第 53 屆全國技能競賽分區賽

網路安全

安全強化暨數位鑑識

112-03-24 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. [**lyonus**] 登入資訊：**deff** / **P@ssw0rd1!**
   - Ubuntu 14 Cli
   - 2GB RAM & 20GB Disk & 1 Core CPU
   - IP: 172.16.70.39/24
2. [**lyondows**] 登入資訊：**user** / **P@ssw0rd1!**
   - Windows 10 Pro
   - 4GB RAM & 60GB Disk & 2 Cores CPU
   - IP: 172.16.70.40/24

任務一：電腦及網路安全系統強化 (20 分)

請注意：任務一的題目可能會有作答先後順序之影響，因此建議選手詳閱整份題目卷後，再規劃作答順序。競賽將以**截圖畫面**作為評分依據。

(一) 帳戶與系統安全強化 (8 分)

以下題目請**使用[lyondows]主機**進行作答，各單題項目全對才給該題分數

1. (1 分)請修改帳戶原則，以符合下列需求：
   (1) 密碼必須符合複雜性需求 [啟用]
   (2) 密碼最長使用期限 [90 天]
   (3) 密碼最短使用期限 [0 天]
   (4) 強制執行密碼歷程記錄 [5]
   (5) 最小密碼長度 [8 個字元]
   請將**帳戶原則設定畫面**截圖貼至答案卷**試題 1** 中

2. (1 分)請修改帳戶原則，以符合下列需求：
   (1) 帳戶鎖定閥值 [3 次不正確的登入嘗試]
   (2) 帳戶鎖定時間 [60 分鐘]
   (3) 重設帳戶鎖定計數器的時間間格 [60 分鐘]
   請將**帳戶原則設定畫面**截圖貼至答案卷**試題 2** 中

3. (1 分)請修改安全性原則，以符合下列需求：
   (1) 登入：不要求按 CTRL+ALT+DEL 鍵 [停用]
   (2) 登入：不要在登入期間顯示使用者名稱 [停用]
   (3) 登入：在密碼到期前提示使用者變更密碼 [10 天]
   請將**安全性原則設定畫面**截圖貼至答案卷**試題 3** 中

4. (1 分)請修改原則，以符合下列需求：

   (1) Windows Installer 禁止移除更新 [已啟用]

   請將**原則設定畫面**截圖貼至答案卷**試題 4** 中

5. (2 分)下圖為 nmap nse 對於 [**lyondows**] 的 SMB2 Service 掃描結果，請透過修改本機原則，修復此問題

```
Host script results:
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
```

   請將**修改的原則設定**截圖貼至答案卷**試題 5** 中

6. (2 分)請安裝並啟用本機 SSH Server，並完成以下項目：

   (1) 新增使用者：使用者帳號 lyon，密碼 P@ssw0rd1!

   (2) 以 ssh 登入本機 ssh 使用者 lyon，輸入 sshd -V 的指令

   (顯示到 sshd 特定版本資訊才算答題正確，沒 -V 的 option 是正常的。)

   請將**操作過程**截圖貼至答案卷**試題 6** 中

(二) 特權帳戶與安全強化 (12 分)

以下題目**請使用[lyonus]主機**進行作答，各單題項目全對才給該題分數

7. (2 分)使用 facl 限制 webadmin 使用者，令其不能執行 ssh 指令。請將**設定方式**及**驗證設定成功**畫面截圖貼至答案卷**試題 7** 中

8. (1 分)設定 webadmin 使用者，令其可以透過 sudo (需輸入密碼)執行 ssh 指令。請將**設定方式**及**驗證設定成功**畫面截圖貼至答案卷**試題 8** 中

9. (1 分)設定 iptables 以禁止 **[lyondows]** ping 到 **[lyonus]** (拒絕所有 ping 封包)，並將**設定方式**及**驗證設定成功**畫面截圖貼至答案卷**試題 9** 中

10. (1 分)以 webadmin 執行 sudo ssh 登入到 **[lyondows]**，透過 **lyon** 帳號，新增下列指定使用者至 [lyondows] 上

    使用者帳號：**weakman**、密碼：**haha456**

    請將**設定方式**及**驗證設定成功**畫面截圖貼至答案卷**試題 10** 中

11. (1) (4 分)提供自簽憑證(RSA 2048 bits)的 https 服務

    (2) (3 分)自動導向 http 至 https，同時轉送該 http 的請求參數，並確保所有目的為 http 的

請求都會抵達至 https 服務

請將**設定方式**及**驗證設定成功**畫面截圖貼至答案卷**試題 11** 中

任務二：數位鑑識與證據蒐集調查 (共 40 分)

(一) 記憶體分析 (20 分)

