

明道中學高中部資訊類專題

113 學年度

專題作品說明書

資訊安全技術入門：Kali Linux 的應用示範

高二十二班 21s361 盧長豐

高二十二班 21s142 嚴煜璽

指導老師：陳郁弦 老師

中 華 民 國 1 1 4 年 3 月 1 7 日

目錄

摘要.....	1
壹、前言.....	2
一、研究動機.....	2
二、研究目的.....	2
貳、文獻探討.....	3
一、網路安全相關文獻.....	3
二、台灣資訊安全的現況.....	4
三、防毒軟體比較.....	4
四、認識 Kali Linux	6
五、Kali Linux 滲透測試的流程	8
六、認識社會工程學－OSINT	8
參、研究方法.....	10
一、研究方法.....	10
二、研究架構.....	10
三、研究流程.....	11
肆、研究過程與方法.....	12
一、資安防護手冊編寫.....	12
二、課程實測.....	15
三、手冊比較分析.....	16
四、SWOT 分析與比較	16
伍、研究結論與建議.....	17
一、結論.....	17
二、建議.....	18
陸、參考文獻.....	19

摘要

在數位轉型加速的時代，資訊安全已成為企業與個人不可忽視的風險管理課題。然而，許多使用者對資安防護的基本概念與實務操作仍缺乏認識，導致容易成為網路攻擊的目標。本研究聚焦於開發一本專為初學者設計的 Kali Linux 資安防護手冊，透過系統化教學，協助使用者快速掌握關鍵資安技術，提升個人與企業的防禦能力。

本手冊內容涵蓋 Kali Linux 的核心工具與應用，包括網路掃描、漏洞分析、社會工程情報蒐集（OSINT）等，並搭配實作示範，以強化學習者的操作技能與資安意識。此外，為提升學習效率，本研究針對手冊的可讀性、學習曲線及實務應用性進行優化，確保零基礎使用者能夠循序漸進地掌握概念，並具備進一步應用於進階資安測試的潛力。

實測結果顯示，本手冊可顯著提升使用者的資安認知與防護能力，適合作為企業內部資安培訓、學校資安教育課程，或資安相關職場人士的自學參考。未來，本研究將進一步擴展手冊內容，涵蓋更高階的資安技術，並整合線上學習平台與互動資源，以打造更完整的資安學習生態系，協助企業與個人強化網路安全防護能力，落實資安風險管理。

關鍵字：資安防護、初學者手冊、Kali Linux

壹、前言

一、研究動機

在當今資訊飛速發展的時代，資訊安全的重要性日益凸顯。隨著科技的進步和網際網路的普及，個人、企業和政府機構對網路技術的依賴程度越來越高。然而，這也帶來了前所未有的安全挑戰和風險。網路攻擊、數據洩露、釣魚攻擊及資訊詐騙等威脅屢見不鮮，給各行各業帶來了極大的困擾和損失。因此，資安的研究和能力提升成為了當務之急，迫使各行業在這一領域投入更多的資源和精力。

透過深入研究網路安全，我們可以全面了解黑客的攻擊手法及其背後的運作原理，從而制定更加有效的防禦策略，以保護個人隱私和企業敏感資訊。這不僅是為了防止財產損失和數據洩露，更是為了維護社會的穩定和信任。在這樣的大背景下，本研究旨在編寫一份簡明易懂的電腦防護手冊，幫助一般用戶建立基本的網路安全意識，並透過 Kali Linux 的實例操作，教授用戶如何應對常見的資訊安全挑戰。藉由這份手冊，讀者不僅能夠學習到基本的網路安全知識，還可以掌握實用的防護技巧，從而在面對日益複雜的網路威脅時具備相應的應對能力。

二、研究目的

本研究旨在撰寫一份**實用且易於理解的資安防護手冊**，針對一般使用者與企業內部員工，建立基礎資安意識，並透過 Kali Linux 的實作示範，提升使用者應對資訊安全威脅的能力。本手冊不僅適用於個人學習，也可作為企業資安培訓的參考教材，強化組織內部的防護機制。

- (一) **建立資訊安全基礎認知**: 介紹個資保護、安全上網、系統更新等核心概念，幫助讀者理解常見資安風險，強化日常防護能力。
- (二) **提升電腦與數據防護能力**: 學習資料備份、密碼管理、防範社交工程攻擊等技巧，降低遭受駭客入侵與詐騙的風險。
- (三) **運用 Kali Linux 進行滲透測試**: 透過模擬攻擊找出系統漏洞，掌握基本資安檢測技術，並學習有效的防禦策略，以強化整體安全性。

本研究透過理論與實務並行的方式，幫助使用者快速掌握資安防護要點，並透過 Kali Linux 進行實作演練，以強化應對網路攻擊的能力。未來，本手冊可進一步應用於企業內訓、學術教育及個人進修，推動資訊安全意識的普及，降低因資安問題導致的營運風險。

貳、文獻探討

一、網路安全相關文獻

表 1：網路安全之文獻

主題	文章標題	作者與年份	摘要	心得
網路安全的影響	個人網路安全行為影響因素之探討	林欣慧 (2023)	網路安全知識對資訊自我效能與網路安全行為有正向影響；網路安全態度對網路安全知識、資訊自我效能與網路安全行為有正向影響	本研究凸顯網路安全知識與態度的重要性，強調提升資訊自我效能能有效促進安全行為，對未來安全教育具有參考價值。
網路攻擊存在隱患	網路安全與網路攻擊偵測之研究	林信漳 (2018)	建構具自適應能力的入侵偵測系統，以分析未知攻擊並迅速定位來源與模式，是網路安全的重要課題。	本研究強調自適應網路入侵偵測的重要性，致力於快速識別未知攻擊來源與模式，為強化網路安全提供有效解決方案。
資訊攔截與抵禦	行動網路安全機制之研究	陳煥文 (2019)	由於傳輸媒體的特質，任何人都可以竊聽或攔截無線傳輸的訊息。此屬性使得身份驗證對在安全性的確保上為一重要因素。在本研究中，我們將詳細說明上面兩個為全球移動網路設計的安全方案所無法抵禦之攻擊及安全缺失。	本研究強調無線傳輸的安全風險，凸顯身份驗證的重要性，並深入分析現有方案的漏洞，為未來安全機制改進提供參考。

