第 50 屆全國技能競賽分區賽

網路安全職類

網路安全防禦試題

109-4-24 上午，時間 3 小時

崗位編號：_____　　選手姓名：_____

注意事項：

1. 開始答題前**手機請設靜音**模式，同時**勿翻閱試題**。
2. 請先在**本試題封面**寫上**姓名、組別**。
3. 練習後請將試題本留在座位上，**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. 作答中**不可離開座位**，若同組中任何一人離開座位，代表該組已答完試題並交卷。
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. 作答時間：**3 小時**，答案請依題目指示填到 USB 上對應的各題答案卷 word 檔案內。

任務一：電腦及網路系統安全強化

任務背景：小明是一間工作室的資訊人員，被賦予替公司電腦進行安全強化的任務，為此小明利用本機**群組原則物件（Group Policy Object, GPO）**進行各項安全強化設定。

說明一：試題環境為一台運行 Windows 10 的虛擬機。請將 USB 隨身碟「**任務一資料夾**」下的 **Windows10-VMware** 映象檔載入並執行。虛擬機的帳號為 **IEUser**，密碼為 **Password!**。

說明二：請登入上述虛擬機，然後透過本機群組原則物件 (GPO) 針對該 Windows 10 進行安全組態強化設定，設定值請以政府組態基準 **TWGCB** (Taiwan General Configuration Baseline) 建議值為標準，此標準請參考 USB 隨身碟「**任務一資料夾**」下的「**本機群組原則 GPO 提示項目**」檔案內容。

說明三：下列題目請依序作答，請在 USB 隨身碟「**任務一資料夾**」下**答案卷**的各題號後面列出您設定的安全強化項目與設定內容，必要時可將設定畫面截圖後貼上。

試題 1　(2 分)
為確保電腦開啟的稽核日誌事件記錄檔大小、事件記錄檔複寫機制等設定應適當開啟，請您透過本機群組原則強化相關安全組態設定

試題 2　(2 分)
由於駭客常利用遠端桌面 RDP 協議竊取伺服器機敏資料，為降低遠端桌面服務遭受駭客攻擊的風險，需透過本機群組原則組態檔設定強化桌面 RDP 協議，請您透過本機群組原則強化相關安全組態設定

試題 3　(2 分)
為允許或限制只有部分使用者或群組可以擁有遠端桌面服務用戶端登入的權限，請您透過本機群組原則強化相關安全組態設定

試題 4　(2 分)
為加強使用者在遠端桌面服務連線期間通訊的安全性，請您透過本機群組原則強化相關安全組態設定

試題 5　(2 分)
工作室的員工都使用 SMB 協定來分享檔案，為降低其使用風險(例如未限制使用時間、未要求密碼必須加密後才能傳送等等)，請您透過本機群組原則設定將 SMB 服務相關的安全組態檔進行強化

試題 6　(5 分)

工作室的員工都使用 IE 瀏覽器上網際網路，請您透過本機群組原則設定將 IE 瀏覽器的安全組態檔進行強化，此強化又分為以下數項：

6.1 為降低使用者使用瀏覽器瀏覽網頁的風險，請針對瀏覽器的安全組態檔進行強化

6.2 為防止使用者擅自更動瀏覽器設定導致資安防護強度降低，請針對瀏覽器的安全組態檔進行強化

6.3 為防止使用者清空歷史瀏覽網頁紀錄，請針對瀏覽器的安全組態檔進行強化

6.4 為降低使用者使用瀏覽器下載檔案的風險，請針對瀏覽器的安全組態檔進行強化

6.5 為防止駭客透過隱藏的表格資訊，在未經使用者同意下取得使用者所儲存的所有個資，例如國別、地址、電話號碼等個人資訊，請針對瀏覽器的安全組態檔進行強化

試題 7　(4 分)

工作室的部分員工使用 Edge 瀏覽器上網際網路，請您透過本機群組原則設定將 Edge 瀏覽器的安全組態檔進行強化

7.1 為降低使用者使用 Edge 瀏覽器瀏覽網頁的風險，請針對瀏覽器的安全組態檔進行強化

7.2 為防止駭客透過隱藏的表格資訊，在未經使用者同意下取得使用者所儲存的所有個資，例如國別、地址、電話號碼等個人資訊，請針對瀏覽器的安全組態檔進行強化

7.3 為防止使用者透過 Edge 瀏覽器在本機端儲存其密碼，請針對瀏覽器的安全組態檔進行強化

7.4 為避免第三方能存取人員個資、數位足跡及個人喜好等，需在 Edge 瀏覽器停用第三方 cookie，以降低使用者行為等資訊被他人蒐集之風險，請您透過本機群組原則組態檔設定強化相關設定

