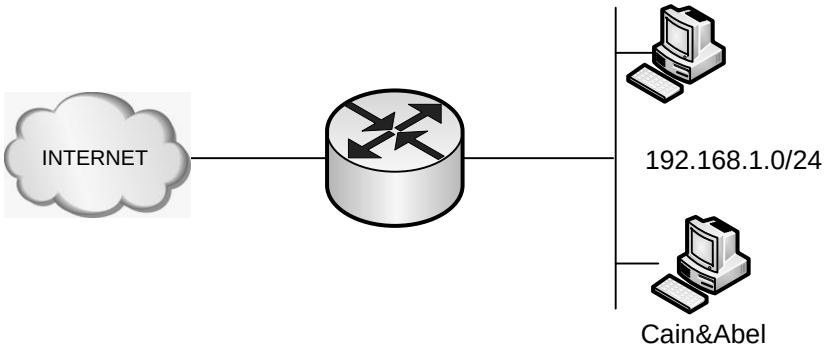
LAB – Sử dụng công cụ Cain & Abel



Mô tả

Cain & Abel là chương trình tìm mật khẩu hoạt động trên hệ điều hành Windows. Nó cho phép dễ dàng tìm ra nhiều loại mật khẩu bằng cách dò tìm trên mạng, giải mã 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 dựa trên các kỹ thuật lưu trữ mật khẩu, phát hiện mật khẩu có trong bộ đệm và phân tích các giao thức định tuyến.

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 cần thiết từ nhiều nguồn.

Trong bài Lab này ta dùng Cain & Abel để làm thay đổi bảng ARP hay giả mạo địa chỉ MAC của những thiết bị được giám sát và từ đó có thể phân tích nội dung của lưu lượng, có được các thông tin nhạy cảm từ một số giao thức cụ thể.

Cấu hình trên Router

```
Router#show run
Building configuration...
Current configuration : 1174 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
```

```
no service password-encryption
!
hostname Router
!
memory-size iomem 15
ip subnet-zero
!
ip cef
!
interface FastEthernet0/0
 ip address dhcp
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
ip classless
ip http server
no ip http secure-server
ip nat inside source list 1 interface FastEthernet0/0 overload
access-list 1 permit 192.168.1.0 0.0.0.255
```

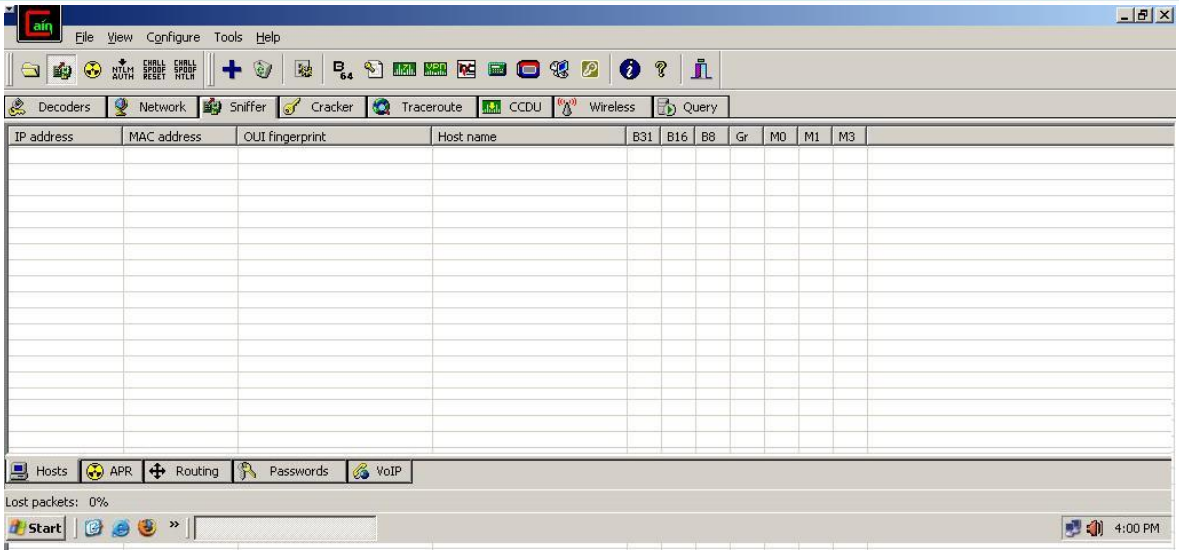
Cấu hình CAIN

Bật tính năng Sniffer (hình 1).

