**Department of Computer Science**

**Project Progress Report – Academic Year 114**

**Title: Implementation of Fake Wi-Fi Hotspot and Phishing Login Page Attack**

**Advisor:** Professor

**Team Leader:** Gao En-Zai

**Date: June 17, 2025**

## Table of Contents

1. **Abstract**
2. **Research Background and Objectives**
3. **Project Content**
4. **Research Methods**
5. **Flowchart**
6. **Planned Tasks and Expected Outcomes**
7. **Work Allocation and Project Schedule (Gantt Chart)**
8. **Problems Encountered and Solutions**
9. **Equipment Requirements**
10. **References**
11. **Legality and Ethical Statement**
12. **Appendix**

**1. Abstract**

This study aims to establish a legal simulation and demonstration platform for phishing attacks and fake Wi-Fi hotspots, thereby raising public awareness of risks in network connections. The experiment simulates a hacker setting up a wireless hotspot and displaying a fake login page in a controlled environment, followed by analysis of scenarios users may encounter after connecting. No real account or password data is collected. Login form inputs are for simulation only and are immediately destroyed. The focus is on promoting defense awareness and user education. The results can be applied to cybersecurity teaching, defensive training, and attack-defense demonstrations.

**2. Research Background and Objectives**

With the widespread availability of public Wi-Fi, many users habitually connect to familiar SSIDs without recognizing potential risks. Hackers can create access points with similar names, luring users to connect and then displaying a fake login page for credential phishing. This research demonstrates the entire attack process and user experience via a simulation platform, performed only with full informed consent. The goal is to help users understand how to identify fake hotspots and suspicious login pages.

**3. Project Content**

| **Item** | **Description** |
| --- | --- |
| Fake AP setup | Using **airbase-ng** to create an SSID named *FreeWiFi* |
| Web-based fake login page | Neutral style, no brand or logo |
| Simulated data submission | Credentials are shown immediately on screen, no storage |
| One-click launch script | Integrates Fake AP + DHCP + Web login page |
| User education page | After login attempt, a message is displayed: *“You have just been simulated in a phishing attack. Please learn to identify risks!”* |

**4. Research Methods**

* Use **Kali Linux** and **airbase-ng** to create a fake AP (*SSID: FreeWiFi*).
* Configure interface at0 with static IP 192.168.168.1.
* Use **dnsmasq** for DHCP (192.168.168.x) and DNS spoofing.
* Deploy **Apache2** web server with login.html fake login page.
* Use post.php to receive submitted data and write to logs.txt.  
  Connect with phone/laptop to test if the login page appears and if logs are recorded.