表 1 資料來源：研究者自行彙整

二、台灣資訊安全的現況

隨著全球數位化發展加速，台灣的資訊安全挑戰日益嚴峻。網路攻擊頻率持續上升，特別針對高科技產業、金融機構、政府機關等關鍵領域，攻擊手法也日趨多元，除了傳統的勒索軟體、社交工程，還出現了供應鏈攻擊、AI 生成威脅等新型態資安風險，對台灣整體商業環境與國家安全構成重大挑戰。此外，生成式 AI 的快速發展，使深偽技術 (Deepfake)、資訊操控等問題更加複雜，進一步提升企業與政府在資安治理上的難度。

(一) 資安產業發展與人才需求

儘管網路威脅增加，台灣的資安產業仍持續成長，企業對資安解決方案與專業人力的需求日益增加，顯示出資安市場的高度發展潛力。目前，台灣企業普遍關注資安合規 (如 ISO 27001、NIST、GDPR)，並投入資源強化防禦機制。然而，資安人才的短缺仍是產業發展的瓶頸，特別是在金融、醫療、政府單位等領域，資安專業人才供不應求，導致企業在資安防禦上面臨更多挑戰。

(二) 資安意識與市場趨勢

近年來，台灣企業與民眾對於資訊安全的重視程度提升，尤其對於來自境外的網路攻擊感到高度警戒。然而，多數企業與個人對資安政策的落實仍存在一定落差，對政府資安防禦能力的信任度也尚待提升。在兩岸關係與國際政治局勢變化的影響下，台灣企業與政府正積極推動資安防禦措施，如強化資安法規、提升攻防演練、推動資安技術升級等，以應對日益複雜的網路攻擊風險。

綜觀台灣資安現況，無論是政府、企業或個人，都必須加強資安意識與防護能力。未來，台灣應持續深化資安技術創新、強化產學合作、推動資安教育，並結合 AI 技術與大數據分析，提升整體資安防禦能力，以因應全球資安趨勢與日益嚴峻的網路威脅，確保企業營運與國家安全的穩定發展。

三、防毒軟體比較

在資訊安全管理中，傳統防毒軟體主要針對已知病毒、惡意程式 (Malware) 與網路攻擊進行偵測與攔截，透過特徵碼比對與行為分析來提供基本防護。然而，隨著資安攻擊手法日益進化，企業與資安專業人員對於更高階的安全工具需求逐漸增加，這時 Kali Linux 的進攻性防禦與滲透測試功能便成為重要選擇。

Kali Linux 相較於市面防毒軟體的優勢：

- (一) **進攻性資安測試能力**：Kali Linux 提供完整的滲透測試(Penetration Testing) 與紅隊演練 (Red Teaming) 工具，可模擬駭客攻擊行為，協助企業找出防護弱點，而傳統防毒軟體則多以防禦為主，較少具備進攻性測試功能。
- (二) **深度漏洞掃描**：內建 Nmap、Metasploit、Burp Suite 等專業資安工具，能夠針對網路環境與系統漏洞進行全方位檢測，相較於一般防毒軟體的被動監控，Kali Linux 能提供更細緻的資安分析與修補建議。
- (三) **開源與高度可客製化**：與市面上封閉式的防毒軟體不同，Kali Linux 為開源系統，使用者可根據企業需求進行**自訂防護策略**，更靈活地強化資安管理。
- (四) **適用於資安教育與企業內部測試**：許多企業開始導入 Kali Linux 進行資安訓練，幫助資安團隊熟悉駭客攻擊手法，強化防禦能力，這是傳統防毒軟體無法達成的效果。

Kali Linux 在進攻性測試、漏洞發現、自訂化安全策略和深度網路分析等方面，提供了比傳統防毒軟體更高層次的安全防護。它主要適用於資安專業人士和進階用戶，用來**加強系統防禦並主動識別漏洞**。雖然防毒軟體提供的是防禦性保護，並能夠阻擋已知威脅，但它無法像 Kali 一樣提供如此全面、深度的測試和漏洞發現功能。

表 2：Kali Linux 防護優勢 vs. 傳統防毒軟體

優勢	Kali Linux	傳統防毒軟體
漏洞發現與修補	可以發現系統中的零日漏洞，並提供加強安全配置的建議。	只能防範已知的病毒、惡意軟體，對零日漏洞防護有限。
高自訂性	完全自訂化測試環境和工具，適合特定的資安需求。	配置選項少，主要依賴預設防禦策略。
全面性測試工具	包含 Metasploit、Nmap、Wireshark 等高級工具，用於深入測試和分析。	多為基本的病毒掃描和行為分析，無法提供滲透測試功能。
錯誤報告率	只會報告經過測試的實際漏洞，無誤判情況	防毒軟體可能會出現誤判，標記無害檔案為惡意。
安全性檢測深度	提供深度的滲透測試，能測試各種潛在的漏洞和攻擊手段。	主要防禦已知的惡意程式和病毒，無法進行深度的安全測試。
網路與封包監控	具有高級的網路流量分析和封包檢測工具(如 Wireshark)，可以偵測異常行為。	主要關注本地端的檔案掃描，無法實時監控網路流量。

