# 第六章

# 嗅探

# 嗅探

- 嗅探（Sniffing）是指一個程式或裝置（Sniffer）在特定的網路上，可以去擷取網路流量中需要的資訊。

- 嗅探器（Sniffer）是一個封包抓取或訊框（抓取程式，它可以接收網路上的流量資訊，並以命令列或圖形介面的方式，將資訊顯示出來。

# 封包（Packet）與訊框（Frame）

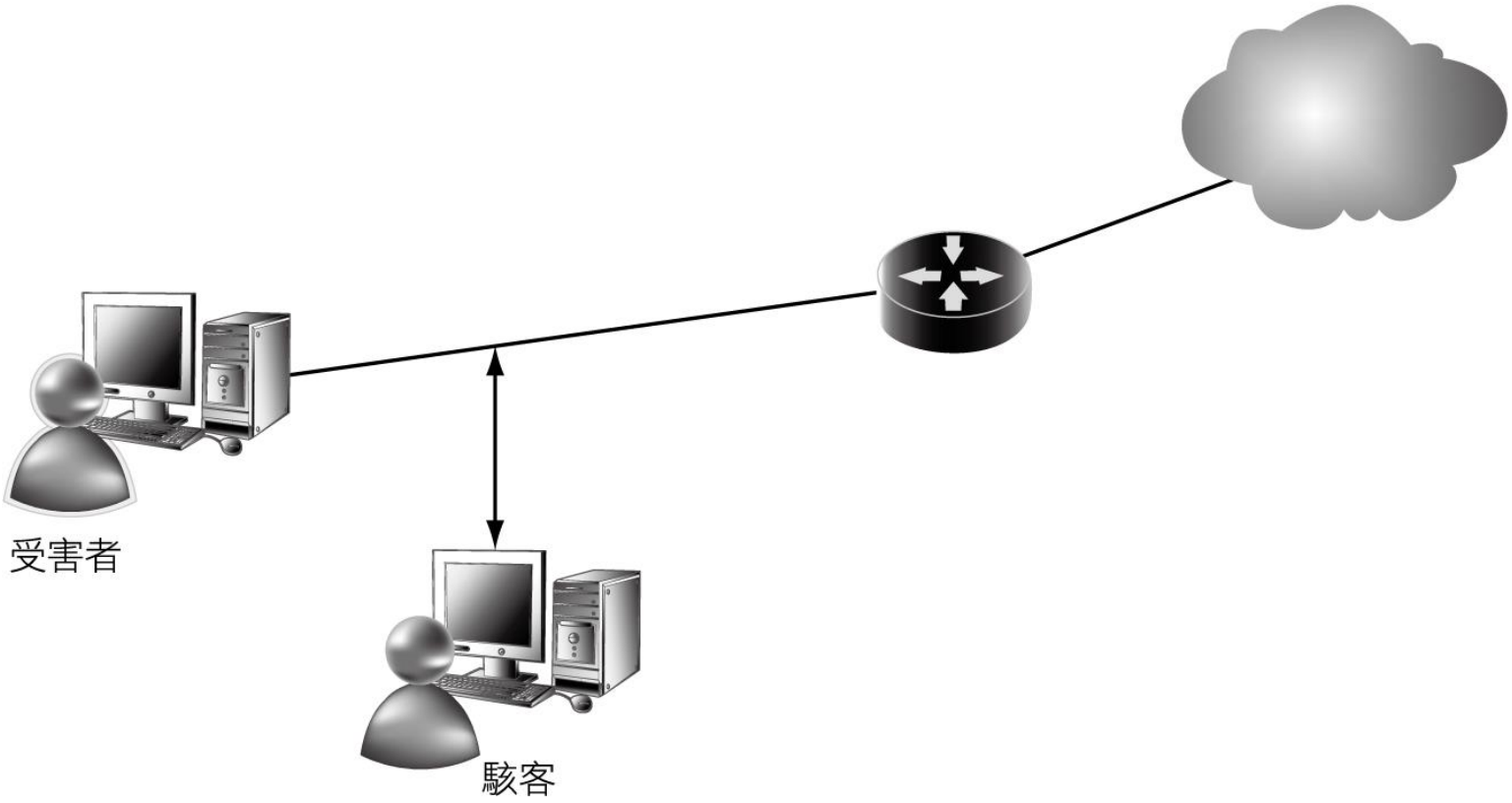
- 封包是OSI網路模型中第三層的傳輸資料單元，以IP做為傳輸的位址。
- 訊框是OSI網路模型中第二層的傳輸資料單元，以MAC做為傳輸的位址。

# 嗅探的目的

嗅探是的目的是為了竊取有關以下的資訊：

（1）攔截密碼。
（2）攔截文字內容。
（3）將檔案攔截。

# 監聽的架構圖



# 監聽的架構

- 駭客會想盡辦法在來源與目的之間擷取及記錄封包，駭客電腦的網卡通常會開啟「混雜模式」，再利用工具程式將資料或密碼還原，最後再利用這些資料直接侵入受害者系統或者受害者使用的伺服器。

# 混雜模式（Promiscuous mode）

網卡有幾種接收資料訊框的狀態，如Unicast、Broadcast、Multicast、Promiscuous等。

- 單播（Unicast）是指網卡在接收時，目的地位址必須是本機的硬體位址（MAC）的資料訊框才會接受。
- 廣播（Broadcast）是指接收訊框類型為廣播的資料。Multicast是只接收特定群組的訊框資料。
- Promiscuous就是混雜模式，是指對訊框中的目的地MAC位址不做檢查，全部接收。

# 混雜模式（Promiscuous mode）

- 對於Hub來說，假如A、B、C接在同一個Hub上，當A對C發送訊框時，依據Hub的工作原理，Hub將會廣播這個訊框給所有的Port，所以B實際上也會收到這個訊框，但是因為這是一個單播封包，一般網卡又都在單播模式下，所以B會將這個發給C的訊框丟棄。但如果B處於混雜模式，B的網路卡驅動程式就不會丟棄這個訊框，而是把這個訊框送給上層的驅動程式或應用程式。

# 容易被偷聽及破解的協定

- 容易被偷聽及破解的協定包括：

（1）Telnet及 Rlogin。

（2）HTTP。

http://php.testsparker.com/auth/login.php

http://210.61.47.85/mooc/login.php/

（3）POP。

（4）FTP。

（5）IMAP。

# 監聽的技術與工具

- 嗅探器可以監聽第二層的訊框（Frame），也可以監聽第三層的封包（Packet）。
- 有的工具在操作與顯示時是以文字模式進行（以Linux系統為主），有的則是以圖形介面顯示結果（以Windows系統為主）。
- 某些工具程式甚至可以將封包的串流重組回原樣

# 監聽的類型

- 「被動監聽（Passive sniffing）」與「主動監聽（Active sniffing）」。

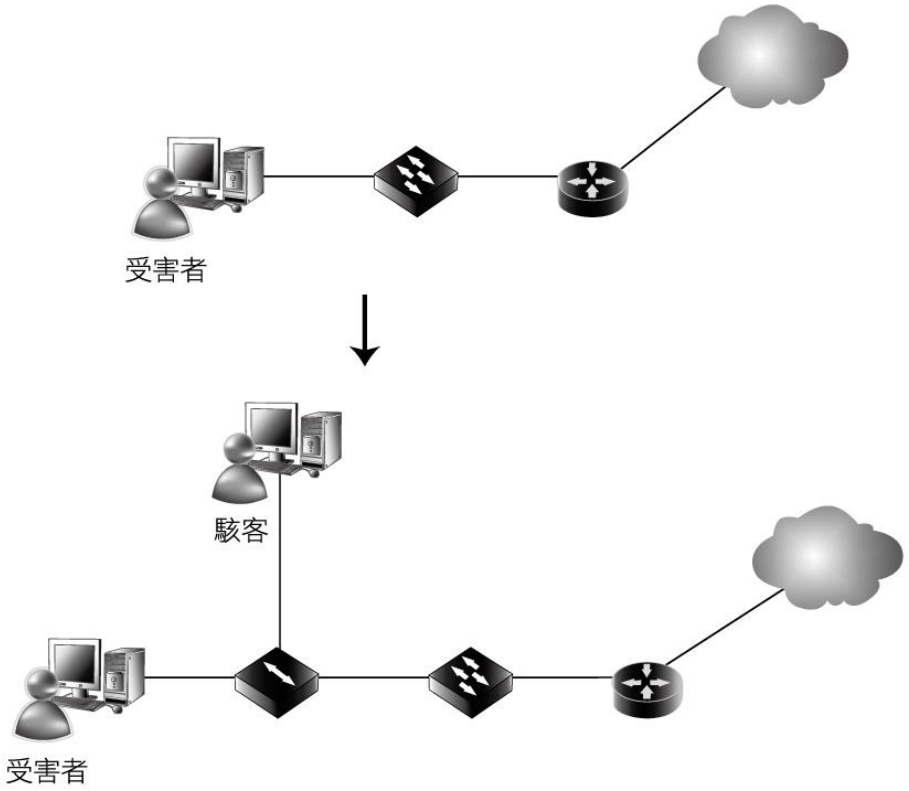
- 被動監聽代表駭客不需要送出訊息，即可以獲得被害者的資料。使用主動監聽時，駭客必須主動送出一些會造成錯亂的訊息，才能監聽到資料。

# 被動監聽

- 被動監聽模式下，駭客的監聽行為很難被察覺，被動監聽可以是透過Hub來進行監聽。

- 受害者的電腦是接到交換器上，但是駭客若要監聽資料，可在受害者電腦與交換器間加裝一Hub，駭客只要將筆記型電腦接在Hub上面，並且開啟筆記型電腦網卡的混雜模式，就可以進行監聽了。

