第十二章

入侵無線網路

無線網路

- 無線網路的安全性非常重要，無線區域網路（WLAN）允許筆記型電腦或桌上型電腦在不需要線路的情況下就可以上網，越來越多的企業使用無線網路，因此無線網路也常常成為企業安全防護的最大漏洞。

- 無線網路的入侵者稱為 whackers (**Wireless Hackers**)，他們只需要簡單的工具及程式，不需要實體的入口，就可以輕易的進入企業網路進行危害。

無線網路

- IEEE在1997年為無線區域網路制定了第一個版本 IEEE 802.11，其中主要定義了 MAC層和實體層，工作頻率在2.4GHz的頻帶上，數據傳輸速率為2Mbit/s。兩個設備之間的通信可以使用 ad hoc 模式來進行，也可以使用存取點 (Access Point，AP）模式進行。

- 為了在不同的通訊環境下取得良好的通訊品質，採用 CSMA/CA (Carrier Sense Multi Access/Collision Avoidance)的溝通方式。

- 1999 年加上了兩個版本：802.11a 及 802.11b，802.11a 定義了在 5GHz 頻道上，數據傳輸速率可達54Mbit/s，802.11b定義在2.4GHz的頻道上，數據傳輸速率為11Mbit/s。 2.4 GHz的開放頻道因為在多數國家都通用，因此 802.11b的使用比 802.11a 廣泛。

- 1999年相關工業界成立了Wi-Fi聯盟，致力解決符合802.11標準的產品之生產和設備相容性的問題，陸續宣佈了許多標準。

無線網路

標準	傳輸速度	頻道	其他特性
802.11	2M	2.4G	通訊距離一般小於 30 公尺
802.11a	54M	5G	通訊距離一般小於 30 公尺，少干擾，穿透力較差。
802.11b	11M	2.4G	通訊距離一般小於 30 公尺，穿透力尚可。
802.11g	54M	2.4G	通訊距離一般小於 30 公尺，接近 802.11b，但是更快速。
802.11n	200~540M	2.4G~5G	最新標準，使用 MIMO室內通訊距離可達 50 公尺，室外通訊距離可大於 150 公尺。

無線網路

- 存取點(Access points)是無線網路存取的中心點，類似於 Hub 提供網路裝置存取的功能，AP 必須經由網路的管理者協同分配與管理。

- 天線對於無線電傳送與接收資料非常重要，有兩種形態的天線:

(1)Omni-directional antennas（全向天線）

(2)Directional antennas（指向天線）

無線網路優點

(1)移動性

(2)初期成本低

(3)容易連接

(4)不同的傳輸資料方式

(5)易於分享

無線網路缺點

(1)移動性太高，傳輸品質視實際環境決定。

(2)後期成本高，後期的維修成本及管理成本都高，因為 AP 可能散佈在各處。

(3)沒有實體連接，隨時可以連上網路，追查來源位置不易。

(4)入侵更容易。

(5)分享資料的危險性高。

(6)易受微波爐、無線電話、金屬櫃等干擾或阻擋電波。

無線網路的弱點

- 設置 WLAN 必須先設定頻道、SSID、IP、遮罩等基本網路設定，一般頻道範圍在 1 到 11 之間。
- SSID全名叫無線網路服務集合識別碼(SSID, Service Set Identifier) 。Access Point 和一堆無線網卡，就可以算是一個無線網路服務集合，這時可以為每一個無線網路服務集合去定義一個識別代號，這個識別代號就是 SSID 。
- 同一個服務集合的設備可以使用同一個 SSID 來驗證，網路設備若要參與此服務集合，就必須修改 SSID。

無線網路的弱點

- Access Point 中可以設定 SSID ，無線網卡中也可以設定 SSID，Access Point 及網卡會借由 SSID 來判斷是否為同一群組。
- 在 802.11 無線網路上，可以將某一些「特殊的無線網卡」設定成監聽模式(Monitor mode)，藉以進行網路的監聽，攻擊者再使用特殊的程式，就可以監聽未加密通訊的所有內容。

開放式系統

- 開放式系統認證就是將無線網卡的服務域名設定成 "ANY" ，此時無線網卡就會發出訊號，詢問週遭是否有無線網路存取點的存在，若存取點被設定成對此類詢問會有所反應，則此存取點就會送出回應給這個無線網路卡，而在此回應中就包含 SSID。