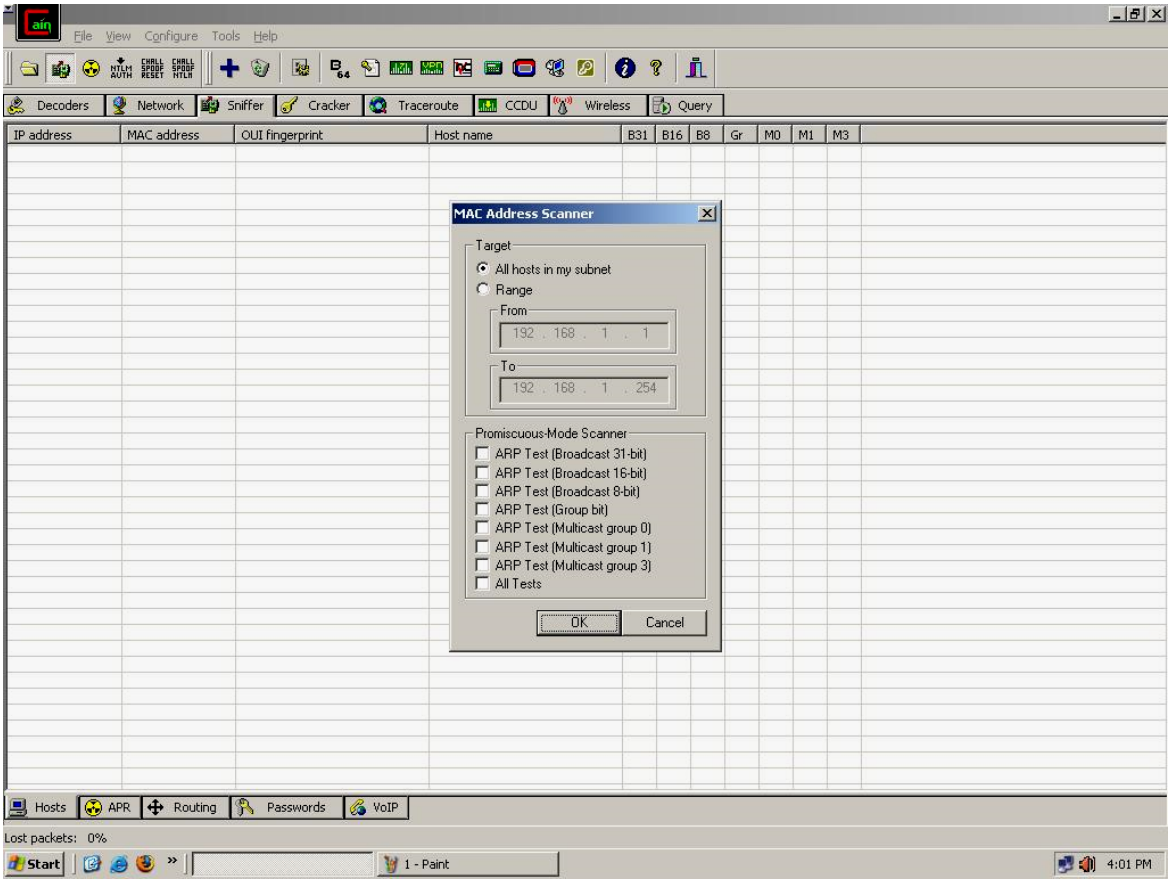
Chọn tab Sniffer → chọn vào dấu "+" để quét các host đang tồn tại trong mạng tấn công. Trong cấu hình này ta chọn quét tất cả các host trong subnet (192.168.1.x/24) → chọn "OK" (hình 2). Xem kết quả ở hình 3.

Trong tab Sniffer -> chọn tab APR (hình 4).

