Taiwan Honeynet Project 教育訓練課程

【Security 系列課程】

No.	課程內容	課程內容說明	實作	時數	講師
Security 1-1: 資訊安全實務基礎 **(2 天)** **(基礎課程)**	**資訊安全概論**	說明資訊安全概念、網路攻擊類型、駭客攻擊手法剖析、亦涵括資訊安全營運中心設計與實例分享。本課程將幫助學員建立基礎技術背景，有助後續能量吸收		1	
	網路封包與行為分析	探討 TCP/IP 通訊協定觀念，帶領學員逐步了解網路安全封包分析與網路攻擊行為分析。課程將介紹並帶領學員了解與操作封包監聽軟體 Wireshark，使學員具備網路行為分析能力。	✓	2	
	系統與應用服務安全防護	本課程將介紹安全防護兩大基本主軸，弱點掃描與入侵偵測實務。內容涵括弱點掃描原理、應用與分析，弱點掃描工具 Nessus 教學，以及主機型(Host-based)入侵偵測系統 OSSEC-HIDS 與網路型(Network-based)入侵偵測系統 SNORT 介紹與實際操作	✓	9	
Security 1-2: 誘捕系統技術與實務基礎 **(2 天)** **(基礎課程)**	**誘捕技術概論**	本課程將介紹國際重要資安組織:Honeynet Project，誘捕技術設計原理、誘捕技術與工具發展現況，並介紹 Honeynet Project 台灣支會。		2	
	低互動式誘捕技術	本課程將介紹將深入介紹功能強大的低互動式誘捕工具 Honeyd，帶領學員逐步佈建誘捕系統，收集與分析攻擊資料，本課程更進一步探討如何避免誘捕系統被偵測。	✓	4	

	高互動式誘捕系統	本課程將說明高互動式系統設計原理，並實際帶領學員建置高互動式誘捕系統 ROO Honeywall，以及如何維運與進行資料分析。	✓	6	
Security 1-3: **弱點掃描與入侵偵測系統** **(2 天)** **(基礎課程)**	**弱點掃瞄與入侵偵測系統建置**	本課程將介紹強而有力的 Open Source 資安防護與檢測工具，Nessus(弱點掃描)與 Snort(入侵偵測系統)，課程將由從介紹資安相關背景知識開始，逐步帶領學員從工具的安裝與使用，到報表的分析與呈現，幫助學員快速建立資安防護的能量，並應用於所防護的網路環境。	✓	12	
Security 2-1 : **惡意程式收集與分析** **(1 天)** **(進階課程)**	**惡意程式誘捕技術介紹**	惡意程式為資安事件發生的主因之一，如何收集與分析惡意程式樣本，將會是惡意程式防堵的第一步。本課程介紹如何將誘捕技術應用於惡意程式收集，並帶領學員實際安裝架設惡意程式誘捕系統。	✓	3	
	惡意程式行為分析	介紹現有 Open Source 工具與資源，逐步帶領學員逐步分析惡意程式，解析惡意程式行為模式。	✓	3	
Security 2-2: **網站應用程式安全** **(2 天)** **(進階課程)**	**網站應用程式威脅與防護**	本課程主要介紹網站應用程式的威脅，常見網站應用程式的弱點，網站應用程式的攻擊與防護原理，並介紹 Open Source 網站檢測工具	✓	9	
	Web-based Honeypot	網站應用程式攻擊手法日新月異，Web-Based Honeypot 可幫助我們得知所建置的網站是否含有被攻擊的危險，最新攻擊手法為何，以及哪些人正在窺視網站。	✓	3	
Security 2-3:	**Google Hacking**	Google Hacking 已成為駭客最新攻擊對象收集寶庫，本課程將介紹 Google hacking 原理以及實際應用	✓	3	

惡意網站探測技術 **(2 天)** **(進階課程)**	**Malicious Web Server 探測技術**	上網瀏覽即中毒屬於 Client-Side Attack 的一種，如何分辨網站是否含有惡意連結與惡意程式已成為資安重點研發方向之一。本課程將介紹新一代的 Client Honeypot 設計原理，並帶領學員藉由 Client Honeypot 工具的使用，配合 Goolgle Hacking 的幫助，找出惡意網站並收集網站上的惡意程式	✓	9	
Security 3-1: **系統探測與分析技術** **(2 天)** **(高階課程)**	**Backtrack 工具與應用**	運作 Backtrack Live CD 所提供之各種工具軟體，內容涵蓋系統分析、探測、資料截取等方面，以期提供學員對於資訊安全所需之各項應用技能有深入的瞭解，並能運作所學針對所管理的系統進行分析工作。	✓	12	
Security 3-2: **數位鑑識實務** **(2 天)** **(高階課程)**	**Digital Forensics**	介紹如何利用資訊科技與嚴謹的程序方法，對電腦或相關資訊設備進行蒐證及分析，建立證物保護方式，確保電子證據沒有遭竄改，提供可信及具有法律效力的鑑識報告及電子證據，協助還原事情真相作為法庭審訊及公司重要決策的依據。	✓	12	

【Linux 系列課程】

No.	課程內容	課程內容說明	實作	時數	講師
Linux 1-1: **Linux 系統管理基礎實務** **(2 天)** **(基礎課程)**	**Linux 系統管理與應用技術**	涵蓋各種 Linux 系統常用的管理技術,學習在 Linux 作業系統中進行系統操作，例如：重要的常用指令、檔案系統的介紹、檔案的管理、檔案存取權限的管理、系統排程的管理、文字編輯器的使用、系統紀錄的管理、系統資源的監控、遠端管理機制等方面，以期提供學員對於學習 Linux 所需要具備的重要觀念與應用技術。	✓	12	
Linux 1-2: **Linux 伺服器管理實務** **(2 天)** **(基礎課程)**	**Linux 伺服器管理課程**	透過課程講解及實機操作，讓學員具備 Linux 伺服器建置及維護之能力。	✓	12	
Linux 2-1: **Linux 網路管理平台建置實務** **(2 天)** **(進階課程)**	**網路管理平台建置技術**	課程內容涵蓋目前主流的網管實務技術，包括設備流量監控、流量分析、事件管理技術，配合 Linux 平台與 OpenSorce 建置一個功能完整的網管平台，針對 SNMP 以及 MIB 的運作，有深入與詳細的介紹，並配合實作的課程，加強學員對於網管技術與工具軟體的熟悉程度。預期效益： 提供學員實用之網路管理技術，透過本課程所介紹之應用技術，可以有效建立預警機制，並且掌握現有設備與網路狀況。	✓	12	
Linux 2-2: **Linux 系統與應用服務安全防護系統實務** **(2 天)** **(進階課程)**	**系統安全防護**	本課程為 Linux 作業系統與網路管理的進階課程，介紹如何配合針對 Linux 上常見的網路服務，進行安全的防護，除了確保網路服務能夠正常運作外，也可以提昇系統的安全性，運用各種防護的技術，能夠有效的降底許多的風險。	✓	12	