表 2 資料來源：研究者自行彙整

雖然傳統防毒軟體仍是企業資安防護的基礎，但隨著攻擊手法變得更加複雜，Kali Linux 作為進攻性測試與防禦強化的工具，在企業資安戰略中扮演越來越重要的角色。未來，企業應考慮整合主動防禦（Kali Linux 滲透測試）與被動防護（傳統防毒軟體），以提升整體資安防護層級，降低遭受攻擊的風險，確保企業營運安全。

四、認識 Kali Linux

Kali Linux 是一款專門為數字取證和滲透測試設計的開源操作系統，由 Offensive Security 團隊開發。它基於 Debian 系統，內置了數百種網路安全、數字取證、逆向工程以及應用程序評估的工具。利用 Kali Linux 中提供的工具進行了深入的實務測試，說明一套完整的滲透測試的思維、流程、步驟和結果輸出等給各位網路管理者提供參考（高廷璋，2018）。以下是 Kali Linux 的核心特點及優勢簡介：

- （一）豐富的滲透測試工具：Kali Linux 包含了超過 600 種預裝的安全工具，涵蓋了從網路掃描、漏洞探測到應用程式分析和逆向工程的各個方面。

表 3：Kali Linux 滲透工具介紹表

工具名稱	功能描述	使用範圍
Nmap	網路掃描工具，用於發現網路上的設備和服務，進行端口掃描。	網路掃描、端口掃描
Metasploit	漏洞利用框架，用於發現並利用系統漏洞，執行安全測試。	漏洞利用、滲透測試
Wireshark	網路流量分析工具，能夠捕獲並分析網路數據包。	網路分析、流量捕獲
Aircrackng	無線網路破解套件，能夠破解 WEP 和 WPA/WPA2 加密的無線網路。	無線網路破解、密碼破解
Burp Suite	網頁應用程式安全測試工具，提供多種功能來識別和修復 web 應用程序漏洞。	Web 應用安全測試
John the Ripper	密碼破解工具，能夠破解多種加密格式的密碼。	密碼破解、密碼強度測試
Nikto	網頁服務器掃描工具，用於檢測網頁服務器上的漏洞和配置錯誤。	Web 服務器安全掃描
Hydra	暴力破解工具，用於破解多種協議的登錄認證。	密碼暴力破解、登錄破解

表 3 資料來源：研究者自行彙整

- (二) **專為滲透測試設計**：Kali 被設計來協助安全專業人員進行各種滲透測試，它的目的是讓使用者能夠模擬各種網路攻擊，找到系統中的漏洞和弱點。它為滲透測試的各個階段提供支持，包括資訊收集、漏洞利用、後滲透行動等。
- (三) **高度可定制性**：Kali 提供了強大的靈活性，允許使用者根據他們的需求自定義操作系統。你可以選擇安裝或移除工具、修改界面以及配置腳本來自動化任務。
- (四) **強大的社區支持**：Kali 的使用者社群十分活躍，提供了大量文檔、論壇、視頻教程等資源。這使得即使是初學者也能快速學習和上手，並從經驗豐富的用戶處獲得幫助。

綜上所述，Kali Linux 是一款功能強大且靈活的網路安全平台，被廣泛用於安全測試、滲透測試和數字取證等領域。如果你對網路安全和數字取證感興趣，它將是學習和提升技能的理想選擇。如下表四所示，Kali Linux、Windows 與 macOS 比較表。

表 4：Kali Linux、Windows 與 macOS 比較表

比較項目	Kali Linux	Windows	macOS
工具與功能數量	專為滲透測試和安全研究設計，內建超過 600 種安全工具	廣泛兼容多種硬體和軟件，提供全面的應用程序支持	與 Apple 硬體緊密整合，性能優化良好
靈活性與使用方式	開源且免費使用，靈活性高，可以從 USB 或 Live CD 啟動	強大的商業支持和用戶社群，技術支持服務完善	強大的用戶界面和穩定性，適合創意工作和日常使用
硬體支援與更新	支援多種硬體和虛擬機，適合專業的安全測試需求	自動更新系統和應用，保持最新的功能和安全補丁	定期自動更新，內建多種安全功能，較少受到病毒攻擊
適用性與穩定性	不適合日常使用，工具可能影響系統穩定性	常成為病毒和惡意軟件的攻擊目標，需額外安裝防護軟件	僅支持 Apple 硬體，對於非 Apple 硬體的支援有限
技術要求與成本	可能需要較高的技術知識，對普通用戶來說不夠友好	收費授權，部分版本需要購買	收費且需購買 Apple 的硬體，操作系統隨硬體預裝
更新與維護依賴性	更新和維護主要依賴手動，安全性可能較低	系統和更新可能影響性能，預裝應用程序可能佔用系統資源	硬體和軟件的可選擇性較少，對於一些專業需求可能不夠靈活

表 4 資料來源：研究者彙整分析。參考網站：中關村在線(2024 年 7 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>。

五、Kali Linux 滲透測試的流程

Kali Linux 滲透測試的過程可以幫助評估系統的安全性，發現潛在的安全漏洞，並提供改進建議，其運作流程如下表五所示。**Kali Linux 工具在滲透測試中的應用廣泛，包括智慧型手機滲透測試、藍牙通信的攻擊、網路流量嗅探以及對 WPA 保護的 Wi-Fi 進行破解等等 (Denis, et al., 2016)。**

表 5：Kali Linux 滲透測試的流程表

運作流程	說明
資訊蒐集	收集目標網路的基本資訊，如 IP 位址、網域、網路架構等。此步驟包括主動和被動資訊收集。
掃描與枚舉	使用掃描技術來探測開放端口、服務和潛在的弱點，並枚舉具體服務和操作系統等詳細資料。
弱點分析	根據前面步驟的掃描結果，分析網路中的弱點並進一步挖掘可利用的漏洞。
漏洞利用	利用已知漏洞進行滲透，獲取對目標系統的控制權或提高權限。
維持訪問	一旦進入目標系統，設置後門來保持持續訪問，這可以讓測試者隨時進入系統進行進一步的操作。
清理痕跡	隱藏滲透測試的痕跡，移除日誌和歷史記錄，以避免被系統管理員發現。
報告與分析	總結滲透測試的結果，記錄發現的漏洞、已利用的弱點和建議的安全措施，提供給相關部門。