# 被動監聽



# 主動監聽

- 這種監聽方式不需要變更硬體環境，只要透過現有的交換器就可以監聽，但是較容易被追蹤。

# 交換器原理

- 某台主機第一次傳送資料時，這個進入交換器的訊框包含了來源主機的MAC。交換器內部有一個MAC表，這個MAC表會記錄這主機的MAC與這訊框來自於那個Port。

- 當其他送往目的地的訊框進入交換器時，會以目的地MAC位址與MAC表進行比對，若發現目的地MAC已存在於MAC表中，就會將訊框送往表中所記錄的Port。

# 交換器毒害

- 攻擊者會試著藉著送出偽造（bogus）的MAC去毒害交換器，此類的技術有：

（1）ARP Spoofing

（2）MAC Flooding。

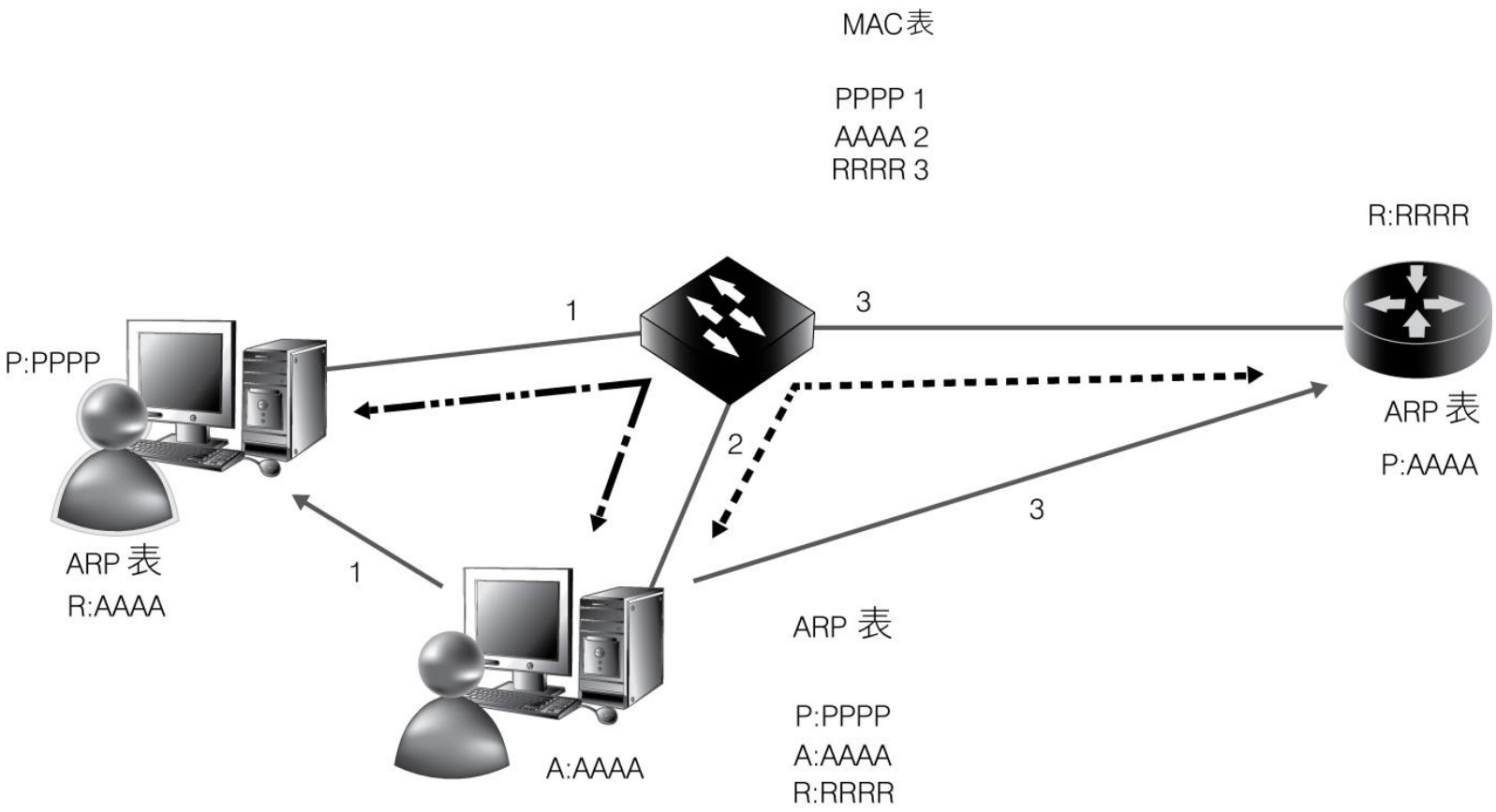
# ARP

- 位址解析協定（Address Resolution Protocol）是網路層的協定用來轉換IP位址成為一個實體位址（MAC address）。
- 為了要得到實體位址，主機會廣播一個ARP的需求（Request）到TCP/IP網路上，因為這個需求是以廣播並帶著目的地IP的方式送出，所有串連的交換器的Port都會收到這個需求訊息，而符合這個IP的主機將會回應，並攜帶著該主機的MAC進行回應（Reply），發出需求的主機在收到回應後，會將此目的地主機的IP與MAC對應放在主機的Cache中。

# ARP Spoofing

- ARP假造（Spoofing）或稱為ARP毒害（Poisoning），攻擊者可以利用ARP通訊時的缺陷，假造回應的訊息，以監聽（轉送）網路上兩台機器間的流量，下面敘述其運作流程。

# ARP Spoofing



# ARP Spoofing

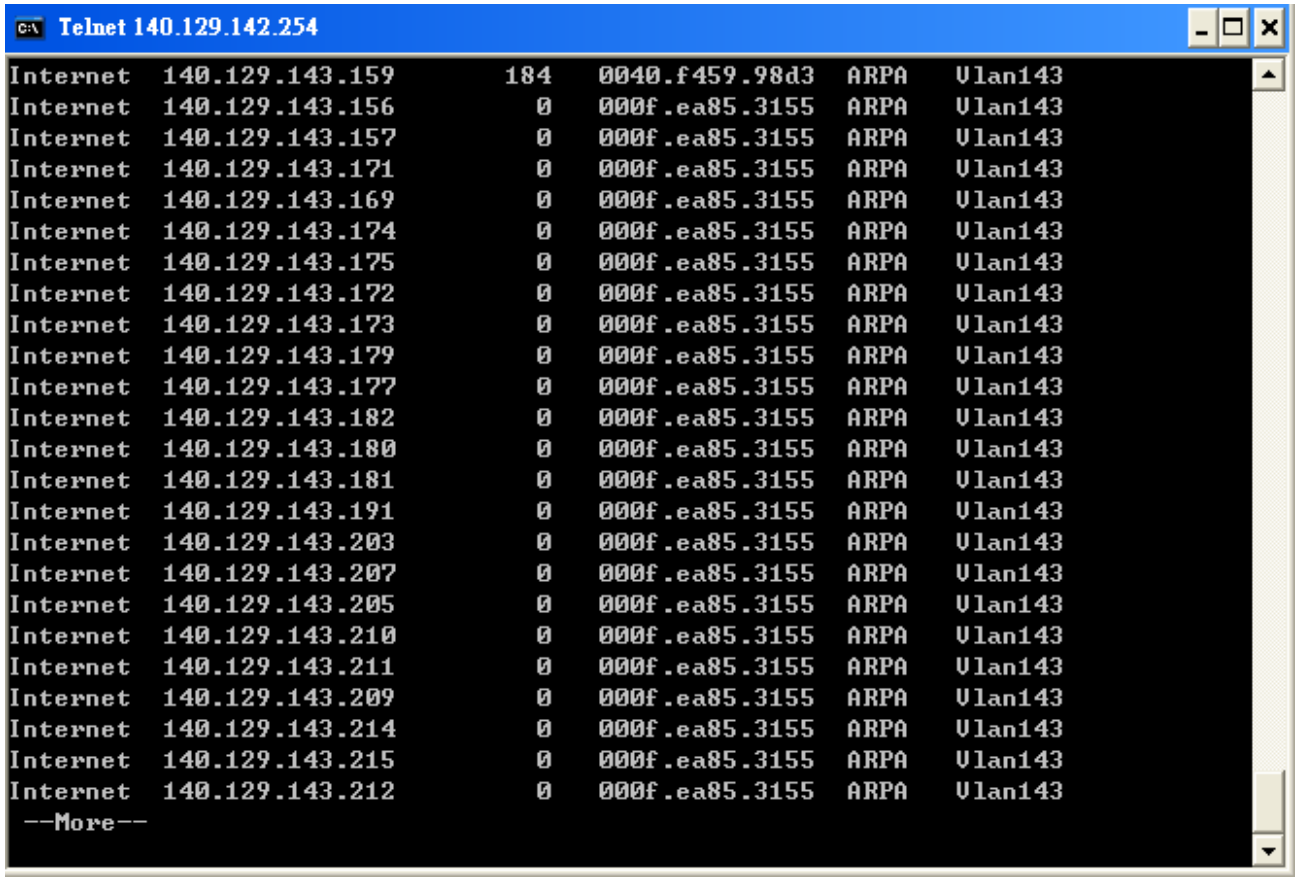
1. 攻擊者假造ARP Reply給受害者A主機，宣稱出路由器的MAC是AAAA（攻擊者的MAC）。（於是紀錄在受害者主機Cache中的閘道IP變成是攻擊者的MAC）
2. 攻擊者會記錄每一個受害者真實的IP與MAC對照。
3. 駭客假造ARP Reply送給路由器，宣稱受害者的MAC是AAAA（攻擊者的MAC）。路由器的ARP表於是就記錄成受害者的IP對應的卻是攻擊者的MAC，。

