2025 年【科學探究競賽-這樣教我就懂】

普高組　成果報告格式

題目名稱：資訊安全技術入門：Kali Linux 的應用示範

一、摘要

本研究聚焦於資訊安全技術，透過 Kali Linux 進行滲透測試與防禦模擬，讓初學者能夠快速建立資安意識與操作能力。隨著網路攻擊日益頻繁，許多個人與企業因資安知識不足而遭受損失，因此，我們設計了一本簡單易懂的「資訊安全防護手冊」，以教學方式引導使用者理解資安核心概念，並實際操作如：Nmap 網路掃描、Wireshark 封包分析與 Metasploit 漏洞測試等工具。本研究採用文獻分析與實作驗證，並透過實地教學測試學習成效，結果顯示手冊能有效提升初學者的資安技能，且具備推廣應用價值。最終，我們期望透過此研究降低一般使用者的網路風險，並提升資訊安全教育的普及性。

二、探究題目與動機

本研究的探究題目為「資訊安全技術入門：Kali Linux 的應用示範」，主要動機來自現今網路攻擊頻率增高，但多數人對資安知識仍相當薄弱。許多駭客攻擊並非高階技術，而是透過釣魚郵件、弱密碼等方式入侵，因此建立資安防護意識至關重要。我們選擇 Kali Linux 作為主要教學工具，因其整合多種資安測試工具，適合初學者學習基礎防禦與攻防技術。我們希望透過撰寫手冊與設計實作教學，幫助使用者快速掌握資安技能，避免成為網路攻擊的受害者。本研究不僅提升個人資安素養，也能為學校與企業提供有效的資安教育參考。

三、探究目的與假設

（一）探究目的：

1、提升資安意識：讓初學者理解網路安全的重要性，避免因資安知識不足而遭受攻擊。

2、建立實作能力：透過 Kali Linux 的工具學習基礎攻防技術，如 Nmap 掃描、Wireshark 封包分析等。

3、設計教學資源：撰寫簡單易懂的「資訊安全防護手冊」，幫助無經驗者快速入門資安領域。

4、驗證學習成效：透過課堂教學與使用者回饋，測試手冊是否能有效提升學習者的資安技能。

（二）研究假設：

1、使用者在學習手冊後，能正確理解資安核心概念（如風險防範、漏洞測試）。

2、初學者可在指導下使用 Kali Linux 進行基本的資安測試與防禦操作。

3、手冊能降低學習門檻，使無經驗者在短時間內掌握基礎資安技能。

4、透過教學驗證，學習者能在實際操作中應用所學，提高資安應對能力。

四、探究方法與驗證步驟

本研究在探究方法的設計上，結合了文獻分析與實作驗證兩大核心策略，並透過課堂教學與使用者回饋，全面評估「資訊安全防護手冊」的教學成效與操作可行性。為了讓初學者能夠在短時間內掌握資安基本技能，我們以科學探究精神為基礎，設計出一套可驗證的學習流程與操作模組，確保研究不僅有理論基礎，更具有實際應用價值。

首先，在文獻分析法部分，我們蒐集並分析多篇與資訊安全、Kali Linux 工具與社會工程學相關的學術資料，作為編寫手冊內容的理論依據。透過整理資料，我們深入了解現今資安風險的演變趨勢與防禦策略的發展現況，並從中選擇最具代表性的實作工具作為教學主軸，例如：Nmap 用於網路掃描、Wireshark 用於流量監控、Metasploit 作為漏洞利用框架等。同時，我們也參考市面上既有的資安教材與防護手冊，分析其優缺點，並根據初學者需求重新規劃架構與語言深度，讓內容既專業又親民，確保無資訊背景的學習者也能理解與操作。

在實作研究法方面，我們於實驗環境中建立完整的模擬測試場域，包括配置不同作業系統（如 Windows、macOS 與 Kali Linux）、設定虛擬機、搭建模擬網路環境等，以進行網路掃描、釣魚測試、漏洞分析等操作練習。我們以「由淺入深」的原則，逐步引導使用者進行操作，並記錄操作步驟、可能錯誤與解決策略，確保每一階段皆具備教學再現性。舉例來說，在進行 Nmap 掃描時，我們會同時說明 IP 結構與端口原理，讓學習者在理解背後原理的同時實際操作，提高學習深度。