表 5 資料來源：研究者自行彙整

六、認識社會工程學—OSINT

公開來源情報 (Open Source Intelligence, 簡稱 OSINT) 是指透過合法且公開的渠道收集資訊，這些來源包括網際網路、社群媒體、新聞報導、公開數據庫等等。OSINT 的核心在於從未受保護的公共領域獲取資訊，而非依賴任何非法或未授權的手段進行情報收集。作為一種技術，開源情報在從公開可用的來源中尋找有價值的資訊方面發揮重要作用，並在滲透測試中具有其關鍵性 (Nobili, 2023)。

(一) OSINT 在社會工程學中的應用

- 1、資訊收集：採用 OSINT 搜集目標的姓名、職位、聯絡方式、社交關係等，幫助設計更精確的攻擊，如針對特定對象的釣魚攻擊。
- 2、背景調查：了解目標的工作環境、公司結構、常用技術等，增加社會工程攻擊成功的可能性。
- 3、情報分析：分析公開資訊，預測其行為模式與心理特徵，優化攻擊策略。

(二) OSINT 技術和工具

- 1、搜尋引擎：利用 Google、Bing 高級搜尋語法精確查找目標資訊。
- 2、社群媒體：從 Facebook、LinkedIn、Twitter 獲取個人資訊與活動記錄。
- 3、數據外洩檢查：透過 Have I Been Pwned 等工具查找外洩資訊。
- 4、公開資料庫：查閱公開的政府或公司數據庫，獲取組織結構和法律資訊。
- 5、圖像搜索：利用 TinEye、Google 反向圖像搜尋識別圖片來源與位置。

(三) 網路社會工程學 vs. 公眾社會工程學

社會工程學已發展出不同分支，其中網路社會工程學聚焦於數位攻擊，而公眾社會工程學則應用於犯罪偵查與安全管理。詳細比較請見表六。

表 6：網路社會工程學與公眾社會工程學的比較表

項目	公眾社會工程學	網路社會工程學
定義	以影響公共安全系統和人群行為為目標的社會工程技術	利用網路技術影響個人或組織行為的社會工程技術
應用範圍	公共安全、警政、社會秩序維護	網路安全、資訊安全、網路詐騙防範
主要手段	假扮政府或公安人員、社會操控、公眾心理影響	網路釣魚、網路偽裝、惡意軟件散佈
攻擊目標	政府機構、公共基礎設施、大規模人群行為	個人用戶、企業網路、數據系統
例子	利用假身份進行社會操縱以影響選舉或社會運動	透過釣魚郵件獲取個人敏感資訊並進行數據盜竊

表 6 資料來源：研究者自行彙整

參、研究方法

一、研究方法

(一) 文獻分析法：本研究透過蒐集並整理網路安全及 Kali Linux 相關文獻資料，深入探討 Kali Linux 中核心工具的功能及應用，並分析社會工程學中的 OSINT 技術，瞭解駭客常用的資訊收集手段與網路攻擊策略。此外，針對現有市場上的資安手冊進行比較，找出其優缺點，確立適合初學者學習的內容框架，作為手冊編寫的理論基礎。

(二) 實作研究法：在實作過程中，實際操作 Kali Linux 中的核心工具，進行網路掃描、流量分析與漏洞檢測等測試，並將具體步驟編寫成手冊內容。此外，透過小範圍實測及使用者回饋，驗證手冊的可行性與操作性，並進一步優化內容，確保手冊能幫助初學者掌握基礎的網路安全防護技巧。

二、研究架構

為了幫助讀者了解網路安全，我們將其進行數個分類進行說明，並以「網路安全手冊」為主旨。手冊共分為三大部分：目的強調提升讀者的安全意識與保護個人資訊的重要性；研究動機聚焦於因應資訊發展帶來的網路攻擊、數據洩露與詐騙威脅；實作則提供基礎電腦保護與 Kali Linux 技巧的操作指導。手冊旨在普及安全知識、提升實戰技能，並為未來網路安全挑戰提供指引。

