

Bài 5:**CÁC PHƯƠNG PHÁP SNIFFER****I/ Giới thiệu về Sniffer****A. TỔNG QUAN SNIFFER**

Sniffer được hiểu đơn giản như là một chương trình cố gắng nghe ngóng các lưu lượng thông tin trên một hệ thống mạng

Sniffer được sử dụng như một công cụ để các nhà quản trị mạng theo dõi và bảo trì hệ thống mạng. Về mặt tiêu cực, sniffer được sử dụng như một công cụ với mục đích nghe lén các thông tin trên mạng để lấy các thông tin quan trọng

Sniffer dựa vào phương thức tấn công ARP để bắt gói các thông tin được truyền qua mạng.

Tuy nhiên những giao dịch giữa các hệ thống mạng máy tính thường là những dữ liệu ở dạng nhị phân (binary). Bởi vậy để hiểu được những dữ liệu ở dạng nhị phân này, các chương trình Sniffer này phải có tính năng phân tích các nghi thức (Protocol Analysis), cũng như tính năng giải mã (Decode) các dữ liệu ở dạng nhị phân để hiểu được chúng

Một số các ứng dụng của Sniffer được sử dụng như: dsniff, snort, cain, ettercap, sniffer pro...

B. HOẠT ĐỘNG CỦA SNIFFER

Sniffer hoạt động chủ yếu dựa trên dạng tấn công ARP.

TẤN CÔNG ARP**1. Giới thiệu**

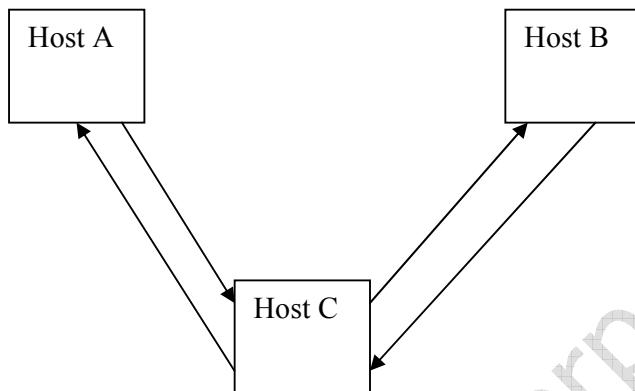
Đây là một dạng tấn công rất nguy hiểm, gọi là Man In The Middle. Trong trường hợp này giống như bị đặt máy nghe lén, phiên làm việc giữa máy gửi và máy nhận vẫn diễn ra bình thường nên người sử dụng không hề hay biết mình bị tấn công

2. 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 gửi 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 gửi ARP reply cho Host A và Host B địa chỉ MAC của Host C, nhưng lại đặt 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 gửi 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



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 gửi dữ liệu cho Victim, cần phải biết địa chỉ MAC của Victim để liên lạc. HostA sẽ gửi 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 gửi 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 Reply 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 gửi đến máy Victim đều có thể chụp lại được để xem trộm

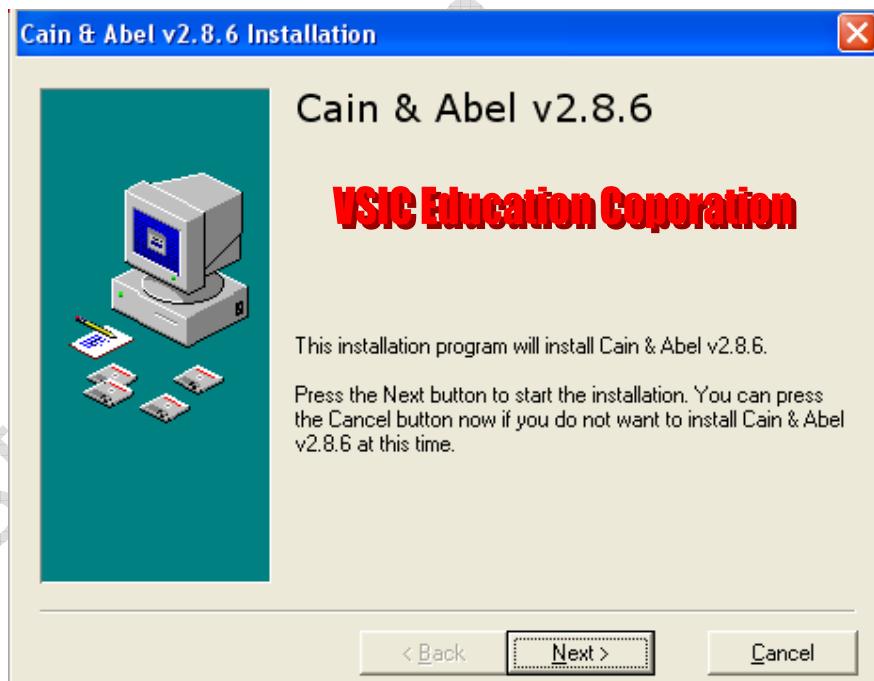
- Attacker thực hiện gửi liên tục ARP Reply chứa thông tin về IP của Victim 10.0.0.12, còn địa chỉ MAC là của Attacker 0000.0000.1011.
- HostA nhận được ARP Reply nghĩ rằng IP Victim 10.0.0.12 có địa chỉ MAC là 0000.0000.1011. HostA lưu thông tin này vào bảng ARP Cache và thực hiện kết nối.
- Lúc này mọi thông tin, dữ liệu HostA gửi tới máy có IP 10.0.0.12 (là máy Victim) sẽ gửi qua địa chỉ MAC 0000.0000.1011 của máy Attacker.

CAIN (Sử dụng phần mềm CAIN)

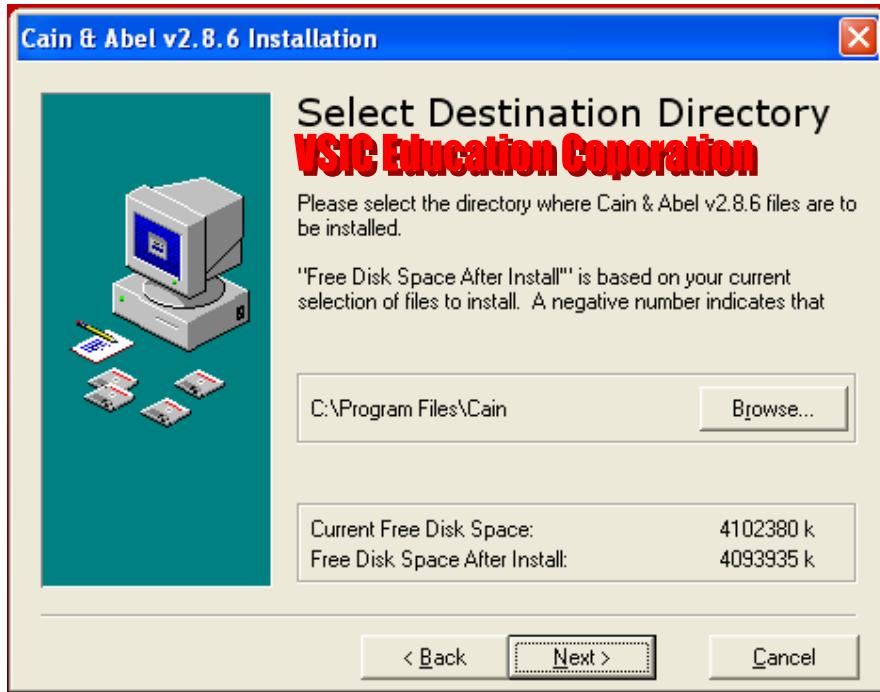
1. Yêu cầu về phần cứng:

- ổ cứng càn trống 10 Mb
- hệ điều hành Win 2000/2003/XP
- cần phải có Winpcap

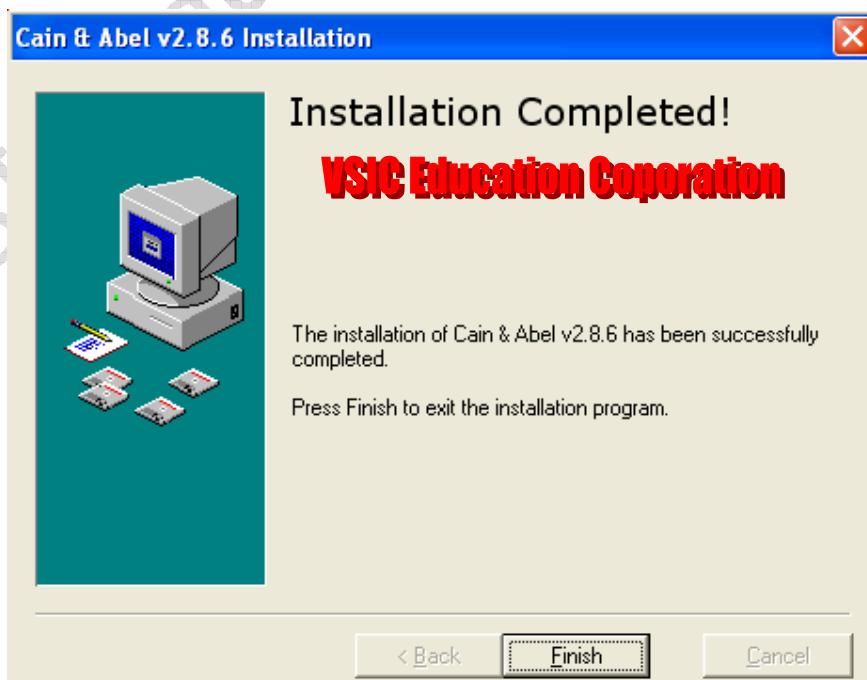
2. Cài đặt:



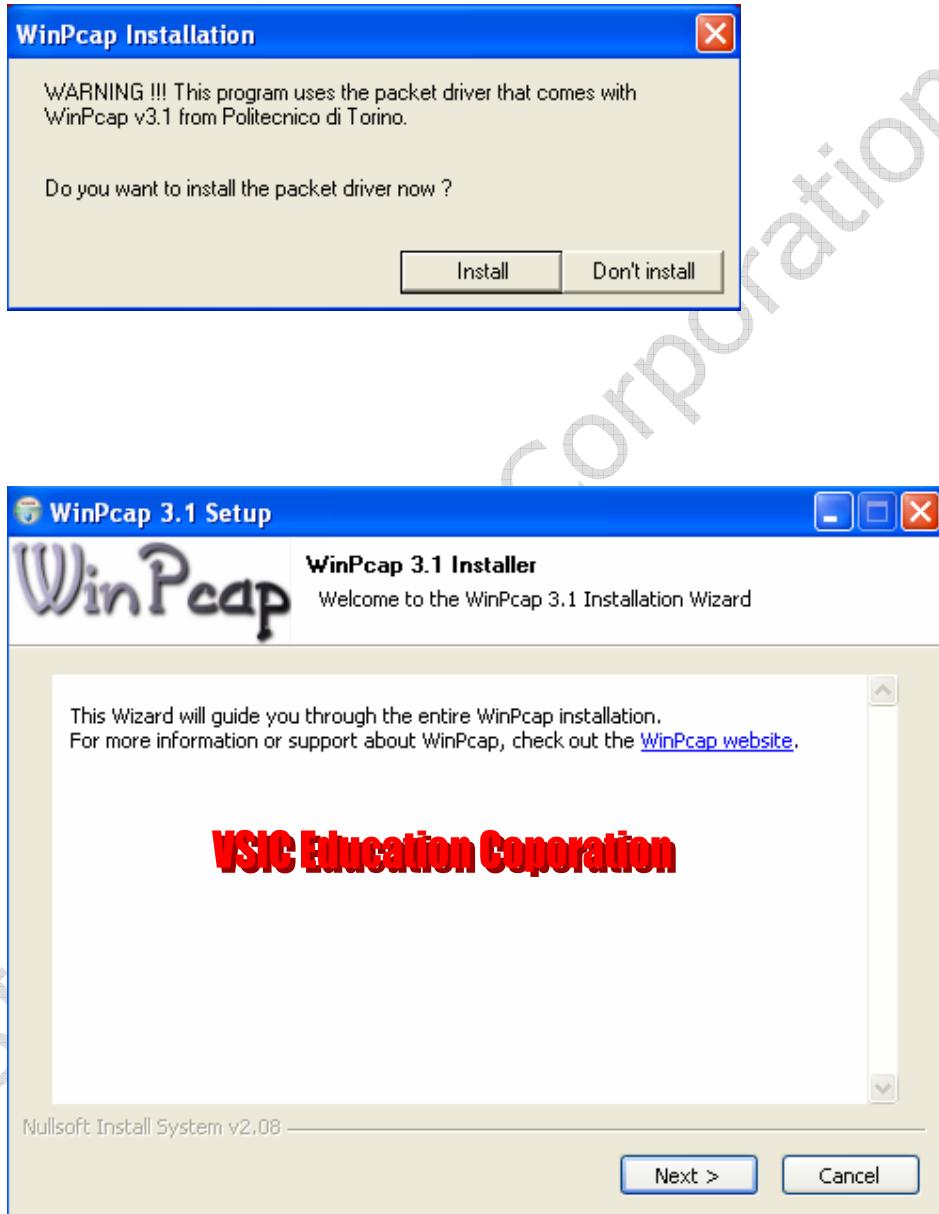
Chọn Next.