# ARP Spoofing

4. LAN是以MAC來運作，受害者電腦閘道的MAC變成是AAAA（攻擊者的MAC），若受害者要傳送資料到網際網路，訊框會先傳送給攻擊者，攻擊者再將這個訊框轉送給路由器。

5. 所有資料都先經過攻擊者的電腦，攻擊者網卡開啟為混雜模式，所以用Sniffer工具可進行監聽。

# ARP Spoofing



# MAC Flooding

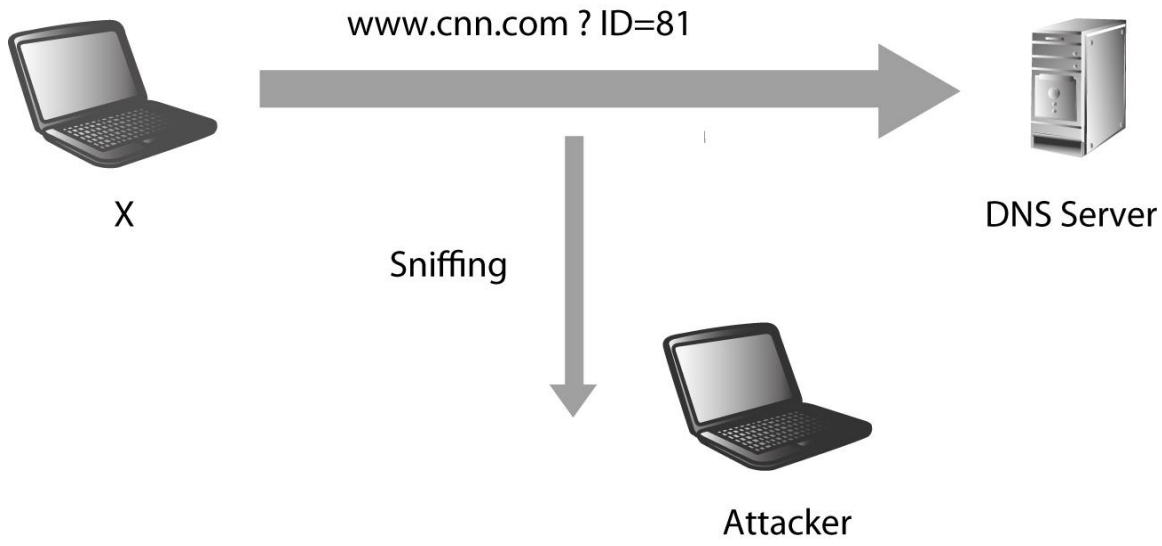
- MAC flooding就是攻擊者的主機會一直大量將假造的隨機MAC位址送給交換器，直到交換器的記憶體被塞滿，再也無法保留任何的MAC。
- 若一個正常訊框這時到達交換器，交換器會檢查這個訊框的目的地是否存在於MAC表中，因為MAC表中現在都是一堆的垃圾MAC，目的地MAC必定無法於MAC表中查到，交換器會把這個訊框複製到每一個Port上。

# DHCP飢餓攻擊

- DHCP運作時，Client端會送一個需求給網路上任何的DHCP Server，DHCP Server會依據需求者的MAC配發一個IP。
- 攻擊主機會結合隨機產生的假MAC，不斷的發送DHCP需求，合法的DHCP Server就必須回應這個需求，最後一定會將合法的DHCP Server的IP耗盡。
- 接著非法的DHCP SERVER將接替合法DHCP Server的工作，為後續發出要求的客戶端主機（Client）分配錯誤的IP、錯誤的閘道（可以利用來監聽流量）、錯誤的DNS IP（可以指向假冒的頁面）等。

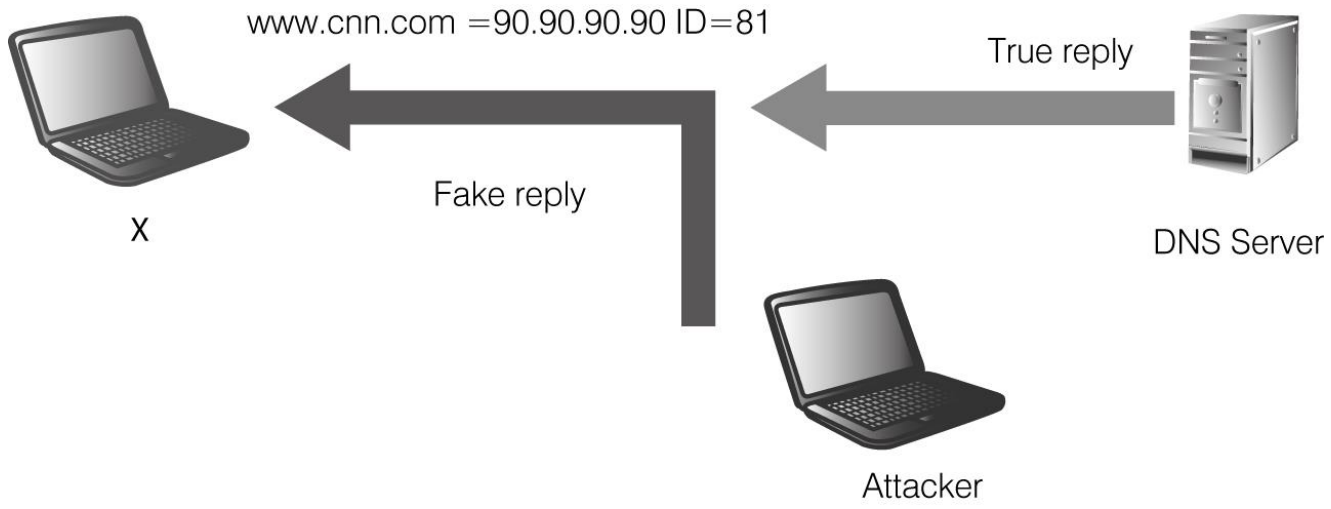
# DNS毒害

- 步驟1：先毒害目標主機（X）的ARP（APR Poisoning），使攻擊主機（A）可以監聽目標主機（X）的流量，流量傳輸方向變成X→A。



# DNS毒害

- 步驟2：若攻擊主機A監聽到X進行了DNS查詢，攻擊主機A會立即發送一個假的DNS回應。
- 步驟3：X主機接下來開啟假的網頁。



# 偵測Sniffing與對策

- 可以利用工具程式，檢查區域網路內那部機器的網卡正在執行混雜模式（Promiscuous mode），這種方式的缺點是不太可能隨時在檢查狀態中。
- 可以在每個個人主機上執行ARPWatch，以隨時監看路由器的MAC是否被改變。（第二個方法在某些單位執行有點困難）
- 要防止被監聽，可以嚴格管制網路媒體的實體存取權限，讓Sniffer無法被安裝在網路媒體上。但是這種方式很難完全阻隔，因為駭客可以透過改變網路線路或拓樸的方式來攔截資訊。

# 偵測Sniffing與對策

- 最好的方法是使用加密（Encryption），把資料在傳輸前先進行加密，即使駭客使用監聽的方式得到這些資料也沒有意義，因為破解這些資料相對較難或較麻煩。
- 在實體設備的設定上，可以進行以下幾種防護設定：
- （1）使用靜態IP與靜態MAC對應的ARP表，讓駭客不能輕易變更ARP表的內容。
- （2）網路上的交換器可以設定port-security，讓不應該出現的MAC不會出現在交換器上。

# DHCP Server攻擊對策

（1）DHCP Snooping（以Cisco交換器設定為例）

switch(config)#ip dhcp snooping
switch(config)#ip dhcp snooping vlan 4,10
switch(config)#no ip dhcp snooping information option
switch(config-if)#ip dhcp snooping trust

Switch收到DHCP請求時，將IP和MAC的對應關係都儲存在記錄表中（DHCP Snooping Binding Table）。

（2）使用路由器上的存取清單（ACL)。

# 工具程式

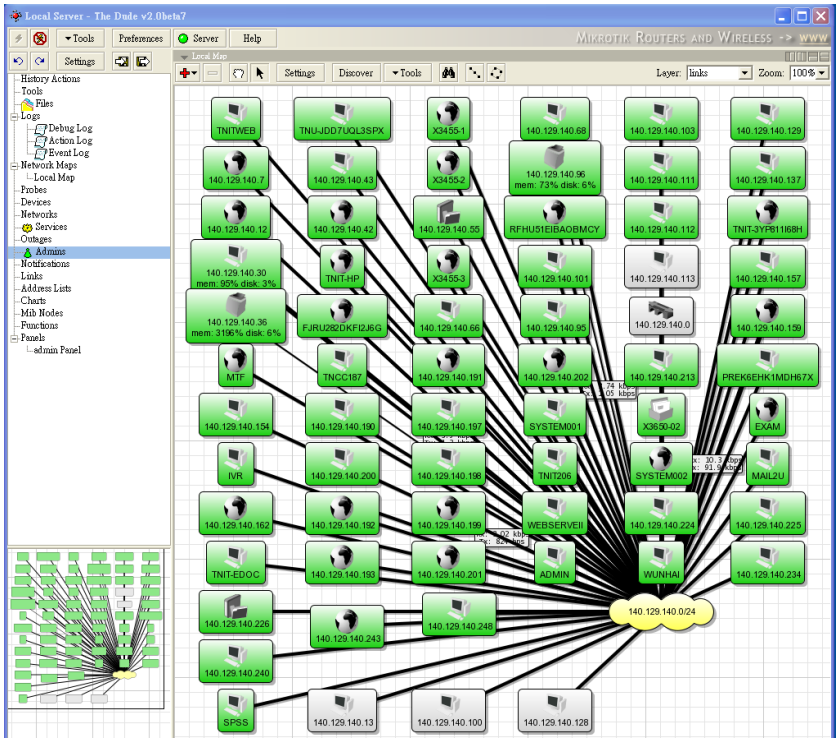
- **Dude**（掃瞄網路裝置的工具）

- Dude支援snmp協定，是一個網路監督程式，方便於管理網路環境，能搜尋出網路中所有的裝置節點並以圖像顯示，且會顯現連結關係。圖像中包括PC、各種功能伺服器、印表機、Router等。

