



# 網路安全

## 安全強化暨數位鑑識

111-04-22 上午，9:00~12:00

時間 3 小時

組別編號：	
選手姓名：	

### 注意事項：

1. 開始比賽前勿翻閱試題。
2. 請先在本試題封面寫上姓名、組別編號。
3. 比賽後請將試題留在座位上，紙筆也不得攜出試場。
4. 作答時，同組可小聲討論，但不得與他組交談，且音量不可影響他人作答。
5. 比賽期間選手可經裁判同意，由專人陪同上廁所，惟不得與他人交談。
6. 參賽者不得以任何方式干擾其他隊伍，若影響考試秩序且經勸導無效者將取消該組競賽資格。
7. 選手拿到隨身碟後，請馬上更改隨身碟中的答案卷檔名。例如「...第 X 組...」改成「...第 20 組...」

## 試題環境主機

1. [noname] 登入資訊：webadmin / P@ssw0rd!
    - Ubuntu 20.14 Desktop
    - 2GB RAM & 30GB Disk & 1 Core CPU
  2. [inzhi] 登入資訊：user / P@ssw0rd!
    - Windows 10 Pro
    - 4GB RAM & 60GB Disk & 2 Cores CPU
- 

## 任務一：電腦及網路安全系統強化 (20 分)

明明是公司新進資訊人員，正在進行在職訓練，過程中遇到如下各式問題，請你給予協助。

### (一) 網站安全強化 (使用 noname 主機)

1. 由於明明不熟悉 Apache 網頁伺服器的設定，以致發生 **IndexOf 目錄結構洩漏**的問題，請你協助解決此問題。

#### 答題要求：

- (1) 將 `http://127.0.0.1/config/` 顯示的畫面截圖以及 `apache2.conf` 的設定畫面截圖(只截取與答案相關的部分即可)，並貼至答案卷試題 1 中。
- (2) 此設定需能夠確保日後新增任意目錄也不會發生 IndexOf 目錄結構洩漏問題。
2. 明明聽說 PHP 裡有些函數可使伺服器執行系統指令，例如 `xxxxx('ping 1.1.1.1')`；可使伺服器執行 `ping 1.1.1.1` 指令，所以 `xxxxx` 被視為**危險函數**。上司要他將這些**危險函數都找出來並禁止使用(disable)**，請你協助他進行正確的設定 (僅需考慮適用於 noname 機器上的 PHP 環境即可)。

#### 答題要求：

- (1) 請連上 `http://127.0.0.1/php1nf0.php`，將包含 **Disable Function 區塊**的畫面截圖並貼至答案卷試題 2 上。
- (2) 設定過程中可擷取 1~2 個畫面並貼至答案卷試題 2 當作佐證資料。

## (二) MySQL (使用 noname 主機)

- 明明剛接手管理一個 MySQL Server (帳號為 `root@localhost`，無密碼)，發現 SDC 資料庫的 `SDC_user` 資料表混雜一般使用者帳號與具管理員權限的帳號，如此增加特權帳號管理的資安風險。為降低此風險，請你協助他列舉 `SDC_user` 資料表內所有具管理員權限的帳號，並將列舉結果截圖貼至答案卷試題 3 中。
- 請你協助明明將擁有管理員權限的帳號從 `SDC_user` 資料表中移除，並加入至 `SDC_admin` 資料表，後者沿用 `SDC_user` 的資料結構。請輸出 `SDC_admin` 內的所有資料，並將輸出結果以及你使用的 SQL 指令截圖貼至答案卷試題 4 中。

## (三) 事件稽核 (使用 inzhi 主機)

明明也要管理公司的 Windows 伺服器，他聽說 Windows 內建的 PowerShell 可以撰寫簡潔的程式來協助他管理系統，因此對下列上司交付的任務躍躍欲試，請你協助他完成任務。

- 請撰寫 PowerShell Script 讀出今天之前 Windows 安全事件代號 4688 的發生次數。請你將 PowerShell Script 完整內容及執行後的輸出結果截圖並貼至答案卷試題 5 中。
- 請找出 2022/4/11 登入密碼錯誤事件的發生次數並將答案數字寫在答案卷試題 6 中。

## (四) 效能監控 (使用 inzhi 主機)

- 明明的上司要求他根據以下需求去設定效能資料收集器集合工具
  - 資料收集器集合工具名稱：**Monitor\_MAYDAY**
  - 新增資料收集器
    - 名稱：**RAM**
    - 類型：效能計數器資料收集器
    - 收集資料：**Memory：Committed Bytes in Use、Available Mbyte**
    - 抽樣間隔：5 秒
  - 新增資料收集器
    - 名稱：**CPU**
    - 類型：效能計數器資料收集器
    - 收集資料：**Processor：% Processor Time、% Idle Time**
    - 抽樣間隔：10 秒

### 答題要求：

請將此集合工具產生的效能報告畫面截圖貼至答案卷試題 7 中，並將「資料收集器集合工

具 Monitor\_MAYDAY」儲存成 xml 範本存入隨身碟。

---

## 任務二：數位鑑識與證據蒐集調查 (共 40 分)

### (一) 記憶體分析

基德是資安調查人員，最近接到有關妨害電腦使用罪的案件委託，其中 **Task01.mem** 是從受害主機 Dump 出的記憶體資訊檔，請協助基德分析該檔案並回答以下問題。

8. 該主機目前使用的**作業系統版本**為何？
9. 該主機目前執行的**惡意軟體名稱**、**PID**、**實體路徑**為何？
10. 該主機的**電腦名稱**及**當前使用者名稱**為何？
11. 該主機執行的**惡意軟體的程式參數**為何？
12. 該主機連線到惡意伺服器所使用的 **IP** 及**連接埠**為何？

### (二) 硬碟分析

在上題妨害電腦使用罪的委託案件中，受害者的私鑰遺失且**加密錢包助記詞**被駭客加密，以致於無法使用錢包，為此基德導出關鍵的硬碟映像檔 **victim.E01**，請你根據以下基德的步驟將受害者的助記詞圖片還原出來。

13. 從硬碟映像檔找到**助記詞加密檔案**。請計算該檔案的 **SHA1** 值，並將該值寫在答案卷試題 13 中
14. 從硬碟映像檔找到**加密程式**。請計算該檔案的 **SHA1** 值，並將該值寫在答案卷試題 14 中
15. 使用上面的加密程式對助記詞加密檔案進行解密。請將**解密指令畫面**及**解密後的助記詞圖片**截圖貼至答案卷試題 15 中。

(溫馨提示：此部分與記憶體分析行為具有關聯性線索)

-----**試題結束**-----