112 年度教育體系資安攻防演練之攻防檢測員招募簡章

一、 目的

因應當前資安情勢之嚴峻與挑戰，教育部規劃辦理資安攻防演練，針對教育體系對外網站系統進行滲透測試，以提升教育體系面對網路攻擊時之應處能力，強化資安事件發生時之緊急應變、系統復原及協調管控等能力。同時為提升演練成效及加強技術交流，培養國內資安人才實戰經驗，敬邀本國教學研究界先進共同參與 112 年教育體系資安攻防演練(下稱本演練)。

二、 辦理單位

指導單位：教育部

承辦單位：教育體系資安檢測技術服務中心（國立陽明交通大學），以下簡稱本中心

三、 對象及資格

（一） 參與對象：

為本國國籍且具相當資安專業知能之人員參與擔任資安攻防演練攻防檢測員。

（二） 具備以下條件者方可優先參與遴選：

1. CEH Master/ECSA(CPENT)/OSCP/OSEP/OSWE 等資安相關滲透實務證照
2. 具備國內外資安相關競賽入圍初賽/複賽等具體實績
3. 為教育體系之副級(含)以上資安技術檢測員
4. 曾擔任行政院網路攻防演練攻擊手
5. 任職於國家安全局、國防部、法務部調查局及內政部警政署刑事警察局等政府機關具備資安實務經驗人員

四、 遴選方式與期程

（一） 報名（即日起至 112 年 10 月 20 日(週五)中午 12 時）

1. 由報名人員線上填列自身及推薦人基本資料於「112 年度資安攻防演練之攻防檢測員報名表」(網址：https://forms.gle/9HNXxuGXvy1r8rgw8)，本中心將依此報名資訊聯繫該人員，並副知其推薦人。
2. 為增進攻防檢測員之技術交流，本次報名亦可填覆是否參與技術交流訓練活動。
   (1) 本活動共 2 個場次，每場次各 2 天，每場次錄取上限 20 人，將依人員滲透實務經歷擇優錄取，最終錄取名單由教育部核定。
   (2) 將於 112 年 10 月 20 日（週五）下午 4 點前電子郵件通知課程報名結果。
   (3) 課程日程：

場次	日期	時間	地點
一	112/10/25(三)~112/11/26(四)	9:00-17:00	國立陽明交通大學資訊技術服務中心 1 樓 玻璃會議室
二	112/11/8(三)~112/11/9(四)		

   (4) 課程大綱

日程	項目
第一天	網頁系統認證繞過手法、交流分享時間
第二天	防護偵測繞過手法、交流分享時間

（二） 前置測驗（112 年 10 月 23 日(週一)至 112 年 11 月 9 日(週四)中午 12 時）

1. 於報名截止後，本中心針對書審資格符合之人員以電子郵件寄發前置測驗相關資訊，須請針對目標主機進行檢測，並撰寫攻擊報告，本中心將依據人員撰寫之報告數量與報告品質進行評選。
2. 最終將依據前置測驗結果呈請教育部核定參與名單。
3. 若具備優先參與遴選資格之人員可無須進行前置測驗。

（三） 結果通知（112 年 11 月 10 日(週一)下午 4 時）

遴選作業完成後，將另行通知遴選結果，並針對通過遴選人員告知演練時間與調查可參與時段，整體時程為 112 年 11 月 27 日(週一)至 112 年 12 月 29 日(週五)之工作天。

（四） 說明會（112 年 11 月 13 日(週一)）

1. 於通過遴選後，將於實體說明會告知攻防檢測員應遵守事項相關守則，須請務必參與，若無法參與該說明會將喪失參與資格。
2. 演練過程中為避免影響網站系統維運及人員社交爭議，不採用 DoS、DDoS 及社交攻擊等手法。
3. 攻擊機統一使用由本中心提供 Windows 與 Kali Linux 雙系統予每位攻防檢測員進行實施，但為安全起見，將限制攻擊手不得安裝來源不明之程式，但若為具有公信力之開發團體或一般釋出原始碼之 exploit code 則不在此限。此外，如有重大資安事件釋出之攻擊程式，經本中心確認後亦可做為使用。