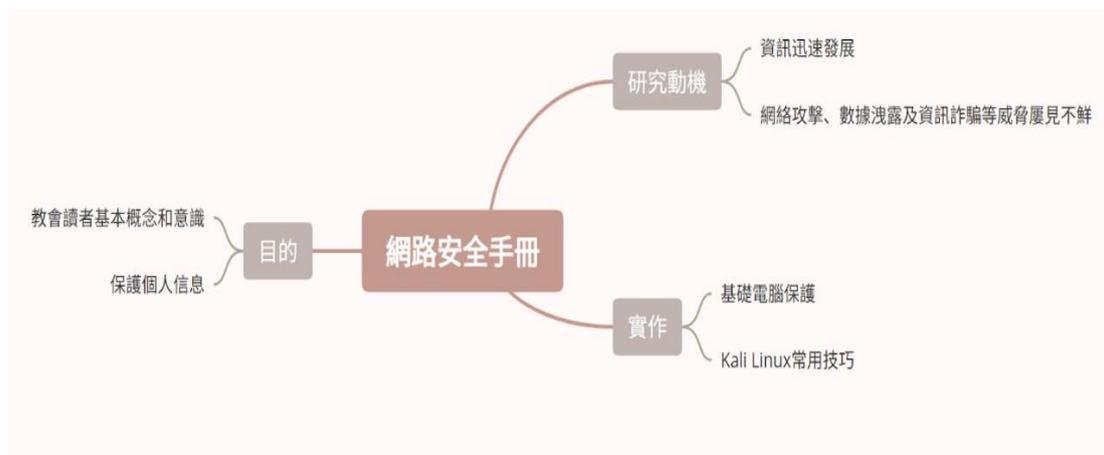


圖 1：研究架構圖

三、研究流程

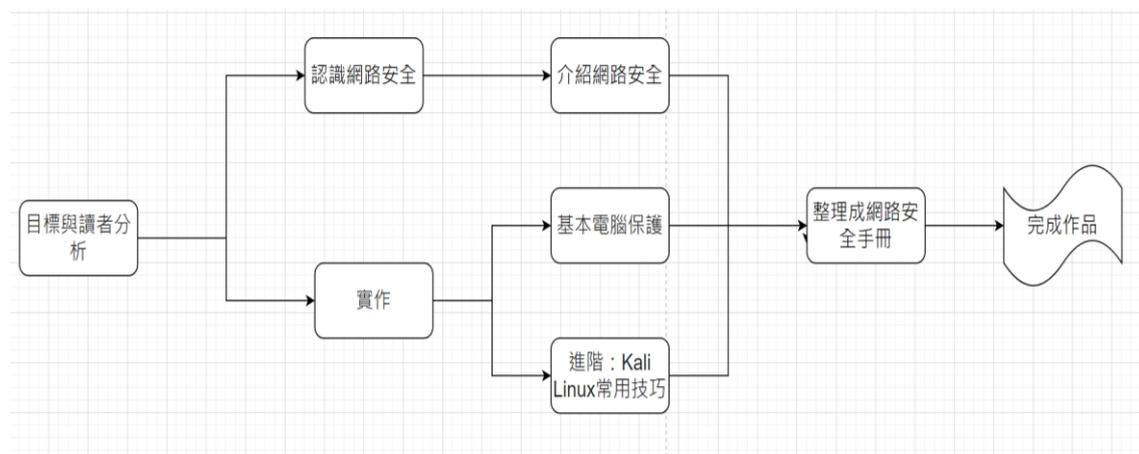


圖 2：研究流程圖

本研究的流程分為六個環節，逐步推進以達成研究目標：

- (一) 目標與讀者分析：明確研究的目標群體，了解讀者需求與背景。
- (二) 認識網路安全：透過介紹網路安全的重要性，建立讀者的基本概念與意識。
- (三) 實作：基本電腦保護，學習電腦系統安全防護的基本方法。進階 Kali Linux 常用技巧，透過實際操作 Kali Linux 工具，學習網路攻防的基礎知識。
- (四) 整理成網路安全手冊：將概念學習與實作成果整合，編寫成實用手冊。
- (五) 完成作品：最終產出一份完整的網路安全手冊，供讀者學習與應用。

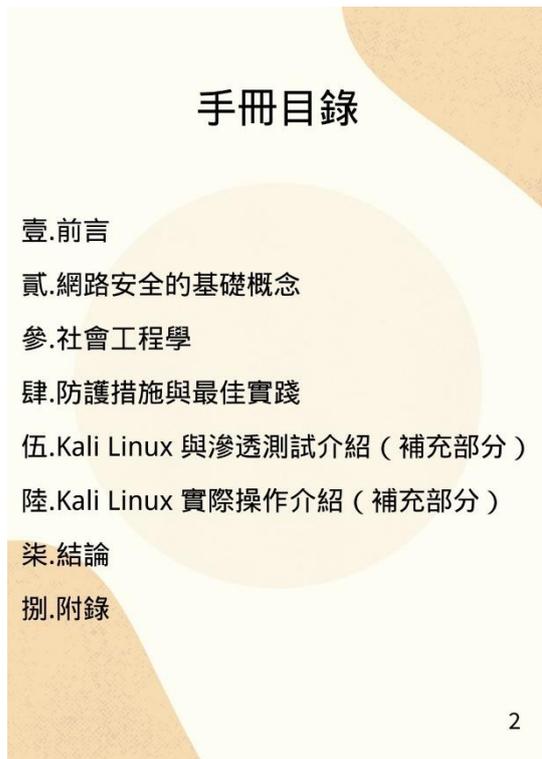
肆、研究過程與方法

一、資安防護手冊編寫

本研究的資安防護手冊旨在幫助初學者快速掌握基礎的網路安全知識與實際操作技能，特別針對 Kali Linux 工具的應用進行講解，內容結構簡單明瞭、實用性強，適合對資訊安全概念和技術陌生的讀者。手冊以初學者的需求為出發點，聚焦基礎理論與實際技能的結合，涵蓋安全意識建立、基本防護措施和進階工具使用三大模塊，為提升使用者的網路安全防護能力提供有效的入門指導。

(一) 手冊的框架

首先，我們確定了手冊的框架，包含基本的網路安全知識、Kali Linux 的簡介、實際操作案例、資料保護與社交工程防範等重要內容。如下圖三所示，為手冊的目錄。

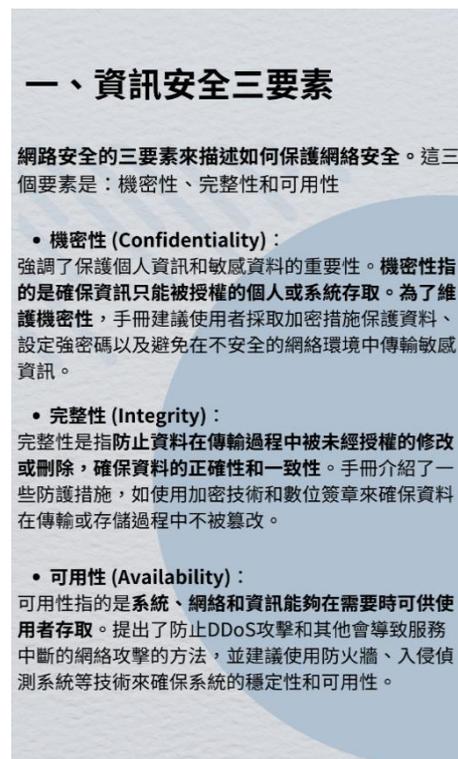


Handbook Table of Contents

- 壹.前言
- 貳.網路安全的基礎概念
- 參.社會工程學
- 肆.防護措施與最佳實踐
- 伍.Kali Linux 與滲透測試介紹 (補充部分)
- 陸.Kali Linux 實際操作介紹 (補充部分)
- 柒.結論
- 捌.附錄

