

**TEAM ASSIGNMENT**

**Chuyên đề bảo mật – Team 15 K16T1**



**MỤC LỤC**

|  |  |  |  |
| --- | --- | --- | --- |
| Ngày | Phiên bản | Người viết | Mô tả |
| 01/10/2013 | 1.0 | Lê Ngọc Châu | Lập tài liệu |
| 01/10/2013 | 1.1 | BigFiveTeam | Cập nhật nội dung tài liệu |
|  |  |  |  |

[1. Thành viên: 1](#_Toc368558414)

[2. Cain and Abel: 1](#_Toc368558415)

[2.1. Cơ bản về Cain and Abel: 1](#_Toc368558416)

[2.1.1. Giới thiệu tổng quát: 1](#_Toc368558417)

[2.1.2. Chi tiết về Cain and Abel: 1](#_Toc368558418)

[2.2. Nguyên tắc hoạt động: 3](#_Toc368558419)

[2.2.1. Sơ Lược Quá trình hoạt động 3](#_Toc368558420)

[2.2.2. CAIN (Sử dụng phần mềm CAIN) 5](#_Toc368558421)

[*2.2.2.1.* *Yêu cầu về phần cứng:* 5](#_Toc368558422)

[*2.2.2.2.* *Cài đặt:* 5](#_Toc368558423)

[*2.2.2.3.* *Cấu hình:* 5](#_Toc368558424)

[2.2.2.4. *Các ứng dụng của CAIN:* 8](#_Toc368558425)

[2.3. Demo: 14](#_Toc368558426)

**LỊCH SỬ TÀI LIỆU**

# Thành viên:

|  |  |
| --- | --- |
| T094054 | Trịnh Thái Anh |
| T103573 | Lê Ngọc Châu |
| T105026 | Khấu Thành Đạo |
| T104898 | Huỳnh Trọng Khang |
| T101184 | Tạ Ngọc Thiên Phú |
| T103569 | Nguyễn Hoàng Fa Thứ |

# Cain and Abel:

## Cơ bản về Cain and Abel:

### Giới thiệu tổng quát:

Cain & Abel là chương trình tìm mật khẩu chạy trên hệ điều hành Microsoft. Nó cho phép dễ dàng tìm ra nhiều loại mật khẩu bằng cách dò tìm trên mạng, phá các mật khẩu đã mã hóa bằng các phương pháp Dictionary, Brute-Force and Cryptanalysis, ghi âm các cuộc đàm thoại qua đường VoIP, giải mã các mật khẩu đã được bảo vệ, tìm ra file nơi chứa mật khẩu, phát hiện mật khẩu có trong bộ đệm, và phân tích các giao thức định tuyến.

Nó bao gồm một số khía cạnh bảo mật / điểm yếu hiện diện trong các tiêu chuẩn của giao thức, phương pháp thẩm định và cơ chế bộ nhớ đệm, mục đích chính của nó là sự phục hồi mật khẩu đơn giản và các thông tin từ nhiều nguồn khác nhau, tuy nhiên nó cũng có một số "không tiêu chuẩn" tiện ích cho người sử dụng Microsoft Windows.

Cain & Abel đã được phát triển với hy vọng rằng nó sẽ hữu ích cho các quản trị mạng, giáo viên, chuyên gia tư vấn bảo mật / các chuyên gia, nhân viên pháp y, các nhà cung cấp phần mềm bảo mật, kiểm tra thâm nhập chuyên nghiệp và mọi người khác có được kế hoạch để sử dụng nó vì lý do đạo đức.

Chương trình này không khai thác những lỗ hổng chưa được vá của bất kỳ phần mềm nào. Nó tập trung vào những khía cạnh/điểm yếu hiện có trong các chuẩn giao thức, các phương pháp đăng nhập và các kỹ thuật đệm; mục đích chính của công cụ này là tìm ra mật khẩu và những thông tin càn thiết từ nhiều nguồn.

Cain & Abel được phát triển với hy vọng rằng nó là công cụ đắc lực cho các quản trị mạng, các nhân viên điều tra có thể truy cập dễ dàng vào các hệ thống máy tính bị mã khóa do hacker tấn công. Được biết, tác giá của công cụ phá mã này là  Massimiliano Montoro, một lập trình viên máy tính nổi tiếng thế giới.Tác giả không giúp đỡ hay hỗ trợ bất kỳ một hành vi bất hợp pháp nào sử dụng chương trình này. Hãy nhớ rằng có thể chương trình này sẽ làm hỏng và/hoặc mất dữ liệu và trong mọi trường hợp, tác giả không chịu bất cứ trách nhiệm pháp lý nào nếu điều này xảy ra. Hãy đọc thật kỹ License Agreement kèm theo trước khi sử dụng chương trình này.

### Chi tiết về Cain and Abel:

1. Cain:

Cain: là phần đầu tiên của phần mềm, với một giao diện người dùng đơn giản, mục đích chính của nó là tập trung vào một số kỹ thuật xâm nhập và những công cụ giúp phục hồi mật khẩu và các authentication credentials từ nhiều nguồn khác nhau.