# Dude

分為兩部分：

- Dude Server
- Dude Client。



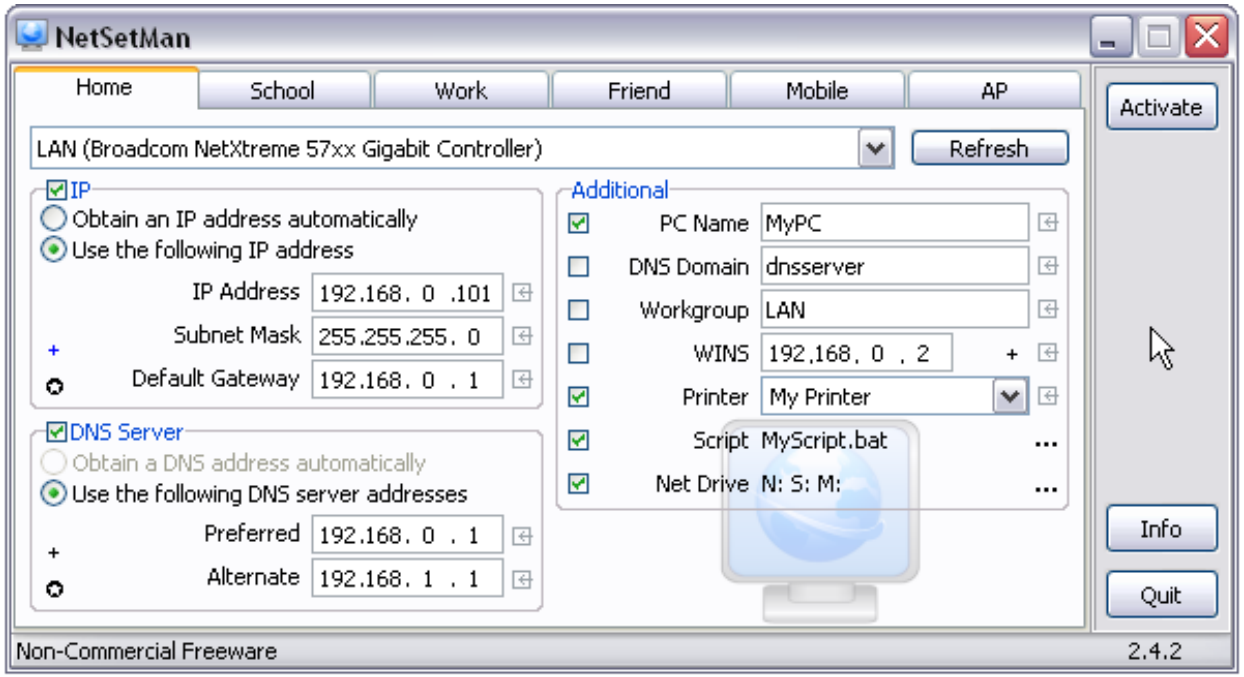
# 工具程式

- NetSetMan Tool

- NetSetMan可以讓使用者快速的更換有關網路的設定，可以預先設定六組Profiles，每一組設定包括IP位址、遮罩、預設閘道、DNS伺服器。

# NetSetMan Tool

- 可以讓管理者或攻擊者在不同網路，需要做不同的設定時，能快速的切換到不同的設定。



# 工具程式

- **Ethereal**

- Ethereal的新版更名為WireShark，是UNIX及Windows的網路分析器。

- 允許使用者從一個活動中的網路去檢驗資料，並且記錄封包將其儲存成檔案放在磁碟上，或者可以即時互動的瀏覽每個被抓到的封包摘要或細節資料。

# Ethereal

（1）要顯示指定的協定：輸入http或tcp…等。

（2）如果要過濾出某個IP位址：ip.addr==140.129.142.220

如果要過濾多的IP，可以輸入ip.addr == 60.199.192.132

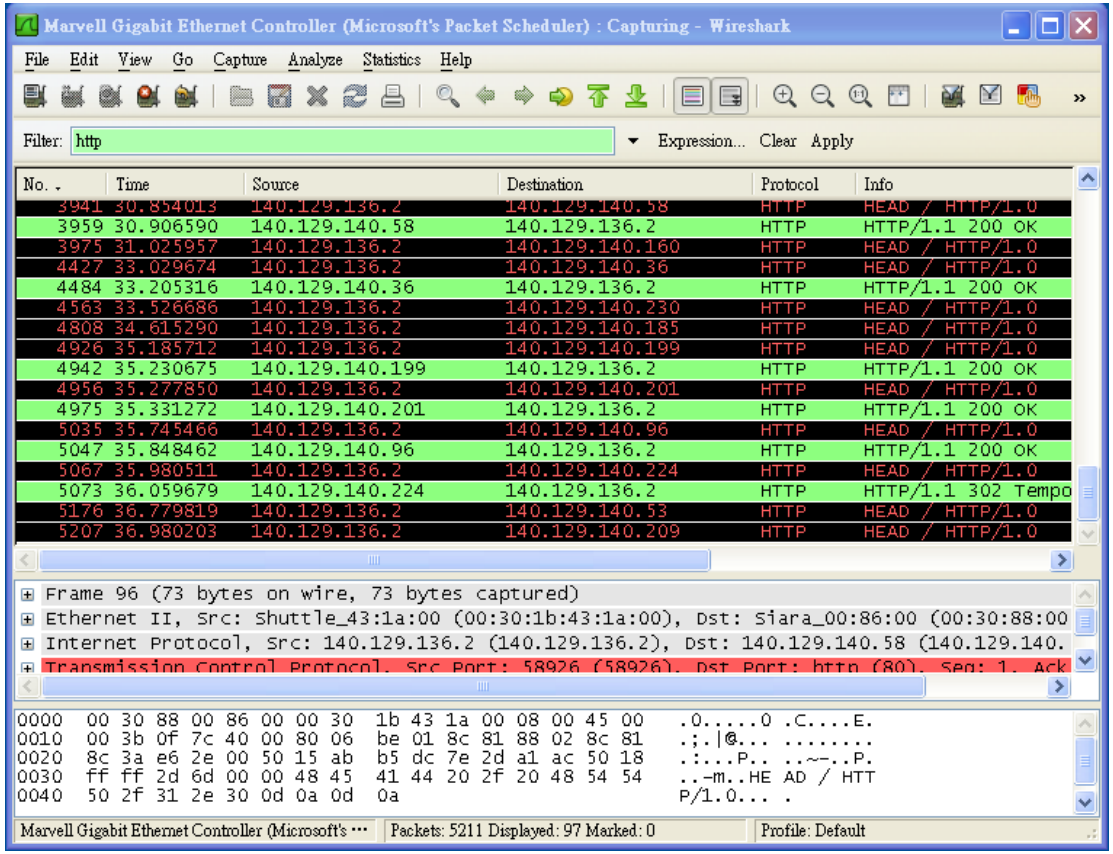
or ip.addr == 60.199.192.123

（3）監督特定的Port：tcp.port==80

（4）指定的主機IP及指定的Port：

ip.addr==60.199.192.132 && tcp.port=80

# Ethereal

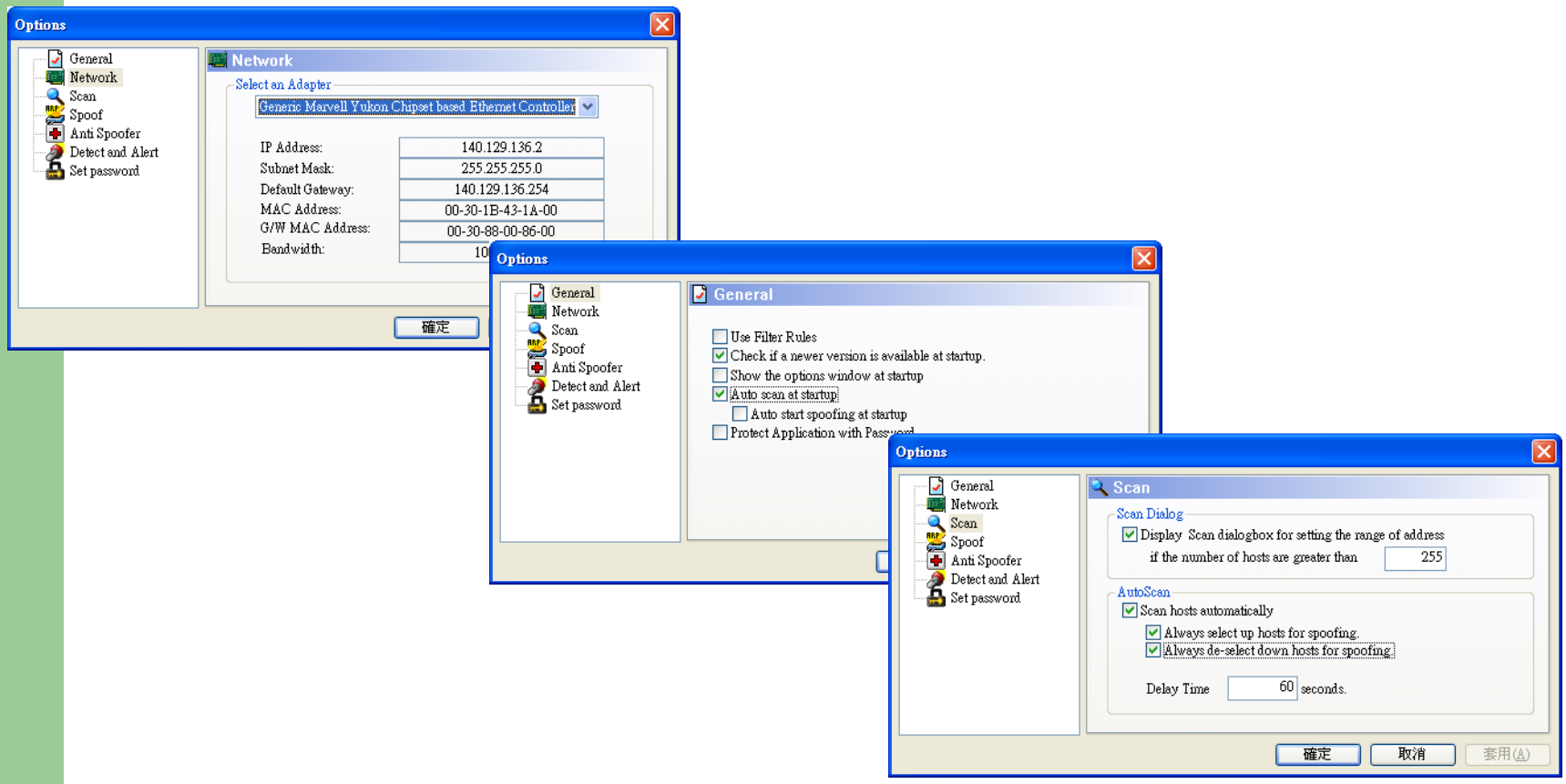

Marvell Gigabit Ethernet Controller (Microsoft's Packet Scheduler) : Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: http
Expression... Clear Apply
No. Time Source Destination Protocol Info
3941 30.854013 140.129.136.2 140.129.140.58 HTTP HEAD / HTTP/1.0
3959 30.906590 140.129.140.58 140.129.136.2 HTTP HTTP/1.1 200 OK
3975 31.025957 140.129.136.2 140.129.140.160 HTTP HEAD / HTTP/1.0
4427 33.029674 140.129.136.2 140.129.140.36 HTTP HEAD / HTTP/1.0
4484 33.205316 140.129.140.36 140.129.136.2 HTTP HTTP/1.1 200 OK
4563 33.526686 140.129.136.2 140.129.140.230 HTTP HEAD / HTTP/1.0
4808 34.615290 140.129.136.2 140.129.140.185 HTTP HEAD / HTTP/1.0
4926 35.185712 140.129.136.2 140.129.140.199 HTTP HEAD / HTTP/1.0
4942 35.230675 140.129.140.199 140.129.136.2 HTTP HTTP/1.1 200 OK
4956 35.277850 140.129.136.2 140.129.140.201 HTTP HEAD / HTTP/1.0
4975 35.331272 140.129.140.201 140.129.136.2 HTTP HTTP/1.1 200 OK
5035 35.745466 140.129.136.2 140.129.140.96 HTTP HEAD / HTTP/1.0
5047 35.848462 140.129.140.96 140.129.136.2 HTTP HTTP/1.1 200 OK
5067 35.980511 140.129.136.2 140.129.140.224 HTTP HEAD / HTTP/1.0
5073 36.059679 140.129.140.224 140.129.136.2 HTTP HTTP/1.1 302 Tempo
5176 36.779819 140.129.136.2 140.129.140.53 HTTP HEAD / HTTP/1.0
5207 36.980203 140.129.136.2 140.129.140.209 HTTP HEAD / HTTP/1.0
Frame 96 (73 bytes on wire, 73 bytes captured)
Ethernet II, Src: Shuttle_43:1a:00 (00:30:1b:43:1a:00), Dst: Siara_00:86:00 (00:30:88:00
Internet Protocol, Src: 140.129.136.2 (140.129.136.2), Dst: 140.129.140.58 (140.129.140.
Transmission Control Protocol, Src Port: 58926 (58926), Dst Port: http (80), Seq: 1, Ack
0000 00 30 88 00 86 00 00 30 1b 43 1a 00 08 00 45 00 .0.....0 .C....E.
0010 00 3b 0f 7c 40 00 80 06 be 01 8c 81 88 02 8c 81 .;.|@... ........
0020 8c 3a e6 2e 00 50 15 ab b5 dc 7e 2d a1 ac 50 18 .:...P.. ..~-..P.
0030 ff ff 2d 6d 00 00 48 45 41 44 20 2f 20 48 54 54 ..-m..HE AD / HTT
0040 50 2f 31 2e 30 0d 0a 0d 0a P/1.0... .
Marvell Gigabit Ethernet Controller (Microsoft's ···
Packets: 5211 Displayed: 97 Marked: 0
Profile: Default