2

圖 3：手冊的目錄



一、資訊安全三要素

網路安全的三要素來描述如何保護網路安全。這三個要素是：機密性、完整性和可用性

- **機密性 (Confidentiality) :**
強調了保護個人資訊和敏感資料的重要性。機密性指的是確保資訊只能被授權的個人或系統存取。為了維護機密性，手冊建議使用者採取加密措施保護資料、設定強密碼以及避免在不安全的網路環境中傳輸敏感資訊。
- **完整性 (Integrity) :**
完整性是指防止資料在傳輸過程中被未經授權的修改或刪除，確保資料的正確性和一致性。手冊介紹了一些防護措施，如使用加密技術和數位簽章來確保資料在傳輸或存儲過程中不被篡改。
- **可用性 (Availability) :**
可用性指的是系統、網路和資訊能夠在需要時可供使用者存取。提出了防止 DDoS 攻擊和其他會導致服務中斷的網路攻擊的方法，並建議使用防火牆、入侵偵測系統等技術來確保系統的穩定性和可用性。

圖 4：手冊有關資訊安全的描述

資訊安全的三要素（機密性、完整性、可用性）共同構建了資訊安全的核心框架。上圖四透過具體說明與防護措施，強調了在面對各類網路威脅時，如何保障個人和系統資訊的安全性。手冊中不僅介紹了加密技術、數位簽章等方法來保護資料，還提出了防止 DDoS 攻擊與系統中斷的建議，為讀者提供實用的資訊安全防護知識與技巧。

(二) 資訊安全的基本概念和意識

資訊安全的基本概念與意識是保障個人與企業數據安全的基礎，核心包括機密性、完整性與可用性三要素，分別對應資料保密、正確性與系統穩定性。常見的威脅如釣魚攻擊、數據洩露與惡意軟體，凸顯提升安全意識的重要性。本章旨在幫助初學者建立清晰的安全框架，掌握基本防護技能，應對多變的網路威脅，確保數據與系統安全。

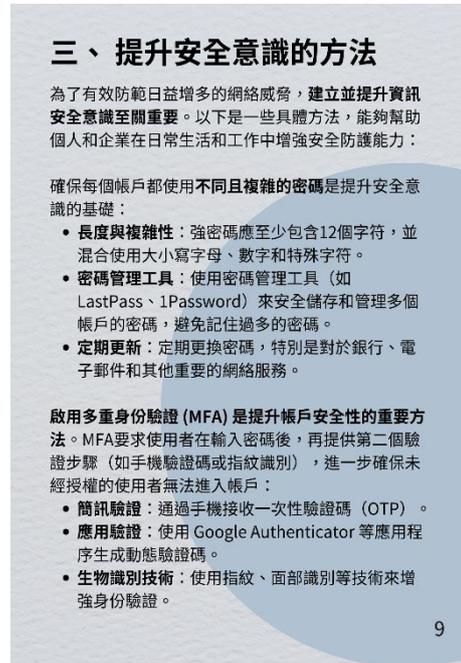
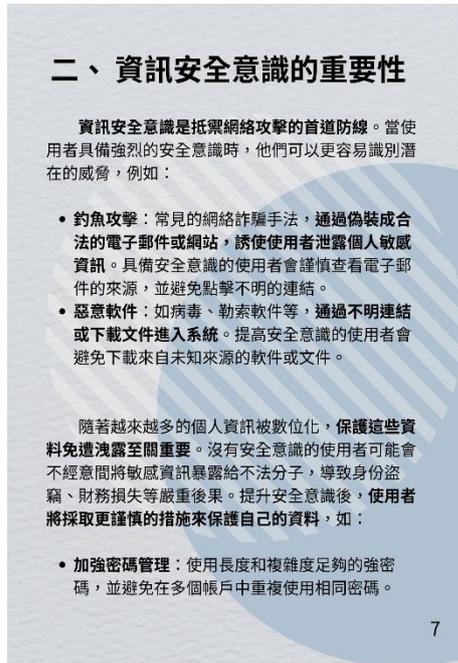


圖 5：手冊中電腦防護安全措施的描述 圖 6：手冊中提升網路安全意識的描述

(三) 社會工程學－OSINT

OSINT（公開來源情報）是社會工程學中的重要技術，透過合法渠道蒐集公開資訊，如社群媒體、搜尋引擎及數據庫，了解目標的個人資訊、組織結構和行為模式，用於滲透測試與攻擊策劃。OSINT 常用工具包括 Google 高級搜索語法、社群媒體分析、數據洩露檢查及圖片反向搜索，可幫助識別潛在弱點。作為滲透測試的起點，OSINT 能快速提供目標背景，提高釣魚攻擊與漏洞利用的成功率。然而，其合法性與道德挑戰需謹慎對待，用戶應透過隱私設置、數據加密和減少公開資料來降低風險。本手冊結合實例講解 OSINT 的應用與防範策略，幫助使用者理解技術的雙面性，並提高資訊安全意識，抵禦社會工程威脅。