* Cisco Config Downloader/Uploader (SNMP/TFTP): Tính năng này cho phép tải về hoặc tải lên tập tin cấu hình của các thiết bị Cisco thông qua SNMP / TFTP.
* MAC Address Scanner with OUI fingerprint: Sử dụng thư viện OUI, cho biết thông tin về một loại thiết bị dựa trên địa chỉ MAC của nó
* Network  Enumerator: Truy xuất tên người dùng, nhóm người dùng, các thư mục chia sẻ và các dịch vụ hiện đang chạy trên một máy trong network
* Remote Registry: Cho phép sửa đổi các thông số registry từ network
* Promiscuous-mode Scanner based on ARP packets: Xác định các sniffers và các hệ thống Intrusion Detection hiện có trên mạng LAN.
* Route Table Manager: Chức năng tương tự như một công cụ có sẵn trong Windows tên là "route.exe" có thêm giao diện người dùng
* Service Manager: Cho phép bắt đầu, dừng, kết thúc, tiếp tục hoặc gỡ bỏ một dịch vụ.
* SID Scanner: Trích xuất tên người dùng associated to Security Identifiers (SIDs) trên một hệ thống từ xa.
* **Password Crackers**
* Password Crackers: Cho phép phục hồi mật khẩu đã bị xáo trộn bởi một số hàm băm hoặc các thuật toán mã hóa thông thường. Chương trình hỗ trợ thuật toán Dictionary và Brute-Force
* Cryptanalysis attacks: Cho phép bẻ mật khẩu sử dụng phương pháp ‘Faster Cryptanalytictime – memory trade off’ của Philippe Oechslin. Kỹ thuật bẻ khóa này sử dụng một tập hợp các bảng lớn chứa các mật khẩu được mã hóa đã tính trước, bảng đó được gọi là Rainbow Tables, để cải thiện phương pháp trade-off được biết đến ngày nay nhằm tăng tốc độ phục hồi mật khẩu
* Rainbowcrack-online client: Cho phép bẻ khóa mật khẩu bằng sức mạnh vượt trội của dịch vụ bé khóa trực tuyến dựa trên công nghệ RainbowTable
* WEP Cracker: Áp dụng phương pháp tấn công WEP của Performs Korek's và PTW trên chuẩn 802.11 để lấy các tập tin chứa các vectơ khởi tạo WEP.
* **Password Decoders**
* Access (9x/2000/XP) Database Passwords Decoder: Giải mã các mật khẩu đã được mã hóa từ các tập tin Microsoft Access Database.
* Base64 Password Decoder: Giải mã các chuỗi được mã hóa Base64
* Box Revealer: Hiện các mật khẩu được hiển thị bằng dấu hoa thị trong hộp thoại password
* Cisco Type-7 Password Decoder: Giải mã mật khẩu Cisco Type-7 được sử dụng trong router and switches configuration files.
* Cisco VPN Client Password Decoder: Giải mã các mật khẩu Cisco VPN Client được lưu trữ trong những tập tin hồ sơ kết nối (connection profiles) (\*.pcf).
* Credential Manager Password Decoder: Giải mã các mật khẩu được lưu trữ trong Enterprise và Local Credential Sets trên Windows XP/2003.
* Dialup Password Decoder: Giải mã các mật khẩu được lưu trữ bởi các thành phần trong Windows "Dial-Up Networking"
* Enterprise Manager Password Decoder: Giải mã các mật khẩu được sử dụng bởi Microsoft SQL Server Enterprise Manager (SQL 7.0 và 2000 cũng được hỗ trợ).
* Protected Storage Password Manager: Giải mã các mật khẩu cục bộ được lưu trữ trong Outlook, Outlook Express, Outlook Express Identities, Outlook 2002, Internet Explorer and MSN Explorer.
* PWL Cached Password Decoder: Cho phép xem tất cả các tài nguyên được lưu trữ và những mật khẩu liên quan dưới dạng văn bản từ danh sách các tập tin (dù bị khóa hay chưa khóa).
* Remote Desktop Password Decoder: Giải mã các mật khẩu trong Remote Desktop Profiles (các tập tin .RPD ).
* Syskey Decoder: Khôi phục lại khóa khởi động được sử dụng bởi tiện ích SYSKEY từ local registry hoặc từ các tập tin hệ thống “offline”.
* VNC Password Decoder: Giải mã các mật khẩu VNC trong registry đã được mã hóa.
* Wireless Zero Configuration Password Dumper: Khôi phục các mật khẩu wireless được lưu trữ trong Windows Wireless Configuration Service.
* 802.11 Capture Files Decoder: Giải mã file chụp 802.11 (wireshark, pcap) bao gồm wireless frames được mã hóa với WEP hoặc WPA-PSK.
* **Password Dumpers**
* LSA Secrets Dumper: Dump các nội dụng của Local Security Authority Secrets
* MSCACHE Hashes Dumper: Lấy lại các mật khẩu băm MSCACHE được lưu trữ trong local registry.
* MySQL Password Extractor via ODBC: Kết nối tới một MySQL server thông qua ODBC và lấy ra thông tin người dùng cũng như mật khẩu từ database
* NT Hash Dumper + Password History Hases (works with Syskey enabled): Lấy lại mật khẩu NT bị phân rã từ file SAM bất kể Syskey có tồn tại hay không
* Oracle Password Extractor via ODBC: Kết nối tới một Oracle server thông qua ODBC và lấy ra thông tin người dùng cũng như mật khẩu từ database
* Microsoft SQL Server 2000 Password Extractor via ODBC: Kết nối tới một SQL server thông qua ODBC và lấy ra thông tin người dùng cũng như mật khẩu từ database chính.
* **Password/Hash Calculators**
* Hash Calculator: Xuất ra các giá trị băm (hash) từ một đoạn text có sẵn
* RSA SecurID Token Calculator: Có thể tính khóa RSA từ tập tin kích hoạt XML có sẵn
* **Sniffer**
* APR (ARP Poison Routing): Cho phép nghe lên trên các mạng chuyển mạch và tấn công theo phương pháp Man-in-the-Middle
* Full HTTPS sessions sniffer for APR (APR-HTTPS): Cho phép bắt (capture) tất cả dữ liệu được gửi trên các phiên truyền của giao thức HTTPS
* Full FTPS sessions sniffer for APR (APR-FTPS): Cho phép bắt (capture) tất cả các dữ liệu được gửi qua các phiên truyền của giao thức ẩn FTPS trên mạng.
* Full IMAPS sessions sniffer for APR (APR-IMAPS): Cho phép bắt (capture) tất cả các dữ liệu được gửi thông qua các phiên truyền của giao thức IMAPS trên mạng.
* Full LDAPS sessions sniffer for APR (APR-LDAPS): Cho phép bắt (capture) tất cả các dữ liệu được gửi thông qua các phiên truyền của giao thức ẩn LDAPS trên mạng.
* Full POP3S sessions sniffer for APR (APR-POP3S): Cho phép bắt (capture) tất cả các dữ liệu được gửi thông qua các phiên truyền của giao thức ẩn POP3S trên mạng.
* Full RDP sessions sniffer for APR (APR-RDP): Cho phép sao chép lại tất cả các dữ liệu được gửi thông qua phiên truyền của giao thức Remove Deskstop Protocal (RDP) trên mạng. Ghi lại toàn bộ các dữ liệu mà người dùng nhập từ bàn phím.
* Full SSH-1 sessions sniffer for APR (APR-SSH-1): Cho phép bắt (capture) tất cả các dữ liệu được gửi thông qua các phiên truyền của giao thức SSH-1 trên mạng.
* Certificates Collector: Lấy các tín chỉ từ các website HTTPS, IMAPS, POP3S, LDAPS, FTPS và sử dụng chúng cho các bộ lọc sniffer APR-\* tương ứng
* TCP/UDP Table Viewer: Cho biết tình trạng của các port cục bộ (như netstat)
* TCP/UDP/ICMP Traceroute with DNS resolver and WHOIS client: Một traceroute cải tiến có thể sự dụng các giao thức TCP, UDP and ICMP và cung cấp các khả năng của máy khách WHOIS.
* Wireless Scanner: Có thể quét tín hiệu wireless, từ đó truy ra địa chỉ MAC, thời gian kết nối gần đây nhất, cường độ của tín hiệu, tên của mạng (SSID), được mã hóa kiểu gì (EWP hay WPA), là một mạng Ad-hoc hay một mạng cơ sở (Infrastructure), những kênh mạng đang hoạt động và tốc độ của nó (vd như 11 Mbps). Chương trình hỗ trợ chế độ quét tự động và nghe lén WEP IVs sử dụng bộ chuyển đổi AirpCap của hang CACE Technologies