五、 弱點提繳獎金計算方式

1. 為鼓勵攻防檢測員提繳弱點及提供完整弱點紀錄報告，將依弱點衝擊性累積總積分之排名提供獎金，攻防演練弱點衝擊性分成重大、高、中及低等 4 個等級，獎金計算原則及規則如下：

衝擊性弱點依累積分數排名		
衝擊性弱點	**積分**	**獎金（排名(人數)：元/名）**
重大衝擊性弱點	5	• 特優(3 名)：20,000 • 優等(3 名)：15,000 • 佳作(15 名)：8000
高衝擊性弱點	3	
中衝擊性弱點	2	
低衝擊性弱點	1	
規則	※需完成弱點紀錄報告，並累計至少 5 積分即可列入排名。 ※若積分相等，以最後一筆最早繳交時間為優先。	

2. 衝擊性判定高低以下表為主要準則：

	重大衝擊性	高衝擊性	中衝擊性	低衝擊性
SQL 權限	透過資料庫語法取得資料庫(明文/密文)帳密或資通系統明文帳密	透過資料庫語法取得資料庫機敏資料或資通系統密文帳密	透過資料庫語法取得資料庫欄位資料(不含機敏/帳密)	透過資料庫語法或錯誤訊息取得資料庫欄位名稱
AP 讀寫	具有可寫入 OS 特權路徑之權限	具有可寫入 Web 目錄、非 OS 特權路徑或讀取 OS	具有可讀取 Web 跨目錄或非 OS	僅可讀取當前 Web 目錄檔案之權限

	重大衝擊性	高衝擊性	中衝擊性	低衝擊性
權限		特權路徑檔案之權限	特權路徑檔案之權限	
惡意語法與提權	成功寫入攻擊語法或竄改頁面，且受影響之頁面為任一使用者並可擴散至其他系統	成功寫入攻擊語法或竄改頁面，且受影響之頁面為任一使用者	成功寫入攻擊語法或竄改頁面，但受影響之頁面限定已登入之任一使用者	▪ 成功寫入攻擊語法或竄改頁面，但受影響之頁面限定該登入使用者 ▪ 攻擊語法須透過其他途徑誘使其他使用者觸發
帳號權限	▪ 取得OS管理者權限或足以證明權限等同system、root或sysadmin之帳號 ▪ 取得資通系統防護需求為高等級之管理者(或帳號控管)權限或OS一般使用者權限	取得資通系統防護需求為中或普等級之管理者(或帳號控管)權限或OS一般使用者權限	取得資通系統(分級不限)業務單位使用者權限但不具帳號控管功能	取得資通系統(分級不限)一般使用者權限
資料外洩與存取控管	▪ 取得特種個資(病歷、醫療、基因、性生活、健康檢查及犯罪前科) ▪ 取得國家機密文書(未達解密條件者)	▪ 取得一般個資且重複攻擊成效具有可預期性 ▪ 取得一般公務機密文書(未達解密條件者)	取得部分一般個資且重複攻擊成效具有不可預期性	取得非機敏但非公開資料

3. 衝擊性判定高低輔以CVSS3.1(如下表)作為次要準則：

衝擊性弱點	CVSS 3.1
重大衝擊性弱點	9.0 - 10.0
高衝擊性弱點	7.0 - 8.9
中衝擊性弱點	4.0 - 6.9
低衝擊性弱點	0.1 - 3.9

六、 聯絡窗口

教育體系資安檢測技術服務中心—資安攻防演練專案

- E-Mail：taccst.code@nycu.edu.tw
- TEL：(03)571-2121 何小姐#52885、陳小姐#31268、呂小姐#52891、廖先生#52861