國立台灣科技大學 114學年 第2學期　課程大綱

Spring 2026 NTUST Course Outline

授課教師：邱建樺

Instructor:CHIU, CHIEN-HUA

課程名稱：資訊系統與作業安全

Course Title：Information System and Operational Security

2026/11/4

課程代號： MI5318701 Course Code 學分數： 3 Credits	必選修：選修/半學年 Required/Electve:Elective/Half Yr. 先修課程： Prerequisites
節次教室： Time/Location	T2(IB-509) T3(IB-509) T4(IB-509)
專業核心能力： Core Professional Competencies	解決問題之能力(Problem Solving)
課程網址： Course Website	
課程宗旨： Course Objectives	本課程內容從企業環境中常見的攻擊行為與威脅情境出發，探討現代資訊系統在作業系統、身分認證、網路通訊與安全監控層面所面臨的風險。教學範圍涵蓋 Windows 與 Linux 作業系統之端點與伺服器環境，分析憑證濫用、可疑登入、暴力破解、惡意程式植入、權限提升、橫向移動與持久化等攻擊行為，並著重於這些行為在系統與網路層所留下的事件與日誌跡象。 在此脈絡下，課程以資安藍隊（Blue Team）技術為主要教學取向，採取高度實務導向的教學方式，透過系統事件紀錄、網路行為、入侵偵測與安全監控平台（SIEM／ELK Stack）的實作與分析，培養學生從防禦與營運角度進行攻擊偵測、事件關聯與判讀的能力。課程同時涵蓋 Active Directory 環境的權限結構與稽核、防毒與行為式偵測機制，以及網路規避與通道技術的防禦觀點，使學生能建立完整的藍隊分析思維，具備支援資安監控與事件回應（SOC）工作的實務基礎。
課程大綱： Outline of Lectures	本課程以企業實務環境中的資訊系統安全為背景，從防禦與營運角度出發，系統性探討作業系統、身分認證、網路行為與安全監控相關議題。課程內容涵蓋下列主題： 1. 資訊系統安全概論與攻擊者行為模型 2. Windows 作業系統架構與端點安全 3. Windows 伺服器端攻擊行為與事件跡象分析 4. Windows 用戶端攻擊行為與社交工程風險 5. Windows 權限提升與錯誤設定之防禦觀點 6. Windows 持久化攻擊技術與系統事件偵測 7. Linux 作業系統架構、端點與伺服器安全 8. Linux 伺服器端攻擊行為與登入異常分析 9. Linux 權限提升與後門植入行為偵測 10. 網路入侵偵測系統（IDS）原理與規則設計 11. 網路攻擊行為與 C2 通訊模式之偵測分析 12. SIEM 系統概念與安全事件集中管理 13. SIEM／ELK Stack 實作：日誌蒐集、查詢與事件關聯 14. Active Directory 架構、身分認證與權限模型 15. Active Directory 枚舉、橫向移動與持久化行為分析 16. 防毒機制、網路規避與通道技術之防禦
授課方式： Method of Instruction	講授 Lecture：60% 分組討論 Group discussion：10% 案例研討 Case study：20%

	操做練習 Practical exercises：10% 講授 Lecture：%
教科書： Textbooks	
參考書目： References	
修課須知： Notice	
評量方式： Grading	平時作業: 40%; 期末考: 30%; 期末專題: 20%; 課堂參與: 10%
備註說明： Notes	