1. Abel:

Abel: là phần thứ hai của phần mềm, được thiết kế như một dịch vụ dành cho Windows NT gồm 2 file Abel.exe và Abel.dll, vì vậy không cần cài đặt ta vẫn có thể sử dụng được. Abel giao tiếp với Cain thông qua đường dẫn có dạng "\\computername\pipe\abel" và có thể kết nối từ nhiều host cùng một lúc. Tất cả dữ liệu truyền qua đường dẫn này đều được mã hóa bằng thuật toán mã hóa đối xứng RC4 với khóa là “Cain&Abel”

* Remote Console: Cung cấp một shell cho hệ thống điều khiển từ xa trên một máy tính từ xa
* Remote LSA Secrets Dumper: Dump các nội dụng của Local Security Authority Secrets trên một hệ thống từ xa
* Remote NT Hash Dumper + Password History Hases (works with Syskey enabled): Lấy lại các mật khẩu băm NT từ tập tin SAM bất kể Syskey đã kích hoạt hay chưa; tính năng hoạt động từ phía Abel.
* Remote Route Table Manager: Cho phép quản lý bảng định tuyến của hệ thống từ xa
* Remote TCP/UDP Table Viewer: Cho biết tình trạng của các port cục bộ (như netstat) của hệ thống từ xa

## Nguyên tắc hoạt động:

### Sơ Lược Quá trình hoạt động

* Trên cùng một mạng, Host A và Host B muốn truyền tin cho nhau, các Packet sẽ được đưa xuống tầng Datalink để đóng gói, các Host phải đóng gói MAC nguồn, MAC đích vào Frame. Như vậy trước khi quá trình truyền Dữ liệu, các Host phải hỏi địa chỉ MAC của nhau.
* Nếu như Host A khởi động quá trình hỏi MAC trước, nó sẽ gởi broadcast gói tin ARP request cho tất cả các Host để hỏi MAC Host B, lúc đó Host B đã có MAC của Host A, sau đó Host B chỉ trả lời cho Host A MAC của Host B(ARP reply ).
* Có 1 Host C liên tục gởi ARP reply cho Host A và Host B địa chỉ MAC của Host C, nhưng lại đăt địa chỉ IP là Host A và Host B. Lúc này Host A cứ nghĩ máy B có MAC là C. Như vậy các gói tin mà Host A gởi cho Host B đều bị đưa đến Host C, gói tin Host B trả lời cho Host A cũng đưa đến Host C. Nếu Host C bật chức năng forwarding thì coi như Host A và Host B không hề hay biết rằng mình bị tấn công ARP.