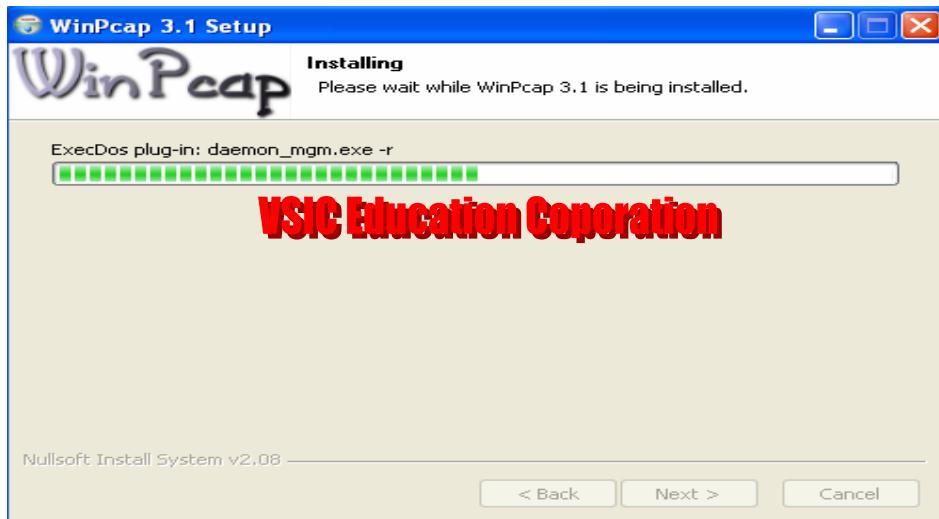


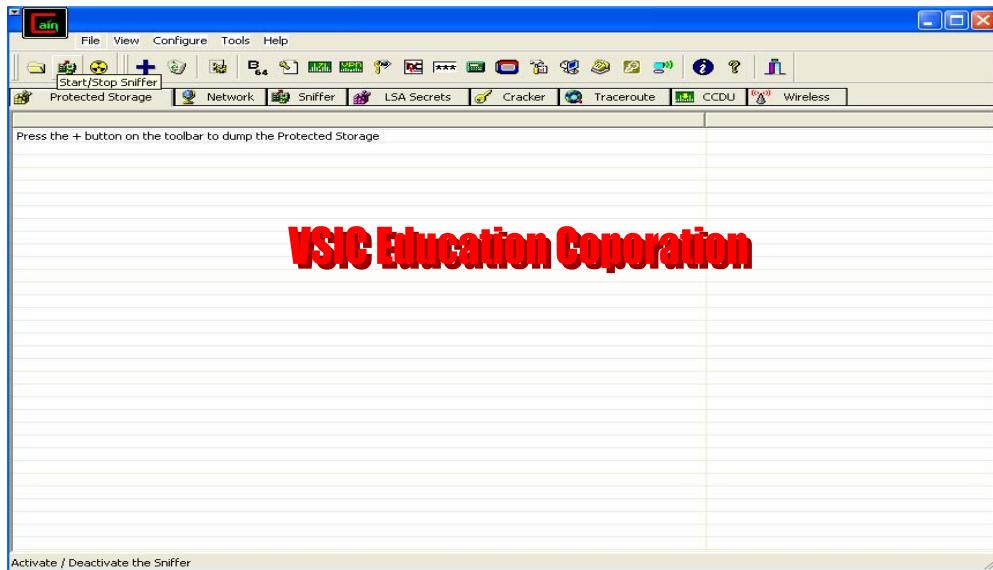
Chọn Next.



Chọn Finish.



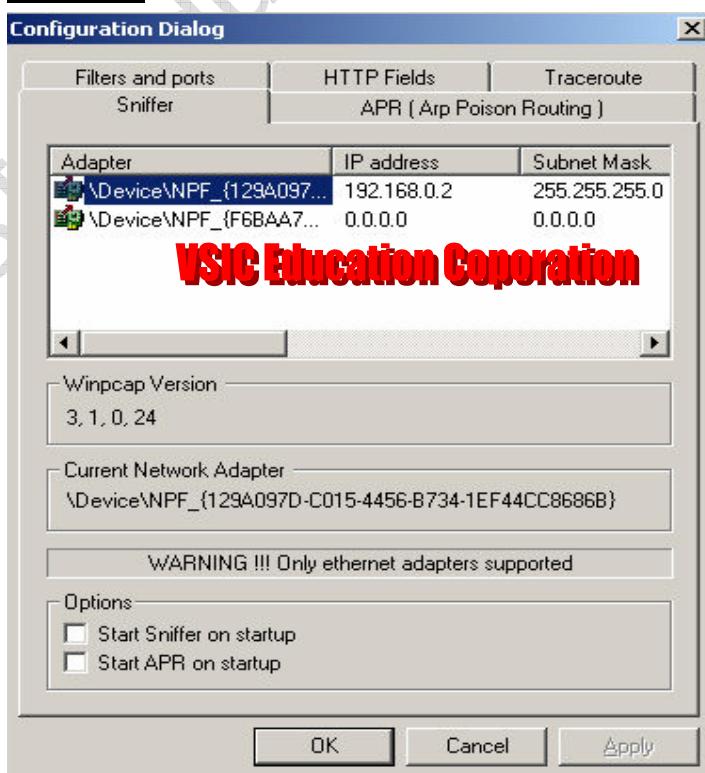




3. Cấu hình

Cain & Abel cần cấu hình một vài thông số, mỗi thứ có thể được điều chỉnh thông qua bảng Configuration dialog.

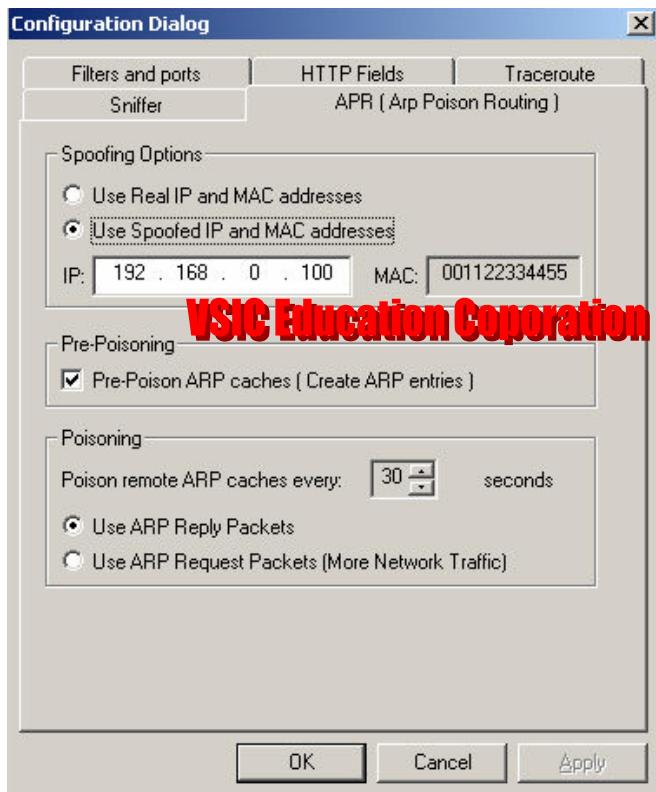
Sniffer tab:



-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:



-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 .

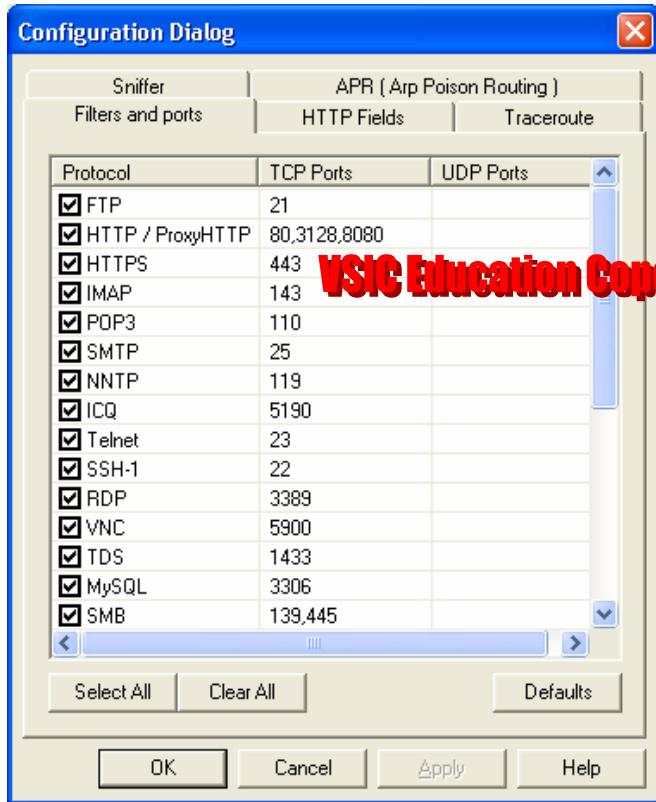
-Tại mục này, ta cần chú ý tới phần Spoofing Options:

+Mục đầu tiên cho phép ta sử dụng địa chỉ MAC và IP thực của máy mà mình đang sử dụng.

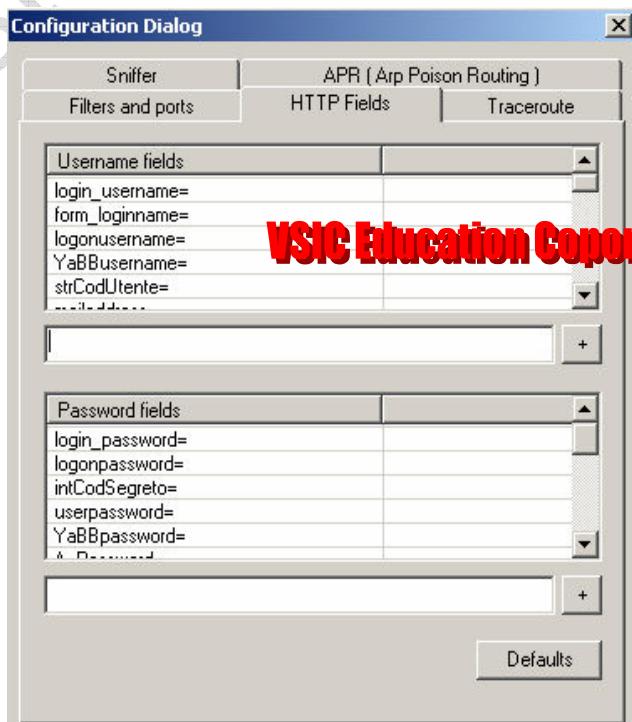
+Mục thứ hai cho phép sử dụng một IP và địa chỉ MAC giả mạo.

(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.

**Fliter and Ports Tab:**

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

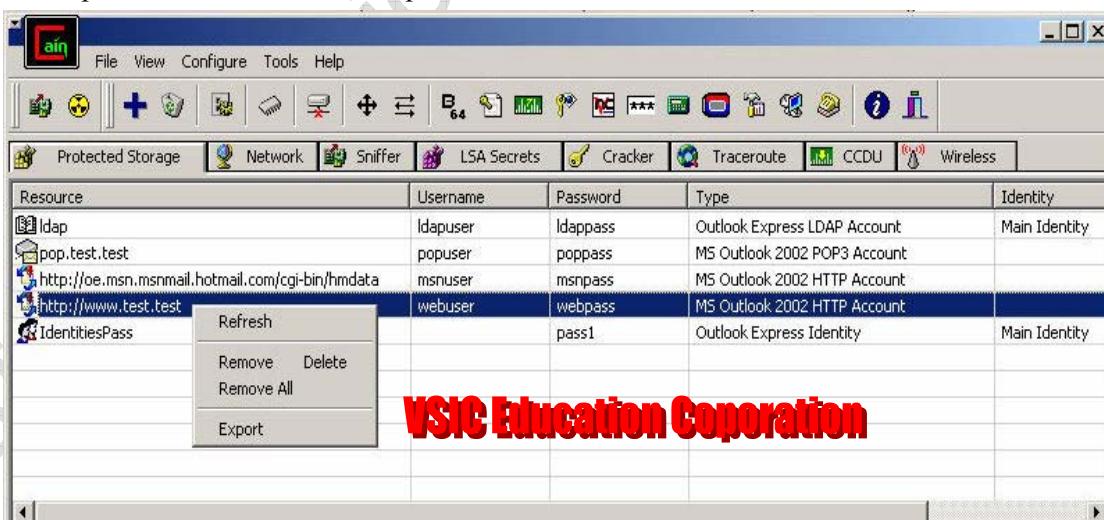
HTTP fields tab:

- Tại đây có 1 list danh sách username và password sử dụng được HTTP sniffer lọc lại.
- Tại tab này cho phép ta biết được 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 đảm nhiệm vai trò là lấy thông tin về password (login password, user pass, webpass v.v....)

4. 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 việc 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, Outlook, Outlook Express



+ 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 .

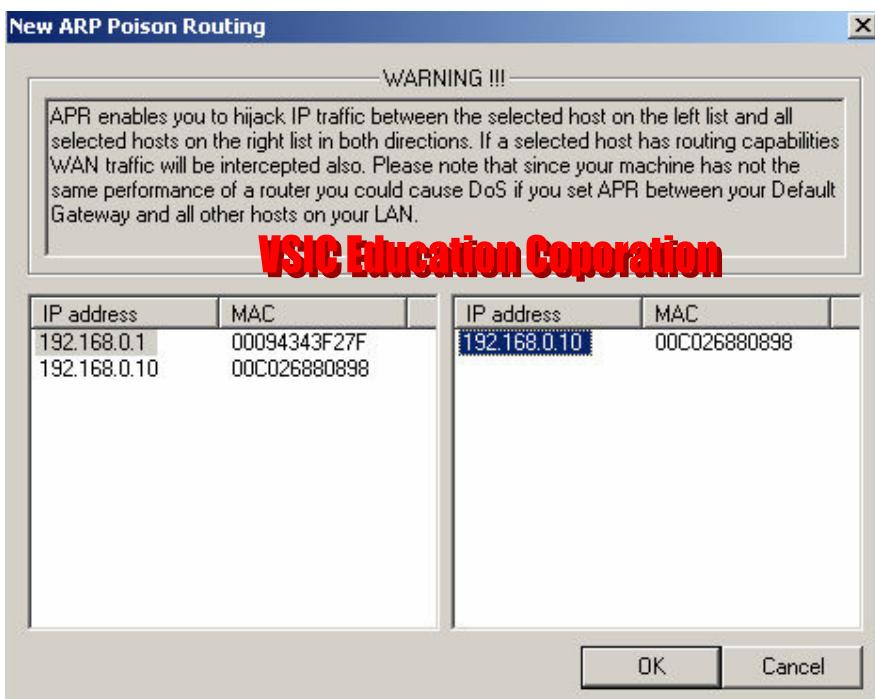
+ Giải mã password Dial-Up:

VSIC Education Corporation

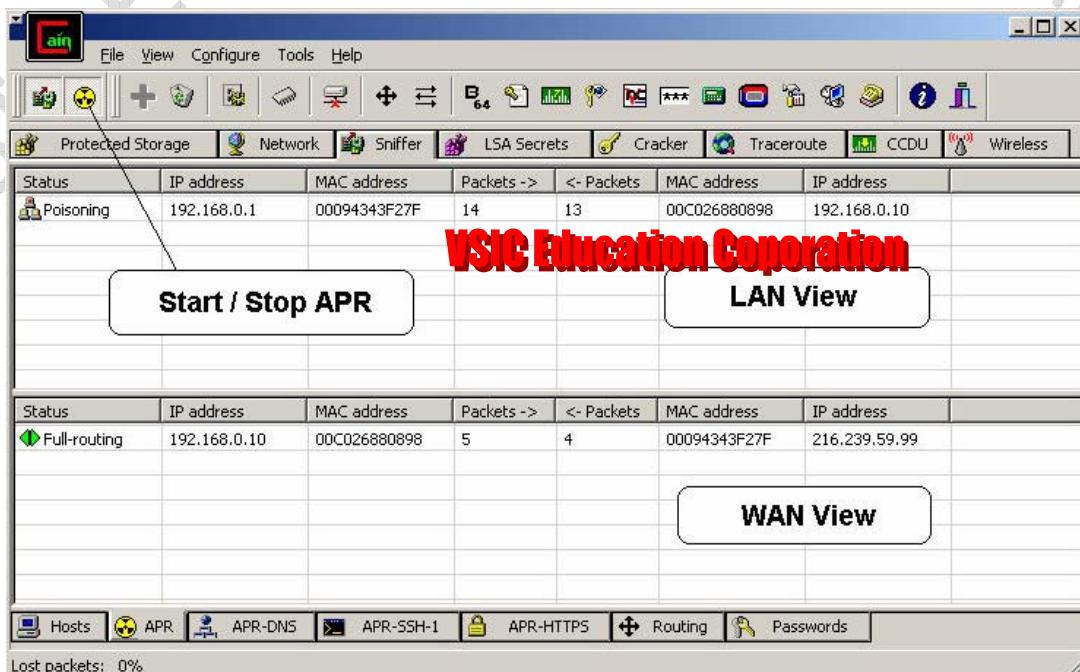
Connection	Number / IP	User	Password	Domain	Device	Type
? * Removed *		utente	password			
? * Removed *		utente2	password2			
? * Removed *		userserial	passwordserial			
ISP1	0123456789	isp1user	isp1password		Standard 56000 bps...	modem
PPP-Site		pppuser	ppppassword		WAN Miniport (PPP...)	pppoe
ISP2		isp2user	isp2password		WAN Miniport (PPP...)	pppoe
VPNCompany	192.168.0.1	vpnuser	vpnpassword		WAN Miniport (L2TP)	vpn
remote-pc		serialuser	serialpassword		Communications cab...	modem
remote-pc2		lptuser	lptpassword		Direct Parallel	parallel
Company	01234567890	rasuser	raspassword	CORPO...	Standard 56000 bps...	modem
gitgber		slipuser	slipass		Communications cab...	modem

+APR:

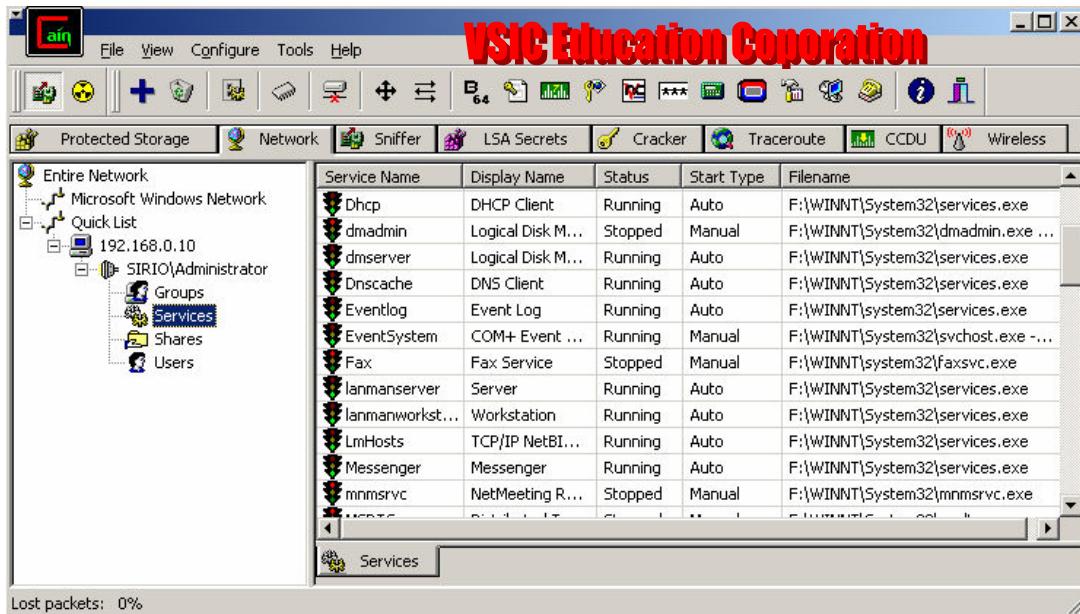
- APR là nét đặc trưng chính của chương trình .Nó cho phép lắng nghe về các mạng chuyển mạch và sự tấn công lưu thông IP giữa các host . “APR poision routing” thực hiện: tấn công và định tuyến chính xác địa chỉ đích
- APR tấn công cơ bản thông qua thao tác của host ARP.Trên 1 địa chỉ IP hay Ethernet 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 lút ở giữa để quan sát



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 poison, 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



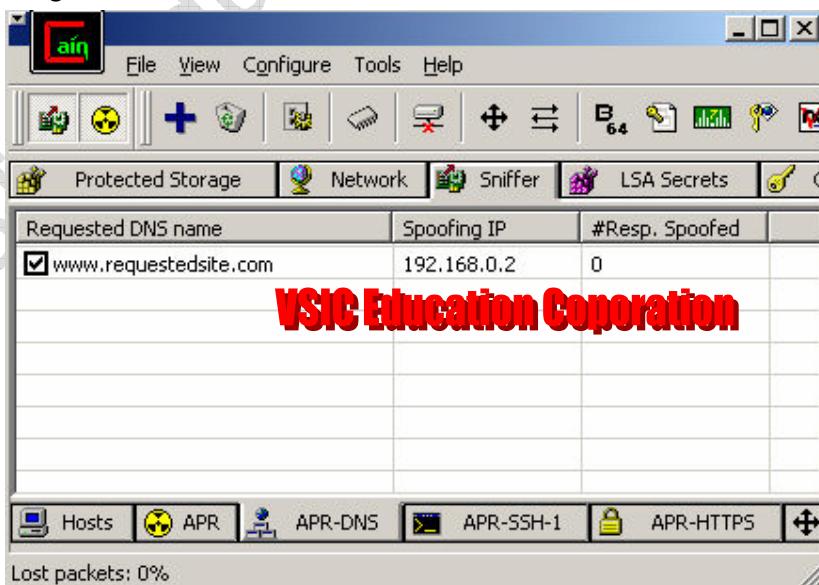
+ Service manager: ta có thể start/stop/pause/continued hay remove bất cứ 1 dịch vụ nào có trên cửa sổ giao diện



+ Sniffer:

ARP-DNS:

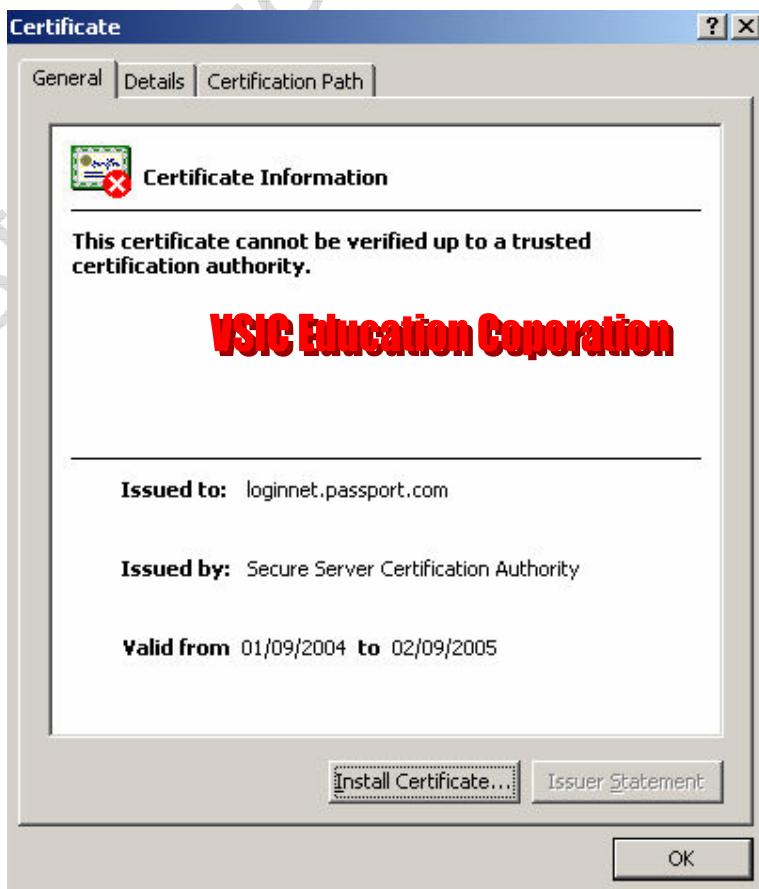
Nét đặc trưng ở đây là cho phép DNS tiến hành giả mạo thành 1 DNS-reply để có thể tấn công.

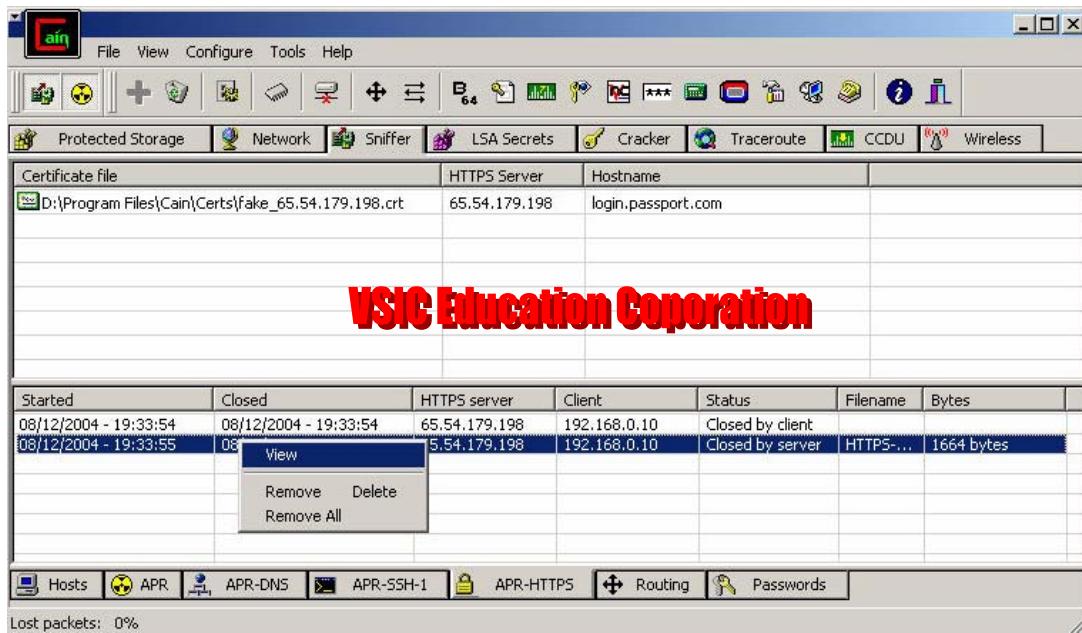


ARP-DNS dễ dàng tạo ra 1 ip address trên DNS-reply .Sniffer dễ dàng rút ra được tên yêu cầu từ gói dữ liệu kết hợp với việc thấy được địa chỉ trên bảng danh sách.Ở đây gói dữ liệu sẽ được chỉnh lại IP address để sau đó re-route đi .Lúc này client sẽ bị đánh lừa để ta dễ dàng biết được địa chỉ đích .

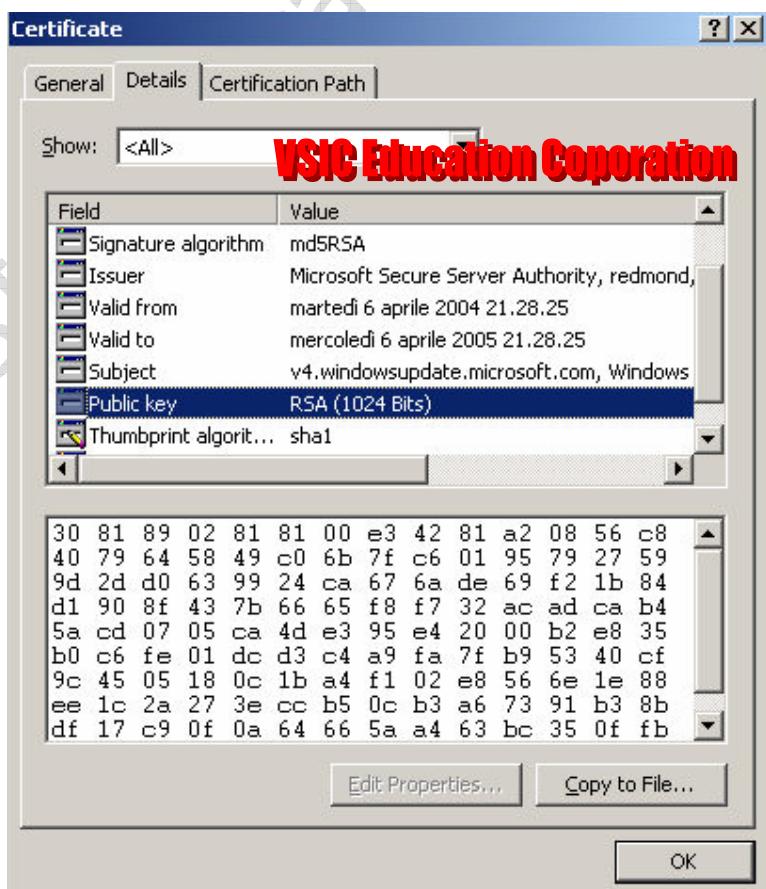
ARP-HTTPS:

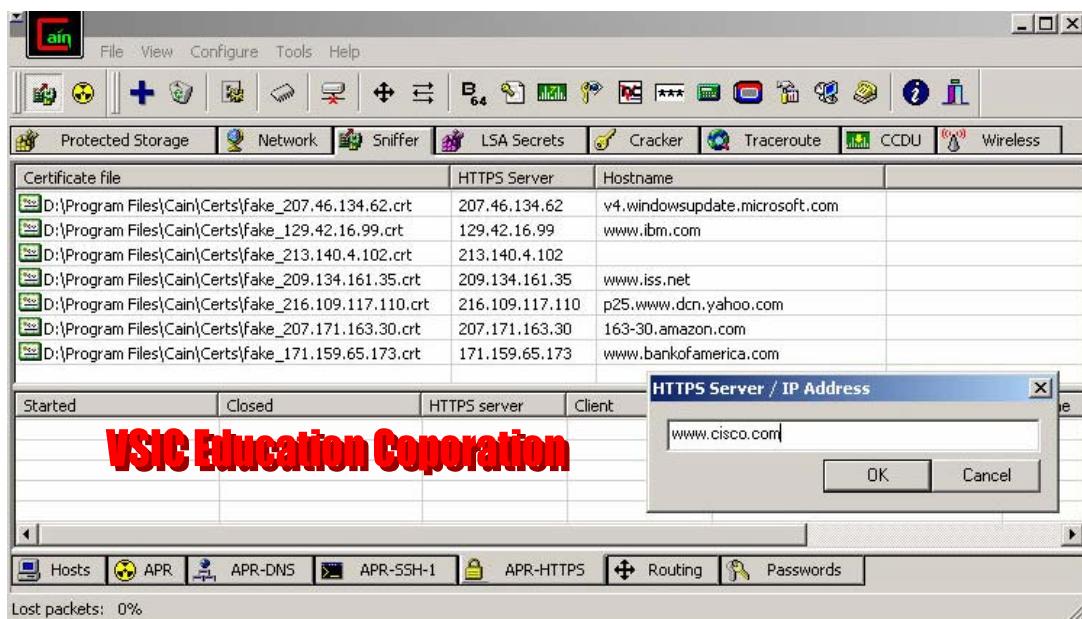
ARP-HTTPS cho phép việc bắt gói và giải mã trong sự lưu thông của HTTPS giữa các host . Đây là công việc kết hợp với công cụ Certificate Collector . Khi mà nạn nhân Start HTTPS trình duyệt của anh ta sẽ hiện lên po-pup báo động .





