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 Vân 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.

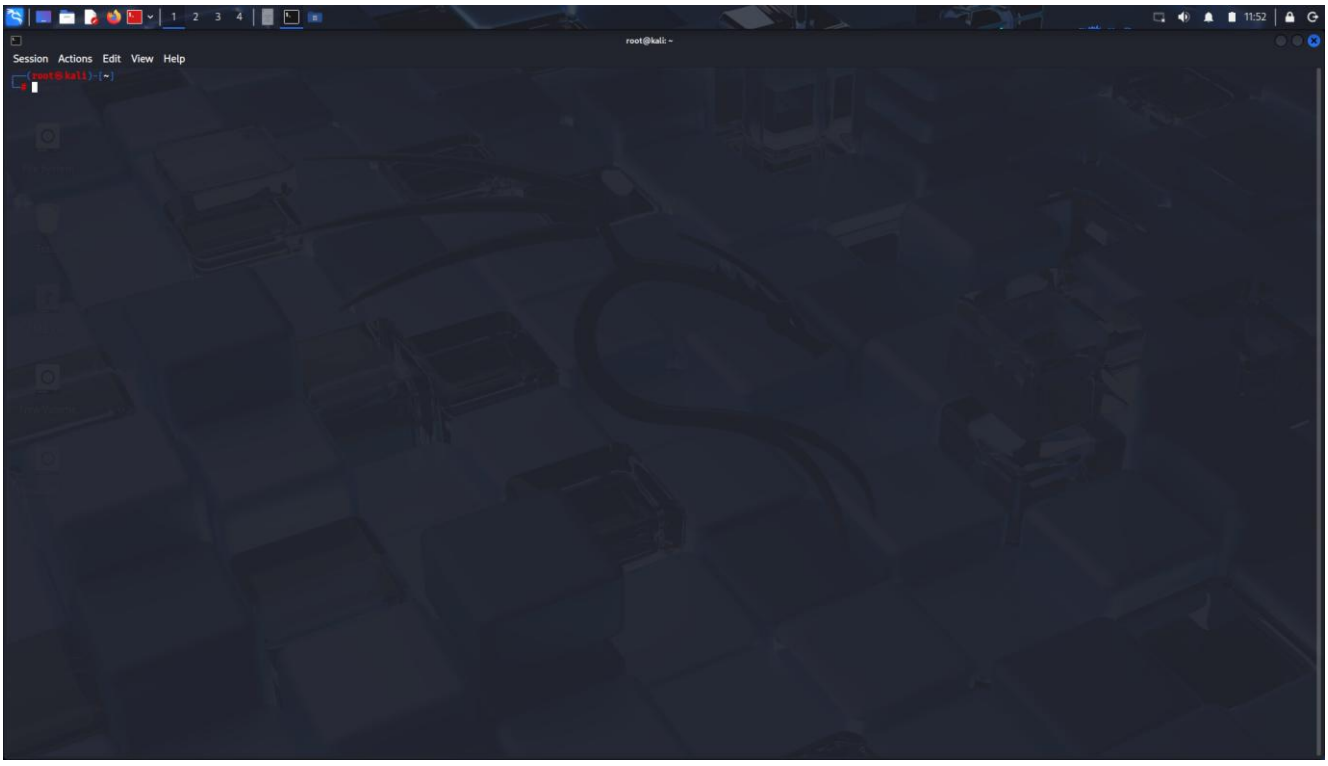
Lưu ý: Tùy từng dòng máy mà cách vào menu boot sẽ khác nhau. Ngoài ra, nên tạm thời vô hiệu hóa chế độ **Secure Boot** tại BIOS để có thể boot trực tiếp từ USB đã tạo.

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)