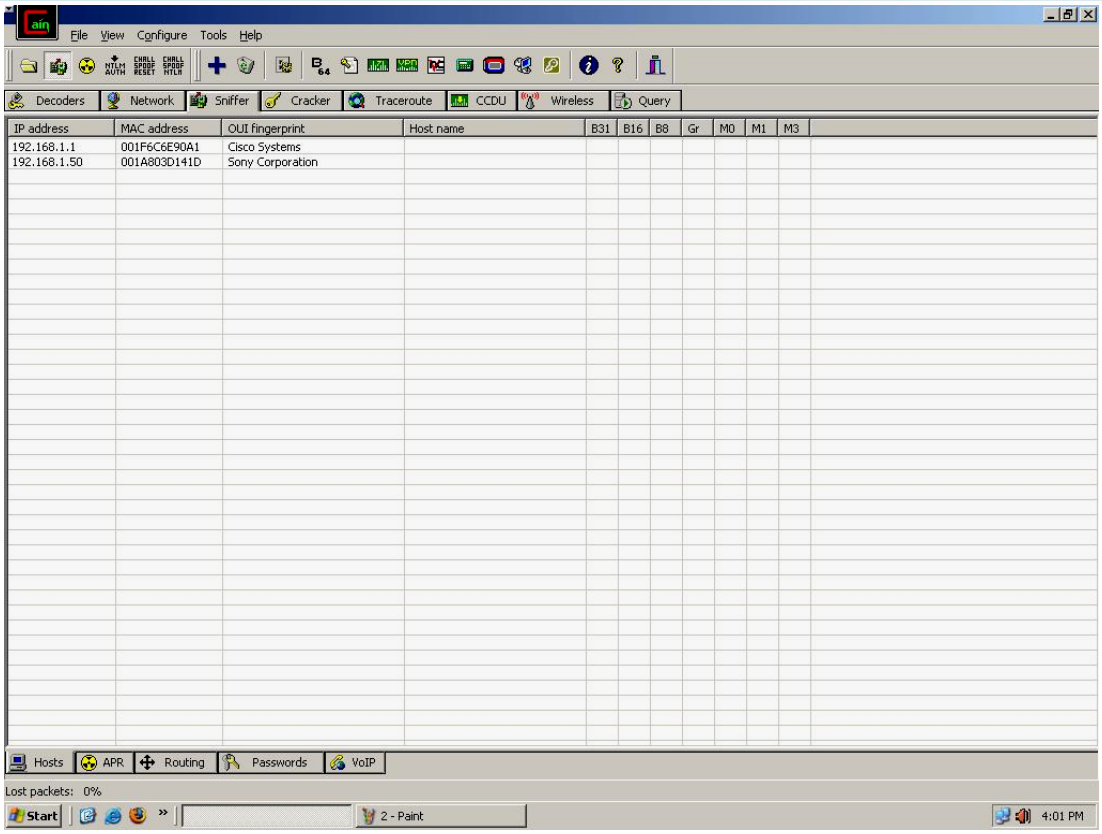
Start ARP Poisoning → bấm chuột vào dấu "+" để chọn host cần tấn công (bên trái) và Default Gateway Router (bên phải) → bấm "OK" → xem kết quả hình 5.