+ Certificates Collector:





ETTERCAP

1. Giới Thiệu

Ettercap là chương trình phân tích các gói tin gửi qua mạng, vì thế Ettercap cũng là một phần mềm hiệu nghiệm cho phép người sử dụng “đánh hơi” các dữ liệu trên mạng LAN, kể cả những thông tin đã được mã hóa. Ettercap có thể giả danh địa chỉ MAC của card mạng bị tấn công, thay vì gói tin được truyền đến máy tính cần đến thì nó lại được truyền đến máy tính có cài ettercap rồi sau đó mới truyền đến máy tính đích

2. Install trên Linux

Trước khi Install, chúng ta cần chuẩn bị 3 gói cài sau:

- + ettercap-NG-0.7.1.tar – có thể download từ website
<http://prdownloads.sourceforge.net/ettercap>
- + libpcap-0.8.1.tar
- + libnet-1.1.2.1.tar – có thể download từ website
<http://www.packetfactory.net/libnet/dist/>

Install *libnet*:

1. # tar zxvf libnet-1.1.2.1.tar.gz
2. # cd libnet
3. # ./configure
4. # make
5. # make install

Install *libpcap*:

6. # tar zxvf libpcap-1.1.2.1.tar.gz
7. # cd libpcap
8. # ./configure
9. # make
10. # make install

Install *ettercap*:

1. # tar zxvf ettercap-NG-0.7.1.tar.gz
2. # cd ettercap-NG-0.7.1
3. # ./configure
4. # make

5. # make install

Quá trình cài đặt hoàn tất, trên cửa sổ console xuất hiện những dòng thông báo

```
root@localhost:~ - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help
[...]
ettercap has been configured as follow...
=====
Install directory: /usr/local

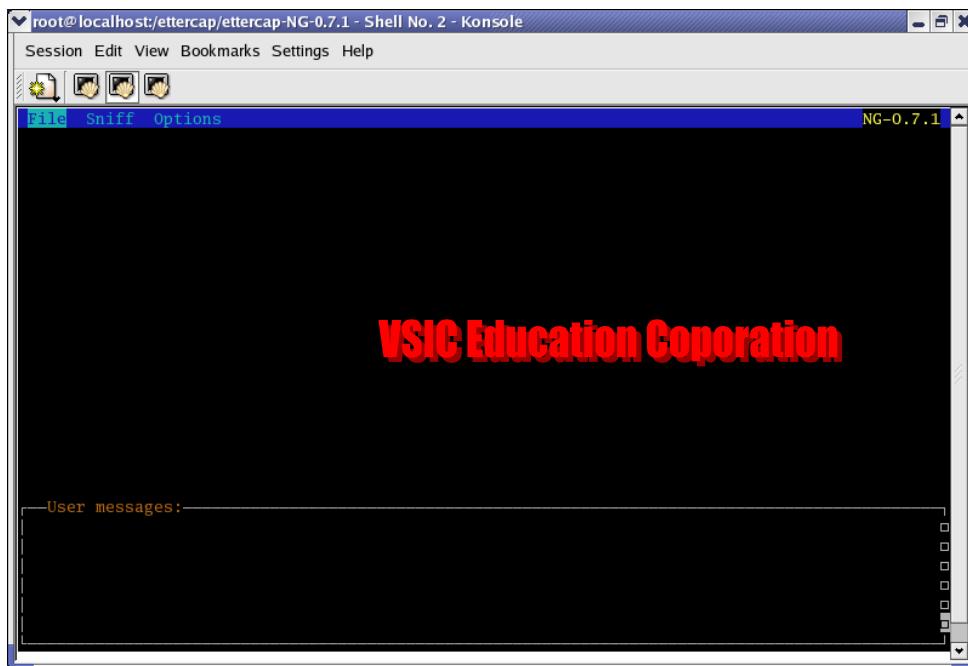
Libraries :
LIBPCAP ..... default
LIBNET ..... default
LIBSSL ..... default
NCURSES ..... default
GTK+ ..... NO

Functionalities :
Debug mode ..... no
Plugin support ..... yes
Passive DNS ..... yes
Perl regex in filters .. no
Iconv UTF-8 support .... yes
=====

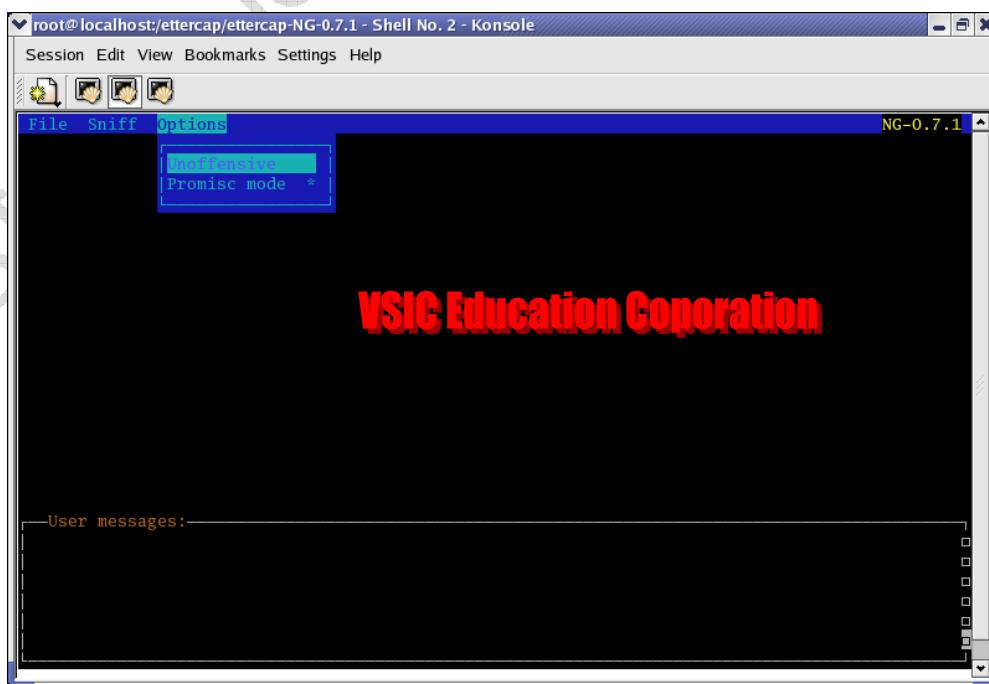
[root@localhost ettercap-NG-0.7.1]# cd
[root@localhost root]# ettercap
[...]
root@localhost:~ - Shell No. 2 - Konsole
[1 2] [root@localhost:~ - Shell No. 2 - Konsole] [3 4] ettercap-NG-0.7.1 (sniffer) - M 14:30
```

3. Cấu Hình và Sử Dụng Ettercap

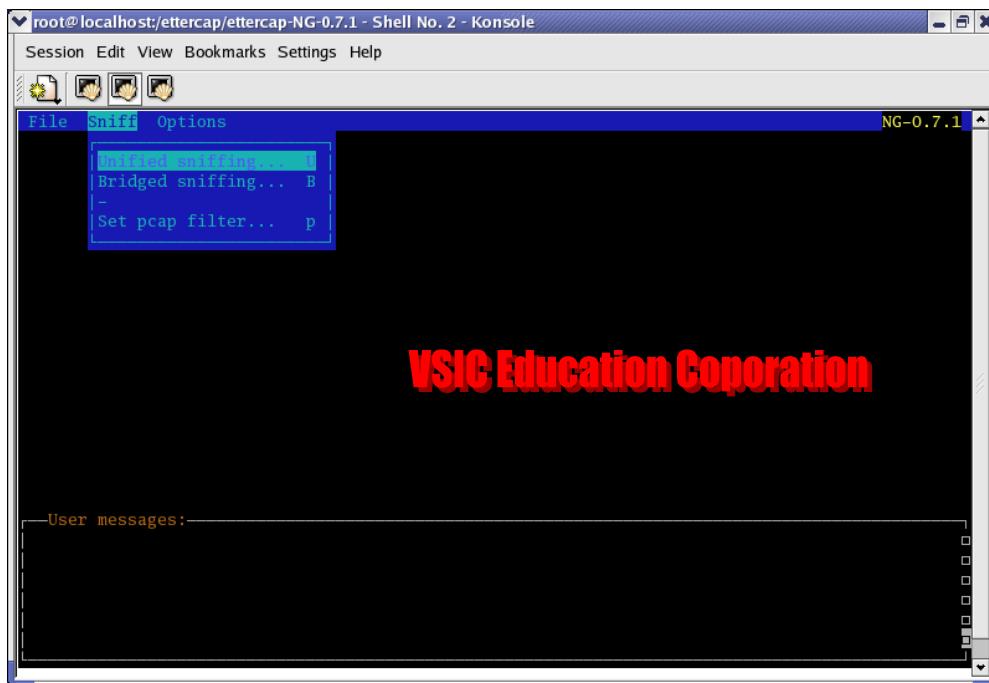
- Mở giao diện Ettercap bằng cách gõ dòng lệnh
ettercap –C



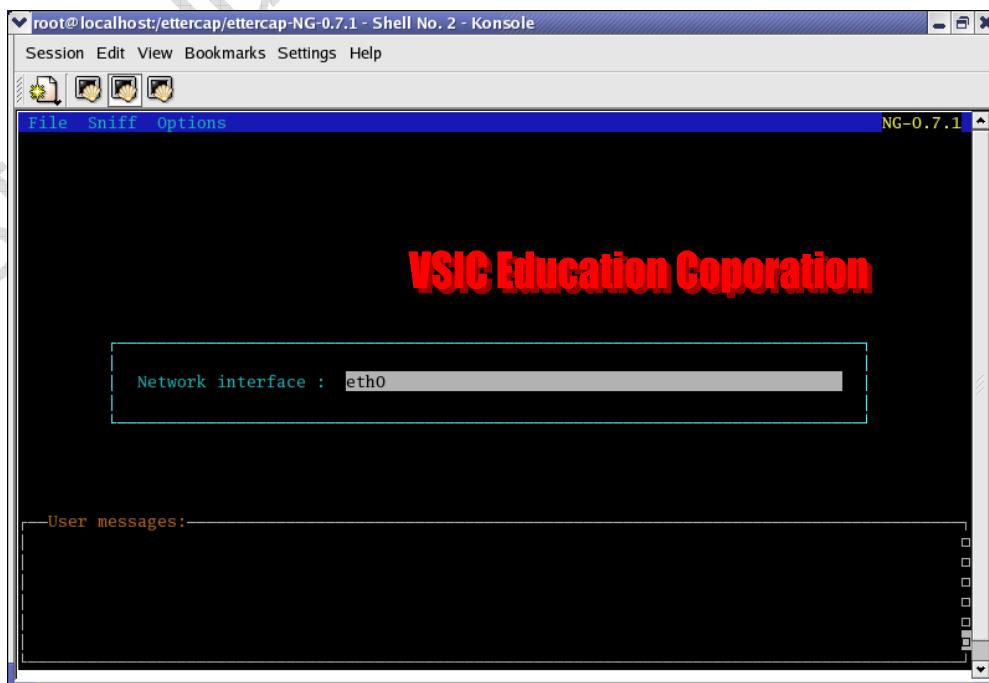
- Trước khi tiến hành cấu hình, ta kiểm tra option Promisc mode có được check chưa, nếu chưa thì chọn check



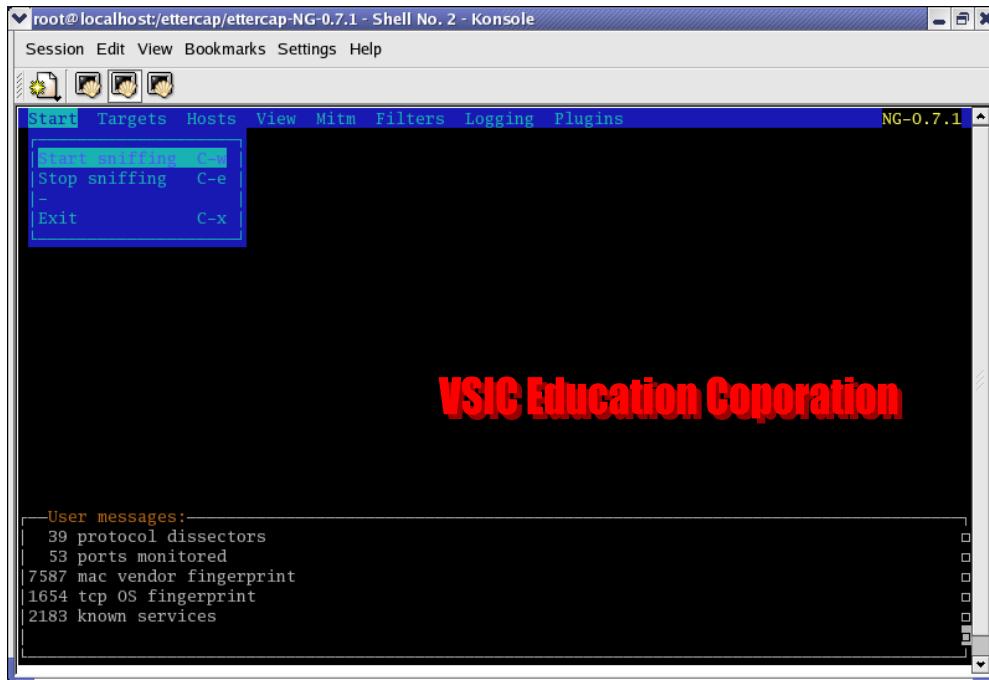
- Trong menu sniff, chọn Unified sniffing..