# 工具程式

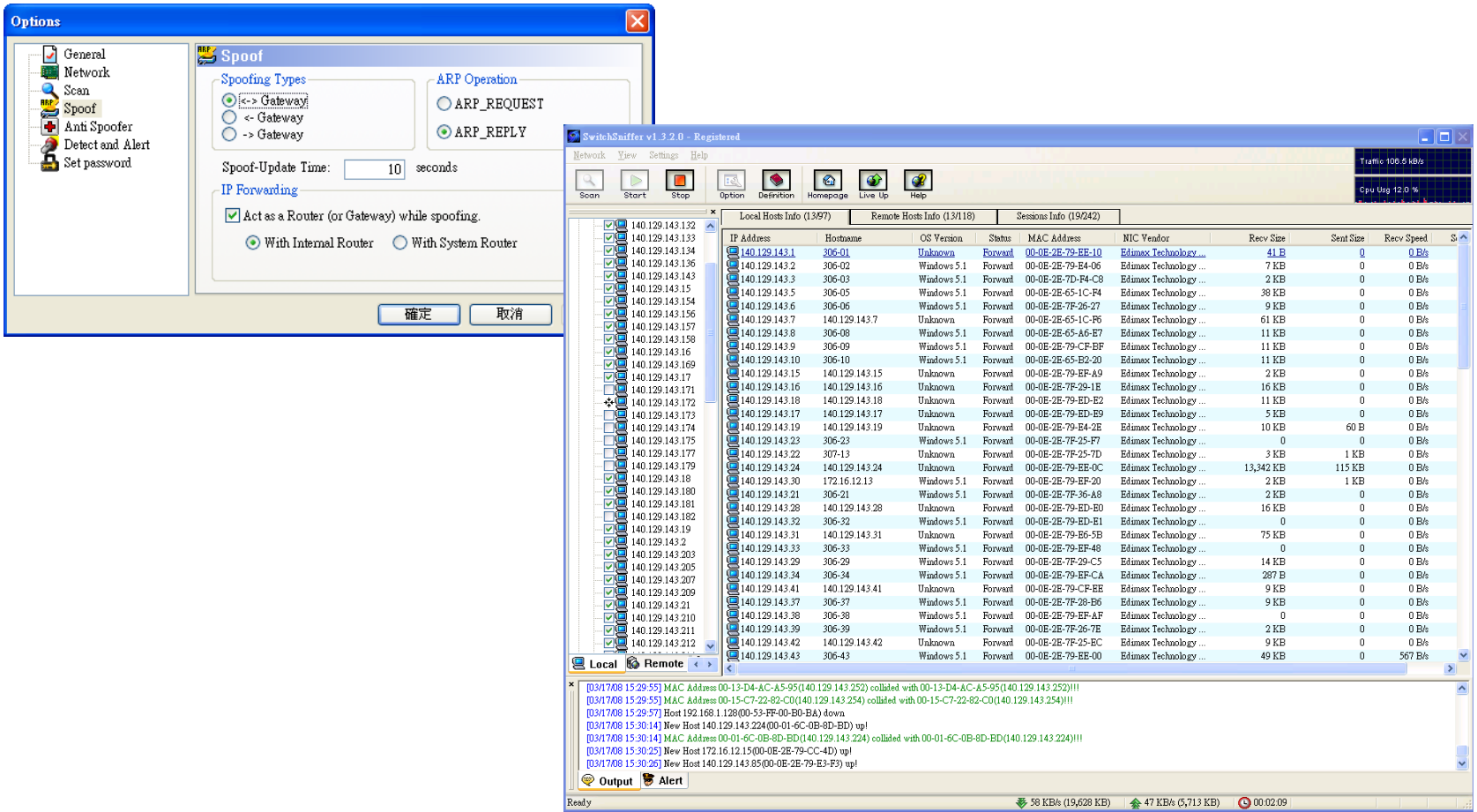
- **SwitchSniffer**

- 類似WinarpSpoofer的工具，但是更加便利。如果要使用這個軟體，不需要付費，但是必須安裝其廣告工具列，此工具列會被某些防毒軟體偵測為廣告軟體。

# SwitchSniffer

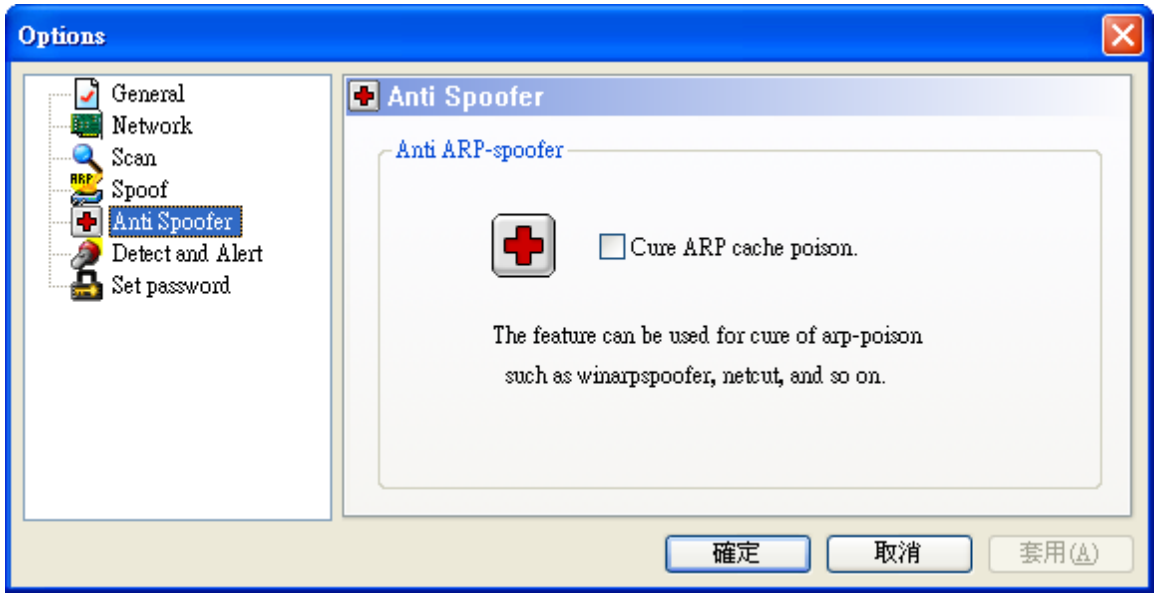


# SwitchSniffer



# SwitchSniffer

- 「藥」即是「毒」，「毒」亦是「藥」。
- 駭客的工具程式，有時就是資安防護的工具。



# 網路剪刀手

- 網路剪刀手（Netcut）是一個網路工具程式，可以用來切斷使用者的連線，軟體本身是一個好用的網路工具，卻被用在惡意的行為。
- 裝有網路剪刀手的A主機向受害B主機發送假的ARP訊息，使得B主機上ARP表中對應到閘道的MAC address錯誤。由於主機上網必須透過閘道傳送，若閘道的MAC位址錯誤，當然會造成主機B的封包無法傳送到閘道上，即便是原本建立好的連線，也會因為timeout而導致斷線。

# 網路剪刀手防治對策

- 在主機上將正確的IP與MAC位址設定成固定的靜態記錄，不准被修改，就可以避免狀況發生。 設定指令如下：

arp -s 閘道的 IP 位址 閘道的 MAC 位址

# 工具程式

- **Etherflood**
- MAC Flooding的工具 。
- 在Windows XP下使用，會被某些防毒軟體辨識為惡意軟體。

# 工具程式

- **WinDnsSpoof**