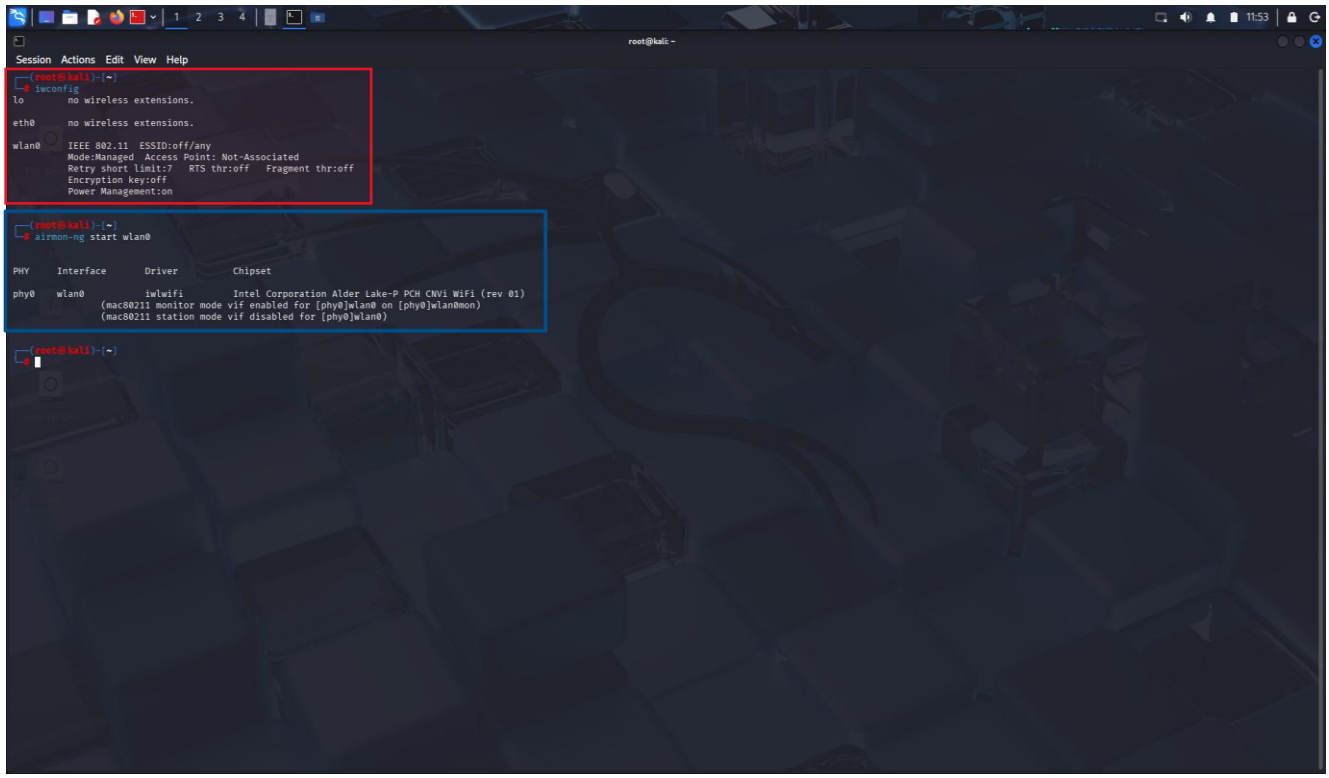
Bước 1: Mở Terminal để thực hiện các câu lệnh