開放式系統

- 利用這個原理，某些工具程式會不斷的對周遭進行廣播式詢問，不斷的送出這種請求，於是收集回應的訊息就可以獲得一個可用無線網路存取點的列表，這些存取點列表再配合全球衛星定位系統(GPS)，就可以記錄無線網路存取點的經緯度，即可再繪製成「可用無線網路的分佈圖」。

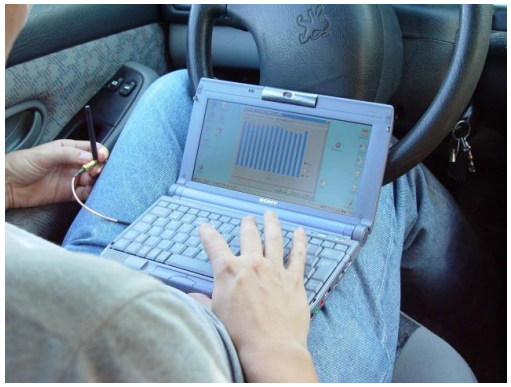
開放式系統

開放式系統

- 利用駕車方式，在市區內掃描可用的無線網路，再配合全球衛星定位系統標記出所有可用的無線網路存取點，這種行為稱之為 WarDriving。

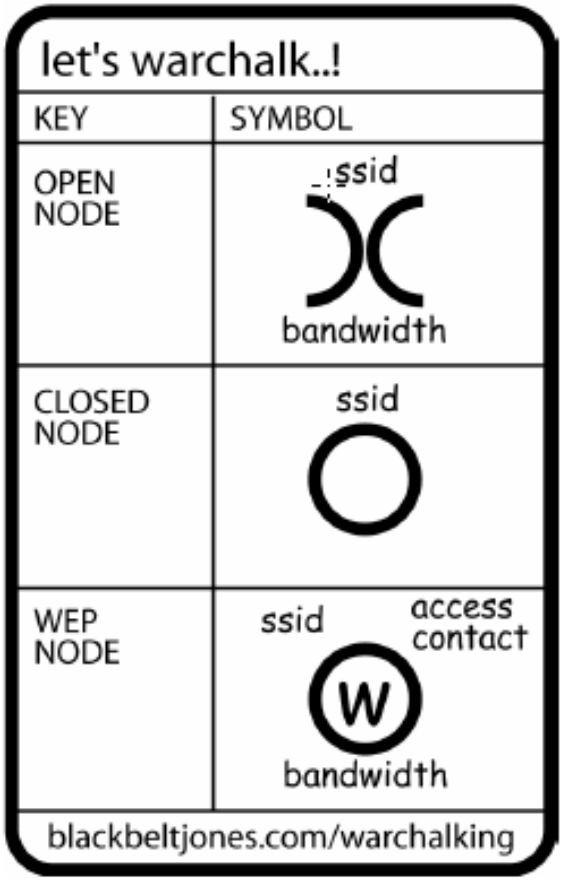
- 若使用走路的方式者，稱之為 WarWalking ，以腳踏車或機車代步的稱為 Warcycling，若使用私人飛行工具的稱為 War Flying。

開放式系統



開放式系統

- 使用藍芽技術，臨時攔截別人的手機使用，稱為 Blue jacking。有些人則選擇在可用無線網路的附近區域，畫上標記以提醒同好附近有網路可使用，這種方式則稱為 WarChalking。



開放式系統

封閉式系統

- 使用開放式系統認證非常危險，容易遭到入侵或使用，那麼假如把認證方式設定為封閉式系統認證，不要讓存取點對任意(ANY)的要求回應，並且使用較複雜的 SSID，這樣是否有用？

- 答案是：這並不能解決問題。

封閉式系統

- 駭客只要監聽附近無線網路的通訊內容，這些通訊內容之中，一定會包含了幾個重要的封包訊息，只要取得訊息中的 SSID，封閉系統就沒有意義了。
- 存取點會定時發出一種標誌訊框(Beacon Frame) ，去告知無線網路的使用者這個存取點的存在，在這訊息封包裡其中就有服務識別碼 (SSID)。
- 此外，在一個使用者加入無線區網之前，無線網卡會送出 "探測請求" (Probe Request)的封包，以確定附近有存取點存在，這個封包也就包含了這個使用者在電腦上所設定的SSID。