- 是 DNS Spoofing的工具。這是在轉送DNS Request時，可以換掉攻擊者的MAC。

- wds -n www.cnn.com -i 123.123.123.123 -g 00-C0-26-DD-59-CF –v

-I 後面接的是偽造網頁主機的IP。

-g 後面接的是真實閘道的 MAC（不同子網路）或真實的 DNS Server（同個子網路）。

# 工具程式

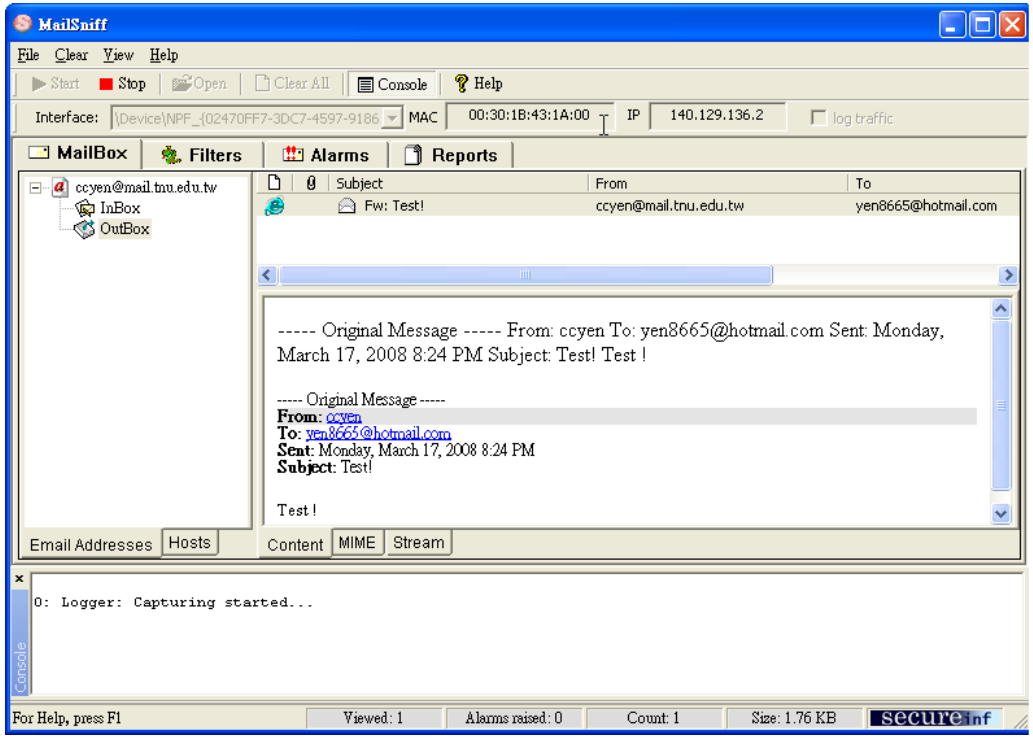
- **MailSniff**

- MailSniff是Windows系統下的工具程式，這個軟體可以攔截電子郵件的內容，並且依據寄件者進行樹狀分類，每個帳號都會有收件匣（InBox）及寄件匣（OutBox）。

- 每封信件都可以直接在畫面上顯示寄件者（From）及收件者（To）的姓名，甚至信件的內容及信件的夾檔都直接顯示出來，不需要使用其他軟體組合信件封包。

# MailSniff

- 這個軟體支援WinXP及Win 2003，利用ARPSpoofing的軟體，可以監聽整個網段中進入及離開的信件。

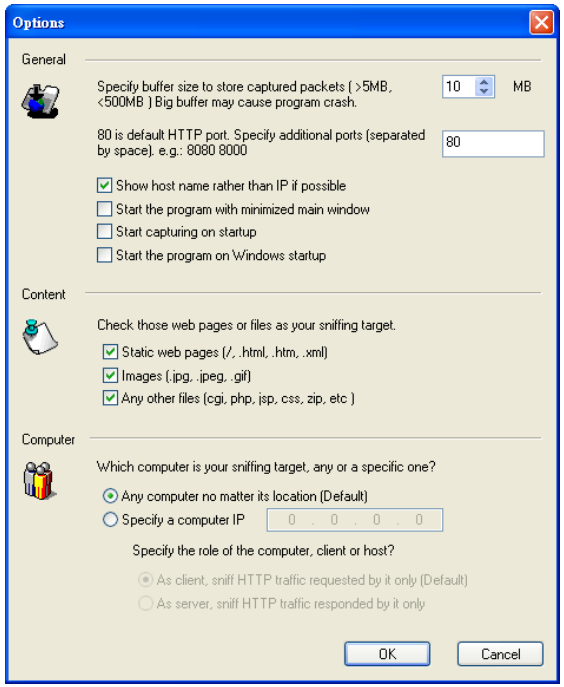


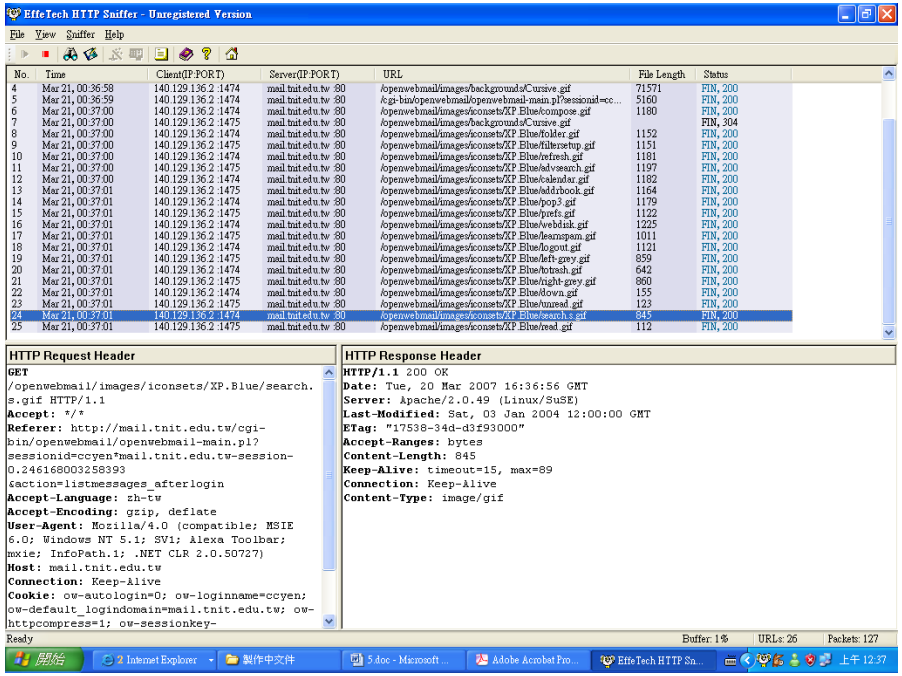
# 工具程式

- **HTTP Sniffer**

- EffeTech HTTP Sniffer是一個HTTP協定的封包探測器，會將IP封包予以重組，並且可以即時顯示封包傳輸的URL及內容，也可將結果輸出成html或CSV格式的報表。