**5. Flowchart**



**6. Planned Tasks and Expected Outcomes**

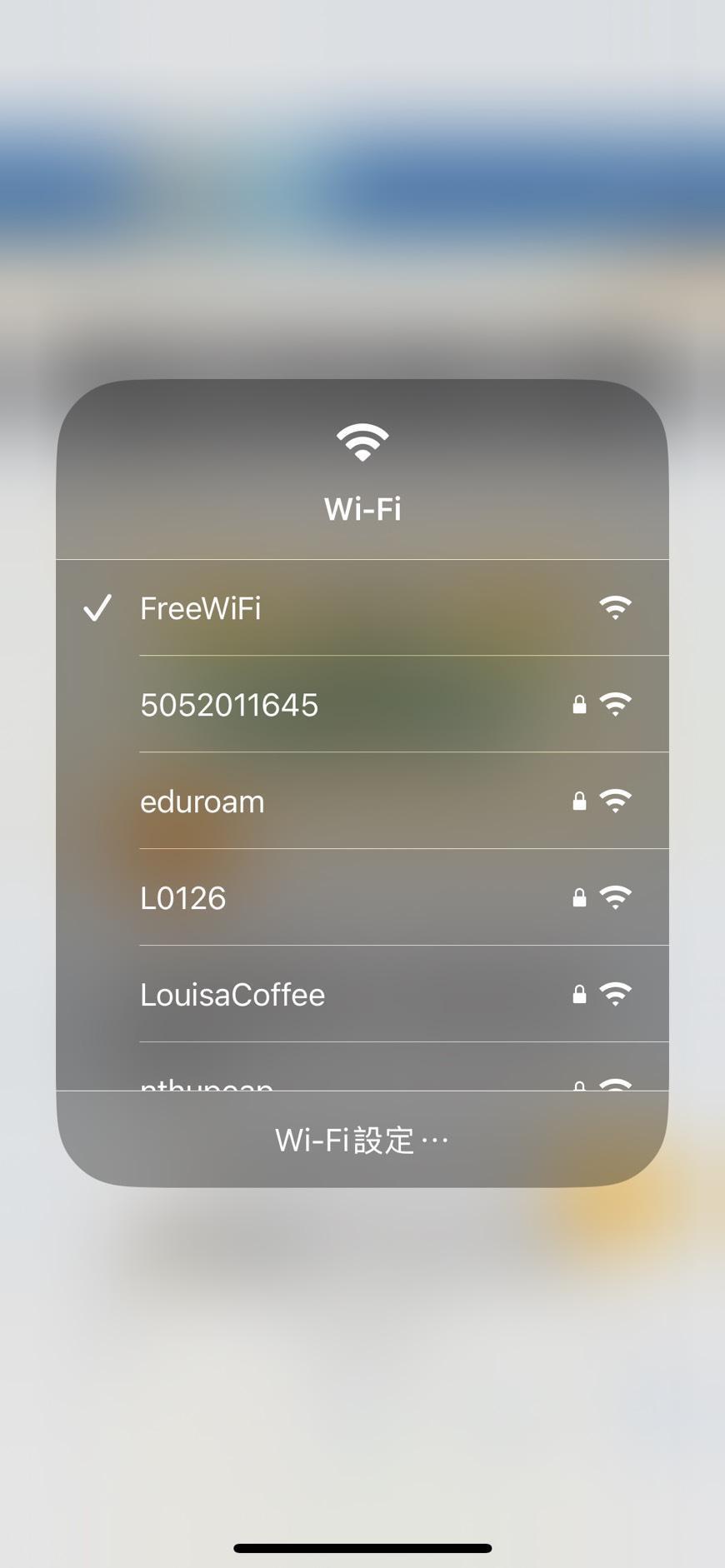
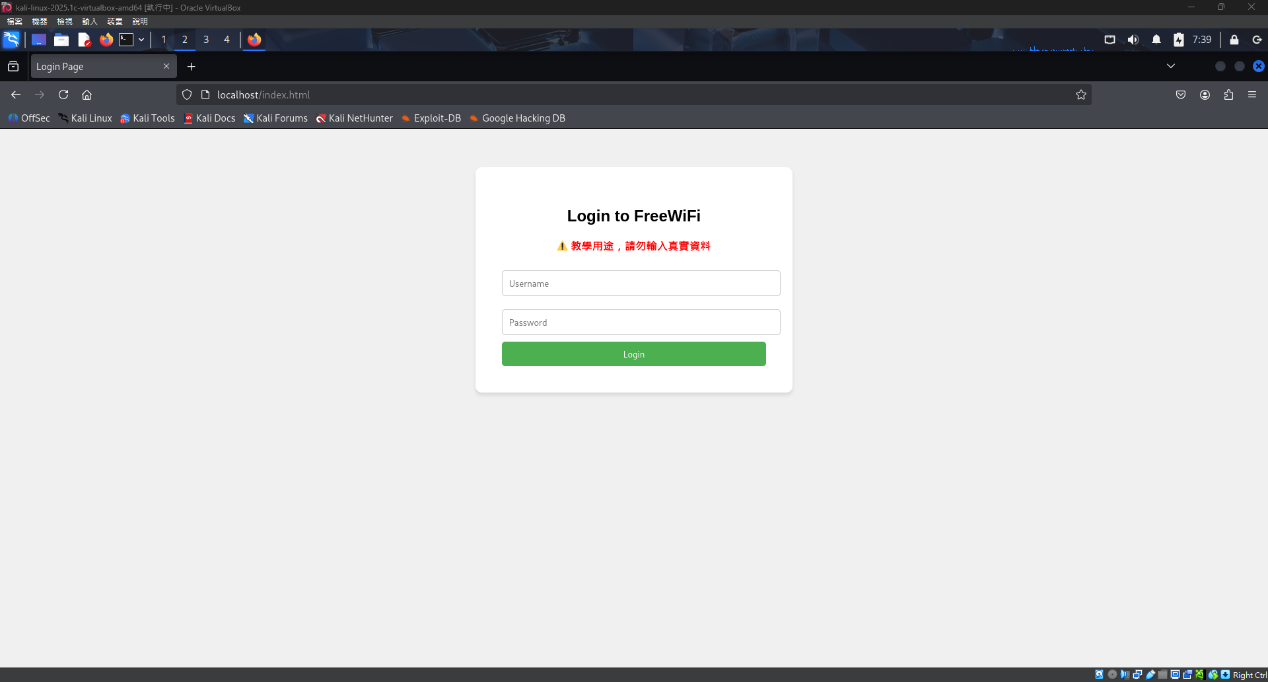
| **Task** | **Outcome** |
| --- | --- |
| Fake Wi-Fi hotspot | SSID *FreeWiFi* successfully broadcast and connected |
| Network interface + DHCP | ifconfig/ip + dnsmasq provide IP/DNS spoofing |
| Login page design | Simple captive portal (7-11/Gmail style) |
| Credential capture script | post.php logs inputs to logs.txt |
| Full integration | One-click script for all steps |
| Reports and presentation | PDF, slides, flowcharts, logs for documentation |