[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

Ví dụ :   
Ta có mô hình gồm các host 

Attacker : là máy hacker dùng để tấn công ARP   
IP : 10.0.0.11   
MAC : 0000.0000.1011   
  
Victim : là máy bị tấn công   
IP : 10.0.0.12   
MAC : 0000.0000.1012   
  
HostA   
IP : 10.0.0.13   
MAC : 0000.0000.1013 

* Đầu tiên, HostA muốn gởi dữ liệu cho Victim, cần phải biết địa chỉ MAC của Victim để liên lạc. HostA sẽ gởi broadcast ARP Request tới tất cả các máy trong cùng mạng LAN để hỏi xem IP 10.0.0.12 (IP của Victim) có địa chỉ MAC là bao nhiêu.
* Attacker và Victim đều nhận được gói tin ARP Request, nhưng chỉ có Victim gởi trả lời gói tin ARP Reply lại cho HostA. ARP Reply chứa thông tin về IP 10.0.0.12 và MAC 0000.0000.1012 của Victim.
* HostA nhận được gói ARP Realy từ Victim, biết được địa chỉ MAC của Victim là 0000.0000.1012 sẽ bắt đầu thực hiện liên lạc truyền dữ liệu đến Victim. Attacker không thể xem nội dung dữ liệu được truyền giữa HostA và Victim.
* Máy Attacker muốn thực hiện ARP attack đối với máy Victim. Attacker muốn mọi gói tin HostA gởi đến máy Victim đều có thể chụp lại được để xem trộm.
* Attacker thực hiện gởi liên tục ARP Reply chứa thông tin về IP của Victim 10.0.0.12, còn địa chỉ MAC là của Attacker 0000.0000.1011.
* HostA nhận được ARP Reply nghĩ rằng IP Victim 10.0.0.12 có địa chỉ MAC là 0000.0000.1011. HostA lưu thông tin này vào bảng ARP Cache và thực hiện kết nối.
* Lúc này mọi thông tin, dữ liệu HostA gởi tới máy có IP 10.0.0.12 (là máy Victim) sẽ gởi qua địa chỉ MAC 0000.0000.1011 của máy Attacker.

### CAIN (Sử dụng phần mềm CAIN)

Phần mềm Cain là phần mềm sniffer khá hiệu quả hiện nay. Các tính năng của cain có thể cho phép sniffer được các thông tin bí mật trong hệ thống mạng LAN như passowrd e-mail, password dịch vụ ftp,telnet,….

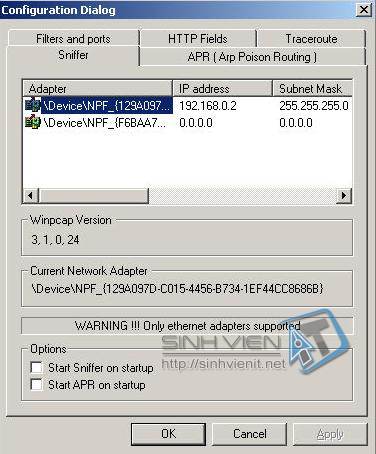
### Yêu cầu về phần cứng:

* Ổ cứng cần trống 10 Mb
* Hệ điều hành Win 2000/2003/XP
* Cần phải có Winpcap

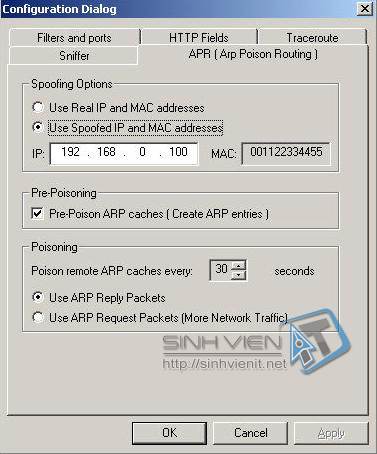
### Cài đặt:

### Cấu hình:

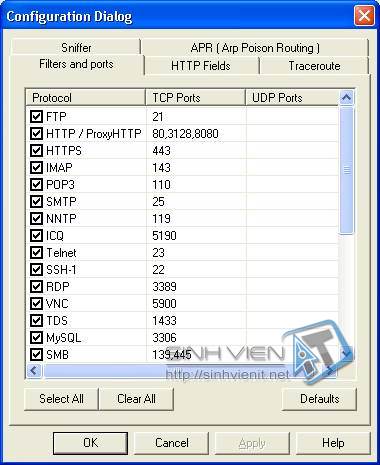
* Cain & Abel cần cấu hình một vài thông số , mọi thứ có thể được điều chỉnh thông qua bảng Configuration dialog.
* Sniffer tab:

[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

* Tại đây chúng ta chọn card mạng sử dụng để tiến hành sniffer và tính năng APR . Check vào ô Option để kích hoạt hay không kích hoạt tính năng.
* Sniffer tương thích với Winpcap version 2.3 hay cao hơn . Version này hỗ trợ   
  card mạng rất nhiều.  
  **APR tab:**