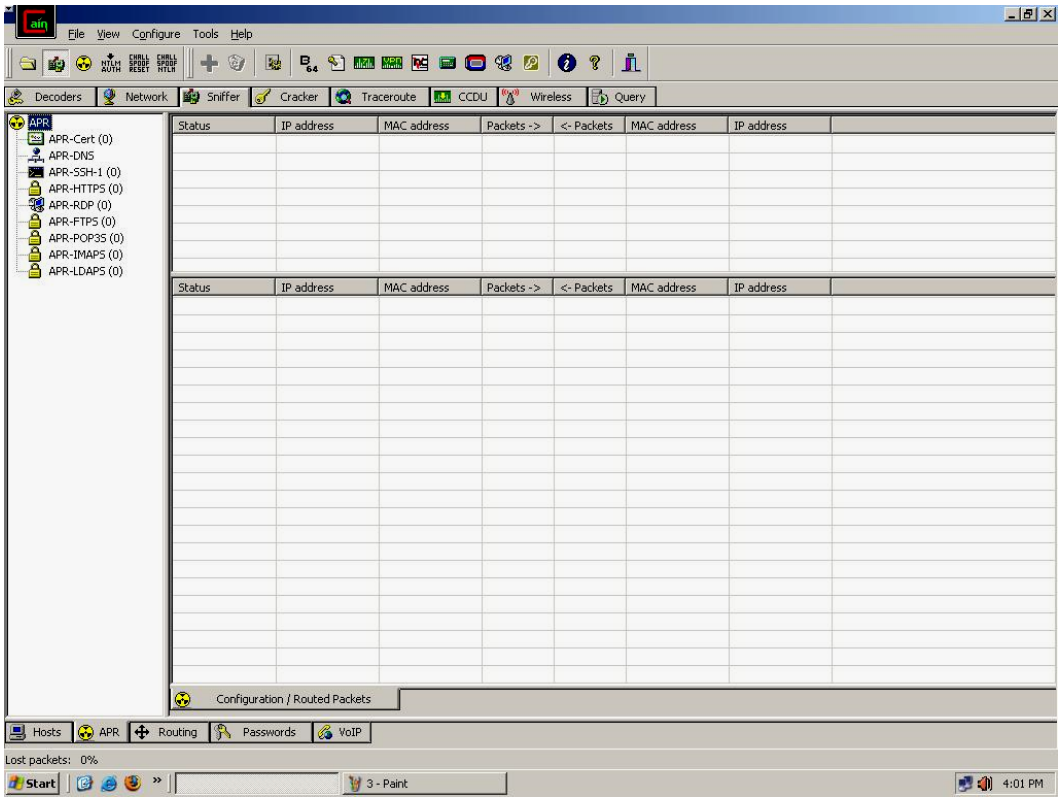
Hình 1: Bật Sniffer



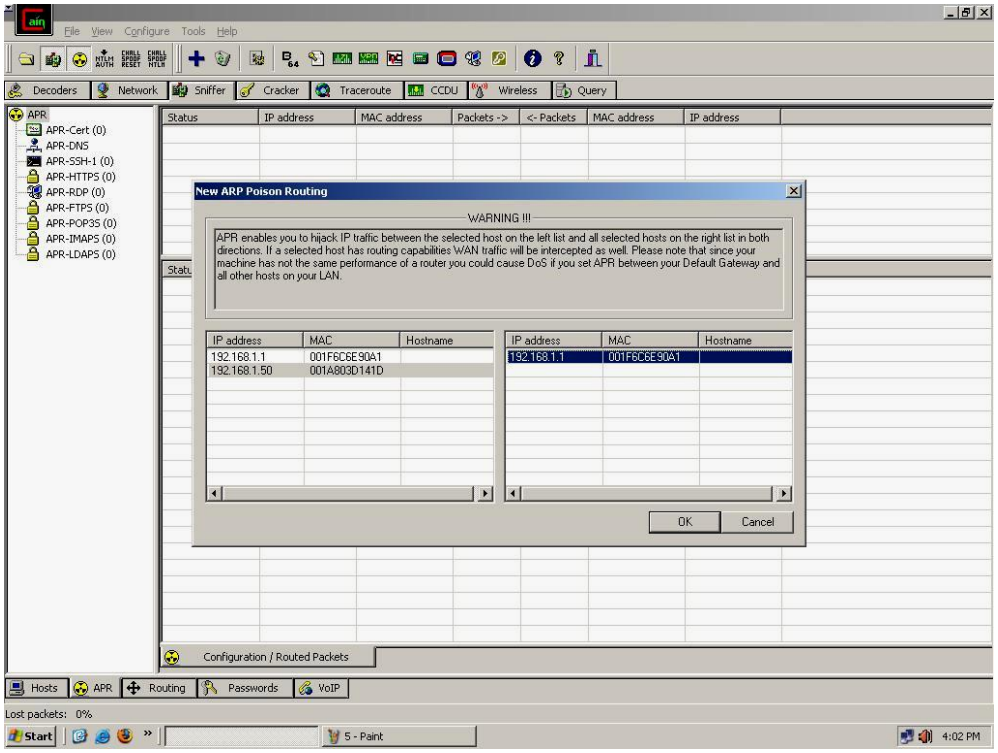
Hình 2: Quét các Host



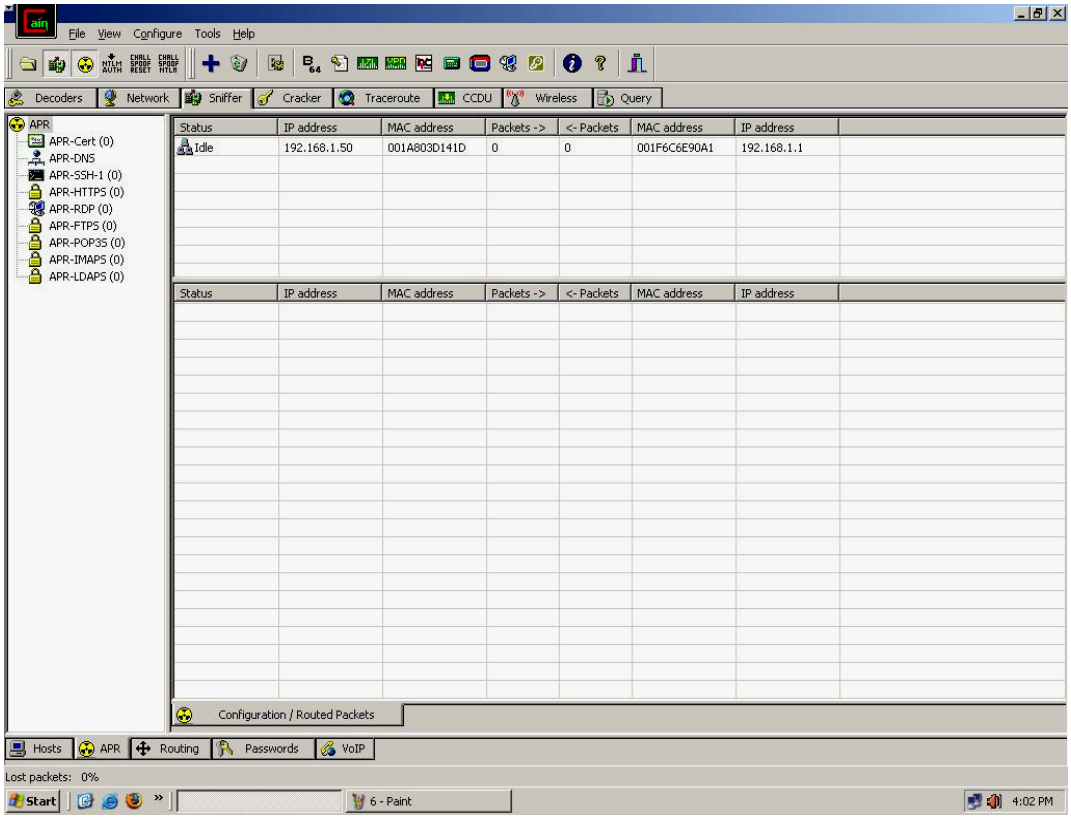
Hình 3: Kết quả



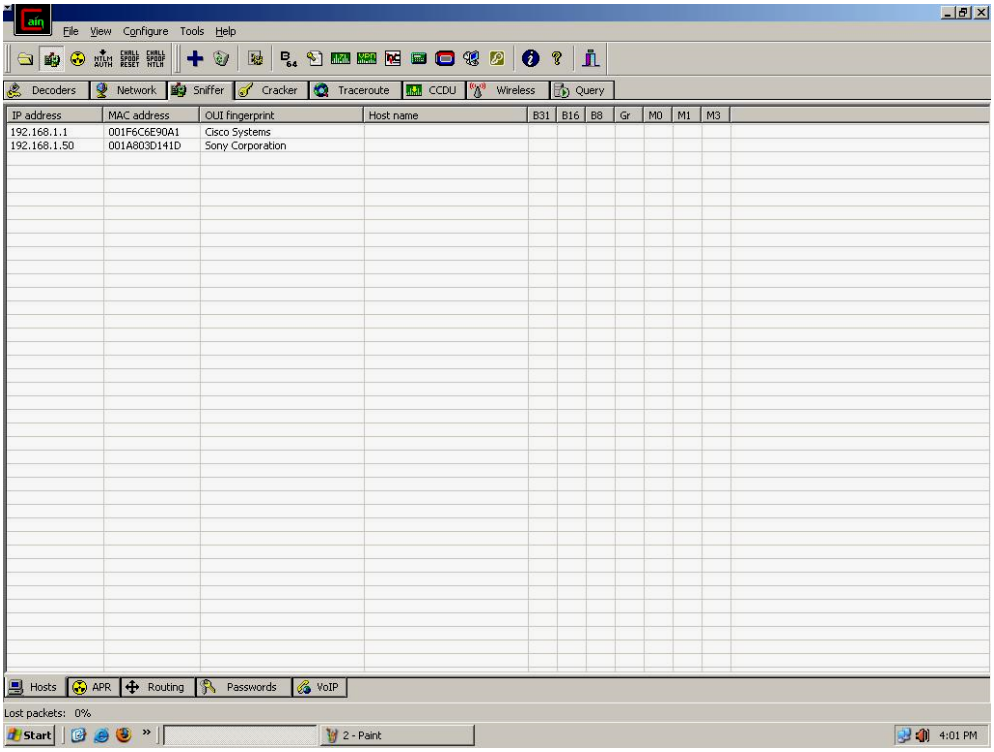