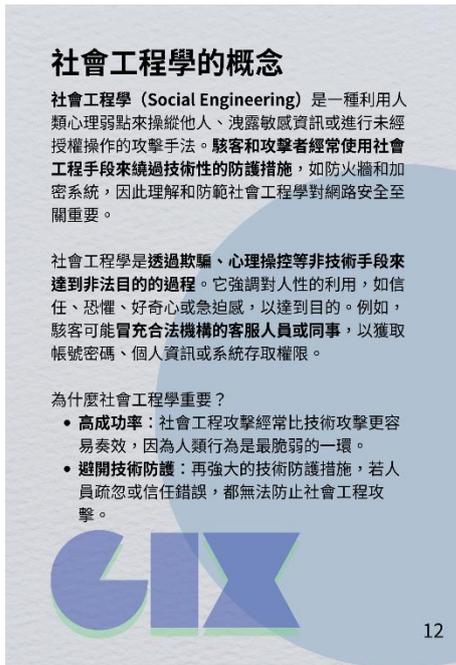


圖 7：手冊中社會工程學的描述

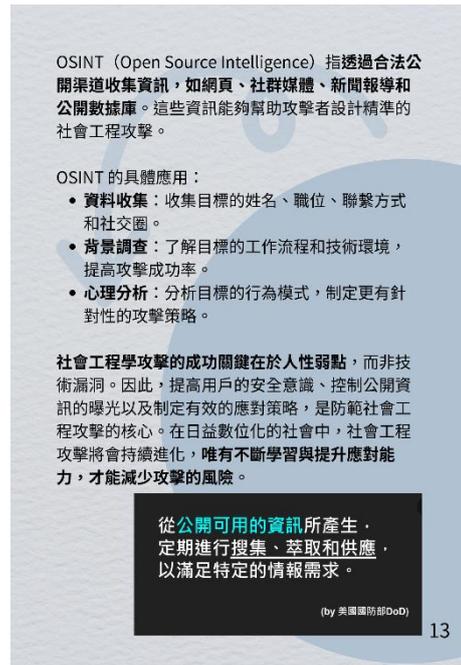


圖 8：手冊中 OSINT 的描述

(四) 電腦系統的防護安全措施

電腦系統的防護安全措施旨在保障數據的機密性、完整性與可用性，透過多層次方法應對網路威脅。如下圖五所示，主要措施包括密碼安全強化、定期更新系統與軟體、資料備份、測試還原能力，安裝防毒軟體與啟用防火牆。實踐中應採用最小權限原則限制用戶存取，並提高防範社會工程學攻擊的意識。

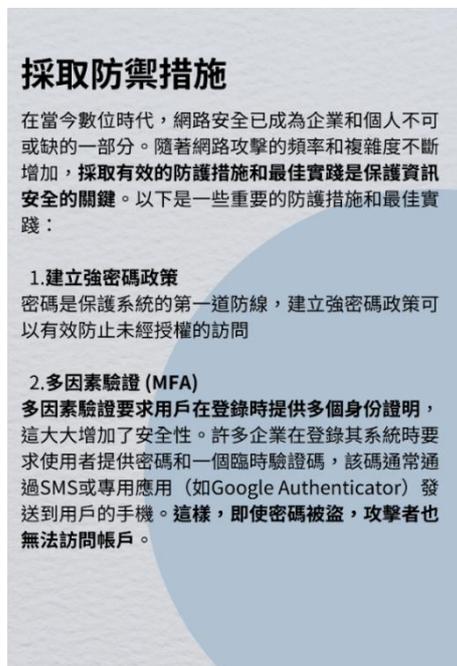


圖 9：手冊中系統防護措施的介紹

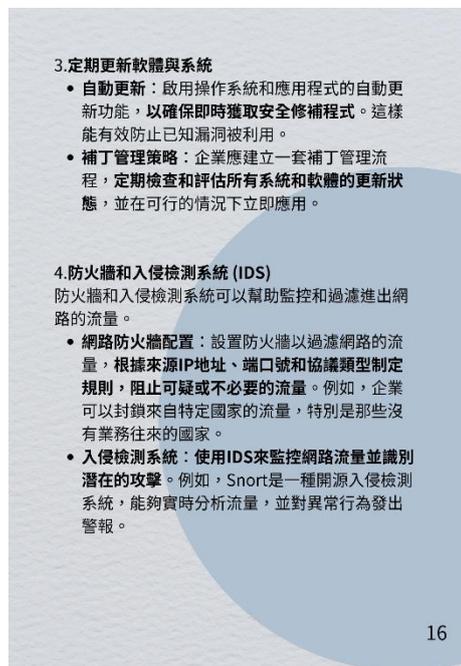


圖 10：手冊中系統防護措施的介紹

(五) Kali Linux 操作說明

使用 Kali Linux 進行網路安全測試時，可透過 Nmap 掃描目標 IP 的開放端口，利用 Wireshark 監控並分析網路封包，最後結合 Metasploit 進行滲透測試，查找並利用已知漏洞進行攻擊模擬。

實作過程中，我們在多台不同操作系統的設備(Windows、macOS、Kali Linux)上進行測試，以確保手冊中所有步驟均能順利執行。在測試環境中，我們模擬了基本的網路攻擊和防護措施，並演示了 Kali Linux 中的常用工具，如 Nmap、Wireshark、Metasploit 等等。如上圖六所示，Kali Linux 常用工具介紹。

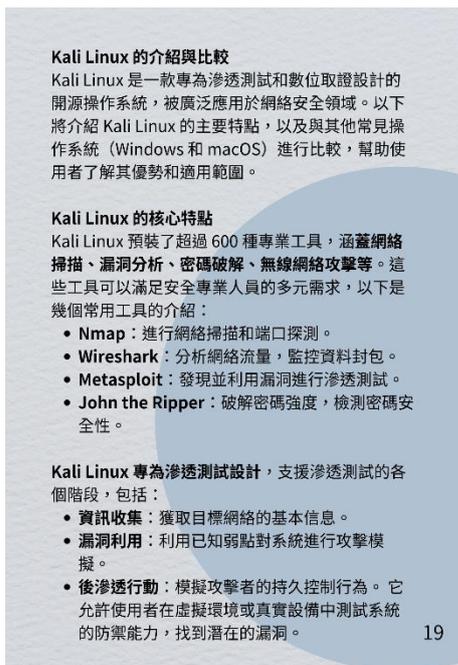


圖 11：Kali Linux 常用工具介紹



圖 12：Kali Linux 常用工具介紹

二、課程實測

實際為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 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簡單、指引清晰，適合用作入門學習的教材。