[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

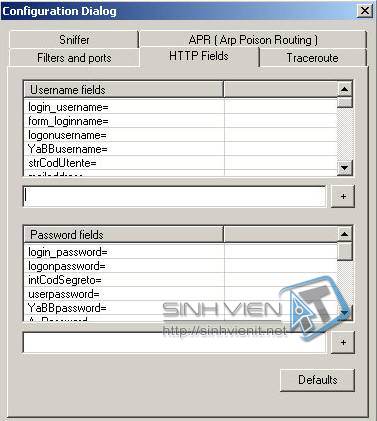
* Đây là nơi bạn có thể config ARP . Mặc định Cain ngăn cách 1 chuỗi gửi gói ARP từ nạn nhân trong vòng 30 giây . Đây thực sự là điều cần thiết bởi vì việc xâm nhập vào thiết bị có thể sẽ gây ra sự không lưu thông tính hiệu . Từ dialog này bạn có thể xác định thời gian giữa mỗi lần thực thi ARP, xác định thông số ít sẽ tạo cho ARP lưu thông nhiều ,ngược lại sẽ khó khăn hơn trong việc xâm nhập.
* *Tại mục này, ta cần chú ý tới phần Spoofing Options:*
  + Mục đầu tiên cho phép ta sử dụng địa chỉ MAC và IP thực của máy mà mình dang sử dụng.
  + Mục thứ hai cho phép sử dụng một IP và địa chỉ MAC giả mạo. (Lưu ý địa chỉ ta chọn phải không trùng với IP của máy khác) Khi click vào tab filters and ports, ta sẽ thấy một số thông tin về giao thức và các con số port tương ứng với giao thức đó.

[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

**Fliter and Ports Tab:**

* Tại đây bạn có thể chọn kích hoạt hay không kích hoạt các port ứng dụng   
  TCP/UDP.

**HTTP fields tab:**

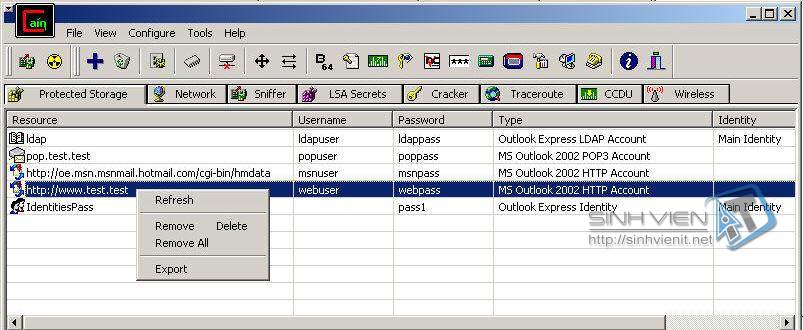
[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

* Tại đây có 1 list danh sách username và password sử dụng được HTTP sniffer lọc lại.
* Tại tab này cho phép ta biết dược chương trình này sẽ bắt 1 số thông tin về trang web như:
* Mục Username Fields: nó sẽ lấy thông tin những gì liên quan đến cái tên (user name, account, web name v.v..).
* Mục Password Fields: lanh vực này sẽ đãm nhiệm vai trò lấy thông tin về password (login password, user pass, webpass v.v…)

### Các ứng dụng của CAIN:

Bảo vệ password manager:

* Trước hết nó được sử dụng như 1 private key bảo mật một số vấn đề cho user . Hầu hết thông tin trong Protected Storage được mã hóa.Sử dụng như 1 key nhận được từ việc logon password của user.Cho phép điều hòa viêc truy cập thông tin để owner có thể an toàn truy xuất.
* Một vài ứng dụng của Windows có nét đặc trưng nên sử dụng dịch vụ này: Internet Explorer, Oulook , Oulook Express

[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

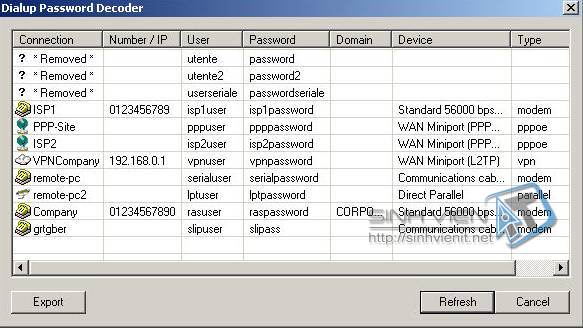
Giải mã password manager:

* Nó cho phép bạn đưa user names và passwords cho 1 tài nguyên mạng khác và 1 ứng dụng ,sau đó hệ thống tự động cung cấp thông tin về những sự viếng thăm thông tin mà bạn không can thiệp.

LSA secrets dumper:

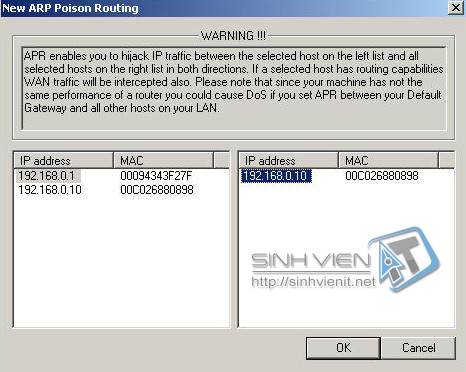
* LSA secrets thì sử dụng thông tin password cho accounts dùng để start một dịch vụ khác dữ liệu cục bộ. Dial Up và một số ứng dụng khác xác định password nằm ở đây.