Hình 1: Terminal được mở

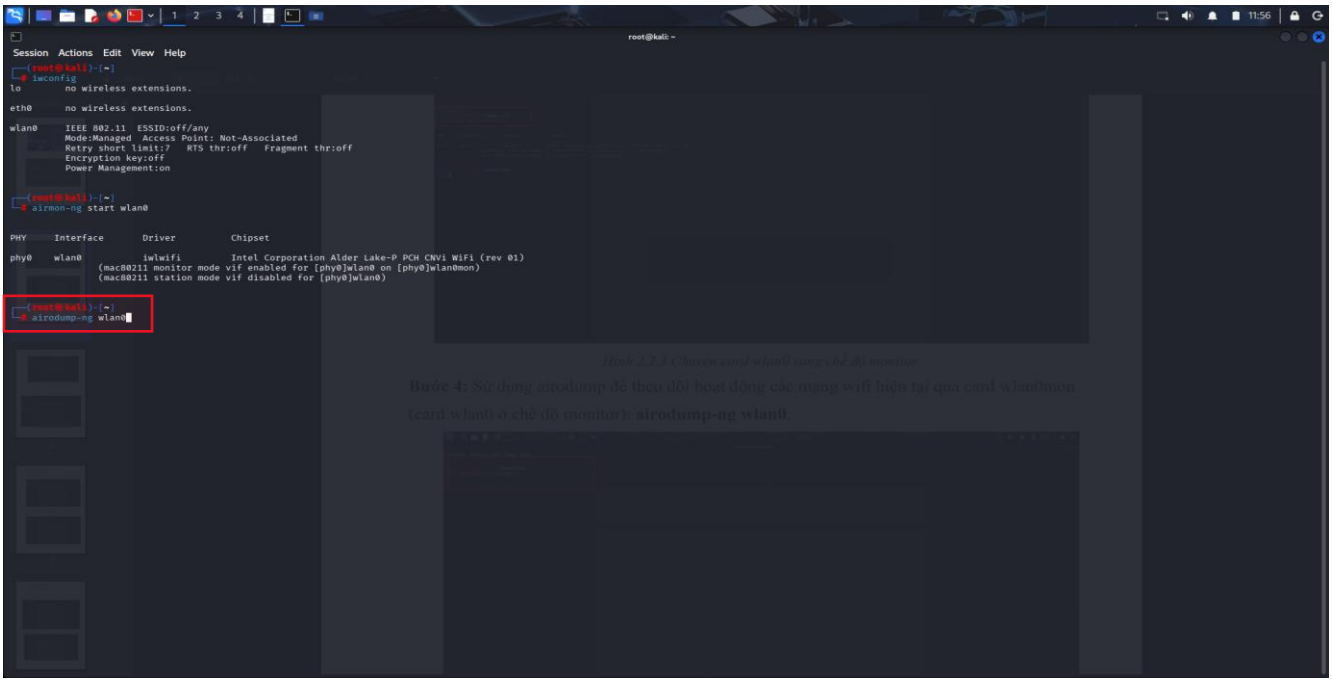
Bước 2 (được khoanh vùng màu đỏ ở hình 2): Kiểm tra tên card Wireless đang sử dụng bằng lệnh **iwconfig**.

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**



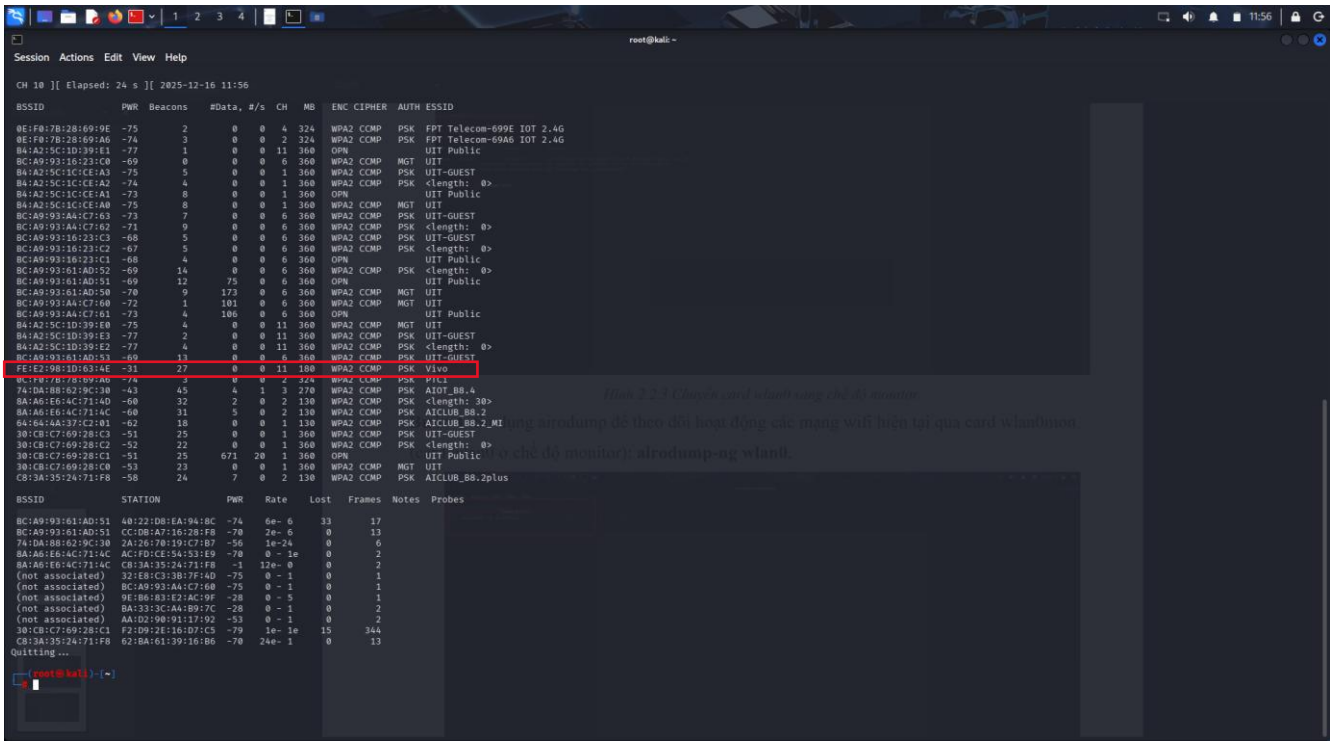
Hình 2: Kiểm tra tên card Wireless đang sử dụng.

