

第 53 屆全國技能競賽



勞動部勞動力發展署
技能檢定中心



暨第 47 屆國際技能競賽國手第一階段選拔賽 worldskills
Chinese Taipei

網路安全

安全強化

112-07-14 下午，13:00~16:00

時間 3 小時

注意事項：

1. 每一段比賽時間包含裁判說明題目時間，在裁判宣布開始比賽前勿作答，違反者將依大會規定處理。
2. 比賽後請將紙筆留在座位上，不得攜出試場。
3. 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。
4. 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。
5. 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。
6. 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...」。
7. 答案卷上務必填上組別與選手姓名，有無作答都需繳交答案卷並將.docx 檔轉換成.pdf 檔，兩種檔案都要存入隨身碟。

試題環境主機

主機名稱	存取方式	帳號 / 密碼
ESXi	http://10.0.54.54	cs02 / Cybersec\$54
Exchange	透過 ESXi	Administrator / P@ssw0rd
UbuntuV2	透過 ESXi	tempuser / Skills54pass

注意事項

1. Ubuntu 主機內建 WordPress 與 Kali 的 docker container，Kali 請參賽者使用已經設定好的 container (name: **kali-preinstall**)，WordPress 可以自由進入 container 進行修補。
2. 如需操作 Kali，可執行：**docker exec -it kali-preinstall bash**
3. 如需修補 WordPress: 可對 WordPress_ 開頭的 container 進行操作。

(一) Windows Hardening (共 7 分)

已知這台主機有 ProxyLogon 漏洞，但目前主機無法進行 Patch 與連上 Internet，以下為 ProxyLogon 概述。

ProxyLogon is the formally generic name for CVE-2021-26855, a vulnerability on Microsoft Exchange Server that allows an attacker bypassing the authentication and impersonating as the admin. We have also chained this bug with another post-auth arbitrary-file-write vulnerability, CVE-2021-27065, to get code execution.

1. (3 分)請撰寫偵測攻擊發生的程式以顯示**攻擊發生時間點與相應的資訊**。完成後將**答案及解題過程截圖**貼至答案卷**試題 1**中。
2. (4 分)承上題，請**實施緩解**讓攻擊無法發生。請注意選手不只要成功阻擋 ProxyLogon 攻擊，同時 OWA (Outlook Web Access/Outlook Web APP) 功能依舊正常，完成後將**答案及解題過程截圖**貼至答案卷**試題 2**中。

(二) WordPress 網頁修補 (共 6.5 分)

你現在擁有一個有漏洞的 WordPress 網站主機，請依據題目敘述找到漏洞點並修改程式碼修復漏洞。

3. (1 分)網站現在可以使用任意帳號進行登入而無須檢查密碼，請你解決這個漏洞，並將**答案及解題過程截圖**貼至答案卷**試題 3**中。
4. (0.5 分)網站後台多出了非法建立的管理員 XXX，請找出用來建立該管理員的漏洞，以及該漏洞所使用的 payload，並將**答案及解題過程截圖**貼至答案卷**試題 4**中。
5. (0.5 分)網站的媒體庫中被上傳了一個 wav 檔案，且 /etc/passwd 資訊洩漏，請寫出攻擊者是利用何種漏洞藉由 wav 檔案獲取 /etc/passwd 資訊，以及攻擊者的 IP 位置，並將**答案及解題過程截圖**貼至答案卷**試題 5**中。
6. (2 分)承上題，請在不影響上傳功能的情況下修補此漏洞，並將**答案及解題過程截圖**貼至答案卷**試題 6**中。
7. (2.5 分)網站中的 Essential Addons for Elementor plugin 允許任何未經身份驗證的用戶將其權限提升為 WordPress 上任意用戶的權限，請修補此漏洞，並將**答案及解題過程截圖**貼至答案卷**試題 7**中。(提示：可在觸發 reset_password 函數之前進行驗證)

(三) Basic Linux Hardening (共 6.5 分)

8. (1.5 分)限制 sudo 使用，具體要求如下：

- (1) 新增一個 sudo 使用者名為 "limit_admin"，並設定其密碼為 Skills54!QAZ。
- (2) 限制 "limit_admin" 使用 sudo 的權限只能在特定路徑執行指令，該路徑為 "/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"。
- (3) 設定 "limit_admin" 使用 sudo 的有效期限為 2 分鐘，超過此時間後需要重新驗證身份。
- (4) 啟用 Sudo 審計日誌，將 "limit_admin" 使用 sudo 的紀錄寫入到 "/var/log/sudo.log" 檔案中。

請將**答案及解題過程截圖**貼至答案卷**試題 8**中。

9. (1.5分)請設定 Linux 系統，當 SSH 登入失敗次數超過 5 次時，

- (1) 自動封鎖該 IP 位址 30 分鐘
- (2) 在封鎖期間拒絕該 IP 的 SSH 登入嘗試。

請將**答案及解題過程截圖**貼至答案卷**試題 9**中。

10. (1.5分)請設定 Linux 系統的密碼策略，要求使用者密碼必須符合以下條件：

- (1) 長度至少為 8 個字元。
- (2) 必須包含大小寫字母、數字和特殊符號。
- (3) 在 90 天後過期。

請將**答案及解題過程截圖**貼至答案卷**試題 10**中。

11. (1分)請檢查 Linux 系統上的使用者帳戶，確保沒有非 root 帳戶的 UID 設定為 0，如果有 UID 為 0 的帳號請寫出來並改善，並將**答案及解題過程截圖**貼至答案卷**試題 11**中。

12. (1分)請設定 Linux 系統，僅允許 root 訪問 CRON 服務。具體要求如下：

- (1) 確保只有 root 能夠使用 crontab 指令進行 CRON 任務的設定和管理。
- (2) 禁止其他非 root 帳戶透過 crontab 命令設定或修改 CRON 任務。

請將**答案及解題過程截圖**貼至答案卷**試題 12**中。

-----**試題結束**-----