Includes **code snippets**:

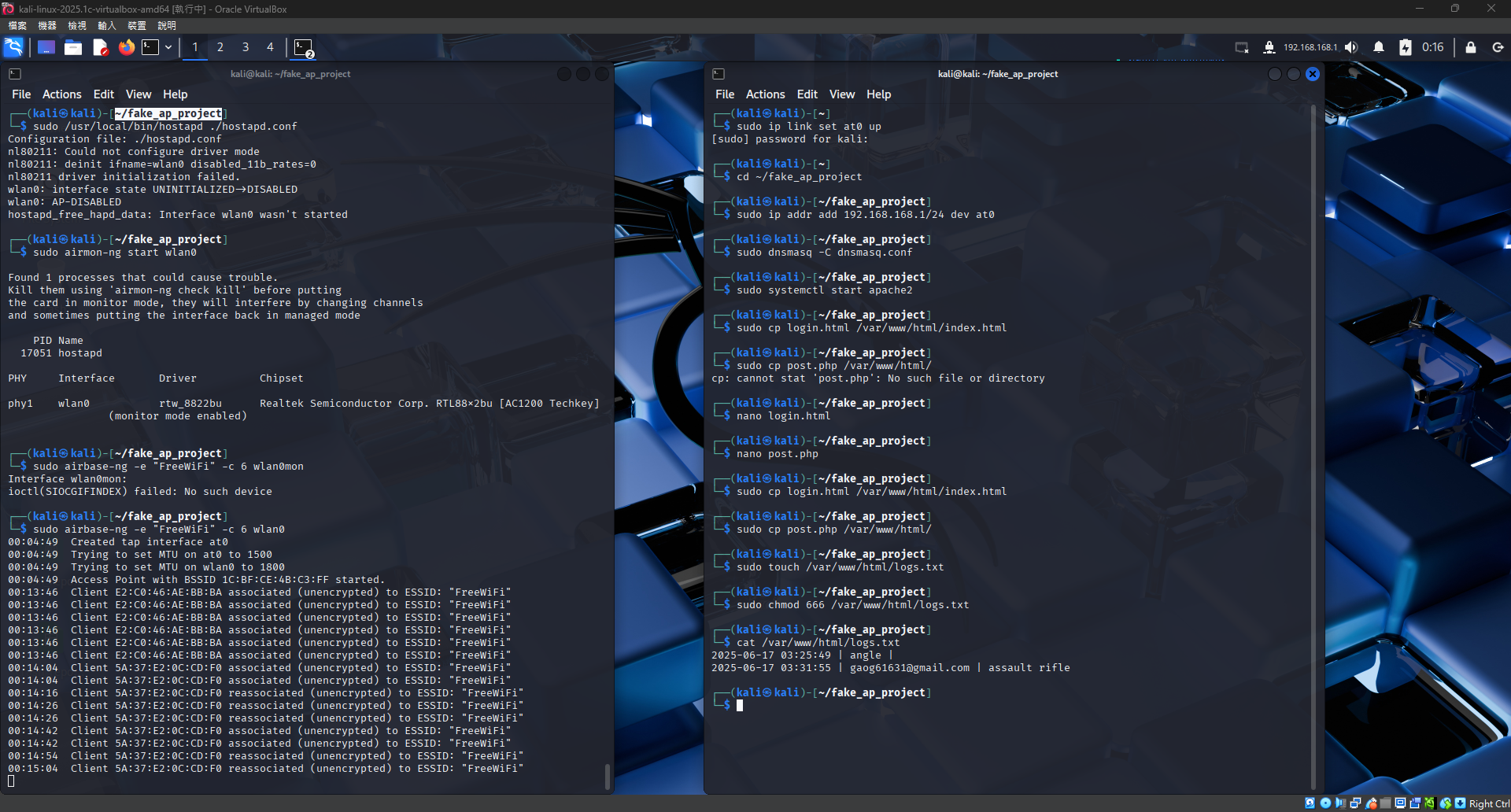
* post.php – captures submitted credentials and logs them.
* login.html – phishing-style login form.
* dnsmasq.conf – DHCP/DNS redirecting all traffic to fake login page.