MAC 過濾

- 有些管理者會以 MAC 位址過濾的功能當做身分認證的一種方法。
- 這種方法最大的問題就是：802.11 並未提供資料鏈結層加密的功能，所以所有的 MAC Address 都可以經由無線網路的竊聽程式得到。
- 攻擊者於是可以藉由改變網卡 MAC 的程式，假裝成一個合法的使用者進入了無線網路

WEP

- WEP (Wired Equivalent Privacy)是一種將資料加密的處理方式，WEP 40 bits (64 bits) 的加密是IEEE 802.11的標準規範，透過WEP的處理，可讓我們的資料於傳輸中更加安全。
- 採用128 bits的 RC4 演算法加密方式，可以在資料連結層阻止未授權的使用者，提供更佳的資料安全保護。但是，對於有心的駭客，只要時間足夠，仍然有可能破解密碼 。

WPA

- **WPA (Wi-Fi Protected Access)**

- 2002 年Wi-Fi 聯盟公佈WPA無線通訊安全標準，WPA 的出現能有效解決過去 WEP 輕易遭破解的問題，WPA 是 802.11i 標準技術的其中一部分。以下是 Wi-Fi 用來解釋WPA 意義的簡單公式，這個簡單的公式說明了 WPA 的組成架構以及每個基本元素。

- WPA=TKIP+MIC+802.1X+EAP

WPA

- 802.1x 和延伸認證協定（EAP）是 WPA 的認證機制，WPA 針對加密機制加以補強，公式中的 TKIP 和 MIC 便是在WPA 中扮演著強化加密的角色。

- 在企業中，驗證工作則通常有專責伺服器來完成。為了簡化使用方式，WPA 提供了一個不需額外設備的簡易認證方式，稱為預先公用金鑰，只需在無線網路的無線基地台及無線網路卡上輸入單一密碼，當密碼相符合， 客戶端便會被視為合法用戶。

惡意存取點(Rogue Access Points)

- 如果同時有兩個AP同時使用同樣的SSID，那麼用戶端會跟哪一個無線存取點建立連線呢？

- 考慮預設的狀況下，用戶端會跟訊號較強的存取點建立連線。利用這種原理，一個惡意的攻擊者可以偽造存取點的 SSID，騙取不知情的用戶端連線後，從偽造存取點對用戶端發動竊聽與攻擊 。

無線網路的阻斷服務

- 無線網路因為透過無線電波送出資訊到公共頻帶上，更容易有意或無意的受到干擾或攻擊。
- 存取點使用相同的頻道，就會間接造成阻斷服務的狀況。
- 某個用戶只要惡意一直送出需求信號，讓存取點為了應付其需求，無法回應其他客戶端的需求。

無線網路防護策略

1. AP 的訊號盡量不要散溢至單位或組織之外。
2. 關閉 DHCP 的自動配發 IP，使用手動設定 IP 及 MAC 對應表。
3. AP 更改預設的 SSID ，且不廣播 SSID。
4. MAC 位址過濾。
5. 使用 WPA 及 802.1x/EAP使用者認證標準。
6. 使用 VPN 技術。