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**.



Hình 3

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

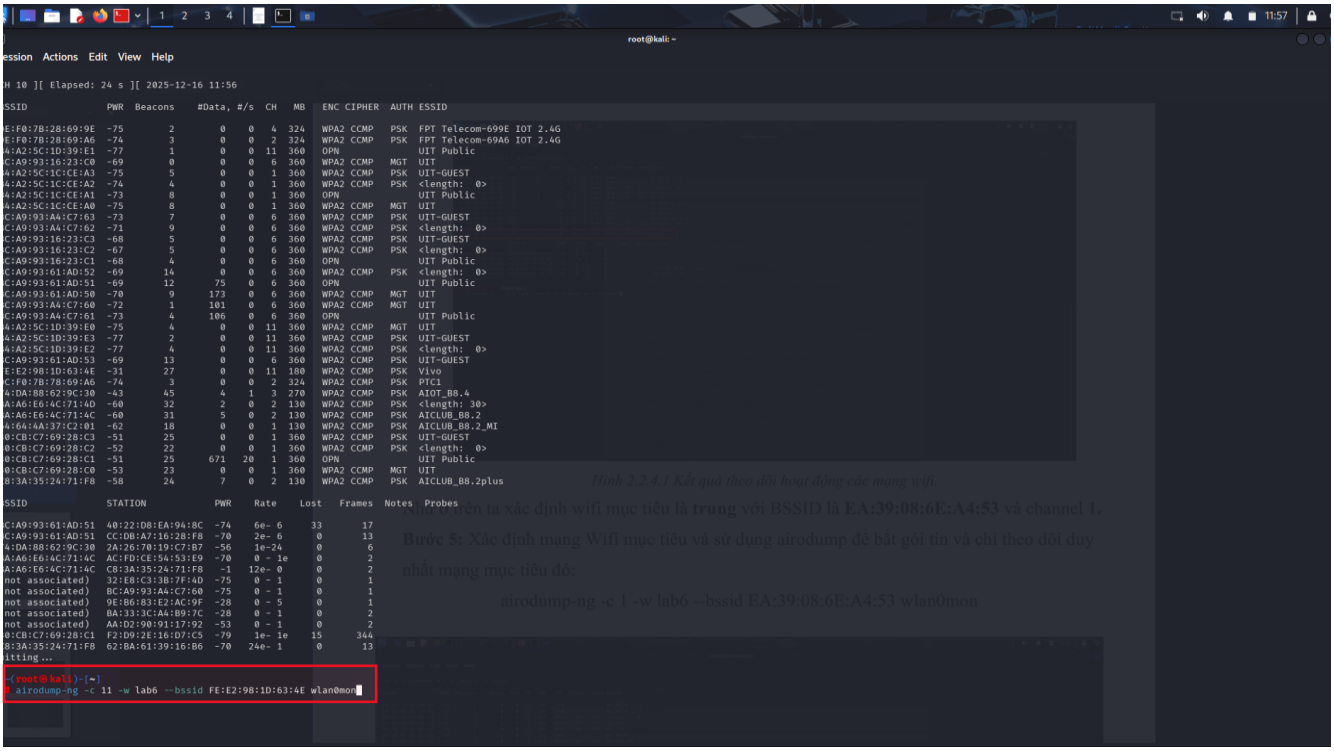


Hình 4: Kết quả theo dõi hoạt động các mạng wifi

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:

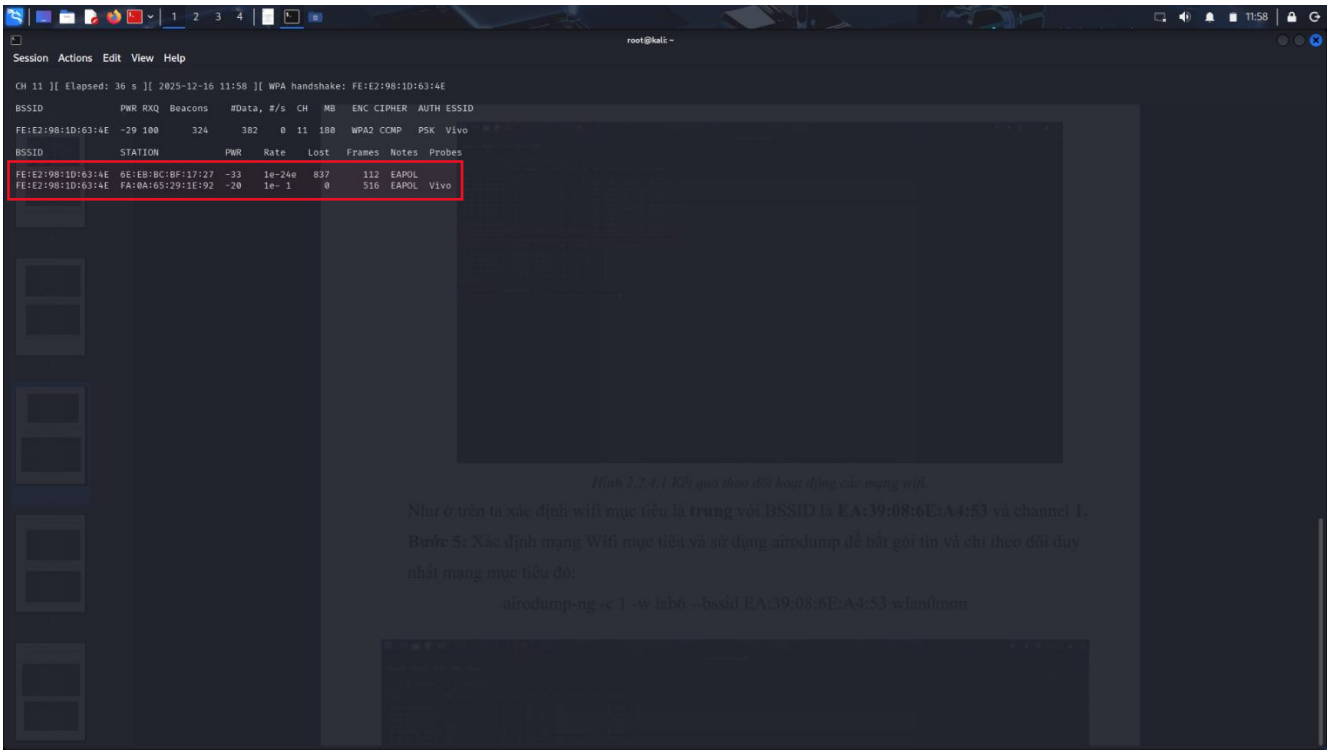
airodump-ng -c 11 -w lab6 --bssid FE:E2:98:1D:63:4E wlan0mon