圖 13：實際授課照片

三、手冊比較分析

(一) 市面上相關系統的比較

- 1、應用導向高：市面上其他網路安全手冊通常是針對專業人員，內容技術性強，涵蓋範圍廣泛，且適合更高階的安全需求。相比之下，本手冊專注於初學者，內容簡潔且以實際操作為導向，便於一般用戶掌握基本的網路安全防護技巧。
- 2、操作性價值強：與 Windows 和 macOS 的自帶安全手冊相比，Kali Linux 獨特的滲透測試功能使其能模擬多種網路攻擊，這在其他操作系統中難以實現。因此，本手冊在網路安全實務方面有更高的實用價值，特別是在演示網路攻擊和防護的過程中。

(二) 研究結果與其他相關研究的比較

- 1、結果表明，本手冊顯著提高一般用戶的網路安全意識，並幫助他們掌握基礎的防護技巧。與其他書籍所著重的高階網路防護不同，本手冊更側重於實用性和易於學習的特點，適合作為網路安全入門的學習材料。
- 2、相較於專業書籍，本研究著重於對常見安全工具的簡單介紹和應用示範，強調操作性和即時結果，這使得該手冊對於一般用戶來說更為實用。

四、SWOT 分析與比較

表 7：資安防護手冊之 SWOT 分析

Strengths 優勢	Weakness 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.網路安全需求上升，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 7 資料來源：研究者自行分析

伍、研究結論與建議

一、結論

(一) 有效提升網路安全意識

本研究透過編寫資安防護手冊，有效提升使用者對網路安全的認識，特別是在釣魚攻擊、數據洩露、惡意軟體與社交工程學攻擊等常見威脅方面，幫助使用者理解其運作機制與防範策略。隨著科技發展與網路環境的變化，資訊安全不再是專業人士的課題，而是每位網路使用者應當具備的基本能力。本手冊以簡單易懂的方式，結合理論與實務，讓初學者能迅速掌握基礎防護概念，建立正確的安全意識，減少日常網路使用中的潛在風險。

(二) 實用且可操作性強的手冊設計

本手冊經過多次測試與優化，確保其具備高可操作性。手冊內容涵蓋基本網路安全概念、防護技巧與 Kali Linux 操作指導，包括網路掃描、漏洞檢測、資料保護等，能夠有效指導使用者網路防護措施。透過這些技術與防護方法，使用者能夠提升實際操作能力，掌握應對網路攻擊的基本技巧，從而在日常使用中應用防護策略，降低被攻擊的風險。經過多次測試與修改，該手冊已證明對初學者具有良好的操作性和實用性。

(三) 針對大眾需求的內容規劃

手冊根據不同層次的使用者需求設計，不僅針對技術較弱的使用者提供了基礎指導，還透過簡單的操作步驟讓他們能夠熟練掌握 Kali Linux 的基本功能，填補了大眾在網路安全防護方面的知識空白。

(四) 為未來資訊安全教育提供基礎

隨著網路攻擊手法的演變，資安教育顯得更加重要。本手冊提供教育推廣的學習資源，未來可作為學校資安課程、企業內部培訓教材或網路安全入門手冊，推廣給更廣泛的受眾。本手冊不僅能幫助個人提升自我防護能力，還能夠為企業與機構提供簡單易學的培訓指引，為更安全的網路環境奠定基礎。

二、建議

(一) 進一步推廣網路安全教育

建議將手冊作為網路安全入門教材在更廣泛的用戶群中推廣，特別是針對沒有安全意識的普通網路使用者，讓更多人了解如何保護自己的個人資訊並應對日益增多的網路威脅。隨著網路犯罪的增加，普及安全意識變得至關重要。未來可以考慮將手冊納入學校課程，作為資訊安全入門教材，幫助學生從小建立良好的安全意識。與企業合作推廣，作為員工培訓課程，提高企業內部的網路防護能力。開發線上課程，透過互動式學習平台，提供影片教學與實作模擬，提高學習效果。

(二) 定期更新手冊內容

隨著網路安全威脅的不斷演變，建議定期更新手冊內容，以納入最新的防護措施和工具，確保手冊能夠持續為使用者提供實時有效的指導，應對新興的網路威脅。定期補充新興網路威脅與防護策略，例如：AI 生成釣魚攻擊、雲端安全風險、區塊鏈安全等。更新 Kali Linux 工具與使用方法，確保手冊內的技術指南與最新版本的工具相容。收集使用者回饋，優化手冊內容，以確保其在實際應用中的可行性與有效性。

(三) 擴展內容涵蓋範圍

未來可進一步擴充手冊內容，加入更高階的網路防護技術與操作指導，並細分不同層次的使用者需求，從入門到高階逐步提高手冊的技術深度，讓使用者能夠從基礎學習逐步過渡到進階操作。

(四) 建立互動學習平台

為了讓學習更具體驗性，可以考慮開發配套的學習網站或應用程式，提供在線模擬測試與練習環境，讓讀者可以實際操作網路安全工具。設計互動式課程，如在線挑戰賽，讓學習者透過實戰加深理解。建立網路安全社群，讓學習者能夠交流心得、分享資安知識，形成學習互助環境。這樣不僅可以提升學習興趣，也能夠讓使用者透過實作驗證自己的學習成效，進一步強化資訊安全技能。

陸、參考文獻

- 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。
- 林信璋 (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/xvK1G4>