Giải mã password Dial-Up: 

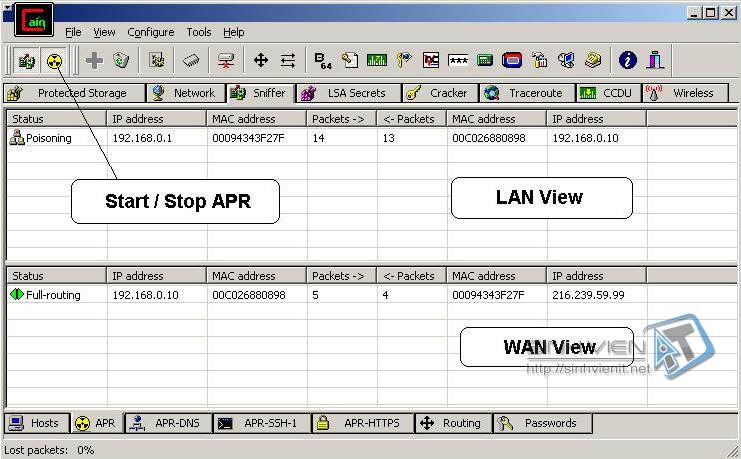
[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

APR:

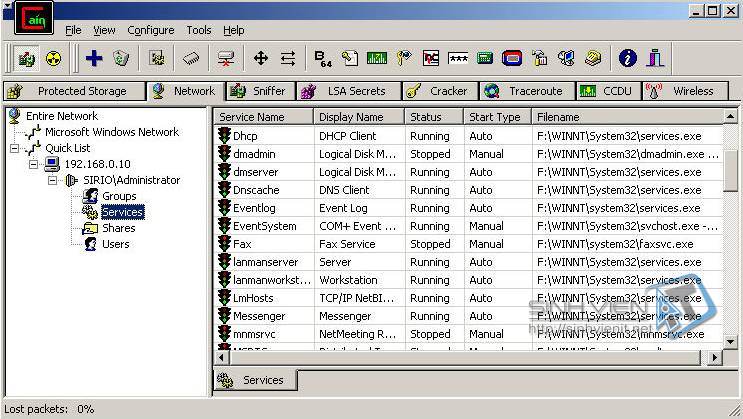
* APR là nét đặc trưng chính của chương trình .Nó cho phép lắng nghe về các mạng chuyển mạch và sự tấn công lưu thông IP giữa các host . “APR poinsion routing” thực hiện : tấn công và định tuyến chính xác địa chỉ đích.
* APR tấn công cơ bản thông qua thao tác của host ARP.Trên 1 địa chỉ IP hay Ethernet khi mà 2 host muốn truyền tin lẫn nhau thì phải biết địa chỉ MAC addresses của nhau. Host gốc thấy bảng ARP nếu mà ở đây có 1 MAC addresses tương ứng với địa chỉ IP addresses của nó. Nếu không, nó là địa chỉ broadcasts ,một lời yêu cầu ARP hỏi địa chỉ MAC của địa chỉ đích. Bởi vì gói thông tin này được gửi trong miền broadcasts, nó sẽ đi đến những cái host cùng subnet , tuy nhiên host với IP address trên lý thuyết khi nhận được yêu cầu sẽ trả lời lại địa chỉ MAC gốc của nó. Trái lại nếu ARP-IP tiếp cận địa chỉ đích của host thì nó sẵn sàng đưa ra soure host trên ARP cache. Điều này sẽ được dùng để phát sinh lưu thông ARP.
* *Config:*  
  Cần chỉnh 1 vài thông số, điều này có thể thực hiện được bằng việc chỉ rõ việc bắt chước MAC và IP addresses bằng việc sử dụng ARP poision packets .   
  Điều này thật sự khó khăn khi không để lại vết tích của việc tấn công bởi vì người tấn công thực tế không bao giờ gửi địa chỉ qua lại trên mạng.Trên mạng người tấn công lúc nào cũng lén lúc ở giữa để quan sát

[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

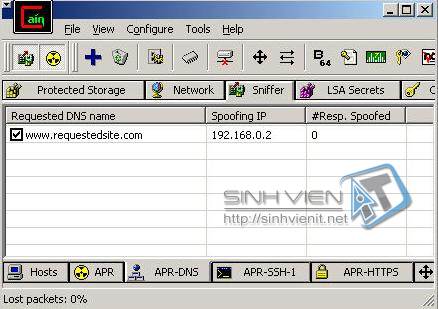
Hình ở trên là ta muốn tấn công ip từ 192.168.0.1 ? 192.168.0.10 .Công việc tiến hành theo cơ chế Người ở giữa , chương trình sẽ thực hiện 1 sự tấn công ARP poision , CAIN có thể phát triển sự tấn công bộ nhớ Của nhiều host trong khoảng thời gian như nhau, bạn cần chọn 1 địa chỉ ở ô bên trái 

[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

Service manager: ta có thể start/stop ,pause/continued hay remove bất cứ 1 dịch vụ nào có trên cửa sổ giao diện

[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

Sniffer:

[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

ARP-DNS:

* Nét đặc trưng ở đây là cho phép DNS tiến hành giả mạo thành 1 DNS-reply để có thể tấn công .

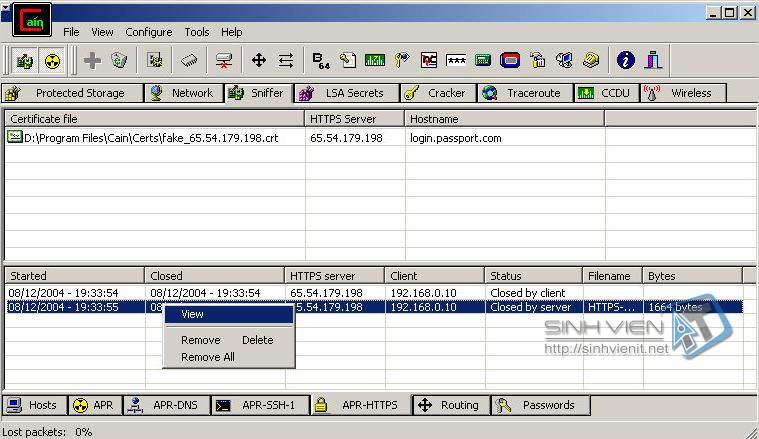
[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

* ARP-DNS dễ dàng tạo ra 1 ip address trên DNS-reply .Sniffer dễ dàng rút ra được tên yêu cầu từ gói dữ liệu kết hợp với việc thấy được địa chỉ trên bảng danh sách.Ở đây gói dữ liệu sẽ được chỉnh lại IP address để sau đó re-route đi .Lúc này client sẽ bị đánh lừa để ta dễ dàng biết được địa chỉ đích.

