資訊安全 課程簡介

UCOM資安 | OffSec | ISC2 | EC-Council | CompTIA | 國際標準 | 鑒真數位

OSCP+認證 | 此課程為「數位發展部資通安全署」認可之資通安全專業證照

OSCP

OSCP+ 認證課程：以Kali Linux進行滲透測試

Penetration Testing with Kali Linux

時數：60小時 | 費用：109,000元 | 點數：34點 | 教材：原廠電子教材

課程目標	OSCP+ (OffSec Certified Professional+) 是由 OffSec 推出的國際知名滲透測試實戰證照，在資安攻防戰領域中也是最具公信力的證照之一。 OSCP+ 認證考試採全程實戰進行，考生須在 23 小時 45 分鐘內完成考試，考試完後須在 24 小時內交出一份滲透測試報告。OSCP+ 考試不僅測驗考生的技術能力，也考驗其耐心、毅力和創造力，因為題目可能會有各種陷阱和挑戰，需要不斷嘗試和思考才能解決。對於想要從事或提升滲透測試相關工作的人員來說，OSCP+ 認證有一定程度的價值，因為其可以用於證明應試者具實際操作和解決問題能力，也增加職場上的競爭力與信任度。 Penetration Testing with Kali Linux (PWK / PEN-200) 是一門針對資安攻防實戰的訓練課程，旨在幫助學員準備 OSCP+ 證照考試。課程主要教授常用的滲透測試技巧，包括資訊收集、漏洞掃描、權限提升、維持化與 AD 攻擊等攻擊方式。透過搭配實機練習環境，強化學員準備證照考試能力。
適合對象	資訊安全測試人員、系統安全分析師、系統或網路安全管理人員
預備知識	具備網路資安進階技術
課程內容	1. 網路安全簡介 (Introduction To Cybersecurity) 2. 滲透測試報告撰寫 (Report Writing for Penetration Testers) 3. 資訊收集 (Information Gathering) 4. 弱點掃描 (Vulnerability Scanning) 5. 網頁應用程式攻擊簡介 (Introduction to Web Application Attacks) 6. 常見的網頁應用程式攻擊 (Common Web Application Attacks) 7. SQL 注入攻擊 (SQL Injection Attacks) 8. 用戶端攻擊 (Client-side Attacks) 9. 找出公開漏洞 (Locating Public Exploits) 10. 修復攻擊程式碼 (Fixing Exploits) 11. 規避防毒軟體 (Antivirus Evasion) 12. 密碼攻擊 (Password Attacks) 13. Windows 權限提升 (Windows Privilege Escalation) 14. Linux 權限提升 (Linux Privilege Escalation) 15. 進階通道技巧 (Advanced Tunneling) 16. Metasploit 框架 (The Metasploit Framework) 17. Active Directory 簡介與列舉 (Active Directory Introduction and Enumeration) 18. 攻擊 Active Directory 認證 (Attacking Active Directory Authentication) 19. Active Directory 內的橫向移動 (Lateral Movement in Active Directory)
備註事項	1. 課程包含一次PEN-200認證考試 2. 獨家贈送90天實機演練模擬環境 3. OSCP+ 認證有效期限為三年，期限內欲延長可以透過以下方法 (1)重新認證考試 (2)通過OSEP、OSWA、OSED、OSEE (3)累積OffSec CPE 不繼續維持證照者，3年到期後降回OSCP證照

OSEP 認證 | 此課程為「數位發展部資通安全署」認可之資通安全專業證照

OSEP

OSEP認證課程：進階躲避技術與防禦突破

PEN-300: Advanced Evasion Techniques and Breaching Defenses

時數：60小時 | 費用：129,000元 | 點數：40點 | 教材：原廠電子教材

課程目標	OffSec 的 PEN-300 課程是在 PEN-200 課程基礎上，深入探討對強化目標進行進階滲透測試的技術。學員將在真實情境中實機操作，學習如何繞過安全防禦並客製攻擊程式，進一步提升在道德駭客與漏洞評估方面的專業能力。 課程最終對應到一場具挑戰性的考試做為結束，通過考試後將獲得 OSEP 認證。取得 OSEP 認證象徵著成為具備了進階滲透測試技能的專業人士，將成為企業防禦高端威脅的搶手專家。
適合對象	資訊安全測試人員、系統安全分析師、系統或網路安全管理人員
預備知識	完成OSCP認證課程：以Kali Linux進行滲透測試課程者
課程內容	1. 作業系統與程式設計理論 (Operating System and Programming Theory) 2. 利用 Office 執行用戶端程式碼 (Client-Side Code Execution with Office) 3. 利用 Jscript 執行用戶端程式碼 (Client-Side Code Execution with Jscript) 4. 程序注入與遷移 (Process Injection and Migration) 5. 規避防毒軟體簡介 (Introduction to Antivirus Evasion) 6. 防毒軟體進階規避手法 (Advanced Antivirus Evasion) 7. 應用程式白名單 (Application Whitelisting) 8. 繞過網路篩選器 (Bypassing Network Filters) 9. Linux 後滲透 (Linux Post-Exploitation) 10. Windows 後滲透 (Windows Post-Exploitation) 11. 自助服務終端機突破 (Kiosk Breakouts) 12. Windows 憑證 (Windows Credentials) 13. Windows 橫向移動 (Windows Lateral Movement) 14. Linux 橫向移動 (Linux Lateral Movement) 15. Microsoft SQL 攻擊 (Microsoft SQL Attacks) 16. 攻擊 Active Directory (Attacking Active Directory) 17. 組合各個部分 (Combining the Pieces) 18. 竭盡全力：線上挑戰環境 (Trying Harder: The Labs)
備註事項	1. 課程包含一次PEN-300認證考試 2. 獨家贈送90天實機演練模擬環境