Hình 4: Chọn APR



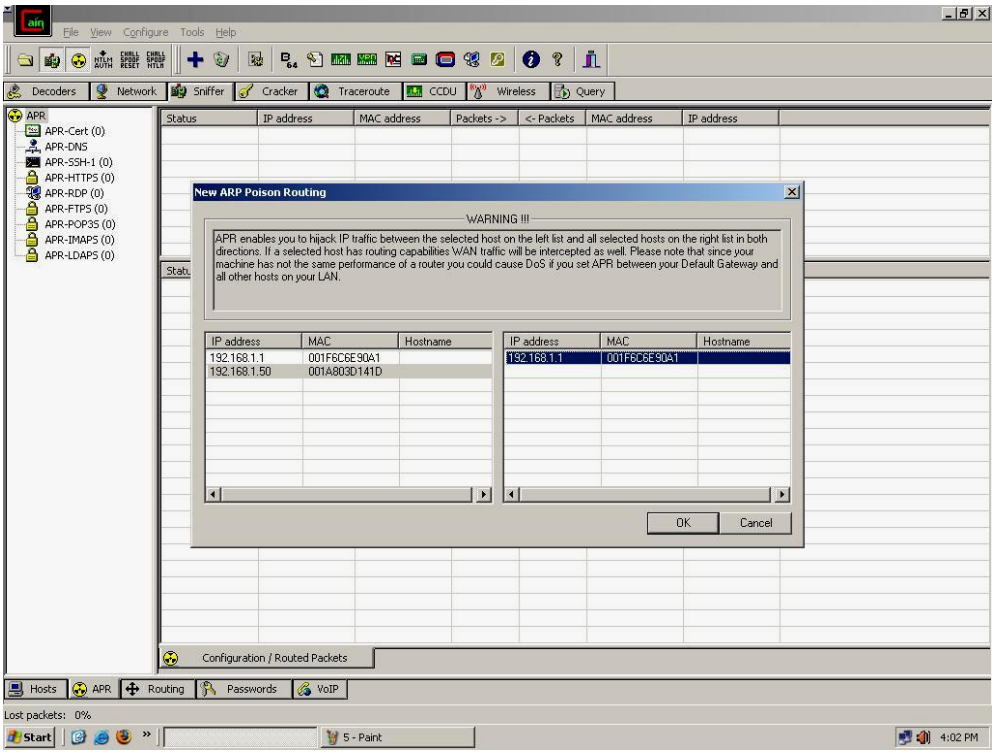
Hình 5



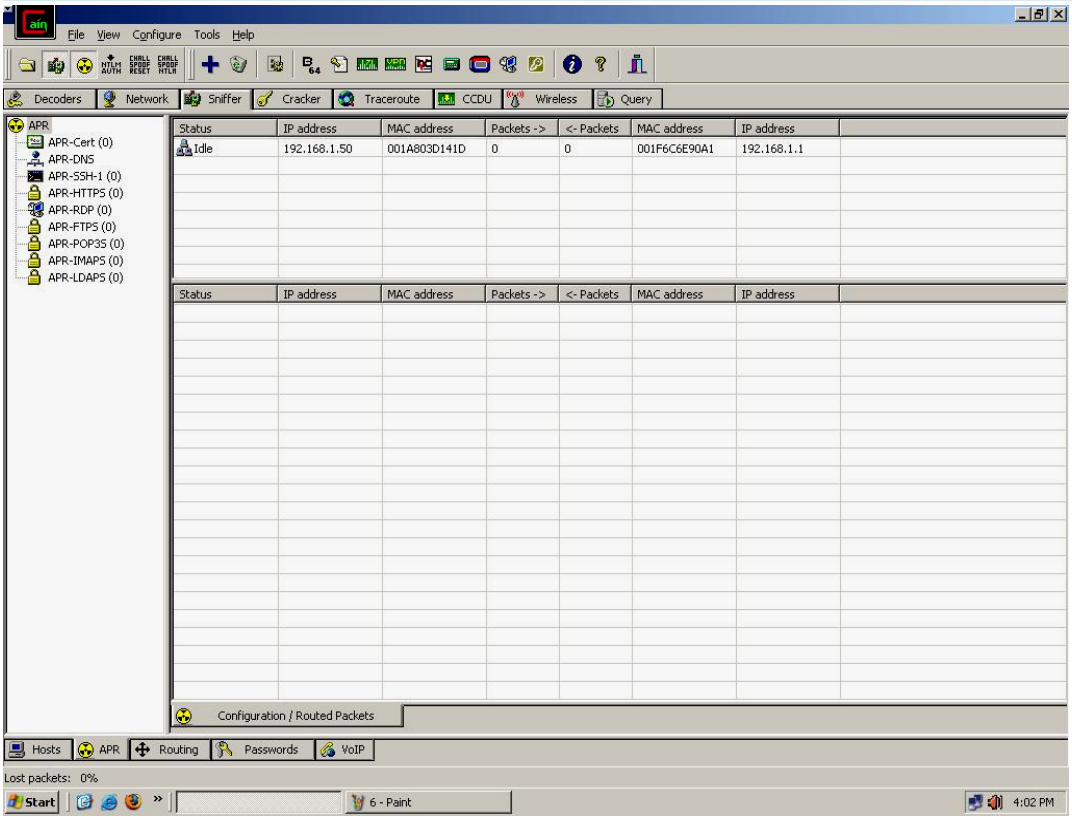
Hình 6:



Hình 7



Hình 8



Hình 9

Kiểm tra

Đến bước này bạn đã hoàn tất việc chuẩn bị bắt gói và thu thập các thông tin. Bước tiếp theo tiến hành kiểm tra xem khi một máy tính nằm trong mạng, truy cập vào hộp thư Yahoo mail có độ bảo mật rất cao có thể bị lấy mất username và password không?