AirPcap

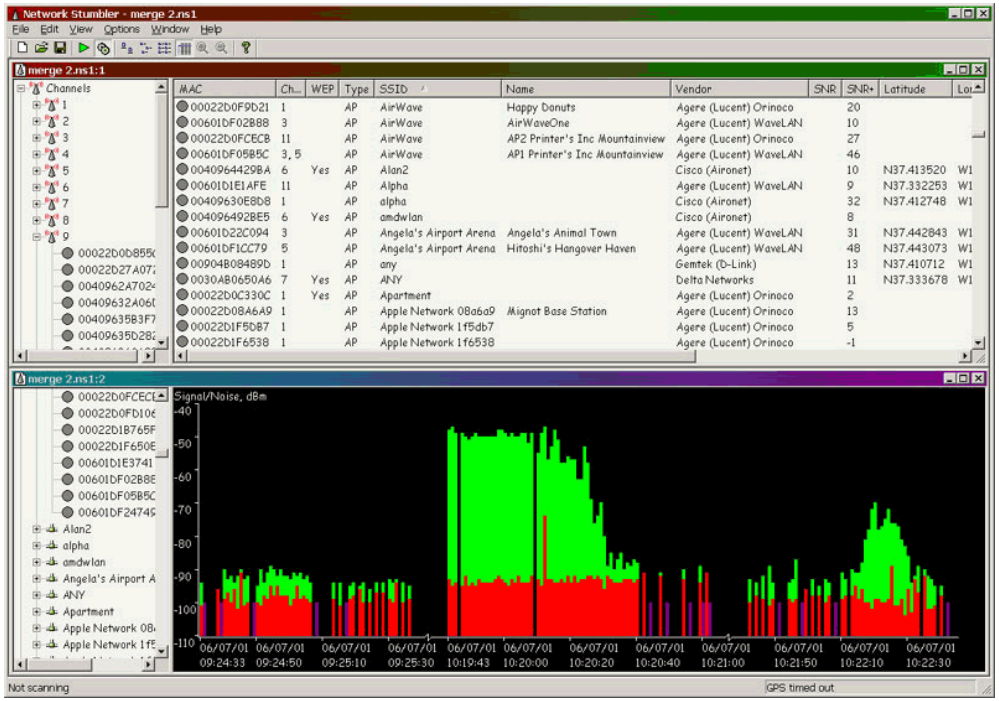
- 可以在 Windows 平台及被動模式 (passive mode)下，記錄無線網路的封包資訊，目前都以 USB 的形式販賣 。

Fake AP

- Fake AP 提供了一個隱藏及假冒 AP 的功能，Fake AP 可以用來混淆網路及監聽，Black Alchemy's Fake AP 會產生數以千計假冒的 802.11b 存取點，Fake AP 執行於 Linux 及 BSD 。

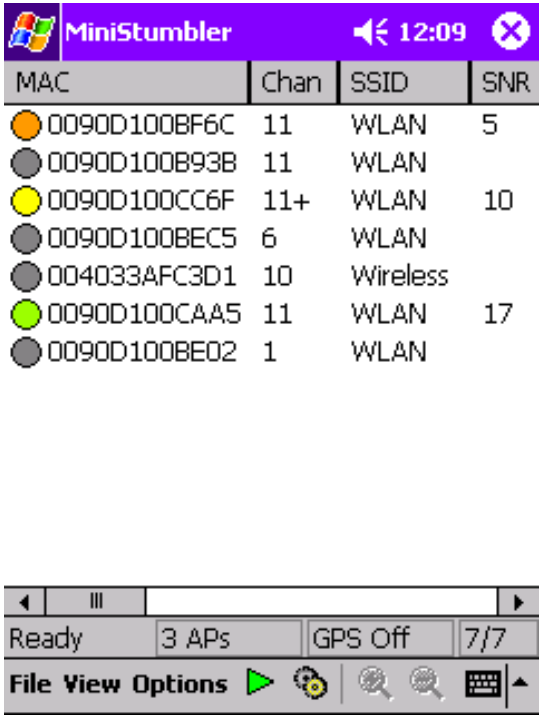
Netstumbler

- NetStumbler 是一個在 Windows 下使用的軟體，可以顯示信號強度、MAC 位址、SSID、頻道細節...。



Ministumbler

- MiniStumbler 是類似 NetStumbler 的免費產品，主要用於 PDA 或 SmartPhone 之 WinCE，它也可連接到一個 GPS。



Wellenreiter V2

- Wellenreiter 是一個被動型的無線網路基地台偵測工具。
- 它可將網卡設成所謂的「rfmon mode」，然後便可竊聽無線傳輸封包，抓取所有發送在空中的無線網路封包，包括整個無線封包框架，框架內便包含有這些封包所使用的SSID。然後將資料顯示在他的圖形介面中。

Aircrack

- 是 802.11 的嗅探器(sniffer) 及 WEP 金鑰掃描兼破解程式。支援 Windows, Linux, 及 MacOS。
- 能獲得 40-bit 或 104-bit WEP 的 key。aircrack由以下程式組成: airodump (一個 802.11 封包擷取程式)、aireplay (一個802.11 封包注入程式) 、 aircrack (WEP 及 WPA-PSK 破解)及 airdecap (破解 WEP/WPA 封包擷取檔)。

