

# 第 54 屆全國技能競賽分區賽網路安全職類

## 試題說明

現代社會對電腦網路依賴日益深切，導致網路安全防護不可一日或缺，且隨著駭客手法日新月異，網路及資訊系統管理者亦需能及時掌握駭客攻擊的種種手法與技巧，因此本次競賽試題分成以下三大部分：

### （一）電腦及網路安全系統強化（占 20%）

此部分競賽重點於選手要能依照企業安全政策要求，做好種種安全設定，題目例如：

1. 公司請您針對開放 SMB 網路芳鄰服務的伺服器作業系統進行存取權限相關的安全組態強化，強化的面向包含但不限於：高權限帳號保護、帳號登入限制、密碼安全、閒置時間管理、指定網路驗證等級等。
2. 公司請您針對提供遠端連線服務的伺服器作業系統進行權限限縮等安全組態強化，強化的面向包含但不限於：遠端登入帳戶限制、本機帳號保護、密碼安全、限制空白密碼、指定連線加密層級等。
3. 公司請您針對開啟稽核日誌的伺服器進行軌跡記錄的保護與權限限縮等組態強化，強化的面向包含但不限於：事件記錄檔大小、事件記錄檔複寫機制、稽核事件啟用、事件記錄檔存取限制等設定。

以上完成任務過程中，每組需將各試題的完成證據，例如螢幕畫面、設定檔等依據題目指示紀錄於配發的 USB 隨身碟。

### （二）數位鑑識與證據蒐集調查（占 40%）

此部分的競賽重點在於發生資安事件後，選手要能快速找出事件證據並判斷攻擊途徑或攻擊過程。例如企業內部某員工之個人電腦疑遭惡意程式感染，經通報公司系統管理人員後，請您對該惡意行為進行數位鑑識調查，調查內容包含但不限於：

1. 在題目指定的虛擬機上，根據虛擬機記憶體以及運作中程序(PROCESS)的資訊，找出惡意行為之程序名稱及其父程序名稱為何？（可能不止一個惡意程序）

2. 承上題，找出對外連往中繼站 (C&C) 的惡意程序，並找出該外部中繼站的 IP 或網域為何？
3. 承上題，找出該惡意程序的映像檔(image)路徑與檔名為何？

以上完成任務過程中，每組需將各試題的完成證據，例如畫面、設定檔等依據題目指示紀錄於配發的 USB 隨身碟。

(一)、(二) 部分作答時間合計 3 小時。

### (三) 奪旗賽 (CTF) (占 40%)

此部分競賽重點在測驗選手對於駭客攻擊技巧的瞭解與掌握程度，主要包括以下技能：系統程式漏洞分析及攻擊、網站程式漏洞分析及攻擊、常見攻擊工具操作、程式混淆及還原、程式反組譯、加解密技能、作業系統及 API 操作、封包分析、Shell Script 撰寫、程式撰寫等。

此部分將以解題方式進行，每組依試題說明，利用題目提供的工具及環境找出題目要求的答案(Flag)。本次比賽的試題將包括但不限於以下種類：

1. 加解密：主要測試選手破解密碼的能力，我們將提供多組密文要求選手解密，密文可能使用凱薩密碼, XOR, Base64, 換位法等，每個類型密文會提供一組範例(包括明文與密文) 供選手參考。
2. Web Hacking：主要測試選手程式逆向工程的能力，例如我們將提供一個簡單小遊戲，選手要在沒有籌碼的情況下贏得遊戲，這中間需要選手透過逆向工程找到遊戲中隱藏的指令，或者透過 Binary Patch 改變成功條件，又或者網站存有漏洞，選手可設法找出漏洞並利用該漏洞達成竄改交易或提權等目的。
3. 封包分析：主要測試選手對網路封包的理解及分析能力，我們將提供一個 pcap 檔，選手需找出 pcap 檔內包含的攻擊來源或題目要求的資訊。
4. WebShell 分析：主要測試選手破解程式混淆的能力，我們將提供選手一個混淆過的 WebShell，選手要找出啟動該 WebShell 的方法

以上解題過程中，每組需將各試題的 Flag、解題思路以及作法依據題目指示紀錄於配發的 USB 隨身碟。

此部分作答時間 2 小時。

**備註：**

1. 本職類競賽每組兩人，每組配發兩部個人電腦（稱為電腦 1 與電腦 2），各組崗位彼此獨立且不對外連線。電腦 1 與電腦 2 安裝 Windows 11，且預先安裝 VMware Workstation player（30 天試用版）以及 Office Word 等文書軟體。選手毋須自備工具、設備或材料。
2. 每組在上下午時段各發給一個 USB 隨身碟，內有解題所需軟體（參考以下附表一所列）以及試題虛擬機映像檔，選手需自行安裝虛擬機來回答問題。

**附表一：（此軟體列表僅供參考，各試題資料夾所提供工具以此表所列為原則）**

軟體（商業軟體部分為免費試用版）	備註
Apache TCPMon	
Autopsy	
burp	
Cports	
Cuckoo sandbox	
ELK	
fiddler	
FTK Imager Lite	
IDA Free	
Java runtime	
Kali Linux (內含Mysql Server/Client, dirbuster, dirb, Hydra, Pwntools, Pwndbg等多種工具)	
Linux OS (use CentOS)	
Log parser	
Microsoft Baseline Security Analyzer (MBSA)	
Metasploit Framework	
Microsoft Server OS 2016	
MySQL	
Nessus	
Nmap	

Notepad++	
OllyDbg	
OSSEC	
OSSIM SIEM	
Processhacker	
PuTTY	
Python 2.7(含)以上	
Radare	
Snort NIDS/NIPS	
Splunk Enterprise	
sqlmap	
Sysinternals Suite	
Tripwire (open source version)	
Unzip tools(e.g. 7 Zip)	
Volatility	
WAF mod_security	
Webserver (on Linux)	
Wireshark	