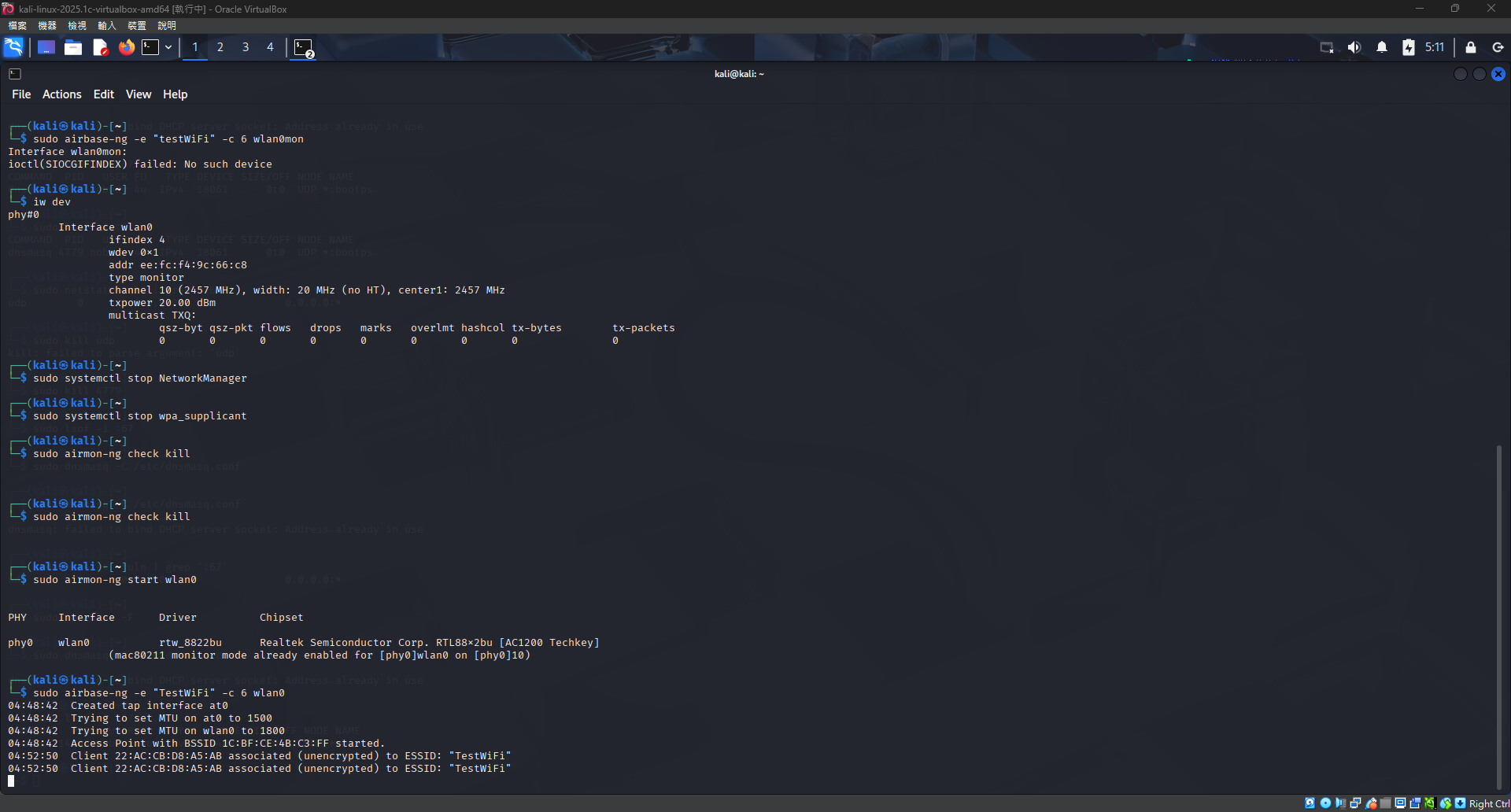
**Experimental Results:**

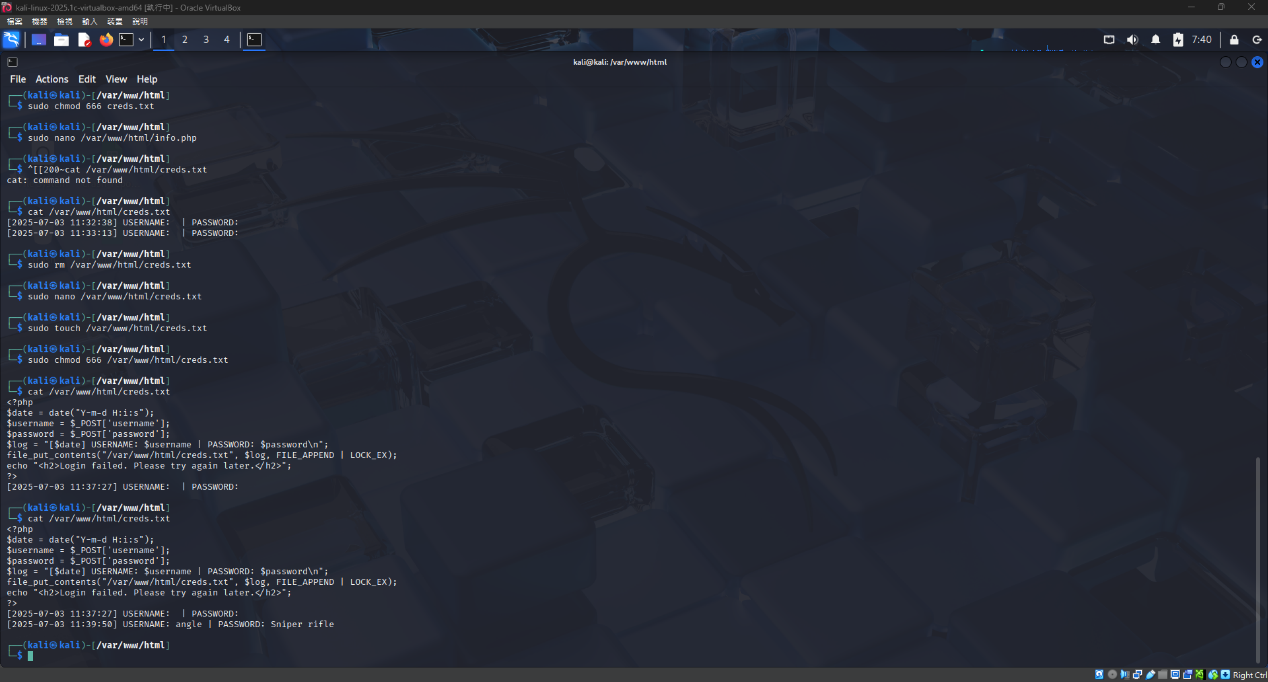
1. SSID "FreeWiFi" broadcast view and the fake login page display (login.html)

2. Captured results recorded in logs.txt (screenshot)









**7. Work Allocation & Gantt Chart**

* Fake AP setup – 2025/06/17
* Login page design – 2025/06/17
* Credential script – 2025/06/17
* DHCP + Apache integration – 2025/06/17
* Testing with phone/laptop – 2025/06/17
* Report & slides – 2025/06/17

**8. Problems Encountered & Solutions**

* USB Wi-Fi card not supporting AP mode → used **airbase-ng** in monitor mode.
* No DHCP/login page → configured **dnsmasq** for at0.
* PHP permission issues → fixed with chmod 666 logs.txt.
* No auto-redirect to login page → added DNS spoofing + index.html captive portal.
* Encoding issues → ensured Apache/PHP UTF-8 setup.

**9. Equipment Requirements**

| **Item** | **Specification** | **Purpose** |
| --- | --- | --- |
| OS | Kali Linux 2025 | Experiment platform |
| USB Wi-Fi adapter | Realtek RTL88x2BU (monitor mode) | Fake AP broadcasting |
| Apache2 | v2.4.x | Hosting login page |
| dnsmasq | v2.89 | DHCP/DNS spoofing |
| airbase-ng | aircrack-ng package | Fake AP |
| PHP | v7.x+ | Handle credentials |
| Client device | Phone/Laptop | Testing connections |

**10. References**

1. Offensive Security. Kali Linux Documentation
2. aircrack-ng Official Site：<https://www.aircrack-ng.org/>
3. dnsmasq 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」
6. SensePost hostapd-mana：<https://github.com/sensepost/hostapd-mana>

**11. Legality and Ethical Statement**

* No real data collection outside test devices.
* Login pages are self-designed, not branded.
* All devices are personally owned and under full control.
* Purpose strictly for **cybersecurity education and defense demonstration**, not unauthorized access.
* Fully compliant with **Personal Data Protection Act** and **Criminal Code §359** regarding unauthorized system access.

**12. Appendix**

* **Topology Diagram**: Attack simulation host (Kali Linux + airbase-ng, IP 192.168.168.1) → Fake AP (SSID: FreeWiFi) → Test device (phone/laptop).
* **Equipment Control Declaration**: All devices legally owned by the researcher, no public access, no external Internet connection, fully controlled closed experiment.