AirSnort

- AirSnort 是被動式監督傳輸封包，等到蒐集到足夠的封包數量之後，就會破解 WEP Key ，能運作於 UNIX/Linux/Windows 系統下。

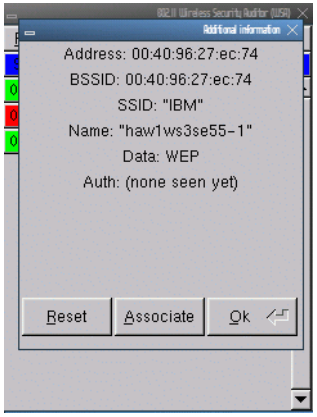
- 因為是被動式收集封包，需要花較長的時間破解（約四個小時以上），因此漸漸被主動式取代。

Kismet

- 是 802.11 第二層無線網路檢測、嗅探器及入侵偵測系統。
- 用於 Linux 系統及支援 raw monitoring (rfmon) mode 的無線網卡，可以嗅探 802.11 a/b/g ，屬被動式收集封包。

Wireless Security Auditor (WSA)

- IBM 的一個 802.11 研究雛形，可以在 Linux 或 iPAQ PDA 上執行，可幫助管理者監聽網路的安全。

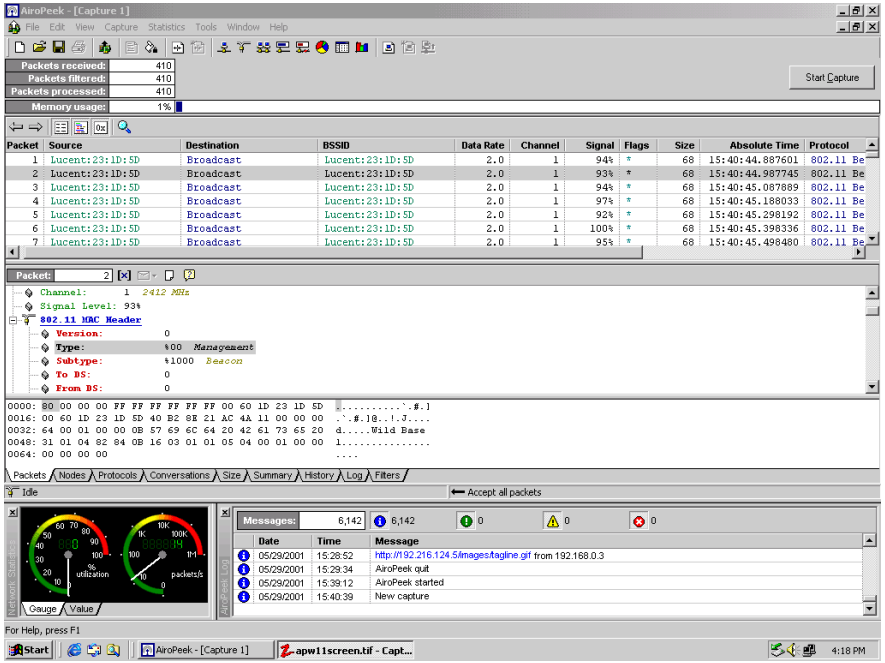


Wifi Finder plus

- 是一個硬體裝置，能夠快速顯示範圍內 802.11a, 802.11b/g 的信號強度及活動中的 Bluetooth。

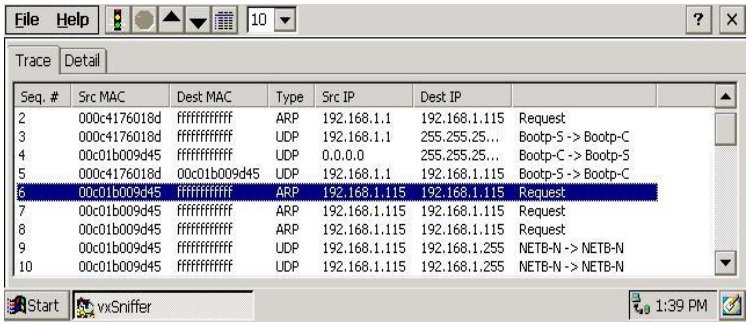
AiroPeek

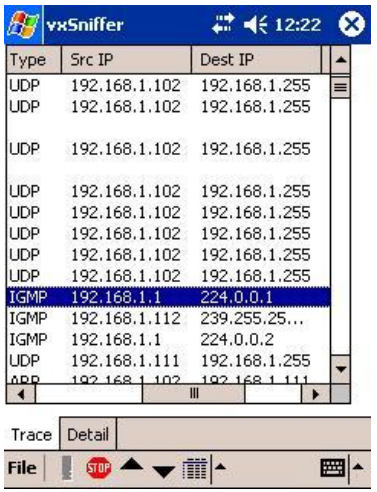