# HTTP Sniffer



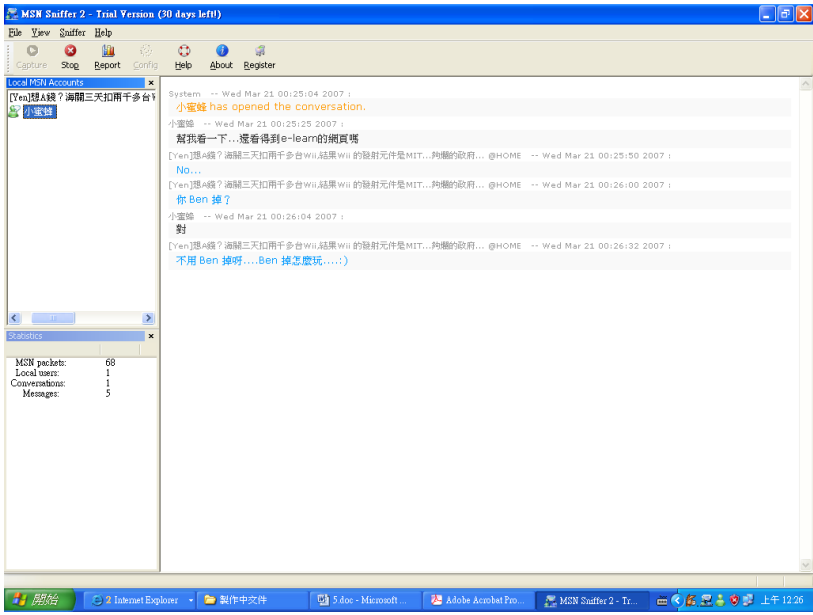
# 工具程式

- MSN Sniffer
- 是一個MSN Messenger 聊天內容抓取程式 。

# MSN Sniffer

- 畫面左邊是帳號，右邊是該帳號的對話內容。

- 安裝完畢並且執行後，按下左上角的「Capture」圖示，就會開始擷取MSN的通訊資訊 。



# 工具程式

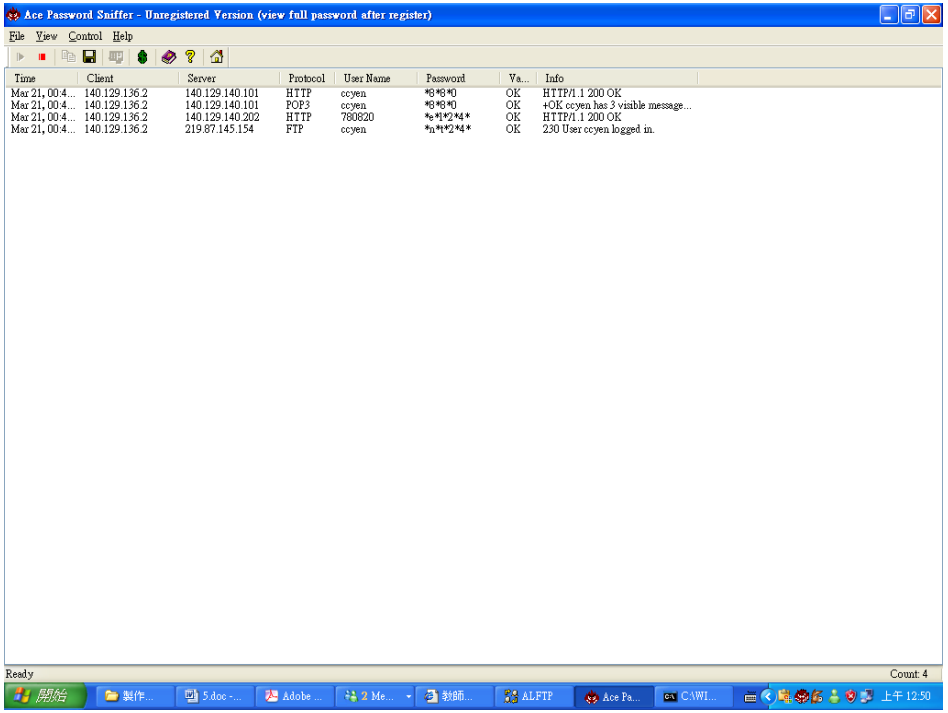
- **Ace Password Sniffer**

- Ace Password Sniffer可監聽及抓取使用者的帳號及密碼，涵蓋的服務有FTP、POP3、HTTP、SMTP、Telnet以及某些web mail的密碼。

- 懶惰的管理者如果將所有系統的帳號與密碼設定成相同，此軟體監聽的內容將會造成非常危險的後果。

# Ace Password Sniffer

- 安裝完畢並且執行後，按下左上角的「start capturing」箭頭，就會開始擷取帳號及密碼。



# 工具程式

- **Cain and Abel**

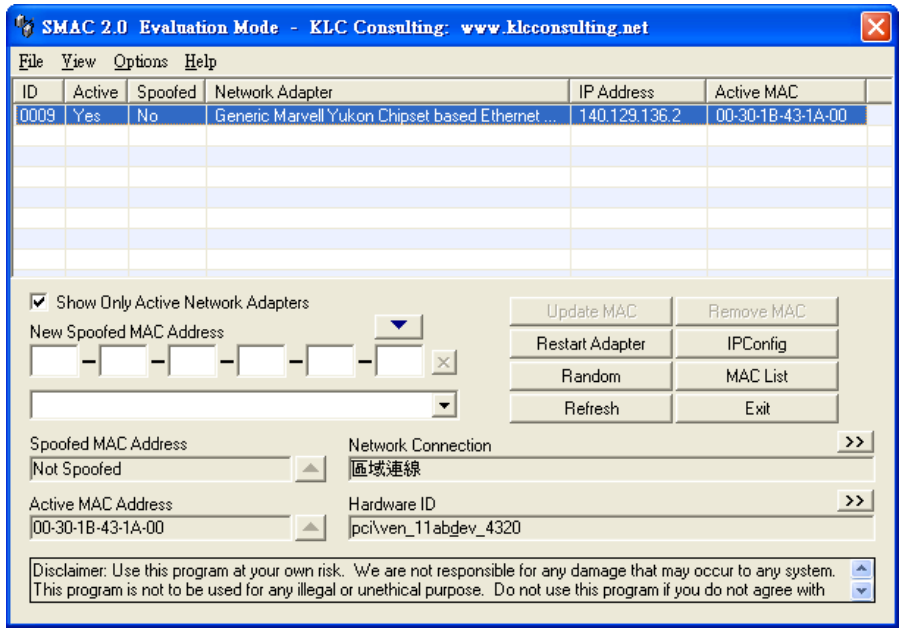
- 這是一個非常有名的工具，具有雜湊字典及暴力破解（Brute-Force Crackers），能過濾出SIP-MD5認證，與Winpcap、Tcpdump、Ethereal的格式相容。

- Cain‘s sniffer可以抓取出SIP/RTP的語音對話，並且存成WAV檔案 。

# 工具程式

- **SMAC**

- SMAC是一個MAC位址的修改工具（Spoofer），在Windows 2000、XP及Server 2003系統下使用，內建記錄能力以追蹤MAC位址修改的活動。



# 工具程式

- **Ntop**

- Ntop是網路流量偵測軟體，能顯示網路的使用。

- 在互動模式下，於使用者的終端機上可以顯示網路的狀態；在web模式下，則如同web伺服器，可以把網路狀態建立成HTML。

# 工具程式

- **Snort**

- Snort是一套開放原始碼（Open Source）的網路入侵預防軟體（IPS）與網路入侵偵測軟體（IDS）。Snort使用了偵測簽章（Signature-based）與通訊協定（Protocol）的偵測方法，被認為是全世界最廣泛使用的入侵預防與偵測軟體。

- Snort 可以被設定成三種模式：sniffer、packet logger及網路IDS（intrusion detection system，入侵偵測系統）。

- WinSnort是Windows版的Snort 。

# Snort

規則範例：

```
alert tcp any any -> 192.168.1.0/24 111 (content:"|00 01
    86 a5|"; msg: "mountd access";)
```

- 第一個括號前是規則表頭（rule header），括號內是規則選項（rule options），規則選項中冒號前的字稱為選項關鍵字（option keywords。