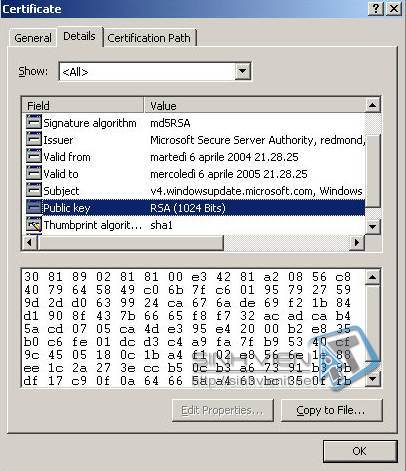
ARP-HTTPS:

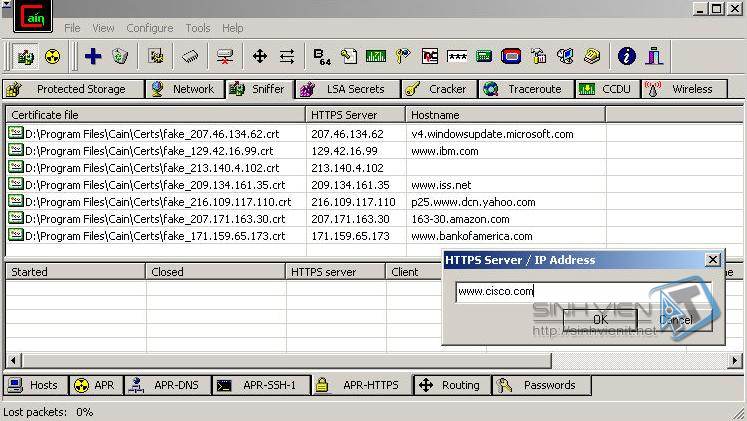
* ARP-HTTPS cho phép việc bắt gói và giải mã trong sự lưu thông của HTTPS giữa các host. Đây là công việc kết hợp với công cụ Certificate Collector . Khi mà nạn nhân Start HTTPS trình duyệt của anh ta sẽ hiện lên po-pup báo động .

[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

Certificates Collector : 

[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

[[](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html)](http://sinhvienit.net/forum/lab-bao-mat-2-sniffer-nghe-len.138186.html" \o " Lab bảo mật 2 - Sniffer (Nghe lén)" \t "_blank)

## Demo:

# Cách phòng chống:

## Làm thế nào để ngăn chặn những kẻ muốn sniffer dữ liệu của tôi?

Có lẽ cách đơn giản nhất để ngăn chặn những kẻ muốn sniffer dữ liệu của bạn là sử dụng các giao thức mã hóa chuẩn cho dữ liệu trên đường truyền. Khi bạn mã hóa dữ liệu, những kẻ tấn công ác ý có thể sniffer được dữ liệu của bạn, nhưng chúng lại không thể đọc được nó…

* SSL (Secure Socket Layer): Một giao thức mã hóa được phát triển cho hầu hết các Webserver, cũng như các Web Browser thông dụng. SSL được sử dụng để mã hóa những thông tin nhạy cảm để gửi qua đường truyền như: số thẻ tín dụng của khách hàng, các password và thông tin quan trọng.
* PGP và S/MIME: Email cũng có khả năng bị những kẻ tấn công ác ý sniffer. Khi sniffer một email không được mã hóa, chúng không chỉ biết được nội dung của email mà chúng còn có thể biết được các thông tin như địa chỉ của người gửi, địa chỉ của người nhận… Chính vì vậy để đảm bảo an toàn và tính riêng tư cho email bận cũng cần phải mã hóa chúng… S/MIME được tích hợp trong hầu hết các chương trình gửi nhận mail hiện nay như Netscape Messenger, Outlock Express…

PGP cũng là 1 giao thức được sử dụng để mã hóa email. Nó có khả năng hỗ trợ mã hóa bằng DSA, RSA lên đến 2048 bit dữ liệu.

* OpenSSH: Khi bạn sử dụng Telnet, FTP… 2 giao thức chuẩn này không cung cấp khả năng mã hóa dữ liệu trên đường truyền. Đặc biệt nguy hiểm là không mã hóa Pasword, chúng chỉ gửi password qua đường truyền dưới dạng Clear Text. Điều gì sẽ xảy ra nếu những dữ liệu nhạy cảm này bị sniffer. OpenSSH là 1 bộ giao thức được ra đời để khắc phục nhược điểm này: SSh (sử dụng thay thế Telnet), SFTP (sử dụng thay thế FTP)…
* VPNs (Virtual Private Networks): Được sử dụng để mã hóa dữ liệu khi truyền thông tin trên Internet. Tuy nhiên nếu 1 Hacker có thể tấn công và thỏa hiệp được những node của kết nối VPN đó thì chúng vẫn có thể tiến hành sniffer được.