士奇是資安公司的鑑識團隊成員，最近獲知同事的電腦遭到駭客入侵，**Task01.mem** 是從受害電腦導出的記憶體映像檔，請協助士奇分析並回答以下問題。

12. (2 分)請分析出該電腦使用的**作業系統**，並將**答案**及**解題過程截圖**貼至答案卷**試題 12** 中

13. (3 分)請分析出該電腦目前執行的**惡意檔案名稱**，並將**答案**及**解題過程截圖**貼至答案卷**試題 13** 中

14. (6 分)請分析出該電腦的**電腦名稱**、**當前使用者名稱**，並將**答案**及**解題過程截圖**貼至答案卷**試題 14** 中

15. (6 分)結合以上資訊，請找出駭客於攻擊中留下的**特徵碼(SK54{...})**，並將**答案**及**解題過程截圖**貼至答案卷**試題 15** 中

16. (3 分)請分析出**惡意伺服器 IP** 及**連接埠(port)**，並將**答案**及**解題過程截圖**貼至答案卷**試題 16** 中

(二) 硬碟鑑識 (14 分)

哈林是資安公司的鑑識團隊成員，最近獲知同事的電腦遭到駭客入侵，**Task02.E01** 是從受害電腦導出的硬碟映像檔，請協助哈林分析並回答以下問題。

17. (4 分)請分析出**曾登入過**該電腦的使用者，並將**答案**及**解題過程截圖**貼至答案卷**試題 17** 中

18. (3 分)請分析出**此電腦的電腦名稱**，並將**答案**及**解題過程截圖**貼至答案卷**試題 18** 中

19. (3 分)已知該同事在電腦被入侵前曾透過瀏覽器下載檔案，請找出**下載的惡意檔案名稱**，並將**答案**及**解題過程截圖**貼至答案卷**試題 19** 中

20. (4 分)結合以上資訊，請找出駭客於攻擊中留下的**特徵碼(SK54{...})**，並將**答案**及**解題過程截圖**貼至答案卷**試題 20** 中

(三) 封包分析 (6 分)

大華是資安公司的 SOC 團隊成員，在網路節點上側錄到一段流量，請協助大華分析 **Task03.pcap**，並回答以下問題。

21. (3 分)請分析出攻擊者所使用的**攻擊套件**，並將**答案**及**解題過程截圖**貼至答案卷**試題 21** 中

22. (3 分)請分析出封包中的**管理者帳號(username)**及**密碼(password)**，並將**答案**及**解題過程截圖**貼至答案卷**試題 22** 中

----------上午試題結束----------

第 53 屆全國技能競賽分區賽

網路安全

CTF

112-03-24 下午，13:00~15:00

時間 2 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…」。

CTF 競賽環境說明

(1) CTF 共包含三個部分，皆使用所附 USB 上的工具即可作答。

(2) 各**試題檔案**位於所附 USB 的「**CTF 試題執行檔**」資料夾內。

第一部分：Reverse (共 23.5 分)

1. **(2.5 分)** 請分析 flag_checker1.exe 的運行邏輯，找出正確的 FLAG。
   FLAG 格式固定為 FLAG{.....}
   請將答案以 **FLAG{.....}**形式寫到答案卷試題 1 上

---

2. **(5 分)** 請分析 flag_checker2.exe 的運行邏輯，找出正確的 FLAG。
   FLAG 格式固定為 FLAG{.....}
   請將答案以 **FLAG{.....}**形式寫到答案卷試題 2 上

---

3. **(7 分)** 請分析 flag_checker3.exe 的運行邏輯，找出正確的 FLAG。
   FLAG 格式固定為 FLAG{.....}
   請將答案以 **FLAG{.....}**形式寫到答案卷試題 3 上

---

4. **(9 分)** 請分析 flag_checker4.exe 的運行邏輯，找出正確的 FLAG。
   FLAG 格式固定為 FLAG{.....}
   請將答案以 **FLAG{.....}**形式寫到答案卷試題 4 上

第二部分：Web (共 9 分)

5. **(4 分)** 請參考 USB 上本題資料後將以下兩題選擇題答案寫到答案卷試題 5 上。

   (1) 請問 webshell.php 是以哪個 PHP 函式呼叫系統指令?

   A. System　　B. Passthru　　C. Exec　　D. shell_exec

   (2) 下方為四種送至 webshell 的 query string，何者會成功讓伺服器執行系統指令?

   A. l33t=1&133=ls　　B. l33t=&133.7=ls

   C. l33t=1&13.3=ls　　D. l33t=&1337=ls

---

6. **(5 分)** 某客戶的系統遭受 APT-KUMA 入侵，根據網管單位的初步處理，錄製到可疑的傳輸封包(檔名為 封包.pcap)，請你協助調查。你在封包中找到的 FLAG，即為本題答案。FLAG 格式固定為 FLAG{.....}。
   請將答案以 **FLAG{.....}**形式寫到答案卷試題 6 上。

第三部分：Code Review (共 7.5 分)

下列題目為原始碼閱讀(Code Review)題型，請指出程式碼中帶有資安弱點的程式碼行數，並從選項中選出弱點的類型。

請注意：

(1) 各題回答之行數及弱點類型皆須正確才給分

(2) 題目中的程式碼皆為部分摘錄，請假設程式碼皆可正常運行，所需函數與變數皆有正常載入與賦值。

(3) 答題時，請以資安弱點產生的核心行數為準，可參考下列範例:

PHP Code Snippet

```
1. <?php
2. $id = $_GET['id'];
3. $sql = 'SELECT * from news WHERE id='.$id;
4. $result = mysql_query($sql);
```

我們可以在 Line: 2 觀察到輸入行為，Line:3 觀察到 SQL 語句的組成，最後在 Line:4 觀察到 mysql query 的執行。從上述的範例，正確答案的行數為 Line:4，弱點類型為 SQL Injection，而非 Line:2 與 Line:3。

---

7. **(2.5 分)** 假設以下程式碼皆可正常運行，請指出程式碼中帶有資安弱點的程式碼**行數**，並從選項中選出**弱點的類型**。

Python Code Snippet

```
1. import hashlib
2. from flask import Flask,redirect
3. from tools import randid
4.
5. secret = "XXXXXXX"
6.
7. app = Flask(__name__)
8.
9. def sign(data):
10.     _data = secret + data
```

```
    return hashlib.sha256(_data.encode('utf-8')).hexdigest()

@app.route('/redirect_to_paygateway')
def redirect_to_paygateway():
    tid = randid()
    parameters = "tid={0}&amount={1}".format(tid, 1399)
    return redirect("https://gateway/payment?" + parameters + "&sign=" +
sign(parameters), code=302)
```

(1) 請問資安弱點發生的行數為?

(2) 請問該弱點為下列何者?

A. 資料庫注入攻擊 (SQL Injection)
B. 資訊洩漏 (Information Leak)
C. 過濾繞過 (Filter Bypass)
D. 本機檔案包含 (Local File Inclusion)
E. 伺服器端請求偽造 (Server-Side Request Forgery)
F. 任意檔案延長 (Arbitrary File extension)
G. 長度延展攻擊 (Length Extension)
H. 長度壓縮攻擊 (Length Zipping)
I. 內容置換攻擊 (Content Replacement)
J. 簽章混淆 (Signature Confusion)
K. 不安全的反序列化 (Insecure Deserialization)

請將以上**兩題**選擇題的正確答案寫到答案卷試題 7 上。

---

8. **(3 分)** 假設以下程式碼皆可正常運行，請指出程式碼中帶有資安弱點的程式碼**行數**，並從選項中選出**弱點的類型**。

PHP Code Snippet

```
$parts = explode('.', $_GET['token']); //JWT
$algorithms = array('HS256', 'HS384');

if (count($parts) !== 3) {
  throw new InvalidArgumentException('Invalid JWT format.');
}

$header = json_decode(JWT::decode($parts[0]), true);

 if (in_array($header['alg'], $algorithms)) {
   ...
 }
```

(1) 請問資安弱點發生的行數為?

(2) 請問該弱點為下列何者?

A. 資料庫注入攻擊 (SQL Injection)
B. 資訊洩漏 (Information Leak)

C. 過濾繞過
(Filter Bypass)

D. 本機檔案包含
(Local File Inclusion)

E. 伺服器端請求偽造
(Server-Side Request Forgery)

F. 任意檔案延長
(Arbitrary File extension)

G. 長度延展攻擊
(Length Extension)

H. 長度壓縮攻擊
(Length Zipping)

I. 內容置換攻擊
(Content Replacement)

J. 簽章混淆
(Signature Confusion)

K. 不安全的反序列化
(Insecure Deserialization)

請將以上**兩題**選擇題的正確答案寫到答案卷試題 8 上。

---

9. **(2 分)**假設以下程式碼皆可正常運行，請指出程式碼中帶有資安弱點的程式碼**行數**，並從選項中選出**弱點的類型**。

Python Code Snippet

```
1.  import base64, pickle
2.  from flask import Flask, request, make_response, redirect
3.
4.  app = Flask(__name__)
5.
6.  @app.route('/')
7.  def index():
8.      username = ''
9.      if request.cookies.get('username'):
10.         username=
    pickle.loads(base64.b64decode(request.cookies.get('username')))
11.         response = make_response("Hello, " + username, 200)
12.         response.mimetype = "text/plain"
13.         return response
14.     else:
15.         username='Unknown'
16.         return redirect('/login')
```

(1) 請問資安弱點發生的行數為?

(2) 請問該弱點為下列何者?

A. 資料庫注入攻擊
(SQL Injection)

B. 資訊洩漏
(Information Leak)

C. 過濾繞過
(Filter Bypass)

D. 本機檔案包含
(Local File Inclusion)

E. 伺服器端請求偽造
(Server-Side Request Forgery)

F. 任意檔案延長
(Arbitrary File extension)

G. 長度延展攻擊
(Length Extension)

H. 長度壓縮攻擊
(Length Zipping)

I. 內容置換攻擊
(Content Replacement)

J. 簽章混淆
(Signature Confusion)

K. 不安全的反序列化
(Insecure Deserialization)

請將以上**兩題**選擇題的正確答案寫到答案卷試題 9 上。

----------下午試題結束----------