第 52 屆全國技能競賽全國賽

網路安全

CTF I

111-08-05 上午，08:30~12:00

時間 3.5 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…」。

任務：紅隊演練-對目標環境找出各種攻擊途徑

說明：你是資安團隊一員，目前你的團隊受某單位 (以下簡稱甲方) 邀請參與一個紅隊演練專案，該專案的目標環境是一個新創小型工作室。為執行此專案，甲方提供一台 Kali 機器給貴團隊，該機器已接入該工作室的 DMZ 網段。目前已知目標環境內共有 5 個 flag，且已經被驗證皆有弱點路線可以取得。請貴團隊找出格式為 flag{xxxx} 的 flag ，並將滲透的方法記錄下來或將滲透過程畫面截圖貼在答案卷上。

甲方窗口提供了一個部落格的網址：

http://10.54.54.100/

請注意：本題目環境類似真實世界，若在滲透期間不慎將題目環境之設備清空或抹除必要之檔案，將無法進行還原。

試題一. 請問 deff 的個人電腦的 IP 地址是？(1 分)

試題二. 請問貼圖畫廊的 IP 地址是？(4 分)

試題三. 請問內網共用的資料庫 IP 地址是？(3 分)

試題四. 4.請列出所有 flag (無順序之分) (每一個 2.4 分，共 12 分)

a. flag1=

b. flag2=

c. flag3=

d. flag4=

e. flag5=

----------試題結束----------