Một ví dụ đơn giản, là một người udngf Internet khi lướt web đã sơ ý để nhiễm RAT (Remote Access Trojan), thường thì trong loại Trojan này thường có chứa sẵn Plugin sniffer. Cho đến khi người dùng bất cẩn này thiết lập một kết nối VPN. Lúc này Plugin sniffer trong Trojan sẽ hoạt động và nó có khả năng đọc được những dữ liệu chưa được mã hóa trước khi đưa vào VPN. Để phòng chống các cuộc tấn công kiểu này, bạn cần nâng cao ý thức cảnh giác cho những người sử dụng trong hệ thống mạng VPN của bạn, đồng thời sử dụng các chương trình quét virus để phát hiện và ngăn chặn không để hệ thống bị nhiễm Trojan.

## Làm thế nào để ngăn chặn những kẻ muốn sniffer password của tôi?

Để ngăn chặn những kẻ tấn công muốn sniffer password, bạn đồng thời sử dụng các giao thức, phương pháp để mã hóa password cũng như sử dụng một giải pháp chứng thực an toàn (authentication).

* SMB/CIFS: Trong môi trường window/ SAMBA bạn cần kích hoạt tính năng LANmanager Authencation.
* Keberos: Một giải pháp chứng thức dữ liệu an toàn được sử dụng trên Unix cũng như Windows.
* Stanford SRP (Secure Remote Password): Khắc phục được nhược điểm không mã hóa password khi truyền thông của 2 giao thức FTP và Telnet trên Unix.

## Làm thế nào để có thể ngăn chặn hành động sniffer trên những thiết bị phần cứng của tôi?

Việc thay thế Hub của bạn bằng những switch, nó có thể cung cấp một sự phòng chống hiệu quả hơn. Switch sẽ tạo ra một “Broadcast Domain” nó có tác dụng gửi đến những kẻ tấn công những gói ARP không hợp lệ (Spoof ARP Packet).

Tuy nhiên các Hacker vẫn có những cách thức khéo léo để vượt qua dự phòng thủ này. Các yêu cầu truy vấn ARP chứa đựng những thông tin chính xác từ IP cho đến MAC của người gửi. Thông thường để giảm bớt lưu lượng ARP trên đường truyền, đa số các máy tính sẽ đọc và sử dụng các thông tin từ bộ đệm (Cache) mà chúng truy vấn được từ Broadcast.

Bởi vậy một Hacker có thể Redirect những máy tính gần mình để vượt qua sự phòng thủ này bằng cách gửi những gói ARP chứa đựng những thông tin về địa chỉ IP của Router đến chính địa chỉ MAC của anh ta. Tất cả những máy tính trong hệ thống mạng cục bộ này sẽ nhầm tưởng anh ta là Router và sẽ thiết lập phiên truyền thông đi qua máy tính của anh ta.

Một cuộc tấn công DOS tương tự trên một hệ thống mạng cục bộ, khi thành công sẽ đá văng mục tiêu mà họ muốn tấn công ra khỏi mạng, rồi bắt đầu sử dụng chính địa chỉ IP của máy tính vừa vị tấn công này. Những kẻ tấn công sẽ khéo léo thừa kế và sử dụng những kết nối này. Bản thân windows khi phát hiện được hành động này, nó không hành động gì cả mà lại tử tế đóng stack TCP/IP của chính mình và cho phép kết nối này tiếp tục.

Để phòng chống lại các cuộc tấn công dạng này, bạn chỉ cần sử dụng các công cụ IDS (Intrusion Detecte Service)

Các IDS như BlackICE IDS, Snort sẽ tự động phát hiện và cảnh báo về các cuộc tấn công dạng này.

Hầu hết các Adapter Ethernet đều hco phép cấu hình địa chỉ MAC bằng tay. Hacker có thể tạo ra các địa chỉ Spoof MAC bằng cách hướng vào các địa chri trên Adapter. Để khắc phục điều này, hầu hết các switch đều không cho phép tự ý cấu hình lại các địa chỉ MAC.

## Tôi có thể sử dụng những adapter không hỗ trợ sniffing không?

Câu trả lời là có. Một số Adapter cũ không hỗ trợ chế độ hỗn tạp (Promiscuos Mode).

Về căn bản những bộ Adapter Token Ring của IBM không hỗ trợ chế độ hỗn tạp. Cũng có 1 số Adapter cũ khác không hỗ trợ chế độ hỗn tạp. Nếu bạn thật sự không muốn sniffing ở chế độ hỗn tạp xảy ra, bạn có thể tham khảo thông tin của những nhà sản xuất sniffer để biết được những Cart Ethernet nào mà họ không hỗ trợ chế độ sniffing ở chế độ hỗn tạp.

## Làm thế nào để tôi có thể phát hiện được sniffer trên hệ thống mạng của mình?

Về mặt lý thuyết thì rất khó có thể phát hiện được sự hiện diện của các chương trình sniffer trên hệ thống. Bởi chúng chỉ chộp và cố gắng đọc các gói tin, chúng không gây ra sự xáo trộn hay mất mát Packet nghiêm trọng nào trên đường truyền cả. Tuy nhiên thực tế lại có nhiều cách để phát hiện ra sự hiện diện của các sniffer.

Khi đứng đơn lẻ trên 1 máy tính không có sự truyền thông tin thì sẽ không có dấu hiệu gì. Tuy nhiên nếu được cài đặt trên một máy tính không đơn lẻ và có sự truyền thông, bản thân sniffer sẽ phát sinh ra lưu lượng thông tin. Bạn có thể truy vấn ngược DNS để tìm thông tin liên quan đến những địa chỉ IP.