此外，我們設計了研究流程圖與驗證步驟，將整體探究歷程劃分為六個階段：（1）目標群體分析、（2）安全概念導入、（3）手冊內容編排、（4）Kali 工具實測、（5）實地教學與觀察、（6）回饋修正與手冊優化。這樣的流程安排有助於在每個階段進行成效評估與問題調整。例如在課堂教學環節，我們實際對同儕進行手冊授課，觀察學習者的理解程度與實作成效，並發放意見回饋單，分析其學習瓶頸與建議修正內容，作為下一版手冊的優化依據。

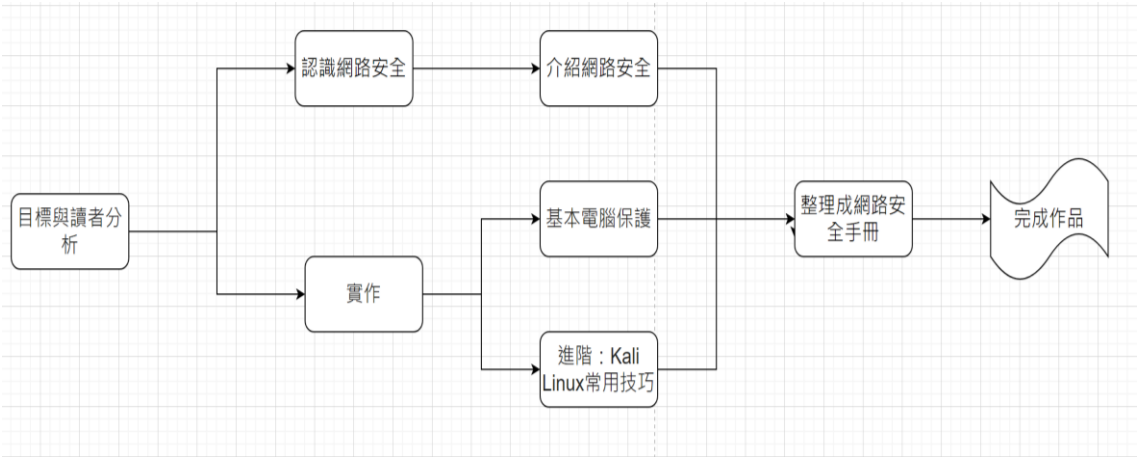

圖 1：研究流程圖

在驗證假設方面，我們聚焦於使用者是否能夠在閱讀手冊後成功完成指定操作任務，例如掃描目標端口、分析封包內容或使用 Metasploit 發現漏洞等。我們將操作過程分為數個標準任務節點，並觀察學習者是否能無誤執行各步驟。根據初步實測結果，大多數學習者在閱讀手冊後，能於 30 分鐘內完成基礎滲透測試任務，且對於 Kali 工具的操作理解度明顯提升，顯示本研究設計的手冊具有實際教學價值與實作引導功能。

為了更全面評估本專題手冊在實務推廣與教育應用上的優劣勢，我們針對本研究進行 SWOT 分析，探討其內部優勢與劣勢，以及外部機會與挑戰，作為後續優化與延伸應用之參考依據。

Strengths 優勢	Weekness 劣勢
1.手冊內容簡單易懂，適合初學者使用 2.針對不同層次的使用者設計，能有效提升安全意識和防護能力	1.對於完全不熟悉 Linux 系統介面的使用者來說，學習曲線仍存在 2.相關高級工具的操作可能超出初學者的理解範圍
Opportunities 機會	**Threats 威脅**
1.網絡安全需求上升，個人與企業急需資安入門級別的安全知識與指導 2.本手冊可作為大眾學習資訊安全的入門教材	1.市場競爭激烈，存在許多針對專業人士的安全書籍，內容技術性強，對於專業需求具有更高的吸引力 2.專業書籍和指南的技術深度較大，可能對本手冊的市場吸引力構成威脅

表一：資安防護手冊之 SWOT 分析

總體而言，本研究的探究方法嚴謹結構化，兼具理論與實作雙重導向，不僅確保手冊內容具有正確性與專業性，也強調學習成效的可驗證性。我們相信，若能持續優化本研究架構，未來將有機會推廣至更多教育場域與資安培訓領域，為資訊安全教育開啟更廣泛的應用契機。

五、結論與生活應用

本研究透過「資訊安全防護手冊」的編撰與 Kali Linux 操作實作，證實即使是資安領域的初學者，只要搭配合適的教學資源與有邏輯的學習流程，也能有效建立起網路安全的基礎能力，進而保護個人資料與系統安全。結論可分為三個主要層面說明：資安意識的提升、操作能力的建立與教學資源的推廣性。

