平台 Hadoop 以及 Spark 為基礎整合以及關聯巨量的資安設備紀錄檔。並提出一套以隱藏馬可夫模型為基礎的偵測模型，透過狀態與觀察值的給定來進行狀態轉移，藉此找出是否有目標正遭受到 APT 攻擊。本計畫第二年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，利用隱藏馬可夫鍊方式建立模型。以偵測APT 攻擊。由於進階持續性滲透攻擊在進行滲透階段時，大多採用寄發社交工程信件的方式進行滲透，因此，在本系統中將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，偵測低頻率持續性滲透攻擊。透過真實資料的收集與分析建立隱藏馬可夫鍊模型以偵測APT攻擊。

## 測試範圍

本文件主要是建置雲端環境下以馬可夫鍊為模型的APT攻擊偵測。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，故本計畫著重於及接受度測試(Acceptance Test)。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。

## 接受準則

本測試計畫總計畫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1:接受測試需求項目表

| 測試需求編號 | 必要性 | 需求內容 |
| --- | --- | --- |
| HMM-TR-001 | 必要 | 必須可以上傳日誌檔 |
| HMM-TR-002 | 必要 | 必須可以擷取巨量資料 |
| HMM-TR-003 | 必要 | 必須可以將日誌檔根據定義之特徵值拆解不同欄位 |
| HMM-TR-004 | 必要 | 必須可以產出可疑IP |
| HMM-TR-005 | 必要 | 必須可以提供可疑IP查詢介面 |

# 測試環境

本計畫第二年主要設計一套系統，該系統可以讀取上傳的日誌檔，並且透過透過隱藏馬可夫模型(Hidden Markov Model)將狀態的發生機率與各狀態給定的觀察值來進行各狀態之間轉移推論，藉此偵測整個進階持續性滲透攻擊模型，並藉此來找出是否有目標已遭受到進階持續性滲透攻擊。本系統測試環境架構圖如下圖1。



圖1:測試環境圖

## 硬體規格

* + Intel i5 7500或以上相容處理器
  + 16GB以上的記憶體
  + 40GB以上剩餘磁碟空間(系統程式本身)

## 軟體規格

* + 作業系統：Ubuntu 10.04 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)

## 測試資料來源

本研究資料來源是利用真實企業(安碁資訊)所提供的範例紀錄檔，包含checkpoint、palo alto等多種不同設備所產出的紀錄檔。

# 測試時程、程序

## 測試時程

各模組單元測試 (Unit Test) (自107/2/1起，應於107/4/20完成)

系統接受度測試(Acceptance Test) (自107/2/28起，應於106/5/1完成)

查核點

* 系統整合與整合測試(107/5/20)
* 系統測試完成(107/7/1)

## 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。各模組的元件測試，由各模組的開發負責人執行，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。

場景1(如下圖2)：日誌檔收集與整合 (HMM-AT-001)



圖2:場景1

場景2(如下圖3)：Log 關聯模組(HMM-AT-002)。對mail log、IPS log等行為進行關聯後再進行IP 比對，判斷是否符合重要角色名單，如下圖所示：



圖3:場景2

場景3(如下圖4)：利用狀態序列紀錄進行偵測模組(HMM-AT-003)。將所有紀錄做狀態序列計算後，輸入到HMM偵測系統進行分析。



圖4:場景3

# 測試案例

目的：

* 驗證系統可以處理日誌檔
* 驗證系統可以利用HMM模式找出可疑IP

表2: HMM-AT-001

|  |  |  |
| --- | --- | --- |
| Identification | HMM-AT-001 | |
| Name | 日誌檔收集與整合 | |
| Test Target | 確保日誌檔正確被處理 | |
| Requirements | HMM-FR-001，HMM-PR-001，HMM-DR-001，HMM-TR-001，HMM-TR-002，HMM-TR-003，HMM-TR-003 | |
| Severity | 必要 | |
| Instructions | Actor Actions | System response |
| 將所有系統的log整合 | 顯示已整合的log檔案 |
| Expected Result | 實驗過程中，本研究整合多個IDS的log資料，以利log資料輸入正確並快速辨識。 | |
| Cleanup | 無 | |

目的

* 驗證系統關聯正確性
* 驗證IP比對正確性

表3: HMM-AT-002

|  |  |  |
| --- | --- | --- |
| Identification | HMM-AT-002 | |
| Name | log資料進行關聯 | |
| Test Target | 將所有log資料進行關聯，有效找到正確的APT步驟 | |
| Requirements | HMM-FR-003，HMM-PR-001，HMM-DR-001，  HMM-TR-002 | |
| Severity | 必要 | |
| Instructions | Actor Actions | System response |
| 將所有系統的log進行關聯 | 關聯之log檔 |
| Expected Result | 實驗過程中，本研究將所有IDS log 進行關聯分析，得到有效的APT步驟。 | |
| Cleanup | 無 | |

目的

* 紀錄狀態序列
* 紀錄觀察序列
* HMM異常行為分析

表4: HMM-AT-003

|  |  |  |
| --- | --- | --- |
| Identification | HMM-AT-003 | |
| Name | 將所有紀錄進行狀態序列的計算，以便輸入HMM系統中進行分析。 | |
| Test Target | 測試是否可以透過HMM模式偵測可疑IP | |
| Requirements | HMM-DR-001，HMM-FR-001，HMM-FR-003 | |
| Severity | 必要 | |
| Instructions | Actor Actions | System response |
| 將所有關聯分析後的資料進行狀態序列計算 | 可疑IP報表 |
| Expected Result | 實驗過程中，token與sub-message被系統正確處理，並產生parser 設定檔 | |
| Cleanup | 無 | |

# 測試結果與分析

表5:測試結果表

|  |  |  |
| --- | --- | --- |
| **Test Case #** | **Results(PASS/FAIL)** | **Comment** |
| HMM-AT-001 | PASS |  |
| HMM -AT-002 | PASS |  |
| HMM -AT-003 | PASS |  |

# 追朔表

表6:系統需求 vs. 測試案例

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Test Case #** | LP-SFR-001 | LP-SFR-002 | LP-SFR-003 | LP-SFR-004 | LP-SFR-005 |
| HMM-AT-001 | V | V | V |  |  |
| HMM-AT-002 | V | V | V |  |  |
| HMM-AT-003 |  |  |  | V | V |