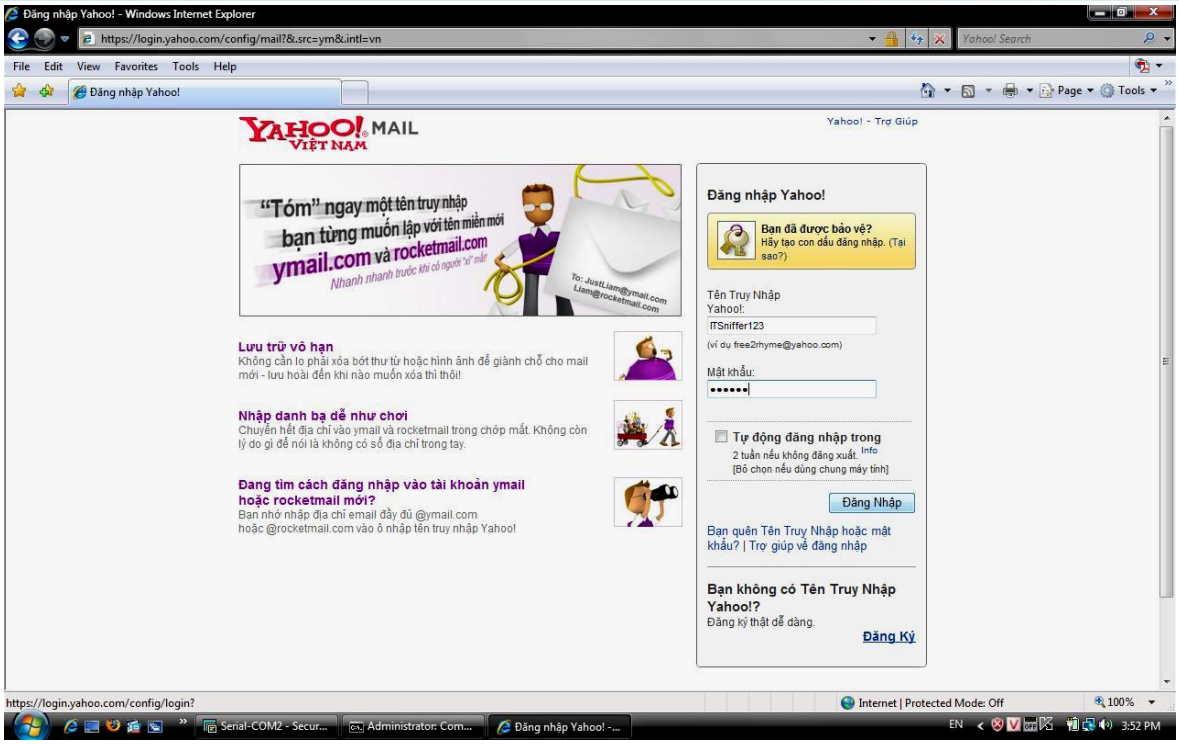
1. Đăng nhập vào hộp thư Yahoo (hình 10).

2. Sau khi nhập username và password → chọn "Đăng Nhập".

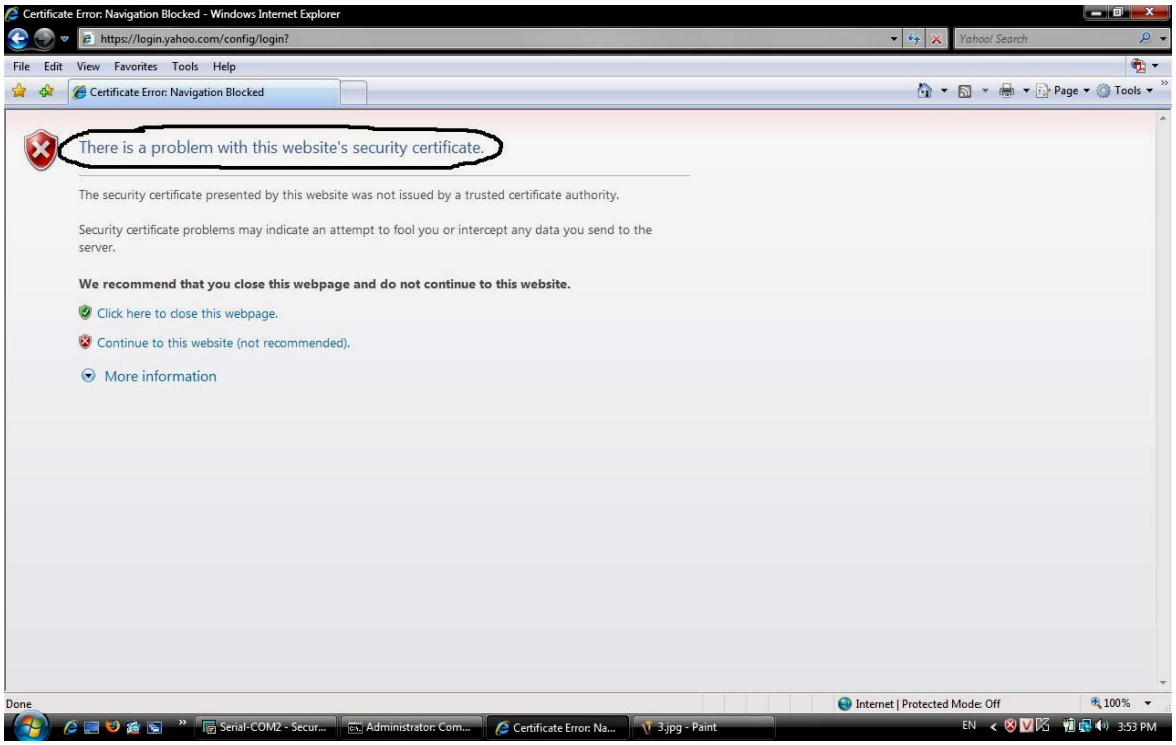
Bình thường sau khi bấm "Đăng Nhập" ta sẽ vào ngay hộp thư của mình nhưng nhìn hình ta thấy trình duyệt IE 7.0 thông báo "*There is a problem with this website's security certificate*" như vậy là có vấn đề xảy ra và thông tin username và password của user đã bị mất (hình 11).

