工業技術研究院
Industrial Technology Research Institute

滲透測試應用實務班

一、課程緣起：

近年來駭客透過應用系統與軟體的漏洞所造成之資安事件層出不窮，軟體開發/管理人員面對資安事件應盡速應變並從安全軟體開發強化產品安全性。軟體開發/管理人員透過了解攻擊原理與步驟，進而可辨識惡意攻擊行為。

本課程設計除透過瞭解資訊安全所面臨之風險與處理方法，駭客可能之攻擊手法，藉以學習如何採取相對應之控制措施之外，並由滲透測試與資安偵測與監控之實務操作，讓學員學習到有效的資安防禦實務!

~本課程歡迎企業包班，請來電洽詢 課程承辦人 黃小姐 02-23701111#306 ~

更多軟體開發相關課程，請參主題館網址：
https://college.itri.org.tw/edm/D1/008/04/edm.html
更多資訊安全相關課程，請參主題館網址：
https://college.itri.org.tw/edm/D1/003/05/edm.html

二、課程目標：

- 了解網頁/系統應用程式攻擊流程以及資安檢測相關技巧。
- 理解駭客攻擊思維並具備資安攻防實務技巧。
- 掌握資安事故，並熟悉既有資安應變措施。

三、適合對象：

1. 資安管理人員、OT(Operation Technology) 維運人員
2. 系統管理人員、網路管理人員
3. 資安（ 訊 ）主管

四、課程注意事項：

請學員自備筆電上課。

五、課程日期：

113 年 8/19-8/20，週一二白天 9:00 ~12:00,13:00~17:00 ，共 2 天、計 14 小時。

六、上課地點：

舉辦地點：工研院產業學院 產業人才訓練一部(台北)，實際地點依上課通知為準!!!!

七、報名方式：

線上報名：到工研院產業學院官網報名
課程洽詢：02-2370-1111 分機 304 或 306 黃小姐

八、課程大綱：

1. 環境工具介紹。
2. 資訊蒐集：此部分將介紹如何蒐集滲透目標對象的服務版本及系統相關資訊。
3. 漏洞偵測與利用：此部分將介紹如何針對滲透目標對象的可能存在之 CVE 或其他常見漏洞進行偵測及利用該漏洞進行攻擊。
4. 後門植入及提權攻擊：此部分介紹駭客如何利用各類後門程式對滲透目標對象建立遠端控制及如何進一步提權。
5. 實際案例介紹：從我國近期油品事業遭勒索病毒案、政府機關遭入侵滲透案中研析駭客進行滲透之手法，提供學員進行反思。

＊ 課程執行單位保留調整課程內容、日程與講師之權利

九、課程費用與繳費：

1. 課程費用含課程、講義、餐點。

	課程費用
課程原價（每人）	$14,000 元
14 天前報名 優惠價(每人)	$12,600 元
14 天前報名+ 3 人(含)以上揪團同行 優惠價(每人)	$11,900 元

2. 課程若未如期開班，費用將全額退還。
3. 繳費方式
   - ATM 轉帳（線上報名）：繳費方式選擇「ATM 轉帳」者，系統將給您一組轉帳帳號「銀行代號、轉帳帳號」，但此帳號只提供本課程轉帳使用，各別學員轉帳請使用不同轉帳帳號！！轉帳後，寫上您的「公司全銜、課程名稱、姓名、聯絡電話」與「收據」傳真至 02-2381-1000 黃小姐 收。
   - 信用卡（線上報名）：繳費方式選「信用卡」，直到顯示「您已完成報名手續」為止，才確實完成繳費。
   - 銀行匯款(公司逕行電匯付款)：土地銀行　工研院分行，帳號 156-005-00002-5（土銀代碼：005）。戶名「財團法人工業技術研究院」，請填具「報名表」與「收據」回傳真至 02-2381-1000 黃小姐 收。
   - 計畫代號扣款(工研院同仁)：請從產業學院學習網直接登入工研人報名；俾利計畫代號扣款。

十、報名確認與取消：

1. 已完成報名與繳費之學員，課程主辦單位將於開課三天前以 E-mail 方式寄發上課通知函；

若課程因故取消或延期，亦將以 E-mail 方式通知，如未收到任何通知，敬請來電確認。

2. 已完成繳費之學員如欲取消報名，請於實際上課日前以書面通知業務承辦人，主辦單位將退還 80% 課程費用。

3. 學員於培訓期間如因個人因素無法繼續參與課程，將依課程退費規定辦理之：上課未逾總時數三分之一，欲辦理退費，退還所有上課費用之二分之一，上課逾總時數三分之一，則不退費。

4. 本單位保留是否接受報名之權利。

5. 如遇不可抗拒之因素，課程主辦單位保留修訂課程日期及取消課程的權利。