工業技術研究院
Industrial Technology Research Institute

網路安全封包分析實務班

一、課程緣起：

網路攻擊時有所聞，特別是 APT 組織與駭客集團經常使用惡意程式，繞過各種資安防護偵測系統，潛伏躲藏於被害人的內部網路。網路活動與惡意程式都會透過網路封包進行通訊傳輸，如何有效分辨異常網路封包活動(行為)?就需要培養網路封包分析能力，在巨量網路封包資料中，分析惡意程式與正常通訊封包的差異。

~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：

本課程旨在訓練學員從網路封包擷取的基礎能力，並能區分木馬後門通訊封包，找出網路惡意通訊封包資訊。

三、適合對象：

對網路安全封包分析的 IT 人員與資安研究人員。

四、先備知識：

- TCP/IP 網路基本觀念
- Windows 電腦基本操作能力

五、課程注意事項：

請學員自備筆電上課，事先安裝 Wireshark。

六、課程日期：

112 年 2/22-2/23，週三四白天 9:00 ~12:00,13:00~17:00 ，共 2 天、計 14 小時。

七、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!!!!

八、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

九、課程大綱：

單元	內容
擷取網路封包的方式	● 網路封包工具簡介 ● IP 位址的判讀 ● 過濾條件的介紹
判斷網路封包 （基礎）	● ARP 與 DNS 的運作 ● HTTP/HTTPS/SMTP/SMB 的運作
網路資安基本檢測方式	● 網路封包擷取與分析 ● 電腦程式的通訊現況 ● 工作管理員與程式執行現況
封包分析操作步驟	● NSPA Skills 準則 ● 封包過濾條件的運用 ● 過濾結果的封包儲存
判斷網路封包 （異常）	● IP Scan 與 Host Scan ● LAN Worm Infection ● Abnormal HTTP ● Abnormal HTTPS ● Abnormal SMTP ● Abnormal SMB
實作：正常網路封包的分析	● 瀏覽網頁的封包概論(DNS 與 HTTP) ● Chrome 的封包行為 ● Edge 的封包行為 ● Firefox 的封包行為 ● Windows Update 的封包行為 ● 不同 Windows 版本的封包行為
實作：病毒蠕蟲封包的分析	● Worm 的觀念介紹 ● SMB 蠕蟲的封包行為 ● 內部網路 SMB 攻擊
實作：木馬程式封包的分析	● Trojan/RAT 的觀念介紹 ● C&C Host 的觀念介紹 ● Trojan/RAT 的封包行為
實作：惡意下載者封包的分析	● Downloader 的觀念介紹 ● Downloader 的封包行為
評量（5 題）與討論	● 惡意程式網路封包(PCAP 檔案) ● Q&A 與 後續學習

＊ 課程執行單位保留調整課程內容、日程與講師之權利

十、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）	$12,000 元
14 天前報名 優惠價(每人)	$9,600 元
14 天前報名+兩人揪團同行 優惠價(每人)	$9,120 元
14 天前報名+四人(含)以上揪團同行 優惠價(每人)	$8,640 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。

十一、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。