3. Bấm chuột vào hàng chữ "*Continue to this website (not recommended)*" khi đó ta sẽ vào được hộp mail của mình.

4. Giờ ta sẽ kiểm tra trước và sau khi bật tính năng ARP Poisoning đã tác động như thế nào đến máy VICTIM (hình 12, 13)?



Hình 10: Đăng nhập Yahoo

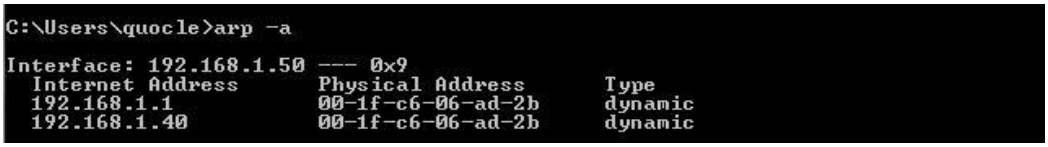


Hình 11: Cảnh báo bảo mật

Trước

Hình 12

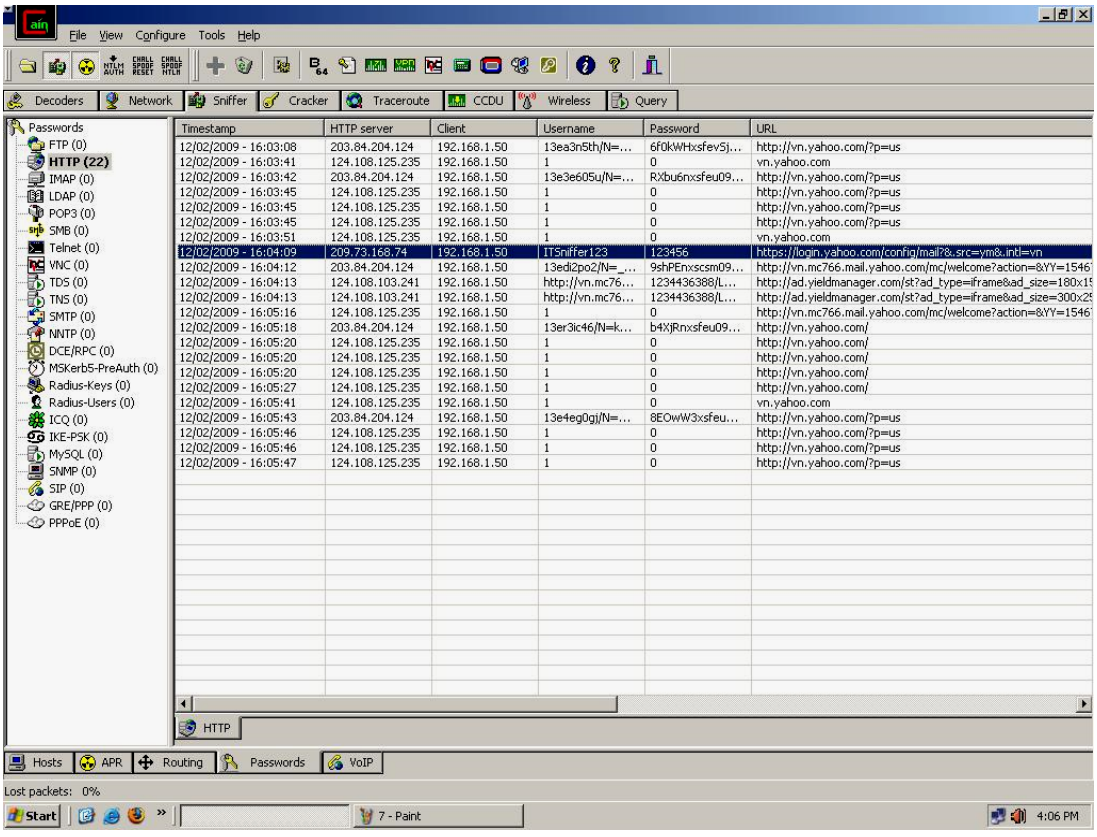
Sau



Hình 13

Kết quả: Máy 192.168.1.50 đã bị giả mạo địa chỉ MAC khiến cho các gói tin đi từ 192.168.1.50 ra Gateway giờ bị chuyển tiếp sang ATTACKER (192.168.1.40).

5. Kiểm tra CAIN để lấy thông tin username và password đã bắt được. *Xem kết quả hình 2.16 phần được tô màu xanh đậm*



Hình 14