首先，資安意識的提升為本研究最直接且顯著的成果。透過手冊內容中對「資安三要素」──機密性（Confidentiality）、完整性（Integrity）與可用性（Availability）的闡述，搭配實例說明如釣魚信件、資料外洩、DDoS 攻擊等常見威脅，讓學習者能在閱讀過程中迅速建立「網路世界不是完全安全」的正確認知。這種意識的建立，對於日常生活中習慣輕忽帳號密碼、任意點擊陌生連結或未更新防毒程式的使用者而言，具有實質的警示與導正作用，也提供了 可依循的自我防護流程與應對策略。

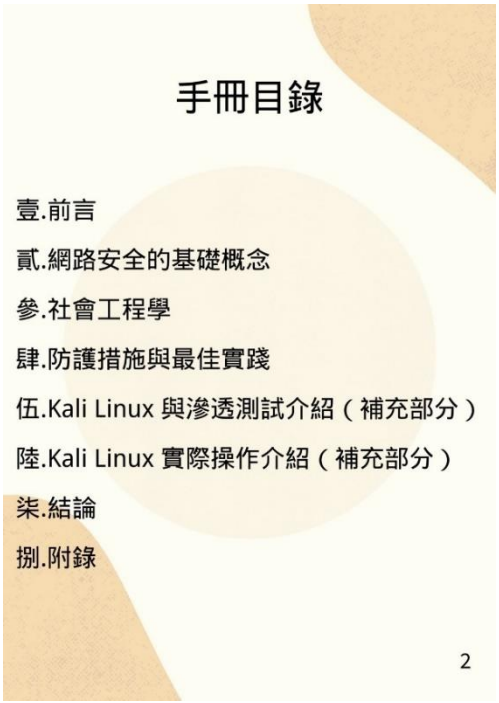

圖 2：手冊的目錄

圖 3：手冊有關資訊安全的描述

其次，操作能力的建立是本手冊的另一項核心成就。Kali Linux 雖為資安專業平台，但透過分段式、任務導向的教學架構，我們成功將如 Nmap、Wireshark 與 Metasploit 等工具模組化呈現，讓初學者在「知道為什麼」的同時也能「知道怎麼做」。這樣的學習模式可應用於多種場景，例如：在公共 Wi-Fi 中辨識不安全熱點、於職場中執行網路掃描偵測異常封包、或在家中檢查個人路由器是否存在已知漏洞等情境，皆能透過手冊中所學之技能加以應用，實現「將資安落實於生活」的目標。

再者，本手冊設計具有高度推廣性與可延展性。無論是中學資訊課程、職場基礎資安訓練，抑或是一般社區電腦教學中心的成人課程，本研究所開發的學習資源皆可作為教材範本進行導入與延伸。手冊已證實具備教學清晰、操作可行、學習友善的特性，未來若能結合數位教學平台，如製作教學影片、開設線上互動模擬或設計資安挑戰賽（CTF），將可進一步擴大其教育影響力，帶動全民資安素養的提升。