- Chọn card mạng sử dụng



- Để khởi động quá trình lắng nghe, chọn menu start, start sniffing



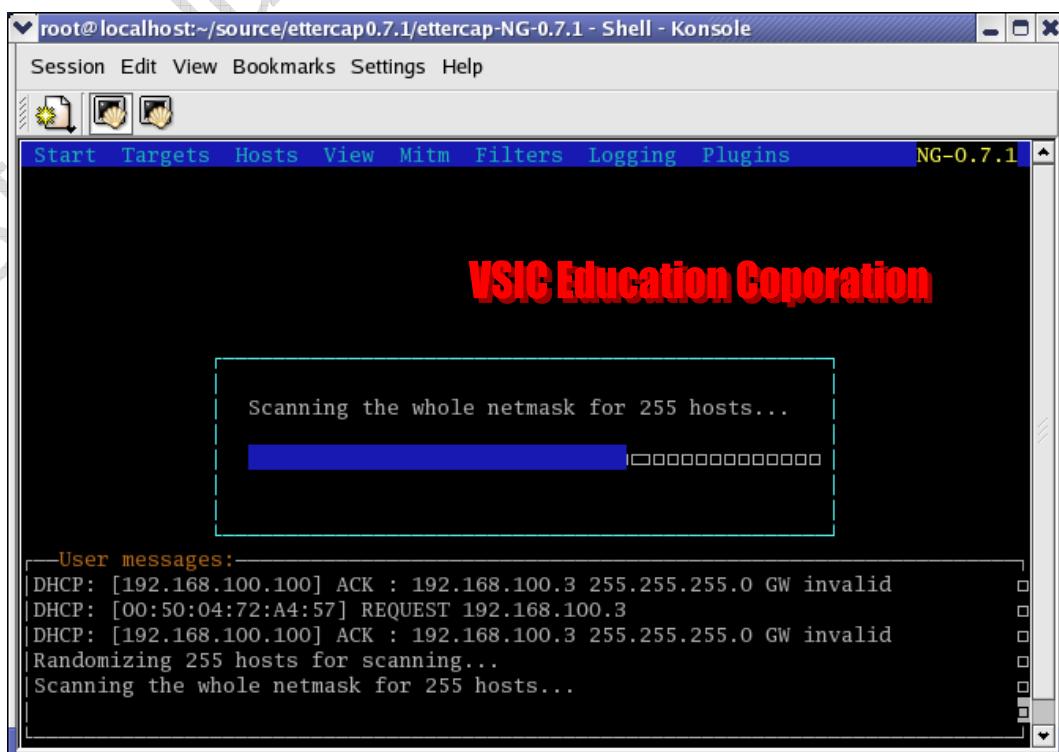
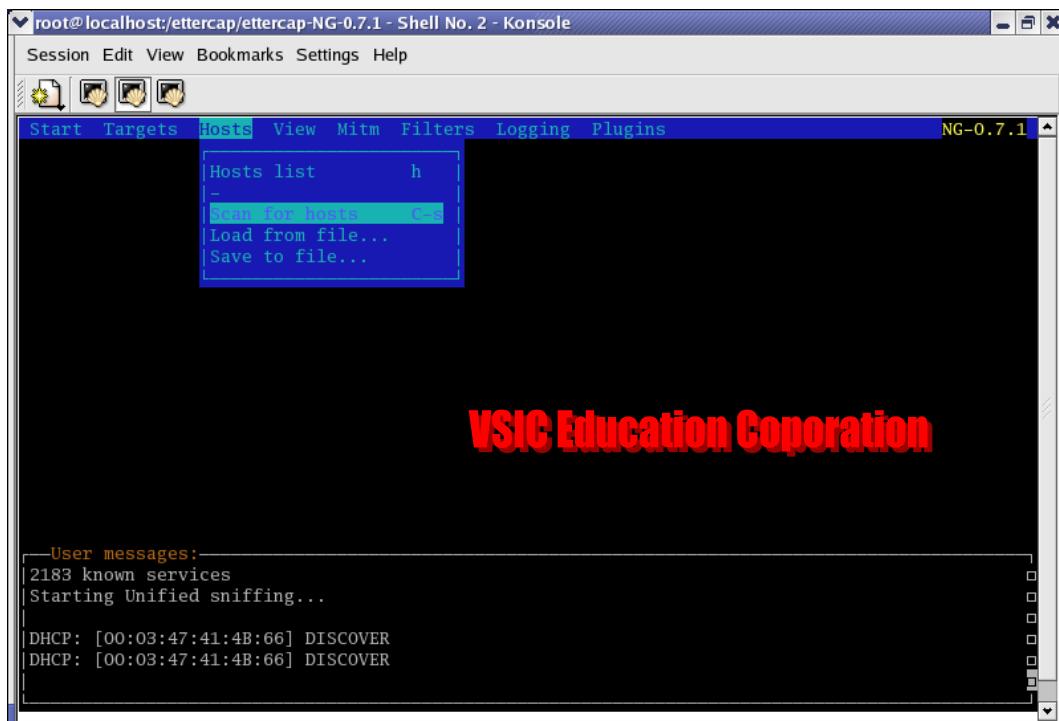
Tại dòng User Messages sẽ xuất hiện thông báo cho biết dịch vụ đang start lên

```
--User messages:
| 2183 known services
| Starting Unified sniffing...
| DHCP: [00:03:47:41:4B:66] DISCOVER
| DHCP: [00:03:47:41:4B:66] DISCOVER
```

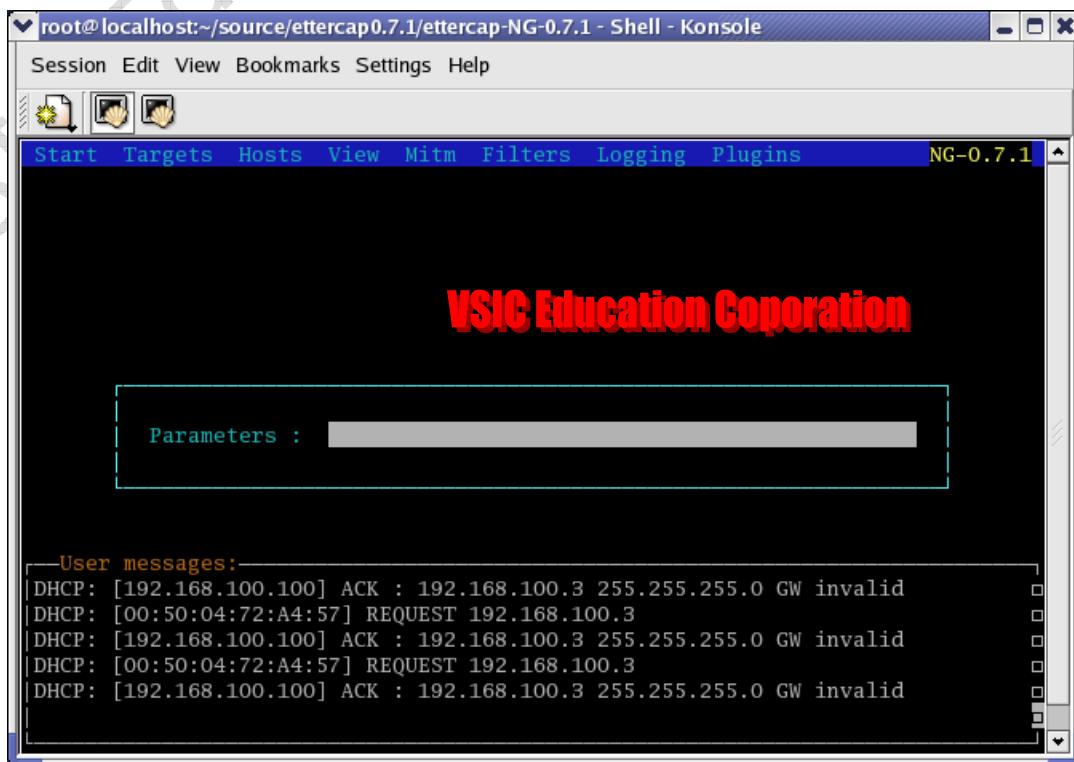
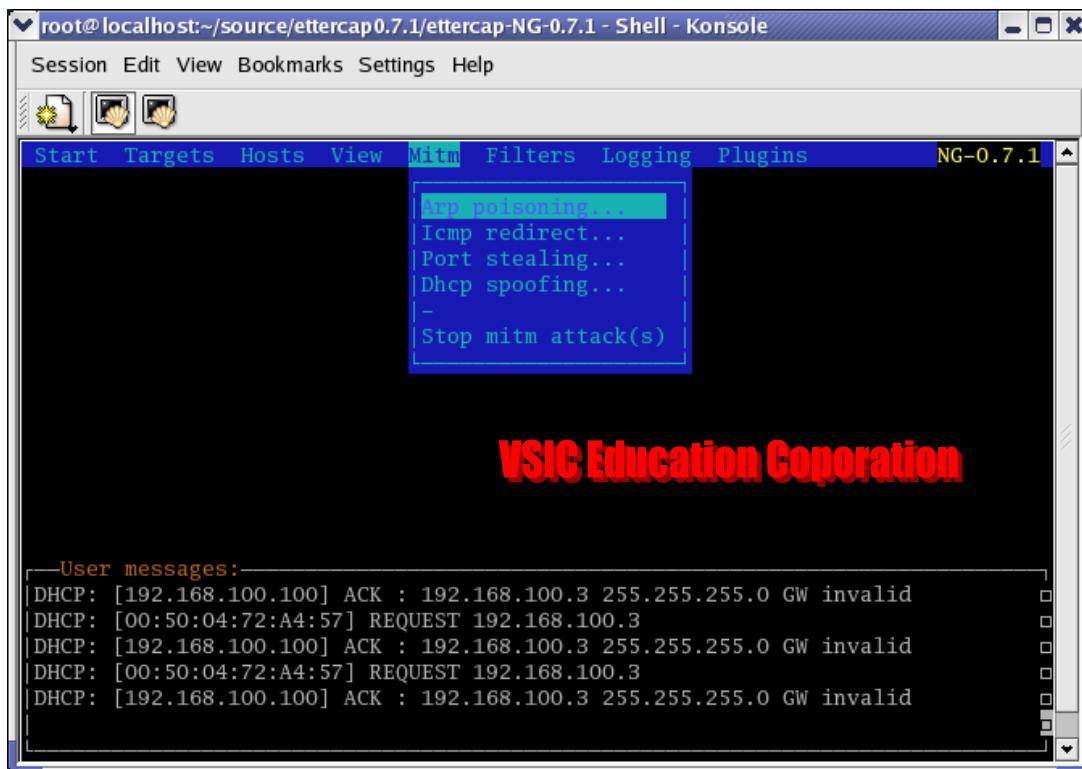
```
--User messages:
| 192.168.101.1 "lotus.edu.vn"
| DHCP: [192.168.101.1] ACK : 192.168.101.210 255.255.255.0 GW 192.168.101.1 DNS
| 192.168.101.1 "lotus.edu.vn"
| DHCP: [192.168.101.1] ACK : 192.168.101.209 255.255.255.0 GW 192.168.101.1 DNS
| 192.168.101.1 "lotus.edu.vn"
```

```
--User messages:
| DHCP: [10.0.0.12] ACK : 0.0.0.0 0.0.0.0 GW invalid
| DHCP: [10.0.0.138] ACK : 10.0.0.244 255.255.255.0 GW 10.0.0.138 DNS 10.0.0.138
| "lan"
| DHCP: [00:50:04:72:A4:57] REQUEST 192.168.100.3
| DHCP: [192.168.100.100] ACK : 192.168.100.3 255.255.255.0 GW invalid
```

- Trong menu Host, chọn Scan from hosts



- Trong menu Mitm, chọn Arp poisoning...



