EC-Council CEH 駭客技術專家認證課程

一、 目的

為培育並輔導可投入資安產業或成為資安新創人才，挖掘具有學術研究潛力之成員，並以培訓資安人才補足資通安全法規範資安人力缺口，配合「臺灣資安卓越深耕—資安卓越中心計畫」特開設 EC-Council CEH 駭客技術專家認證(EC-Council Ethical Hacking and Countermeasures)課程，並透過協助教育部所屬機關（構）及各級學校進行資訊安全檢測及提出建議，提升學術網路防護安全性，增進國家資通安全之能量。

二、 辦理單位

教育部、竹苗區域網路中心(國立陽明交通大學 資訊技術服務中心)

三、 授課對象及資格

1. 為臺北第一區域網路中心（國立臺灣大學）、臺北第二區域網路中心（國立政治大學）、桃園區域網路中心（國立中央大學）、新竹區域網路中心（國立清華大學）及竹苗區域網路中心（國立陽明交通大學）就讀資訊相關系所（如資訊工程/管理/安全等）之在學學生。

   ※由於通過認證考試者，未來得參與教育體系資通系統安全檢測作業，故應屆畢業生(如大四及研二學生)不宜報名參與。

2. 若有其他資訊相關證照或比賽經歷證明等可擇優錄取。

四、 參與人數及方式

1. 本研討訓練共 5 天，名額 30 人，邀請各系所推薦合適人選，最終錄取名單由教育部核定，備取人員依序遞補。

2. 本次課程主要採實體授課，考量部分學員交通距離較遠，故開放限額 6 名學員遠端參與，並依距離遠近進行篩選。

五、 報名方式與期程

1. 【報名作業】：即日期起至 111 年 3 月 25 日(五)中午 12:00 止，受理線上報名。

   報名連結：https://forms.gle/WS9auY6hCQxDMq1P8。

2. 【結果通知】：111 年 3 月 31 日(四)前，由本中心審查報名人員清單並送教育部核定，再以電子郵件通知學員及推薦人報名結果。

3. 【課程時程】：共 5 天，8 小時/天，共 40 小時，如下表：

階段	日期	時間	講師	地點
1、	111 年 4 月 30 日(週六)	9:00-18:00	唐任威	國立陽明交通大學（陽明校區）圖書資訊暨研究大樓 4 樓 401 電腦教室（台北市北投區立農街二段 155 號）
2、	111 年 5 月 1 日(週日)			
3、	111 年 5 月 15 日(週日)			
4、	111 年 5 月 22 日(週日)			
5、	111 年 5 月 29 日(週日)			

4. 【認證考試】：

(1) 第一場：111 年 7 月 2 日(週六) 09:00-13:00，地點:國立陽明交通大學(陽明校區)圖書資訊暨研究大樓 4 樓 401 電腦教室。

(2) 第二場：111 年 7 月 3 日(週日) 13:00-17:00，地點：國立陽明交通大學(光復校區)資訊技術服務中心 1 樓 訓練教室。

六、 課程介紹

本課程主要是在於教導、介紹一些駭客常用的工具和方法，藉以實際了解駭客的行為，進而知道如何保護網路、系統免受攻擊。透過互動與實務操作，教導如何掃描及測試系統的安全漏洞，藉以保護系統安全，課程中將加強實際的上機操作，針對系統安全有更深一層的了解，藉由上課所模擬的網路環境中，了解駭客如何掃描並攻擊網路系統，也將學到如何制定策略、權限，以防堵不法駭客的入侵。

七、 課程大綱

1. 認識與了解資訊安全與道德駭客相關議題
2. 使用各種技巧搜集網路情報
3. 使用弱點掃描工具檢測電腦及網路系統安全
4. 使用各種駭客手法檢測電腦系統、網路、網站、手機、無線網路、物聯網及雲端環境安全
5. 認識與檢測惡意程式
6. 透過社交工程攻擊評估組織人員安全意識
7. 認識與阻擋分散式阻斷服務攻擊
8. 使用各種加解密技術保護資料

八、 課程內容

1. Introduction to Ethical Hacking（介紹何謂道德入侵）
2. Footprinting and Reconnaissance（蒐集蛛絲馬跡與網路勘查）
3. Scanning Networks（網路服務與弱點掃描）

4. Enumeration（列舉系統資訊）
5. Vulnerability Analysis（弱點分析）
6. System Hacking（入侵電腦系統）
7. Malware Threats（惡意程式威脅）
8. Sniffers（網路監聽與攻擊）
9. Social Engineering（社交工程）
10. Denial-of-Service（阻斷服務攻擊與傀儡網路）
11. Session Hijacking（連線劫持）
12. Evading IDS, Firewalls and Honeypots（規避入侵偵測/防火牆與誘捕系統）
13. Hacking Webservers（入侵網站）
14. Hacking Web Application（入侵網站程式）
15. SQL Injection（資料隱碼攻擊）
16. Hacking Wireless Network（入侵無線網路）
17. Hacking Mobile Platforms（入侵行動平台）
18. IoT Hacking（入侵物聯網）
19. Cloud Computing（雲端運算）
20. Cryptography（密碼學）

九、 聯絡窗口

國立陽明交通大學 資訊技術服務中心(竹苗區域網路中心)
E-mail:hcrc@nycu.edu.tw
呂小姐 TEL：(03)571-2121 #52891
何小姐 TEL：(03)571-2121 #52885
柯先生 TEL：(03)571-2121 #31706

十、 注意事項

1. 為因應新冠肺炎疫情之影響，本次作業將視疫情指揮中心後續公告措施動態調整實施情形，有任何變動將另以電子郵件告知。
2. 本課程具現場實際操作演練，可自備個人筆電。
3. 本課程提供茶水、便當，敬請自行攜帶環保水杯。
4. 因本校停車位有限，請多加利用大眾交通工具前往。
5. 為因應新冠肺炎疫情之影響，課程當天請配合量測體溫，若有發燒情形(額溫≧37.5℃/耳溫≧38℃)者，本中心得禁止其參與；室內活動建議自主配戴口罩。