- AiroPeek是一套針對IEEE 802.11 無線網路環境設計的無線網路管理系統，主要功能包括流量統計分析管理、監控無線通訊狀況、協助網路故障排除、辨識潛在安全問題、客戶端除錯、應用層分析、VoIP 分析...等。



vxSniffer

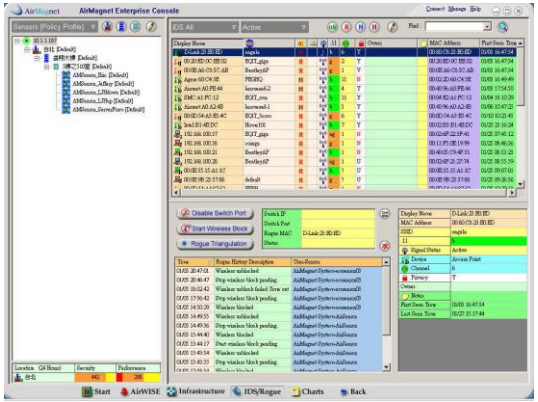
- 是安裝於手持式設備的無線網路監督工具，運作於 Handheld 2000 HPCs, Pocket PCs, Pocket PC 2002s, and Windows Mobile 2003s，需要有無線網卡及支援 NDIS 。





AirMagnet WiFi Analyzer

- AirMagnet系统可以對整個無線網路進行管理，它可以對無線網路的安全性，效能和穩定性實施監控，並提供多達百種以上無線網路安全及效能的偵測，本身亦具備入侵偵測系統(IDS)功能。此外它也支援手持式設備及 GPS 定位。



破解 WEP KEY

- 2001 年八月，兩位以色列魏茲曼研究所的專家與一位思科公司的研究員，在多倫多的密碼會議中公佈破解加密技術的結果。
- 這三位解密專家利用裝置無線網路卡的筆記型電腦，成功竊取網路中的一小部分資料，在不到一小時內即破解用戶密碼。此外AT&T 實驗室的研究員也號稱可以同樣的方法成功破解密碼，目前網路上到處都可找到破解 WEP 的工具。