UECR 企業網路靶場Cyber Range實機攻防演練課程

Enterprise Cyber Range Hands-on Workshop

時數：35小時 | 費用：60,000元 | 點數：18點 | 教材：恆逸自製教材

課程目標	在數位時代，網路安全的重要性日益增強。本實作課程旨在提供一個沉浸式的學習環境，通過模擬的網路靶場進行實戰訓練，進一步強化學員的安全技能。學員將在網路靶場環境中，從攻擊與防禦的雙重視角，磨練實戰技巧，學習如何識別及應對各類網路威脅。 課程將以實務操作為基礎，重點在於提升學員對網路攻擊的偵測與防禦能力。在課程中，學員將學習如何有效識別與分析各類網路威脅，並掌握應對措施。防禦情境包括網路攻擊的偵測技術、攻擊事件的分析過程以及建立防範策略。雖然課程中亦會介紹常見的攻擊手法，如網頁應用程式攻擊、系統與Active Directory(AD)環境中的掃描、爆破、入侵及橫向移動等，但重點將放在如何通過有效的防禦手段來抵禦這些威脅。 透過本課程，學員將能夠在不斷變化的網路威脅中立足，提升應對複雜安全挑戰的能力，並增強實戰應變的自信與技巧。
適合對象	對實機攻防操作演練有興趣者
預備知識	本課程為實機操作課程，需具備 Windows與Linux實機操作能力
課程內容	Part I：網路靶場環境介紹 1.如何連接網路靶場 2.如何連接靶場之防火牆與SIEM服務 3.如何使用模擬攻擊 Part II：攻防演練矩陣介紹 1.如何使用ATT&CK矩陣分析駭客攻擊行為 2.如何使用D3FEND矩陣建立與評估有效防禦機制 Part III：紅隊攻擊靶場實戰演練 1.模擬Web攻擊之實戰演練 2.基於ATT&CK矩陣之實戰演練 3.模擬AD攻擊之實戰演練 Part IV：藍隊防禦靶場實戰演練 1.基於D3FEND矩陣之實戰演練 2.AD防禦實戰演練 3.安全防禦之極限挑戰
備註事項	1. 報名課程贈送OffSec Cyber Range2個月(價值超過USD 666，約台幣$20,000元，於開課日期起算) 2. 上過恆逸CPENT或OSCP者，報名再贈送$2,000元即享券

2026新課

OSDA OSDA 認證課程：安全性作業與防禦分析

SOC-200: Security Operations and Defensive Analysis

時數：40小時 | 費用：99,000元 | 點數：30點 | 教材：原廠電子教材

課程目標	本課程旨在培養學員具備防禦導向的資安思維與分析能力，深入理解Security Operations Center(SOC)的核心運作流程與防禦策略。課程將帶領學員熟悉從監控、威脅偵測、警報分類到事件升級的完整流程，並學習如何運用企業級SIEM平台(如 ELK 與 Splunk)進行資料蒐集、關聯分析與惡意活動判讀，培養即時發現與分析攻擊跡象的能力。透過OffSec挑戰式學習模式，本課程結合理論講解與實戰演練，讓學員能親手解析日誌、追蹤攻擊路徑、分析惡意行為並回應真實威脅。完成課程後，學員不僅能奠定進入SOC或藍隊工作的專業基礎，亦可挑戰OSDA(OffSec Defense Analyst)認證，展現其在真實環境中識別、分析與防禦網路攻擊的能力。
適合對象	資安監控分析人員、SOC 分析師、系統與網路安全人員、資安事故與分析人員、有志於加強資安監控與分析技能者
預備知識	建議完成或具備下列課程之知識或技術能力： NSPA：網路安全封包分析認證課程 CEH：EC-Council CEH駭客技術專家認證課程 CND：藍隊資安防禦通識-EC-Council CND認證課程
課程內容	1. 攻擊方法概論(Attack Methodology Introduction) 2. Windows端點簡介(Windows Endpoint Introduction) 3. Windows伺服器端攻擊(Windows Server-Side Attacks) 4. Windows用戶端攻擊(Windows Client-Side Attacks) 5. Windows權限提升(Windows Privilege Escalation) 6. Windows持續性維護(Windows Persistence) 7. Linux端點簡介(Linux Endpoint Introduction) 8. Linux伺服器端攻擊(Linux Server-Side Attacks) 9. 網路偵測(Network Detections) 10. 防毒警示與規避(Antivirus Alerts and Evasion) 11. 網路規避與通道技術(Network Evasion and Tunneling) 12. Active Directory枚舉(Active Directory Enumeration) 13. Windows橫向移動(Windows Lateral Movement) 14. Active Directory持續性維護(Active Directory Persistence) 15. SIEM第一部份(SIEM Part One) 16. SIEM第二部份(SIEM Part Two)
備註事項	1. 課程包含一次SOC-200認證考試 2. 獨家贈送90天實機演練模擬環境