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

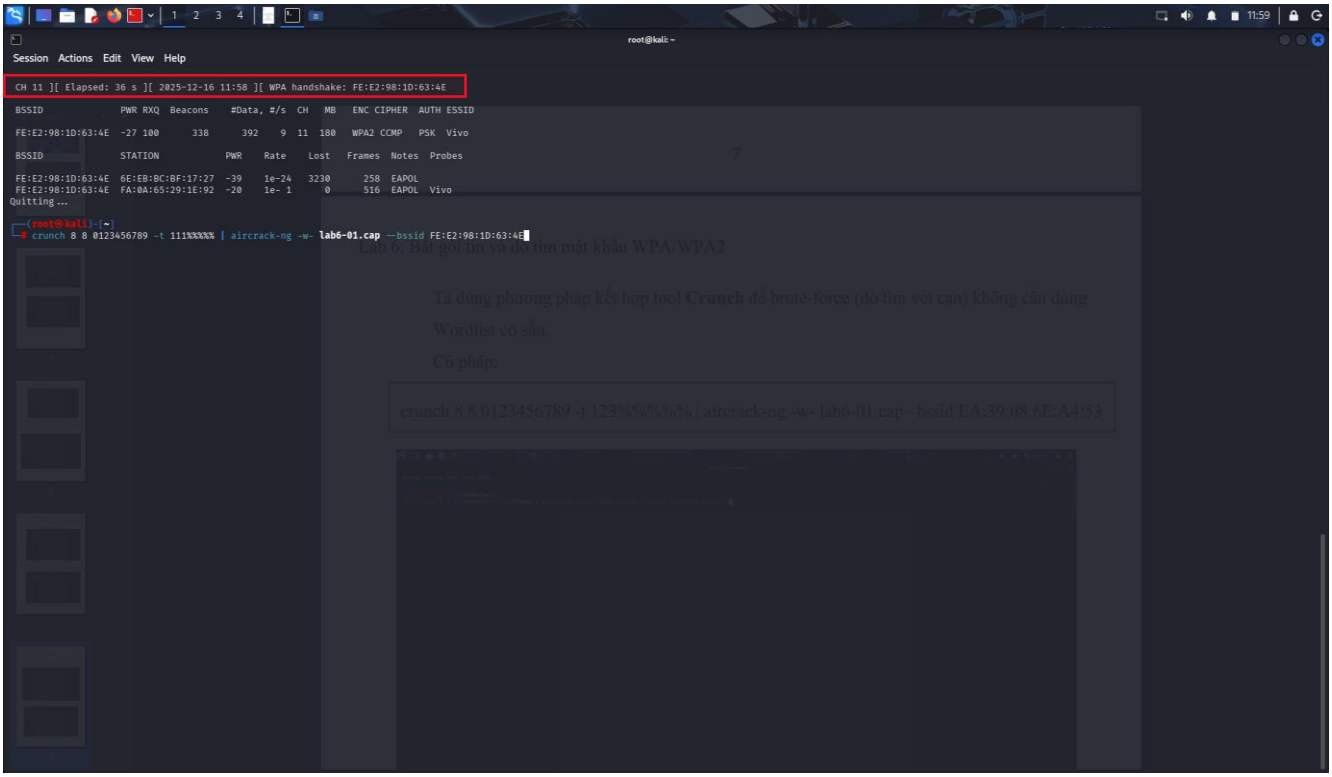
Bước 6: Thu thập gói tin bắt tay WPA handshake (bắt tay 4 bước) trong quá trình đăng nhập để dựa vào đó dò tìm mật khẩu. Dùng cách chờ người dùng nào đó đăng nhập vào wifi đang theo dõi.