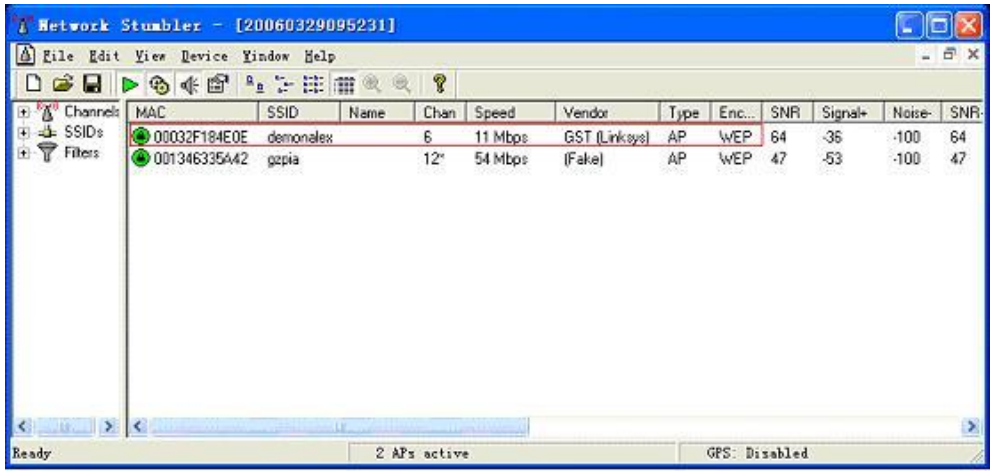
破解 WEP KEY

1.準備無線網卡

- 網卡必須支援 AirCrack ，可以在購物網站上購買，價格約台幣 800-2200。必須使用適當的網卡才能進行封包抓取。

2.發現 AP

- 首先使用 NetStumbler確認區域內的 AP，並透過AP信號進行資料搜集。



破解 WEP KEY

3.破解WEP

- 使用 WinAirCrackPack 工具包。

程式名稱	功能
aircrack.exe	原WIN32版aircrack程式。
airdecap.exe	WEP/WPA解碼程式。
airodump.exe	資料訊框捕捉程式。
Updater.exe	WIN32版aircrack的升級程式。
WinAircrack.exe	WIN32版aircrack圖形介面。
wzcook.exe	檢驗本地無線網卡緩衝區中的WEPKEY記錄程式。

破解 WEP KEY

```
                    airodump 2.3 - (C) 2004,2005 Christophe Devine

usage: airodump <nic index> <nic type> <channel(s)> <output prefix> [ivs only flag]

Known network adapters:

16  D-Link AirPlus G DWL-G122 Wireless USB Adapter(rev.B)
26  BUFFALO WLI-PCM-L11/GP Wireless LAN Adapter

Network interface index number  -> 26

Interface types:  'o' = Hermesl/Realtek
                  'a' = Aironet/Atheros

Network interface type (o/a)  -> o

Channel(s): 1 to 14, 0 = all  -> 6

(note: if you specify the same output prefix, airodump will resume
 the capture session by appending data to the existing capture file)

Output filename prefix        -> last

(note: to save space and only store the captured WEP IVs, press y.
 The resulting capture file will only be useful for WEP cracking)

Only write WEP IVs (y/n)      -> n
```

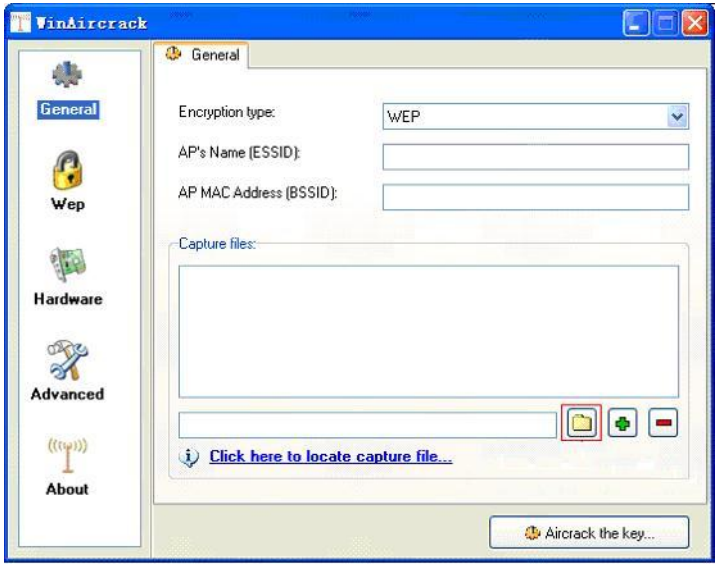
BSSID	PWR	Beacons	# Data	CH	MB	ENC	ESSID
00:03:2F:18:4E:0E	41	13026	15573	6	22	WEP	demonalex

BSSID	STATION	PWR	Packets	ESSID
00:03:2F:18:4E:0E	00:15:E9:2B:3B:A6	41	285	demonalex
00:03:2F:18:4E:0E	00:15:E9:2B:3D:08	42	6544	demonalex
00:03:2F:18:4E:0E	00:15:E9:2B:3C:F2	52	8340	demonalex

