工業技術研究院
Industrial Technology Research Institute

自動化安全檢測與網路封包分析實務

一、課程緣起：

隨著網路攻擊手段日益精進化，資安人員在進行資安健診或資安事件時，常面臨大量流量資料。傳統僅依賴圖形化介面（GUI）的分析方式，在處理大型封包檔（Pcap）時效率低落，且難以實現檢測作業的自動化與標準化。本課程旨在協助學員掌握從手動分析到自動化偵測的轉型。透過 Wireshark 的進階篩選、Tshark 的命令行處理能力，以及 Maltrail 惡意流量偵測系統的聯動，使學員能在有限的時間內精準定位威脅。課程將結合實務經驗，將抽象的封包數據轉化為具備證據價值的分析報告。

~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：

1. 掌握 Wireshark 高階過濾邏輯與自定義分析介面。
2. 熟練使用 Tshark 進行大規模封包欄位提取與自動化腳本撰寫。
3. 學習部署與應用 Maltrail 進行威脅情資(Threat Intelligence)異常偵測。
4. 具備整合工具進行完整資安事故調查(Cybersecurity Incident Investigation)的實戰能力。

三、適合對象：

對資安工程師、網路管理、SOC 監控、資安健診、網路鑑識人員。

四、課程注意事項：

請學員自備筆電上課。

五、課程日期：

115 年 9/17，週四，白天 9:30 ~16:30 ，共 6 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 609 林小姐或 306 黃小姐

*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

八、課程大綱：

單元	內容
Wireshark 分析技巧	● **自定義環境**：設定分析設定檔與專屬欄位。 ● **流量提取**：封包重組與檔案導出技巧。
Tshark 命令自動化處理	● **腳本實戰**：撰寫 Shell Script 進行多檔案批量化分析。
Maltrail 威脅偵測系統應用	● **架構部署**：感應器(Sensor)與伺服器(Server)的安裝與流量導向。 ● **情資分析**：識別 C&C 控制、惡意掃描(Mass Scanning)與異常連線。
資安事故分析 SOP	● **情境模擬**：勒索軟體或後門程式流量分析。 ● **綜合應用**：結合 Maltrail 預警、Tshark 快速過濾與 Wireshark 深度鑑識。

＊ 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。

課程方案	課程費用
課程原價（每人）	$6,000 元
14 天前報名 優惠價(每人)	$5,400 元
14 天前報名+三人(含)以上揪團同行 優惠價(每人)	$5,100 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 林小姐 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 林小姐 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。