試題 8 (1 分)

Cortana 已經成為駭客入侵上鎖 Windows10 的管道，因為其能在電腦鎖定狀況下於背景執行語音指令，開啟帶有惡意程式的網站。為降低此類安全風險，請您透過本機群組原則強化相關安全組態設定

任務二：數位鑑識與證據收集

說明：企業內部某員工之作業主機疑遭惡意程式感染，觸發資安設備，經通報公司內部網路安全管理人員，在與受害員工進行簡短的問答後，調查人員旋即進行數位鑑識調查。請您協助調查人員調查 USB 隨身碟「任務二資料夾」下的 **IR_LAB 虛擬機**，並回答以下問題。

注意事項：

1. 請**勿調整 VM 之系統設定**，以免答案與正確答案有出入
2. 試題中所需之**工具**位於**受害主機之 E:\Tools** 目錄之下
3. 試題答案請統一用**西元時間與 24 小時制**表示，並記錄**年月日時分秒**
4. 各題答案請寫在 USB 隨身碟「任務二資料夾」的**答案卷.docx 檔**上。無法紀錄在答案卷檔上的佐證資料，請放在 USB 隨身碟中**指定的佐證資料夾**內。

證物資訊紀錄

試題一. 請於答案卷列出以下資訊：**(4 分)**

- 主機**名稱**
- 作業系統**版本**
- 作業系統**建立時間**
- 硬碟容量（請以**位元組 byte** 為單位，否則不予計分）
- 網路資訊（**IP/SUBNET/GATEWAY/DNS**）
- 該主機**特權帳號名稱**與**最後修改密碼**之時間
- 該主機所有開啟的 **UDP 及 TCP 連接埠**（TCP 及 UDP **分開列出**，且依據連接埠數字大小，**由小列至大**）
- 網路**路由表**（Routing table，請**截圖**貼至答案卷）

記憶體及程序鑑識

請分析記憶體中之資訊，及運作中程序之資訊後回答以下問題，並將答案列於答案卷中。

試題二. 從記憶體及運作程序中，可觀察到的惡意行為之**程序名稱**及其**父程序名稱**為何？（不止一個惡意程序）**(8 分)**

試題三. 承上題，哪個惡意程序**對外連往中繼站（C&C）？中繼站 IP 或網域為何**？（虛擬機應設為 NAT）**(4 分)**

試題四. 承試題二，惡意「程式」**路徑與檔名**為何？**(8 分)**

試題五. 承試題四，其中一個惡意程式為**鍵盤側錄**程式，請問該**程式的名稱**為何？其常駐於**機碼之位置**為何？其**植入機碼**之時間為何？ **(6 分)**

網路日誌分析

請分析受害主機 C:\Log 目錄中的網路日誌，回答以下問題，並將答案列於答案卷中。

試題六. 從網路日誌中，可觀察到的惡意攻擊來源 IP 為何？該惡意攻擊來源 IP 之攻擊行為為何？請將攻擊行為的相關 Log 截圖以資佐證。（可能不只一個惡意攻擊來源 IP、每個惡意攻擊來源 IP 也可能不只一種惡意攻擊行為）**(10 分)**

第 50 屆全國技能競賽分區賽

網路安全職類

網路安全 CTF 試題

109-4-24 下午，時間 2 小時

崗位編號：_____　選手姓名：_____

注意事項：

1. 開始答題前**手機請設靜音**模式，同時**勿翻閱試題**。
2. 請先在**本試題封面**寫上**姓名、組別**。
3. 練習後請將試題本留在座位上，**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. 作答中**不可離開座位**，若同組中任何一人離開座位，代表該組已答完試題並交卷。
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. 作答時間：**2 小時**，答案請依題目指示填到 USB 上對應的各題答案卷 word 檔案內。