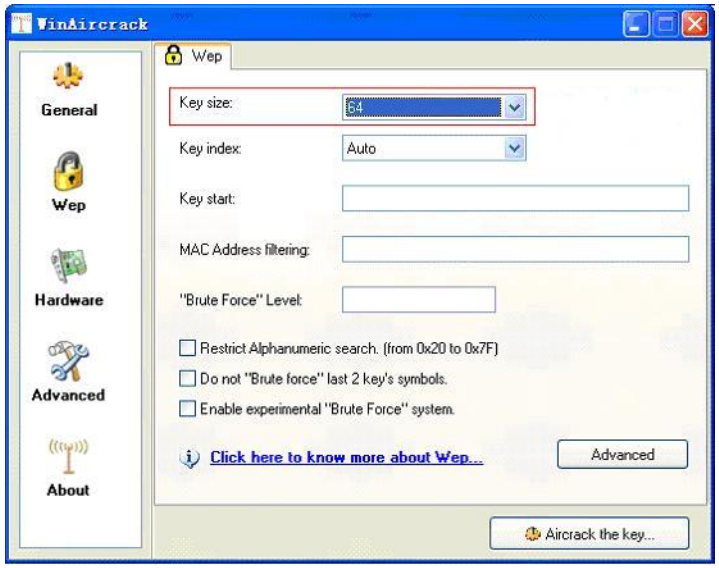
破解 WEP KEY

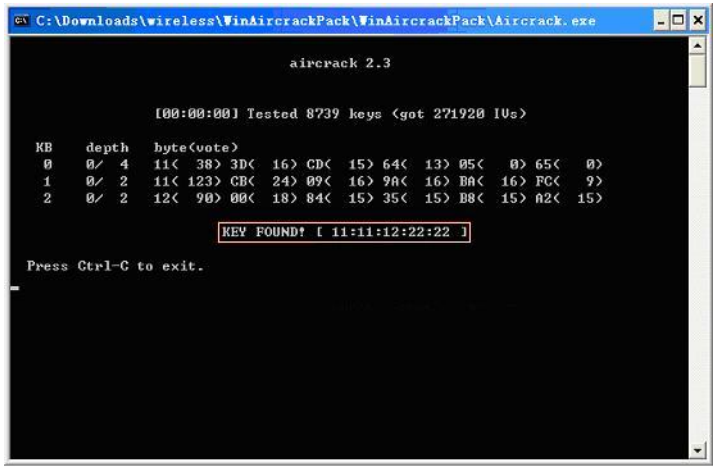
```
BSSID, First time seen, Last time seen, Channel, Speed, Privacy, Power, # beacons,
# data, LAN IP, ESSID
00:03:2F:18:4E:0E, 2006-03-27 17:12:20, 2006-03-27 18:05:55,  6,  22, WEP ,  37,
25499,   271922, 192.168.  1.  1, demonalex

Station MAC, First time seen, Last time seen, Power, # packets, BSSID, ESSID
00:15:E9:2B:3C:F2, 2006-03-27 17:12:21, 2006-03-27 18:03:42,  52,    18514,
00:03:2F:18:4E:0E, demonalex
00:15:E9:2B:3D:08, 2006-03-27 17:35:17, 2006-03-27 18:04:34,  38,    21230,
00:03:2F:18:4E:0E, demonalex
00:15:E9:2B:3B:A6, 2006-03-27 17:36:43, 2006-03-27 18:05:55,  40,   302687,
00:03:2F:18:4E:0E, demonalex
```



破解 WEP KEY


WinAircrack
General
Wep
Hardware
Advanced
About
Wep
Key size:
64
Key index:
Auto
Key start:
MAC Address filtering:
"Brute Force" Level:
Restrict Alphanumeric search. (from 0x20 to 0x7F)
Do not "Brute force" last 2 key's symbols.
Enable experimental "Brute Force" system.
Click here to know more about Wep...
Advanced
Aircrack the key...


C:\Downloads\wireless\WinAircrackPack\WinAircrackPack\Aircrack.exe
aircrack 2.3
[00:00:00] Tested 8739 keys (got 271920 IVs)
KB depth byte(vote)
0 0/ 4 11(38) 3D(16) CD(15) 64(13) 05(0) 65(0)
1 0/ 2 11(123) CB(24) 09(16) 9A(16) BA(16) FC(9)
2 0/ 2 12(90) 00(18) 84(15) 35(15) B8(15) A2(15)
KEY FOUND! [11:11:12:22:22]
Press Ctrl-C to exit.

破解 WEP KEY

4.使用破解的 AP

- 打開無線網卡的設置視窗，設置參數 。