- Không chọn parameters, nhấn enter bỏ qua
- Tại dòng User messages xuất hiện thông báo

```
User messages:
ARP poisoning victims:
GROUP 1 : ANY (all the hosts in the list)
GROUP 2 : ANY (all the hosts in the list)
```

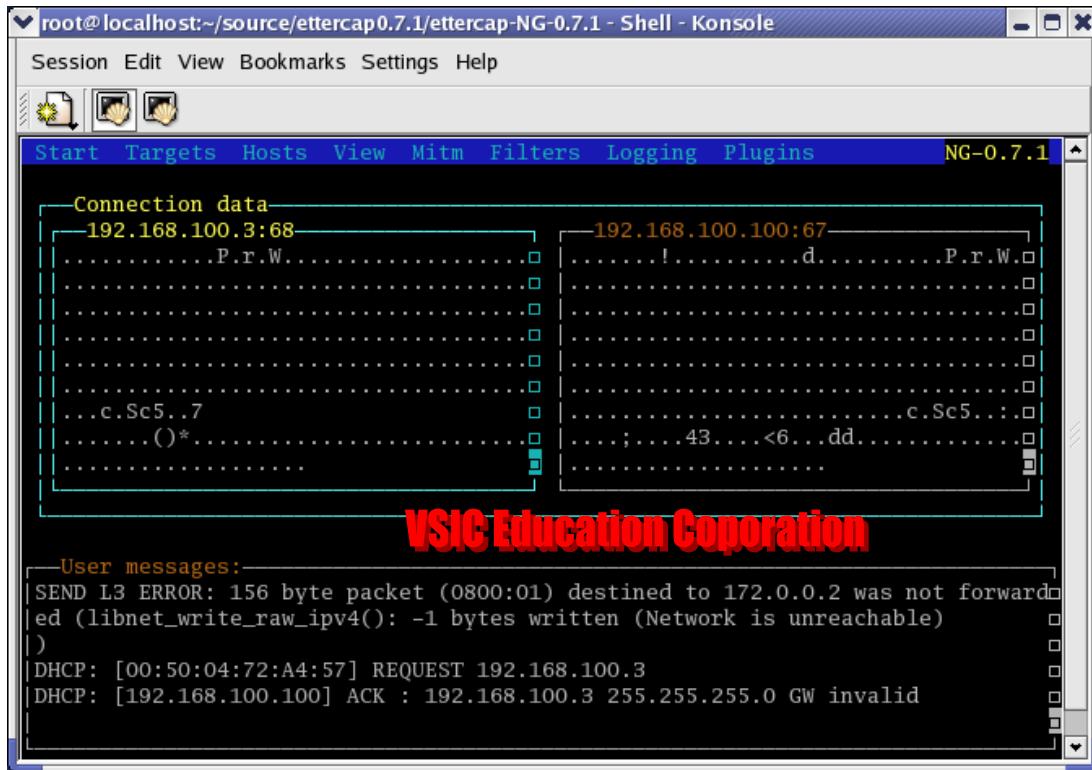
- Để xem các host đã được quét, chọn Connections, trong menu View

The screenshot shows the Ettercap NG-0.7.1 interface running in a terminal window titled "root@localhost:~/source/ettercap0.7.1/ettercap-NG-0.7.1 - Shell - Konsole". The menu bar includes Session, Edit, View, Bookmarks, Settings, and Help. The toolbar has icons for Start, Targets, Hosts, View, Mitm, Filters, Logging, Plugins, and NG-0.7.1. The main window displays "VSIC Education Corporation"水印. The "Targets" tab is selected, showing a list of "Live connections:":

Source IP:Port	Destination IP:Port	Status	TX: TX Count
1.1.1.1:138	- 1.255.255.255:138	U idle	TX: 4900
1.1.1.1:137	- 1.255.255.255:137	U idle	TX: 3104
192.168.100.3:68	- 192.168.100.100:67	U idle	TX: 8400
2.2.2.2:138	- 2.255.255.255:138	U idle	TX: 4365
1.1.1.1:1346	- 229.55.150.208:1345	U idle	TX: 854
192.168.101.1:67	- 255.255.255.255:68	U active	TX: 5079
192.168.106.1:138	- 192.168.106.255:138	U idle	TX: 2211
10.0.0.223:138	- 10.255.255.255:138	U idle	TX: 1206
172.16.0.10:138	- 172.16.255.255:138	U idle	TX: 1206

Below the connections list, there is a "User messages:" section with several log entries related to DHCP requests and ACK responses.

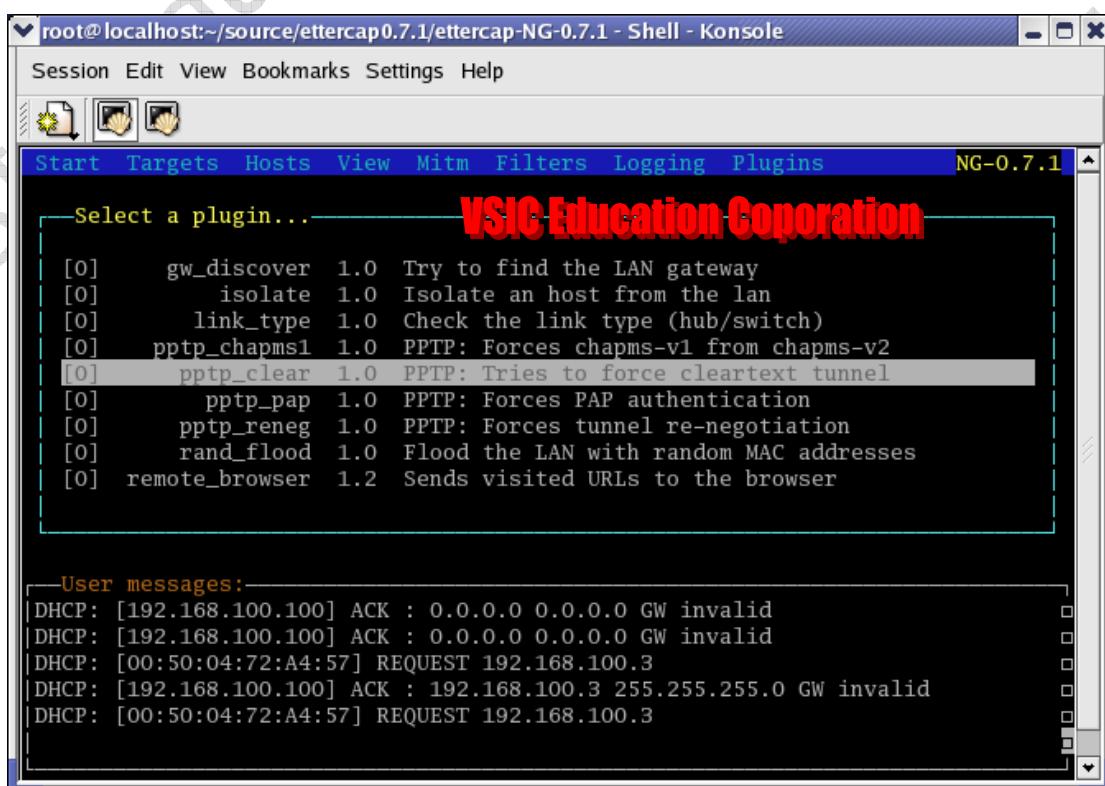
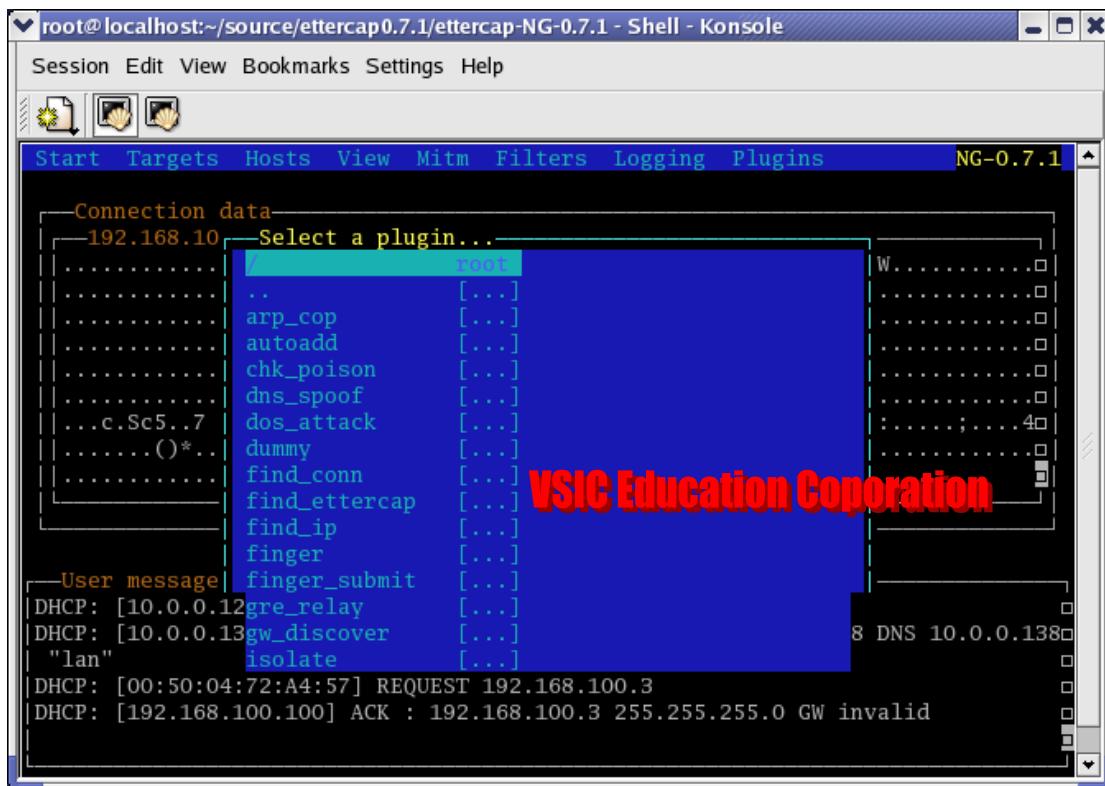
- Để bắt gói, chọn host nào đang ở chế độ active, sẽ hiện ra bắn các gói bắt được, các gói này sẽ hiển thị dưới dạng mã hóa



- Chọn Log all packets and infos... trong menu Logging để save những file logs chứa các gói bắt được lại
- Để có thể đọc được các gói dưới dạng mã hóa đó, trong cửa sổ console, gõ lệnh
etterlog -p -k -i -ascii logfile.eci | less

4. Tính Năng Của Ettercap

Ettercap cung cấp cho ta một số plug-in, bằng cách chọn những plug-in này, ta có thể ứng dụng một số tính năng quan trọng của ettercap



Ngoài ra Ettercap còn có 2 plug-in rất quan trọng là arpcop và leech

Nó cho phép ta có thể dùng chính Ettercap để bảo vệ máy mình trước các chương trình sniffer khác trên mạng.

1. Arpcop: Nếu nghi ngờ ai đó đang “nghe lén” trên mạng, bạn khởi động ettercap và chọn plug-in này, đối tượng sử dụng ettercap hay dsniff ta vẫn có thể dò tìm được, lúc đó một cửa sổ mới sẽ hiển thị những máy tính đang chạy các chương trình spoofing arp trên mạng.
2. Leech: Khi xác nhận được đối tượng tấn công, ta có thể tiến hành cô lập máy tính này khỏi mạng ngay lập tức bằng cách sử dụng plug-in này. Còn có thể dùng ettercap để phát hiện các máy bị nhiễm virus đang phát tán trên mạng rồi cô lập chúng bằng leech, sau đó diệt bằng các chương trình chống virus rất hiệu quả.

Bài 6:**Tấn Công từ chối dịch vụ DoS****I/ Giới thiệu:**

DoS attack là gì? (Denial Of Services Attack)

DoS attack (dịch là tấn công từ chối dịch vụ) là kiểu tấn công rất lợi hại, với loại tấn công này, bạn chỉ cần một máy tính kết nối Internet là đã có thể thực hiện việc tấn công được máy tính của đối phương. Thực chất của DoS attack là hacker sẽ chiếm dụng một lượng lớn tài nguyên trên server (tài nguyên đó có thể là băng thông, bộ nhớ, CPU, đĩa cứng, ...) làm cho server không thể nào đáp ứng các yêu cầu từ các máy của người khác (máy của những người dùng bình thường) và server có thể nhanh chóng bị ngừng hoạt động, crash hoặc reboot.

Các loại DoS attack hiện đang được biết đến và sử dụng:

a.) Winnuke:

- DoS attack loại này chỉ có thể áp dụng cho các máy tính đang chạy Windows 9x. Hacker sẽ gửi các gói tin với dữ liệu "Out of Band" đến cổng 139 của máy tính đích. (Cổng 139 chính là cổng NetBIOS, cổng này chỉ chấp nhận các gói tin có cờ Out of Band được bật). Khi máy tính của victim nhận được gói tin này, một màn hình xanh báo lỗi sẽ được hiển thị lên với nạn nhân do chương trình của Windows nhận được các gói tin này nhưng nó lại không biết phản ứng với các dữ liệu Out Of Band như thế nào dẫn đến hệ thống sẽ bị crash.

b.) Ping of Death:

- Ở kiểu DoS attack này, ta chỉ cần gửi một gói dữ liệu có kích thước lớn thông qua lệnh ping đến máy đích thì hệ thống của họ sẽ bị treo.
- VD: ping -l 65000

c.) Teardrop:

- Như ta đã biết, tất cả các dữ liệu chuyển đi trên mạng từ hệ thống nguồn đến hệ thống đích đều phải trải qua 2 quá trình: dữ liệu sẽ được chia ra thành các mảnh nhỏ ở hệ thống nguồn, mỗi mảnh đều phải có một giá trị offset nhất định để xác định vị trí của mảnh đó trong gói dữ liệu được chuyển đi. Khi các mảnh này đến hệ thống đích, hệ thống đích sẽ dựa vào giá trị offset để sắp xếp các mảnh lại với nhau theo thứ tự đúng như ban đầu. Lợi dụng sơ hở đó, ta chỉ cần gửi đến hệ thống đích một loạt gói packets với giá trị offset chồng chéo lên nhau. Hệ thống đích sẽ không thể nào sắp xếp lại các packets này, nó không điều khiển được và có thể bị crash, reboot hoặc ngừng hoạt động nếu số lượng packets với giá trị offset chồng chéo lên nhau quá lớn !

d.) SYN Attack:

- Trong SYN Attack, hacker sẽ gửi đến hệ thống đích một loạt SYN packets với địa chỉ IP nguồn không có thực. Hệ thống đích khi nhận được các SYN packets này sẽ gửi trả lại các địa chỉ không có thực đó và chờ đợi để nhận thông tin phản hồi từ các địa chỉ IP giả. Vì đây là các địa chỉ IP không có thực, nên hệ thống đích sẽ chờ đợi vô ích và còn đưa các "request" chờ đợi này vào bộ nhớ, gây lãng phí một lượng đáng kể bộ nhớ trên máy chủ mà đúng ra là phải dùng vào việc khác thay cho phải chờ đợi thông tin phản hồi không có thực này. Nếu ta gửi cùng một lúc nhiều gói tin có địa chỉ IP giả như vậy thì hệ thống sẽ bị quá tải dẫn đến bị crash hoặc boot máy tính. ==> ném đá đầu tay .

e.) Land Attack:

- Land Attack cũng gần giống như SYN Attack, nhưng thay vì dùng các địa chỉ IP không có thực, hacker sẽ dùng chính địa chỉ IP của hệ thống nạn nhân. Điều này sẽ tạo nên một vòng lặp vô tận giữa trong chính hệ thống nạn nhân đó, giữa một bên cần nhận thông tin phản hồi còn một bên thì chẳng bao giờ gửi thông tin phản hồi đó đi cả . ==> Gây ông đập lưng ông .

f.) Smurf Attack:

- Trong Smurf Attack, cần có ba thành phần: hacker (người ra lệnh tấn công), mạng khuếch đại (sẽ nghe lệnh của hacker) và hệ thống của nạn nhân. Hacker sẽ gửi các gói tin ICMP đến địa chỉ broadcast của mạng khuếch đại. Điều đặc biệt là các gói tin ICMP packets này có địa chỉ IP nguồn chính là địa chỉ IP của nạn nhân . Khi các packets đó đến được địa chỉ broadcast của mạng khuếch đại, các máy tính trong mạng khuếch đại sẽ tưởng rằng máy tính nạn nhân đã gửi gói tin ICMP packets đến và chúng sẽ đồng loạt gửi trả lại hệ thống nạn nhân các gói tin phản hồi ICMP packets. Hệ thống máy nạn nhân sẽ không chịu nổi một khối lượng không lồ các gói tin này và nhanh chóng bị ngừng hoạt động, crash hoặc reboot. Như vậy, chỉ cần gửi một lượng nhỏ các gói tin ICMP packets đi thì hệ thống mạng khuếch đại sẽ khuếch đại lượng gói tin ICMP packets này lên gấp bội . Tỉ lệ khuếch đại phụ thuộc vào số lượng máy tính có trong mạng khuếch đại . Nhiệm vụ của các hacker là cố chiếm được càng nhiều hệ thống mạng hoặc routers cho phép chuyển trực tiếp các gói tin đến địa chỉ broadcast không qua chố lọc địa chỉ nguồn ở các đầu ra của gói tin . Có được các hệ thống này, hacker sẽ dễ dàng tiến hành Smurf Attack trên các hệ thống cần tấn công . ==> một máy làm chảng si nhê, chục máy chụm lại ta đánh chò thua .

g.) UDP Flooding:

- Cách tấn công UDP đòi hỏi phải có 2 hệ thống máy cùng tham gia. Hackers sẽ làm cho hệ thống của mình đi vào một vòng lặp trao đổi các dữ liệu qua giao thức UDP. Và giả mạo địa chỉ IP của các gói tin là địa chỉ loopback (127.0.0.1), rồi gửi gói tin này đến hệ thống của nạn nhân trên cổng UDP echo (7). Hệ thống của nạn nhân sẽ trả lời lại các messages do 127.0.0.1(chính nó) gửi đến, kết quả là nó sẽ đi vòng một vòng lặp vô tận. Tuy nhiên, có nhiều hệ thống không cho dùng địa chỉ loopback nên hacker sẽ giả mạo một địa chỉ IP của một máy tính nào đó trên mạng nạn nhân và tiến hành ngập lụt UDP trên hệ thống của nạn nhân . Nếu bạn làm cách này không thành công thì chính máy của bạn sẽ bị đáy .

h .) Tân công DNS:

- Hacker có thể đổi một lối vào trên Domain Name Server của hệ thống nạn nhân rồi cho chỉ đến một website nào đó của hacker. Khi máy khách yêu cầu DNS phân tích địa chỉ bị xâm nhập thành địa chỉ ip, lập tức DNS (đã bị hacker thay đổi cache tạm thời) sẽ đổi thành địa chỉ ip mà hacker đã cho chỉ đến đó. Kết quả là thay vì phải vào trang Web muốn vào thì các nạn nhân sẽ vào trang Web do chính hacker tạo ra. Một cách tấn công từ chối dịch vụ thật hữu hiệu !.

g .) Distributed DoS Attacks (DDos):

- DDoS yêu cầu phải có ít nhất vài hackers cùng tham gia. Đầu tiên các hackers sẽ cố thâm nhập vào các mạng máy tính được bảo mật kém, sau đó cài lên các hệ thống này chương trình DDoS server. Bây giờ các hackers sẽ hẹn nhau đến thời gian đã định sẽ dùng DDoS client kết nối đến các DDoS servers, sau đó đồng loạt ra lệnh cho các DDoS servers này tiến hành tấn công DDoS đến hệ thống nạn nhân .

h.) DRDoS (The Distributed Reflection Denial of Service Attack):

- Đây có lẽ là kiểu tấn công lợi hại nhất và làm boot máy tính của đôi phương nhanh gọn nhất . Cách làm thì cũng tương tự như DDos nhưng thay vì tấn công bằng nhiều máy tính thì người tấn công chỉ cần dùng một máy tấn công thông qua các server lớn trên thế giới . Vẫn với phương pháp giả mạo địa chỉ IP của victim, kẻ tấn công sẽ gửi các gói tin đến các server mạnh nhất, nhanh nhất và có đường truyền rộng nhất như Yahoo .v.v..., các server này sẽ phản hồi các gói tin đó đến địa chỉ của victim . Việc cùng một lúc nhận được nhiều gói tin thông qua các server lớn này sẽ nhanh chóng làm nghẽn đường truyền của máy tính nạn nhân và làm crash, reboot máy tính đó . Cách tấn công này lợi hại ở chỗ chỉ cần một máy có kết nối Internet đơn giản với đường truyền bình thường cũng có thể đánh bật được hệ thống có đường truyền tốt nhất thế giới nếu như ta không kịp ngăn chặn . Trang Web HVA của chúng ta cũng bị DoS vừa rồi bởi cách tấn công này đây .

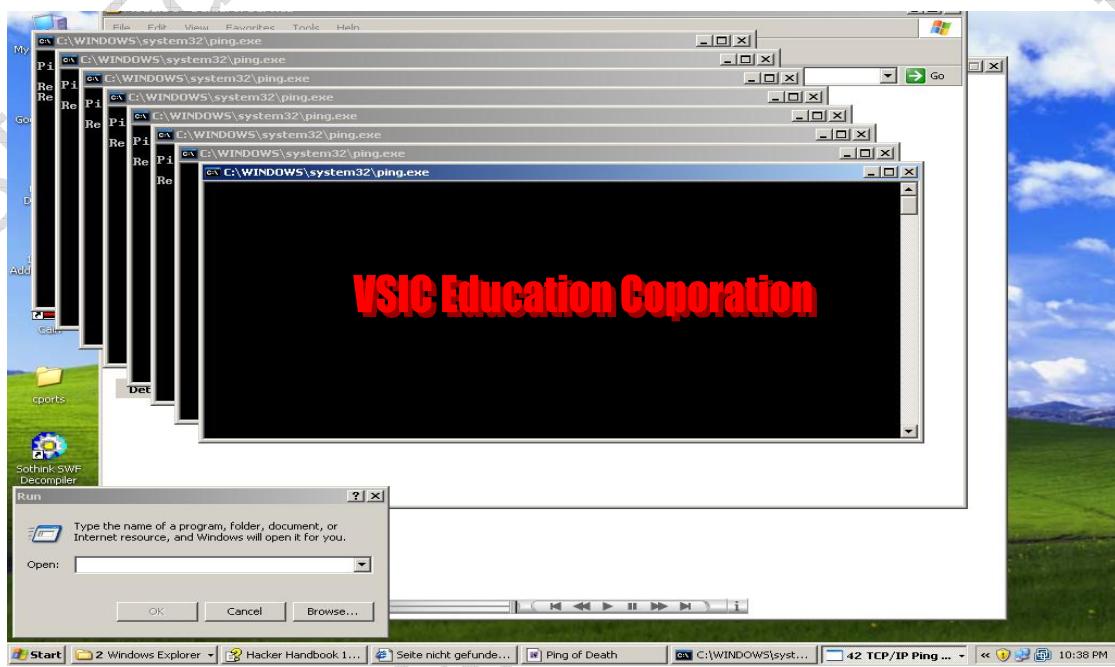
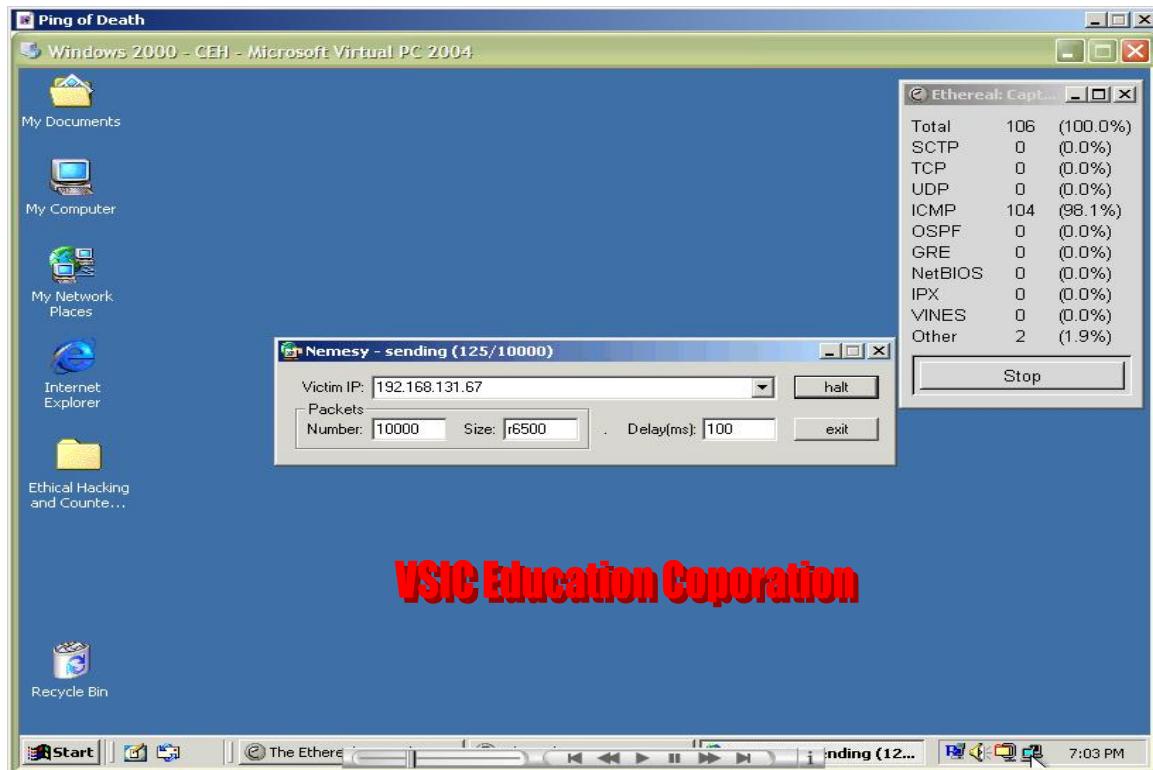
(Trích dẫn Netsky (vniss))

II/ Mô tả bài lab:

Bài Lab 1: DoS bằng cách sử dụng Ping of death.

Ngoài việc sử dụng các tool Nemesy ta còn có thể sử dụng lệnh sau để có thể khởi động ping of death

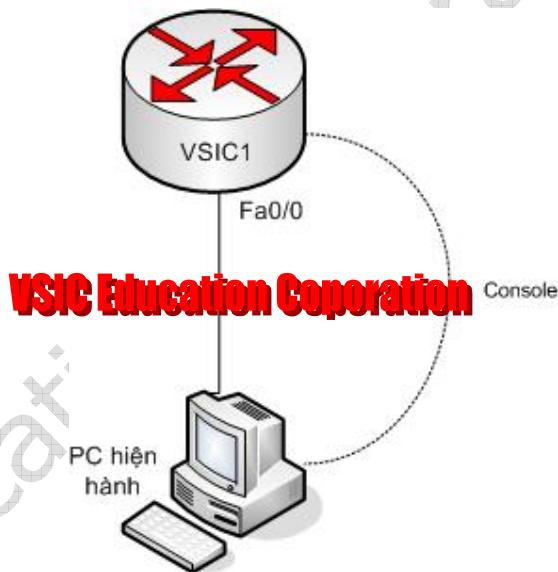
For /L %i in (1,1,100) do start ping [ip victim] -l 10000 -t



Ta có thể chạy câu lệnh này nhiều lần, để có thể làm cho máy Client bị DoS hoàn toàn.

Bài lab 2: DoS 1 giao thức không sử dụng chứng thực(trong bài sử dụng giao thức RIP)

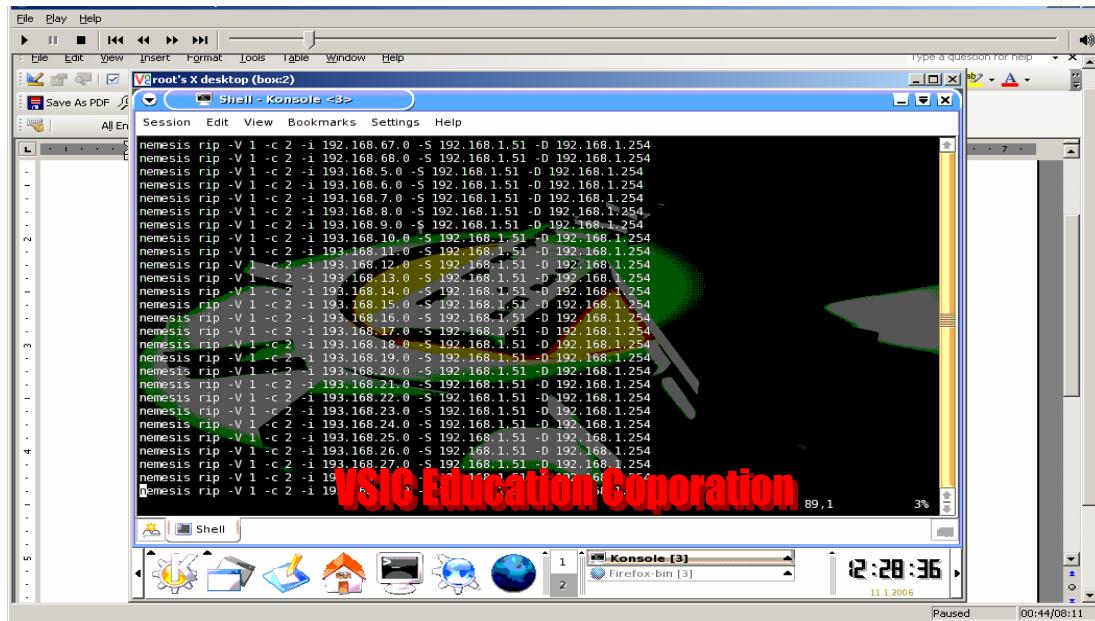
Trong bài này chúng ta sử dụng Cisco router để chạy phiên bản RIP version 1 và sử dụng tool Nemesis từ máy CD Boot Linux để chèn vào các thông điệp RIP update trên Router. Router khi nhận được thông điệp update sẽ lưu lại trong bản định tuyến. Do vậy ta có thể thực thi chương trình Nemesis nhiều lần và làm cho bộ nhớ của Router đầy.