- 如果要把所有的封包記錄到硬碟上，你需要指定一個日誌目錄，snort就會自動記錄封包：

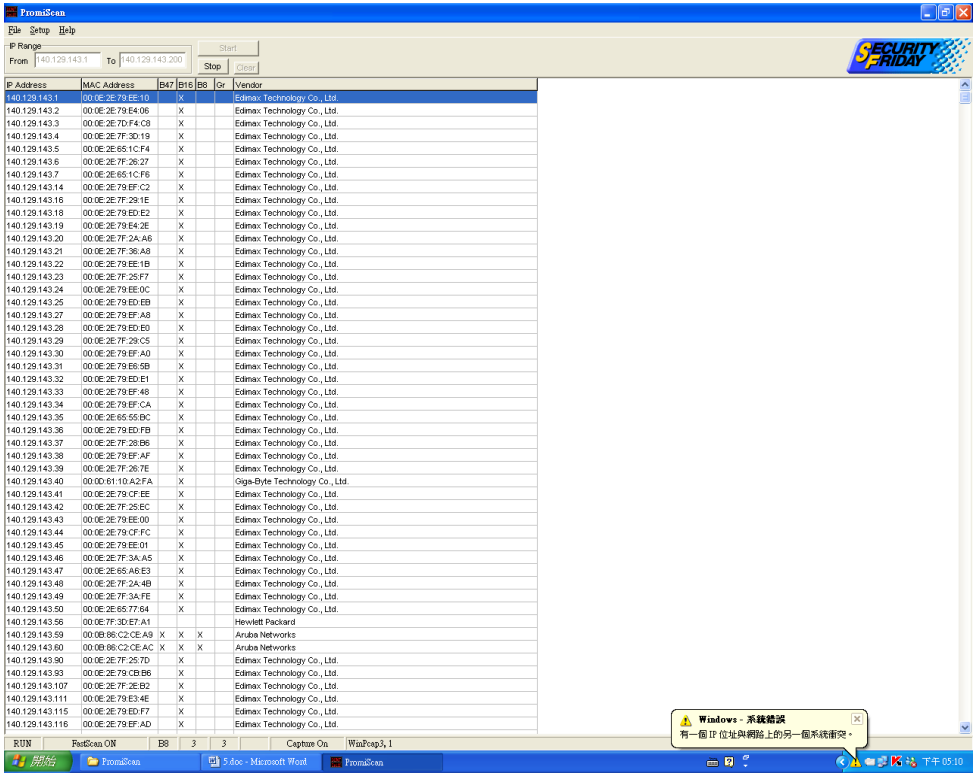
```
./snort -dev -l ./log
```

# 工具程式

- **Promiscan**

- PromiScan是網路竊聽節點（sniffing node）的偵測工具，會送出ARP封包並分析其回應，以了解本地端網路是否有主機的網路卡處於混雜模式中，藉以判定在本地端網路中是否有網路竊聽節點及行為的存在。

# Promiscan


PromiScan
File Setup Help
IP Range
From 140.129.143.1
To 140.129.143.200
Start
Stop
Clear
SECURITY FRIDAY
IP Address | MAC Address | B47 | B16 | B8 | Gr | Vendor
140.129.143.1 | 00:0E:2E:79:EE:10 | | X | | | Edimax Technology Co., Ltd.
140.129.143.2 | 00:0E:2E:79:E4:06 | | X | | | Edimax Technology Co., Ltd.
140.129.143.3 | 00:0E:2E:7D:F4:C8 | | X | | | Edimax Technology Co., Ltd.
140.129.143.4 | 00:0E:2E:7F:3D:19 | | X | | | Edimax Technology Co., Ltd.
140.129.143.5 | 00:0E:2E:65:1C:F4 | | X | | | Edimax Technology Co., Ltd.
140.129.143.6 | 00:0E:2E:7F:26:27 | | X | | | Edimax Technology Co., Ltd.
140.129.143.7 | 00:0E:2E:65:1C:F6 | | X | | | Edimax Technology Co., Ltd.
140.129.143.14 | 00:0E:2E:79:EF:C2 | | X | | | Edimax Technology Co., Ltd.
140.129.143.16 | 00:0E:2E:7F:29:1E | | X | | | Edimax Technology Co., Ltd.
140.129.143.18 | 00:0E:2E:79:ED:E2 | | X | | | Edimax Technology Co., Ltd.
140.129.143.19 | 00:0E:2E:79:E4:2E | | X | | | Edimax Technology Co., Ltd.
140.129.143.20 | 00:0E:2E:7F:2A:A6 | | X | | | Edimax Technology Co., Ltd.
140.129.143.21 | 00:0E:2E:7F:36:A8 | | X | | | Edimax Technology Co., Ltd.
140.129.143.22 | 00:0E:2E:79:EE:1B | | X | | | Edimax Technology Co., Ltd.
140.129.143.23 | 00:0E:2E:7F:25:F7 | | X | | | Edimax Technology Co., Ltd.
140.129.143.24 | 00:0E:2E:79:EE:0C | | X | | | Edimax Technology Co., Ltd.
140.129.143.25 | 00:0E:2E:79:ED:EB | | X | | | Edimax Technology Co., Ltd.
140.129.143.27 | 00:0E:2E:79:EF:A8 | | X | | | Edimax Technology Co., Ltd.
140.129.143.28 | 00:0E:2E:79:ED:E0 | | X | | | Edimax Technology Co., Ltd.
140.129.143.29 | 00:0E:2E:7F:29:C5 | | X | | | Edimax Technology Co., Ltd.
140.129.143.30 | 00:0E:2E:79:EF:A0 | | X | | | Edimax Technology Co., Ltd.
140.129.143.31 | 00:0E:2E:79:E6:5B | | X | | | Edimax Technology Co., Ltd.
140.129.143.32 | 00:0E:2E:79:ED:E1 | | X | | | Edimax Technology Co., Ltd.
140.129.143.33 | 00:0E:2E:79:EF:48 | | X | | | Edimax Technology Co., Ltd.
140.129.143.34 | 00:0E:2E:79:EF:CA | | X | | | Edimax Technology Co., Ltd.
140.129.143.35 | 00:0E:2E:65:55:BC | | X | | | Edimax Technology Co., Ltd.
140.129.143.36 | 00:0E:2E:79:ED:FB | | X | | | Edimax Technology Co., Ltd.
140.129.143.37 | 00:0E:2E:7F:28:B6 | | X | | | Edimax Technology Co., Ltd.
140.129.143.38 | 00:0E:2E:79:EF:AF | | X | | | Edimax Technology Co., Ltd.
140.129.143.39 | 00:0E:2E:7F:26:7E | | X | | | Edimax Technology Co., Ltd.
140.129.143.40 | 00:0D:61:10:A2:FA | | X | | | Giga-Byte Technology Co., Ltd.
140.129.143.41 | 00:0E:2E:79:CF:EE | | X | | | Edimax Technology Co., Ltd.
140.129.143.42 | 00:0E:2E:7F:25:EC | | X | | | Edimax Technology Co., Ltd.
140.129.143.43 | 00:0E:2E:79:EE:00 | | X | | | Edimax Technology Co., Ltd.
140.129.143.44 | 00:0E:2E:79:CF:FC | | X | | | Edimax Technology Co., Ltd.
140.129.143.45 | 00:0E:2E:79:EE:01 | | X | | | Edimax Technology Co., Ltd.
140.129.143.46 | 00:0E:2E:7F:3A:A5 | | X | | | Edimax Technology Co., Ltd.
140.129.143.47 | 00:0E:2E:65:A6:E3 | | X | | | Edimax Technology Co., Ltd.
140.129.143.48 | 00:0E:2E:7F:2A:4B | | X | | | Edimax Technology Co., Ltd.
140.129.143.49 | 00:0E:2E:7F:3A:FE | | X | | | Edimax Technology Co., Ltd.
140.129.143.50 | 00:0E:2E:65:77:64 | | X | | | Edimax Technology Co., Ltd.
140.129.143.56 | 00:0E:7F:3D:E7:A1 | | | | | Hewlett Packard
140.129.143.59 | 00:0B:86:C2:CE:A9 | X | X | X | | Aruba Networks
140.129.143.60 | 00:0B:86:C2:CE:AC | X | X | X | | Aruba Networks
140.129.143.90 | 00:0E:2E:7F:25:7D | | X | | | Edimax Technology Co., Ltd.
140.129.143.93 | 00:0E:2E:79:CB:B6 | | X | | | Edimax Technology Co., Ltd.
140.129.143.107 | 00:0E:2E:7F:2E:B2 | | X | | | Edimax Technology Co., Ltd.
140.129.143.111 | 00:0E:2E:79:E3:4E | | X | | | Edimax Technology Co., Ltd.
140.129.143.115 | 00:0E:2E:79:ED:F7 | | X | | | Edimax Technology Co., Ltd.
140.129.143.116 | 00:0E:2E:79:EF:AD | | X | | | Edimax Technology Co., Ltd.
RUN | FastScan ON | B8 | 3 | 3 | | Capture On | WinPcap3, 1
Windows - 系統錯誤
有一個 IP 位址與網路上的另一個系統衝突。
開始
PromiScan
5.doc - Microsoft Word
PromiScan
下午 05:10

# 練習

- **注意！盜取他人資料是違法的行為，測試過程中請勿監聽他人的機器！**
- 進行本實驗前需注意，同網段不能有其他主機使用類似軟體，以免互相干擾。

1. 在一台電腦上安裝WinPcap及SwitchSniffer，模仿攻擊者。
2. 再安裝HTTPSniff、MSNSniff、PasswordSniff。
3. 另一台電腦模仿受害者，操作攻擊者電腦的SwitchSniffer軟體，使受害者電腦的資料流量開始流經攻擊者的電腦。

# 練習

4. 在攻擊者電腦上開啟HTTPSniff，然後在受害者電腦上操作瀏覽器，隨意看一些網頁，看看攻擊者電腦的軟體畫面有什麼狀況。
5. 在攻擊者電腦上開啟MSNSniff，然後在受害者電腦上操作MSN，進行聊天的行為，看看攻擊者電腦的軟體畫面有什麼狀況。
6. 在攻擊者電腦上開啟PasswordSniff，然後在受害者電腦上登入一些Webmail的畫面、進行一些Telnet的動作（例如進入BBS）、利用OutLook Express收信件或登入FTP，看看攻擊者電腦的軟體畫面有什麼狀況。
7. 思考如何使自己的電腦不被竊聽？