科技部SP-ISAC計畫-資訊安全教育訓練　課程日期、大綱及講師簡介　（附件二）

地點	日期	星期	課程名稱	課程內容	課程介紹	講師	助教	參加對象	招訓人數
新竹國網電腦教室	2018/8/15	三	系統日誌分析實務	上課環境為 CDX 與 Linux系統，學員將學習如何透過常見的 Linux 指令，進行大部分日誌的處理與分析工作，另外也會介紹透過進階的工具，更有效率地處理大數據資料分析以及資料視覺化的議題。 內容包含： -- Log背景、架構、原理 -- Log分析系統介紹、概念、優點 -- Log分析系統設定 -- Log分析系統實作	資訊安全的領域中，日誌就像是陽光、空氣和水一樣：平常沒事的時候，都不會注意到它的存在，但是一旦發生事情時，如果缺乏它，就會是致命的危險。本課程將會介紹日誌分析系統的架構與原理，並且透過實例操作讓學員熟悉日誌分析的技術。	安興彥	高偉碩	對系統維運日誌分析、事件調查、大資料分析等有興趣之學員。	25人
新竹國網電腦教室	2018/8/28	二	誘捕系統實務	誘捕系統介紹(Kippo、Amun、Dionaea、Nepenthes等)以及誘捕系統操作 誘捕系統日誌分析	誘捕系統介紹與實作	蘇正育	張成睿	對誘捕系統運作與分析有熱誠者，建議具備Linux使用經驗尤佳。	25人
新竹國網電腦教室	2018/9/11	二	網路攻防實務	1. 資訊系統安全管理 2. 入侵過程探討 3. 系統程式弱點分析 4. Web攻擊手法剖析	本課程將介紹駭客入侵手法的概念、特點和技術，並且以實作方式進行駭客入侵手法實作。	陳信文	許清雄	對網站安全性測試有興趣者。建議具備Linux使用經驗與撰寫網站應用程式經驗尤佳。	25人
新竹國網電腦教室	2018/9/26	三	主機效能與系統監控	1. 說明網管系統整體架構 2. 介紹如何安裝及使用網路服務監控軟體 3. 說明如何與google的行事曆相結合，完成一個具有行事曆風格的網管日誌系統	1. 開源碼網路服務監控軟體實作 2. 結合google行事曆之網管日誌功能實作 3. 開源碼網路服務掃描軟體實作	國立中山大學資管系吳惠麟工程師		對於建置開源碼網管系統有興趣者，略懂linux系統尤佳	25人
新竹國網電腦教室	2018/10/9	二	惡意程式分析	1.惡意程式介紹 2.惡意程式分析工具介紹 3.惡意程式分析技術教學 4.惡意程式實作	從近年來的重大資安事件分析結果可以得知，大多數的事件均與惡意程式脫離不了關係，攻擊者往往喜歡透過惡意程式來維持被入侵主機的控制權，以利後續發動更近一步的攻擊。對於資安事件處理人員來說，學習惡意程式分析技術是相當重要的，本課程將針對惡意程式進行介紹，並以實機操作的方式，帶領學員了解惡意程式分析工具的操作方式，以及學習惡意程式分析的技術及方法，輔助學員未來在資安事件處理時，能夠更加	魏宏吉	葉永信	對惡意程式分析技術有興趣的學員，建議至少具備Windows系統操作及Command Line工具使用經驗。	25人
新竹國網電腦教室	2018/10/23	二	網路行為封包分析	1.Wireshark工具使用 2.封包擷取 3.攻擊封包實例分析	本課程將介紹常用網路協定介紹及分析，Wireshark分析工具使用、熟悉BFP過濾器及常用操作技巧 ，進行網路攻擊封包分析，課程將包含上機實作。	張育涵	李柏毅	對網路封包分析有興趣者。	25人