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



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

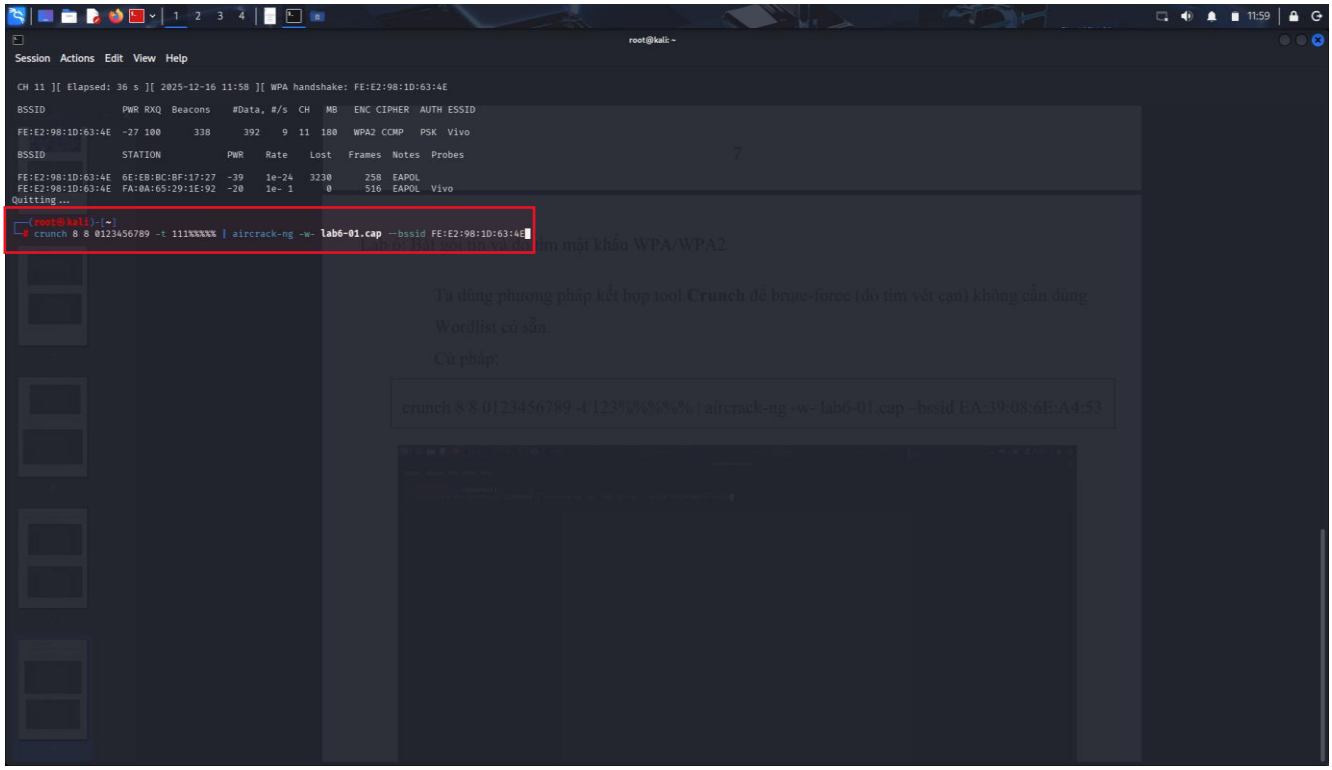
Bước 7: Thực hiện chờ đến khi nhận được gói tin WPA handshake của mạng mục tiêu tương ứng, ta dừng quá trình bắt gói tin (Ctrl+C) và tiến hành dò tìm mật khẩu dựa vào file .cap đã bắt được.



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

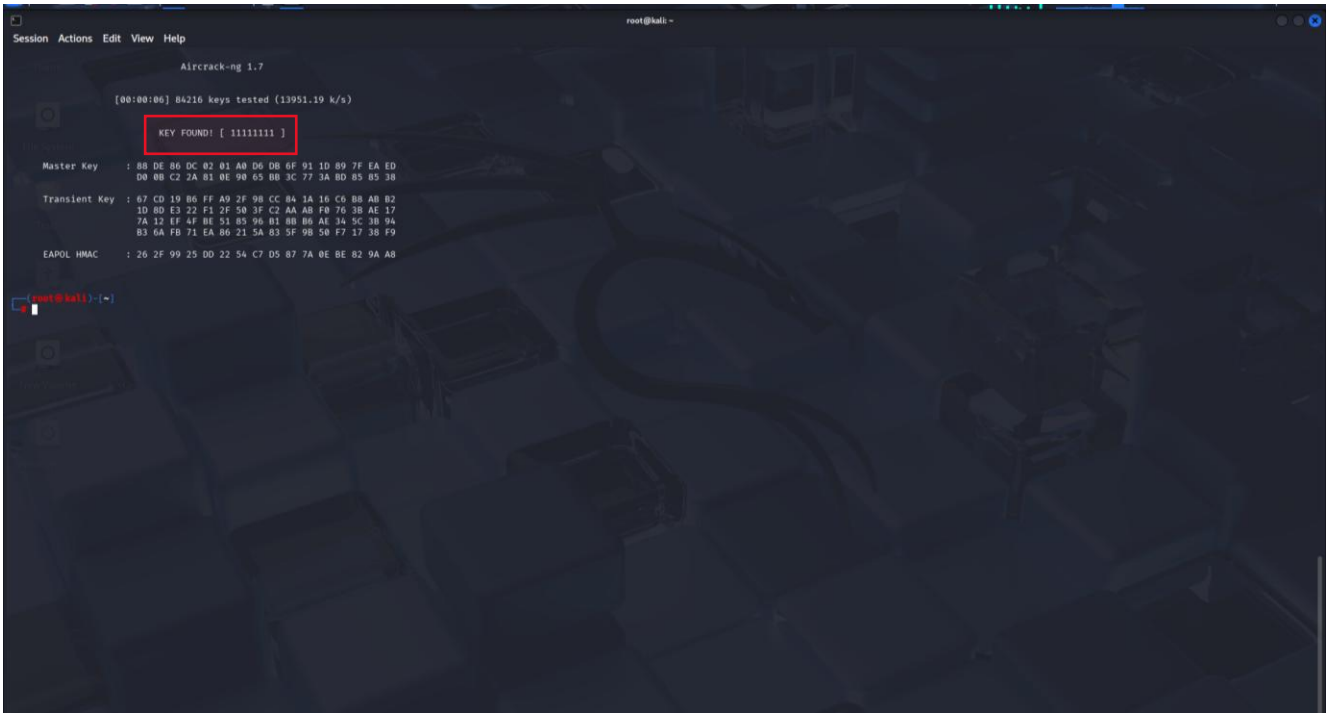
Ta dùng phương pháp kết hợp tool **Crunch** để brute-force (dò tìm vét cạn) không cần dùng Wordlist có sẵn. Cú pháp:

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



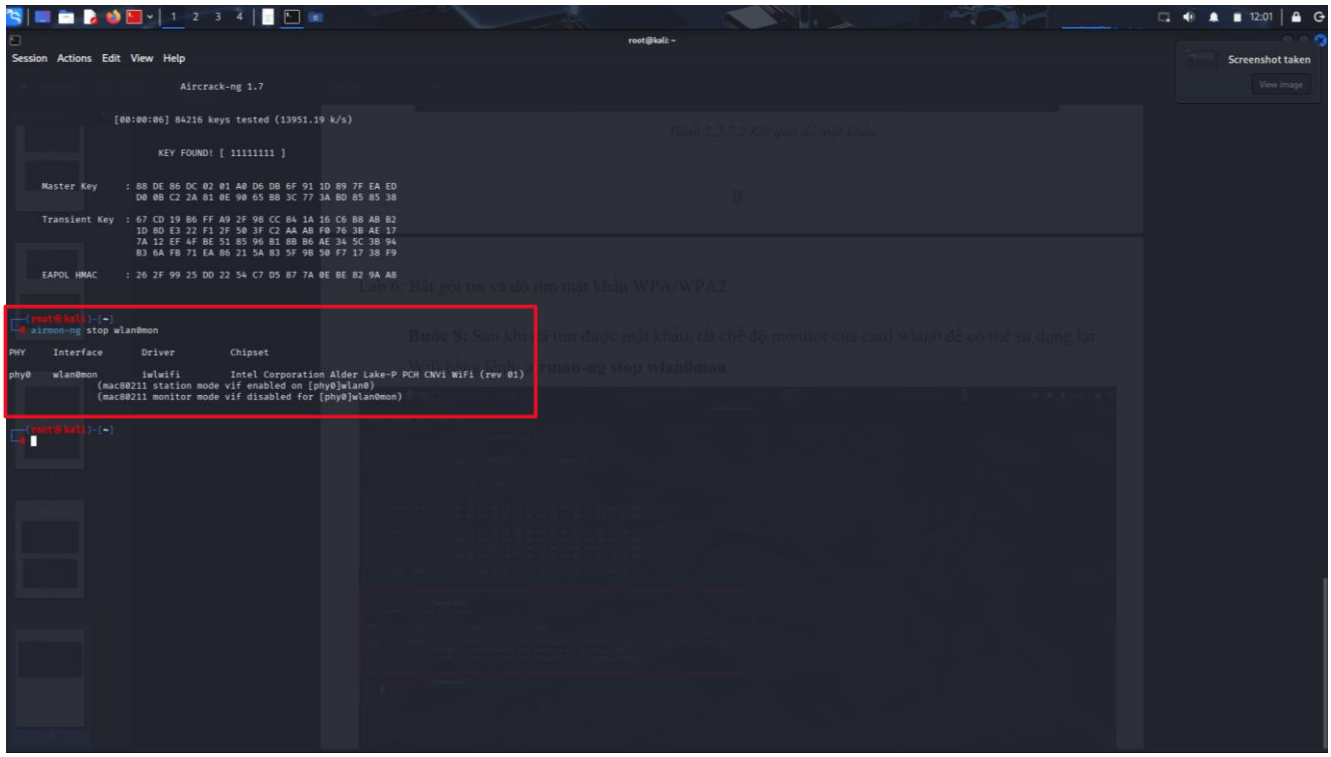
Hình 8: Tiến hành dò tìm mật khẩu dựa vào file .cap đã bắt được

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**



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**