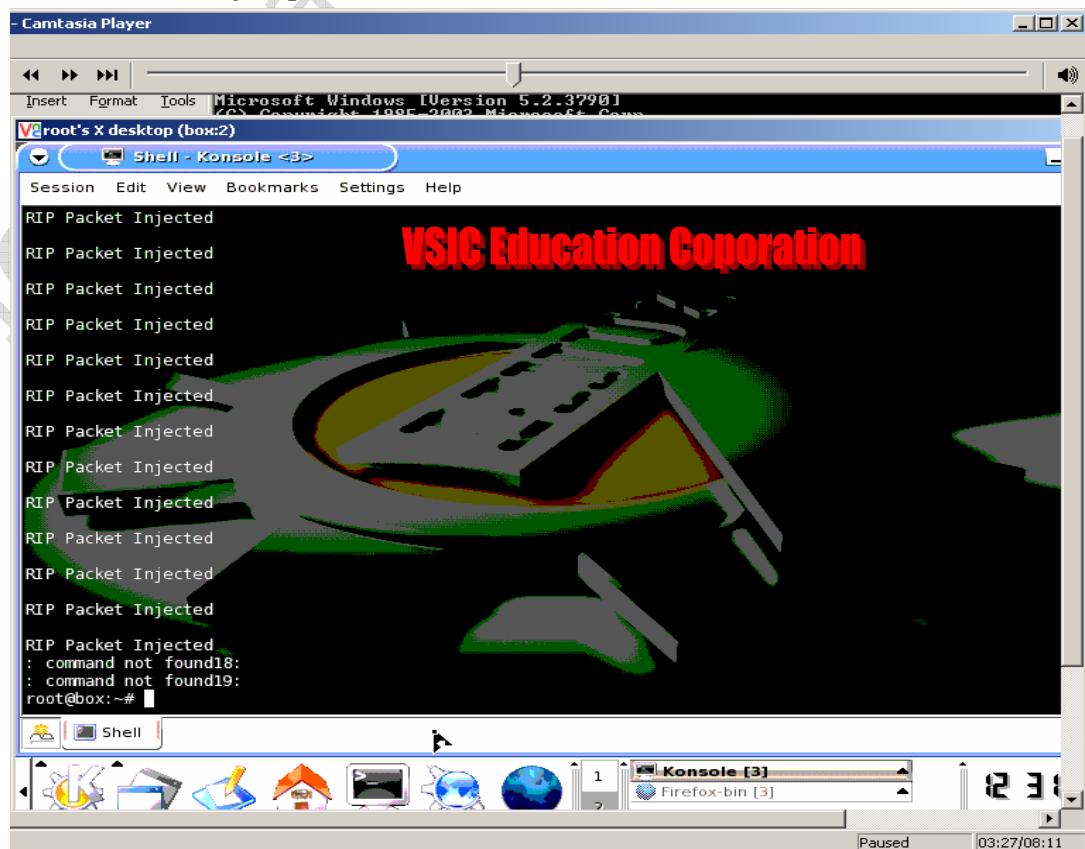
Trước tiên ta thử lệnh sau:

```
nemesis rip -V 1 -c 2 -i 192.168.5.0 -S 192.168.1.51 -D 192.168.1.254
```

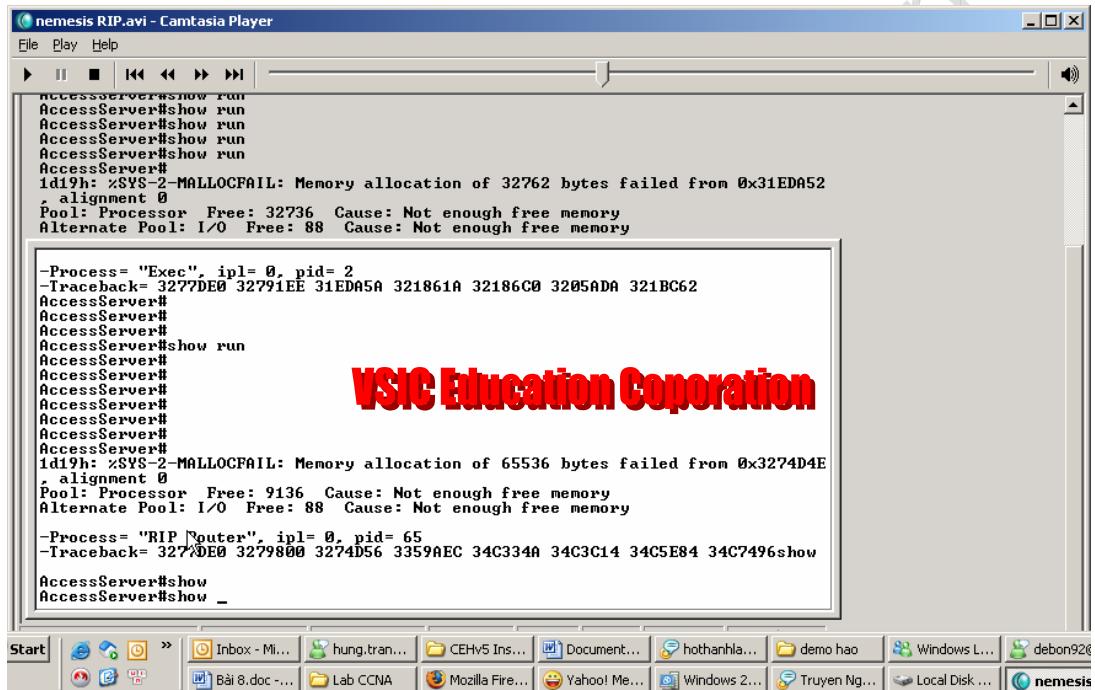
Trong đó **-V 1** là ta đang sử dụng rip version 1, **-c 2** là thông tin update, **-i 192.168.5.0** là route mà chúng ta quảng bá, **-S 192.168.1.51** là địa chỉ nguồn thông tin(có thể không phải là địa chỉ của PC), **-D 192.168.1.254** là địa chỉ của fa0/0 Router VSIC1. Sau khi thực hiện lệnh này, ta kiểm tra trên router đã có route này chưa, sau đó soạn 1 script có các route khác nhau và chạy script.



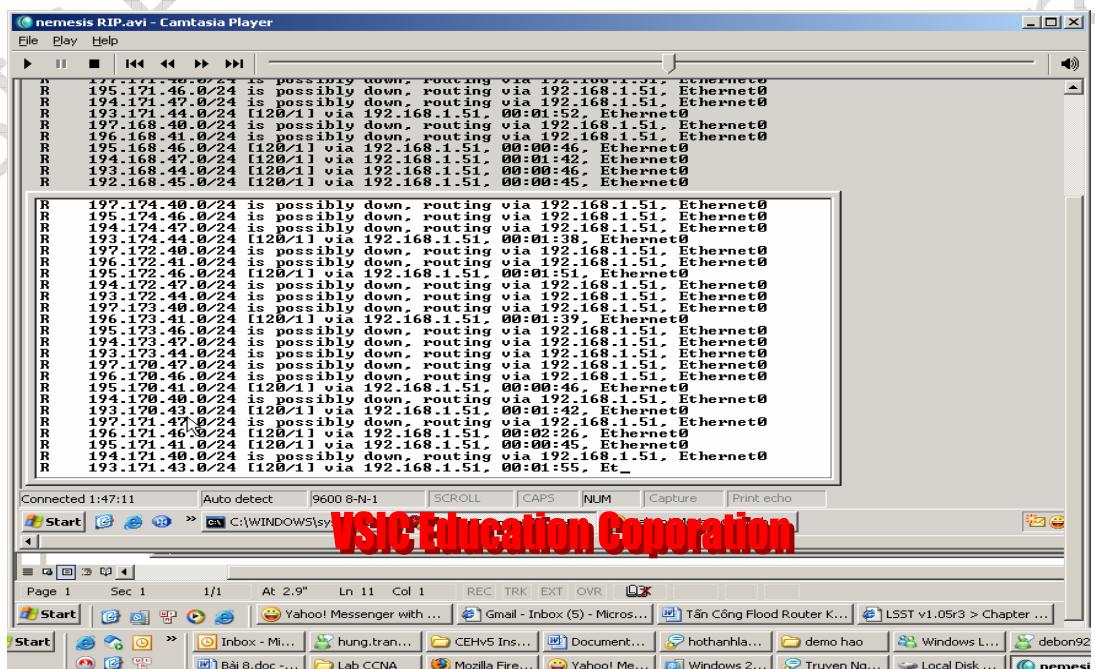
Quá trình inject packet vào Router



Router sẽ bị tràn Memory



Bản định tuyến của Router lúc tấn công



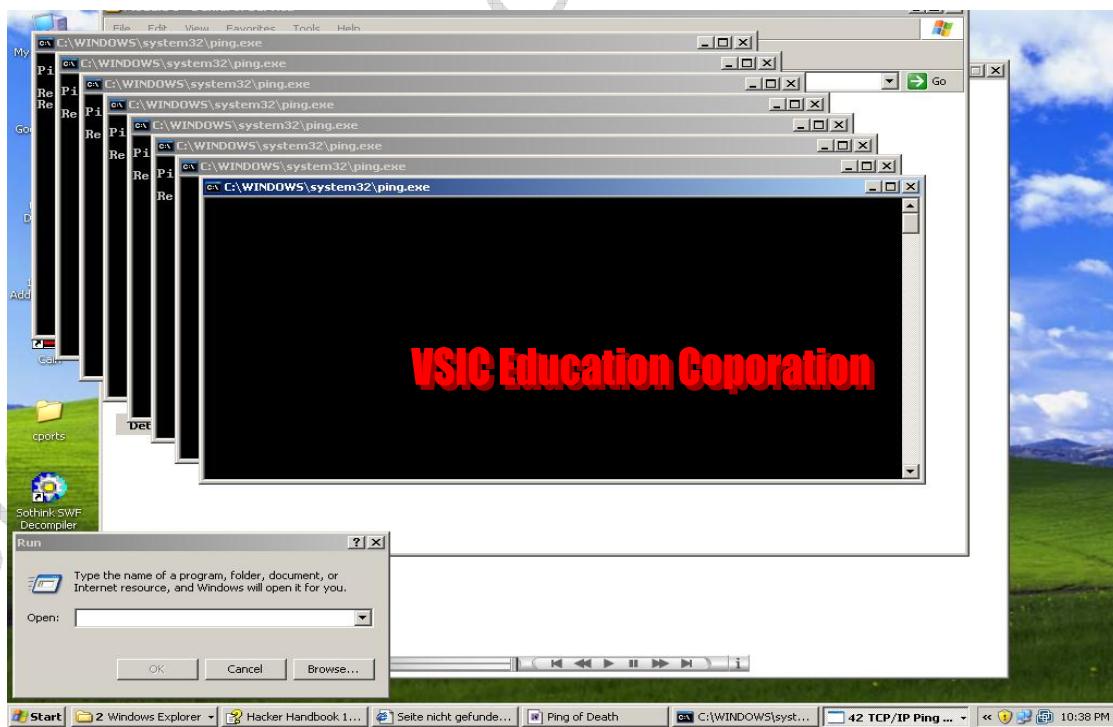
Như vậy với việc chèn vào những thông tin update của giao thức không chứng thực, chúng ta có thể làm cho Router không hoạt động được. Điều này nói lên tầm quan trọng của

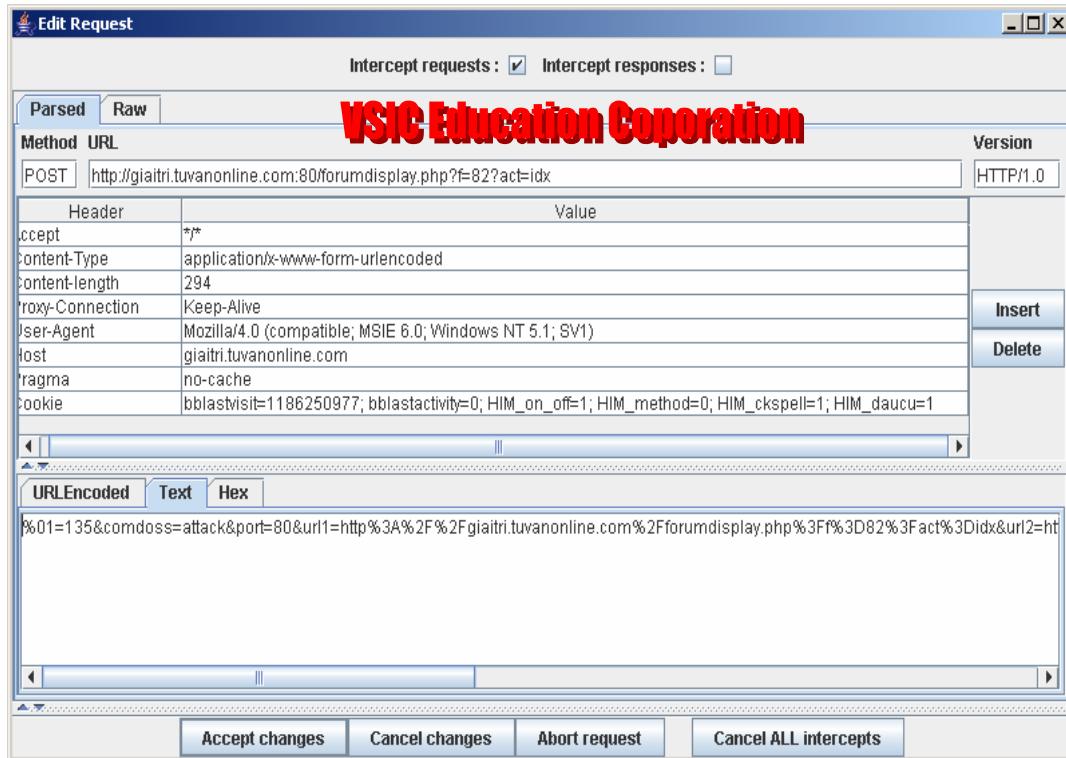
chứng thực. Trung Nemesis còn rất nhiều option về các giao thức ARP, OSPF v.v. Học viên có thể tự test những giao thức còn lại.

Bài Lab 3: Sử dụng flash để DDoS

Ngoài việc tấn công trực tiếp thông qua các giao thức như là RIP, OSPF, ARP v.v. Hacker còn có thể sử dụng các file flash để lén các forum, khi người sử dụng chạy file flash này(có thể là đoạn phim) thì đồng thời sẽ gửi “HTTP POST “ đến nạn nhân. Như vậy nếu như file flash này được tải lên nhiều forum cũng như được nhiều người xem cùng 1 lúc, thì vô tình các Server chứa các file này đã tấn công DoS vào Server nạn nhân.

Ta sử dụng file Flash trong CD (Module 8)sau đó, chạy file này bằng internet explorer, phân tích bằng webScarab proxy.





File flash mở rất nhiều của số Internet Explorer và mỗi explorer gửi “HTTP POST” về phía Server nạn nhân.