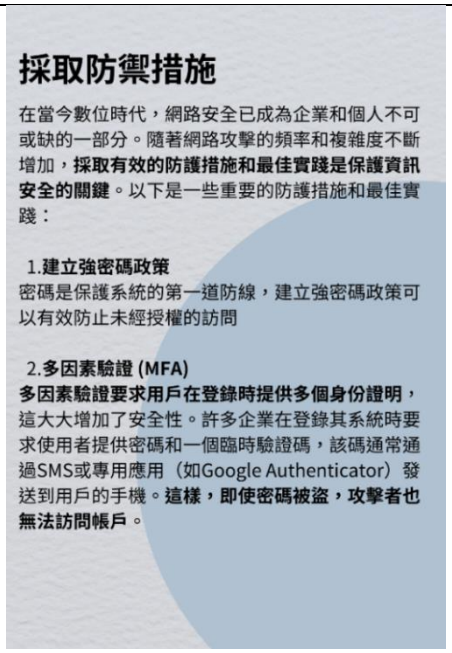

圖 4：手冊中系統防護措施的介紹

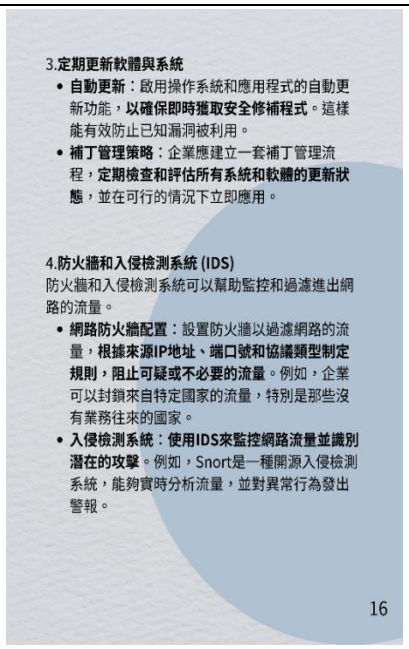

圖 5：手冊中系統防護措施的介紹

在生活應用層面，本手冊內容的延伸價值相當多元。舉例來說，一般家庭成員可以透過學習 OSINT（開源情報蒐集）技術，避免於社群媒體過度揭露個人資訊，降低社會工程攻擊風險；中小企業主可以透過手冊中的滲透測試流程，自行檢視內部網路架構是否有開放性漏洞，及早修補防火牆與端口設定，避免遭勒索軟體入侵；學生族群亦可透過 Wireshark 監控封包行為，了解網路環境是否受到監控或資安異常，進而保護個人隱私權。

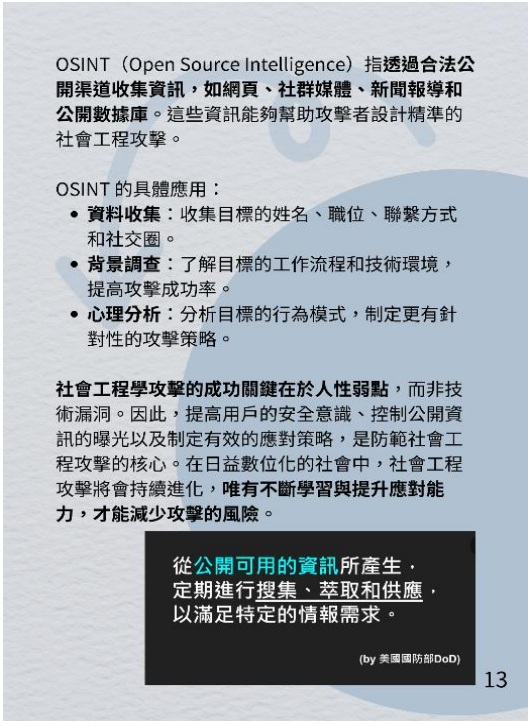

圖 6：手冊中 OSINT 的描述

圖 7：Kali Linux 常用工具介紹

為了驗證「資訊安全防護手冊」的實用性與可操作性，我們特別安排了實地課程實測，實際位同學授課的結果顯示，手冊能有效幫助用戶理解網路安全的基本原理，並能夠透過對 Kali Linux 進行簡單的滲透測試和防護操作。測試同學的反饋表明，該手冊對於初學者來說操作點單、指引清晰，適合入門學習的教材。

圖 8：實際授課照片

結合前述成果與實測回饋，我們可以確定：資訊安全不應只是科技領域的研究課題，而應成為現代生活中的一種基本素養與生存能力。本研究手冊正是朝此方向邁出的一步，不僅解決了初學者無從下手的學習難題，也讓資安教育能夠更貼近人們的生活需求與應用場景。

未來，我們期望這份專題成果不僅止步於校內展示，而能擴展為實質應用的學習工具，提供給更多對資訊安全感興趣，卻無從入門的大眾使用，最終實現「從教育端建構資安防線」的長遠目標。

參考資料

林欣慧（2022）。**個人網路安全行為影響因素之探討**。國立中央大學資訊管理學系：碩士論文。

林信漳（2018）。**網路安全與網路攻擊偵測之研究**。國立東華大學資訊工程學系：博士論文。

陳煥文（2019）。**行動網路安全機制之研究**。國立臺中科技大學 資訊工程系碩士班：碩士論文。

高廷瑋（2018）。**開源碼網站之安全性滲透測試研究-以 Kali 平台為例**。國立高雄科技大學資訊管理系研究所：碩士論文。

中關村在線（2024 年 07 月 14 日）。操作系統大對決 Windows、macOS 還是 Linux 哪款最適合你。https://reurl.cc/oyK0E3。

Denis, M., Zena, C., & Hayajneh, T. (2016). Penetration testing: Concepts, attack methods, and defense strategies. *In 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT)* (pp. 1-6). IEEE.

Nobili, M. (2023, September 01). Review OSINT tool for social engineering. *Frontiers in Big Data, 6*, 1169636. https://reurl.cc/xvKlG4