CTF 競賽說明：

1. 本 CTF 部分共包含四個試題，都使用相同的虛擬機 Windows 10 系統，請在 USB 隨身碟上找到 **ctf-windows10 image** 檔並載入執行，毋須輸入帳號密碼。
2. 四個試題所需的解題資訊分別在虛擬機桌面上的試題一、試題二、試題三、試題四資料夾內。
3. 解題所需用到的工具皆已安裝在虛擬機上，只需按下「開始」按鈕即可找到工具來使用。
4. 各題答案請寫在 USB 隨身碟的**答案卷.docx** 檔上。Flag 的格式如下：flag{可列印字元} 或 FLAG{可列印字元}，flag 的大小寫沒關係，也就是 flag ... flAg fLaG flAG ... FLAG 都是可以的。

試題 1(encoding) (12 分)：

1-1. 由於市場競爭激烈，我們希望破解競爭對手的加密以得知對方最近想買什麼東西！ 根據先前的情報我們已經知道明文為:

alphabet - a character set that includes letters and is used to write a language.

以及其加密結果為:

cnrjcdgv - c ejctcevgt ugv vjcv kpenwfgu ngvvgtu cpf ku wugf vq ytkvg c ncpiwcig.

這次探子得到對方加密後新的購物清單，已知對方使用同樣的加密法與密鑰加密，其密文內容為: **uekuuqtu**，請回答此購物清單內容為何？

1-2. 對方似乎發現我們能夠破解他的購物清單了，於是更換了加密法與密鑰，請再次協助破解加密以得知對方最近在想什麼？根據探子的努力，我們已經知道明文:

put oneself in someone's shoes

與其加密結果為:

p elisee ouosfnoo'setne mnshs

已知對方使用同樣的加密法與密鑰加密了自己的心情，其加密結

果為(不包含雙引號" "): **"eaymt ph"**，求解密內容？

1-3. 對方開始使用電腦保護他的秘密訊息，請你破解加密，讓我們知道他到底最近在學習什麼新東西？根據在垃圾桶撿到的部分程式碼，我們已經知道明文:

We usually input "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA" to test buffer overflow.

與其加密結果為:

JxJOBQQbERsCCVcHHgcbBFdMMTYvMTYvMTYvMTYvMTYvMTYvMTYvMTYvMTYvMTYvMTYvUlcaH1caFQQaUBUbFhELAlcBBhIcFhsBB1k=

已知對方使用同樣的加密法與密鑰加密了最近的練習目標，其加密結果為:

IAAAUB4dUBZOHBILBAQeFRYFUAQCERkJUAMLAhpOFBIcGQELFFcIAhgDUAMGFVcYFQUMUBgZHlk=

求解密內容？

備註: 由於加密結果有不可視字元，故使用 base64 編碼，處理前記得先做 base64 decode

試題 2(Reverse) (12 分)：

小明沈迷於剪刀石頭布的遊戲，經過多年鍛鍊，小明已經成為剪刀石頭布之王。打遍天下無敵手的小明因為找不到值得一戰的對手，於是委託了奇異果博士研發超級厲害的剪刀石頭布軟體，如果連續獲勝 1 萬次，將會得到獎品。

根據奇異果博士的說法，這個遊戲不是一般的遊戲，考驗的不是運氣與手速而是智慧。

請你分析並戰勝此遊戲軟體：**PaperScissorStone.exe** 以成功取得 Flag。

試題 3 (Pcap)　(8 分)：

某個新手站長的網站受到入侵，他希望我們協助調查對方到底做了什麼事情，並提供了當時的 pcap 檔　，希望我們可以幫幫他。

3-1. 請問網站被破解的使用者帳號與密碼為何？

3-2. 攻擊者的來源 IP 為何？

3-3. 攻擊者竊取了主機根目錄下的什麼檔案？(僅需檔案名稱)

3-4. 請問攻擊者竊取的檔案內容為何？

試題 4 (Webshell) (8 分)：

小明是一個新手站長，由於網站遭受攻擊被植入了惡意程式，於是呼叫了資安團隊進行數位鑑識。資安團隊發現一隻疑似後門程式檔案，你可以回答下列問題以解開駭客攻擊手法嗎？

4-1. 啟動後門程式的密碼為？

4-2. 後門程式的指令參數名稱為？

4-3. 後門程式使用以下哪種函數執行指令？

(A) system

(B) Eval

(C) command.exe

(D) Powershell