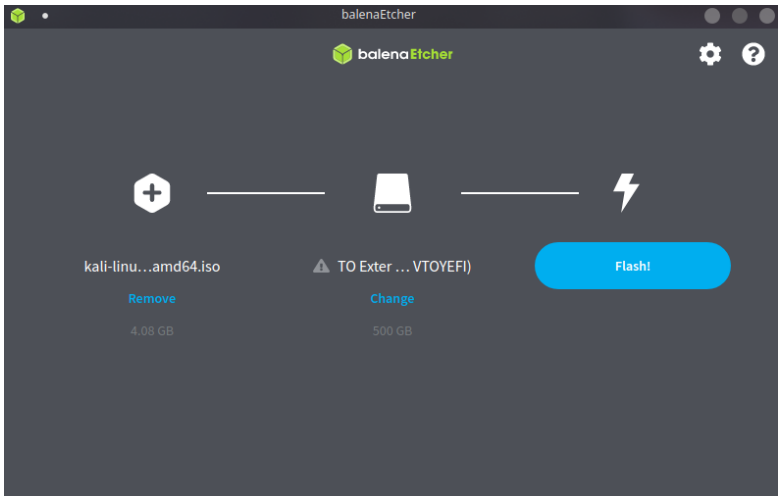
THỰC HÀNH NHẬP MÔN MẠNG MÁY TÍNH
Lab 6 - Scanning WPA_WPA2 Passwords

Họ và Tên: Lê Hoàng Khánh
MSSV: 21522205
Lớp: IT005.N12.MMCL

I. Tạo USB Boot và Boot vào Kali Linux

Sử dụng Etcher để tạo USB boot, ở đây chúng ta có thể sử dụng các phần mềm khác để tạo USB Boot như Rufus, Unetbootin… Hình 1 cho thấy config để tạo USB Boot sử dụng Etcher.



Hình 1

Truy cập vào BIOS của máy tắt tính năng Secure Boot sau đó vào Boot Menu chọn đến USB Boot mà chúng ta vừa tạo từ các bước ở trên. Nếu thành công chúng ta sẽ truy cập được vào Boot Menu của Kali Linux như Hình 2.

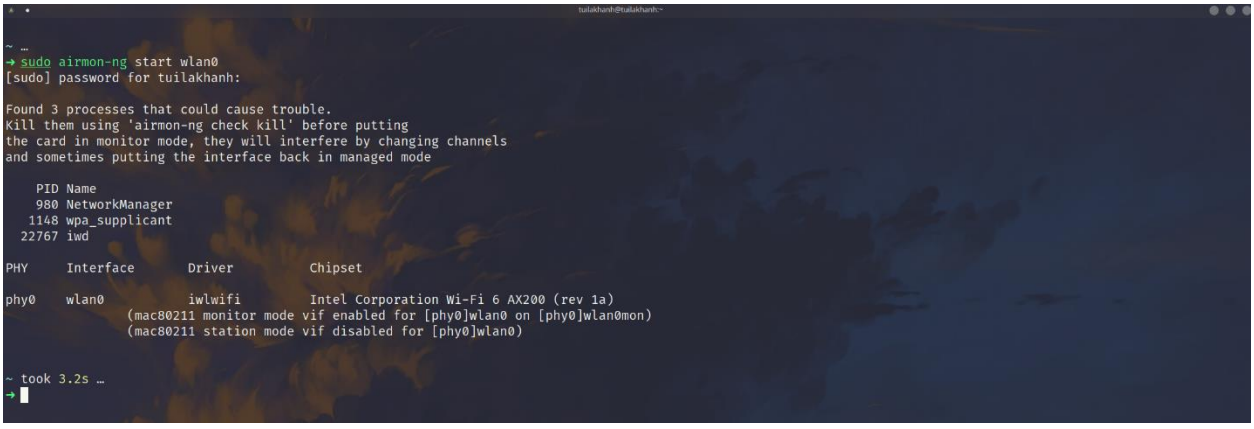
Hình 2

II. Dò tìm mật khẩu với bộ công cụ Aircrack-NG

Tôi sẽ sử dụng Linux đã được cài sẵn trên máy thay vì sử dụng Kali Linux để thuận tiên cho quá trình thực hành. Thông tin về phiên bản Linux được đề cập ở Hình 3.

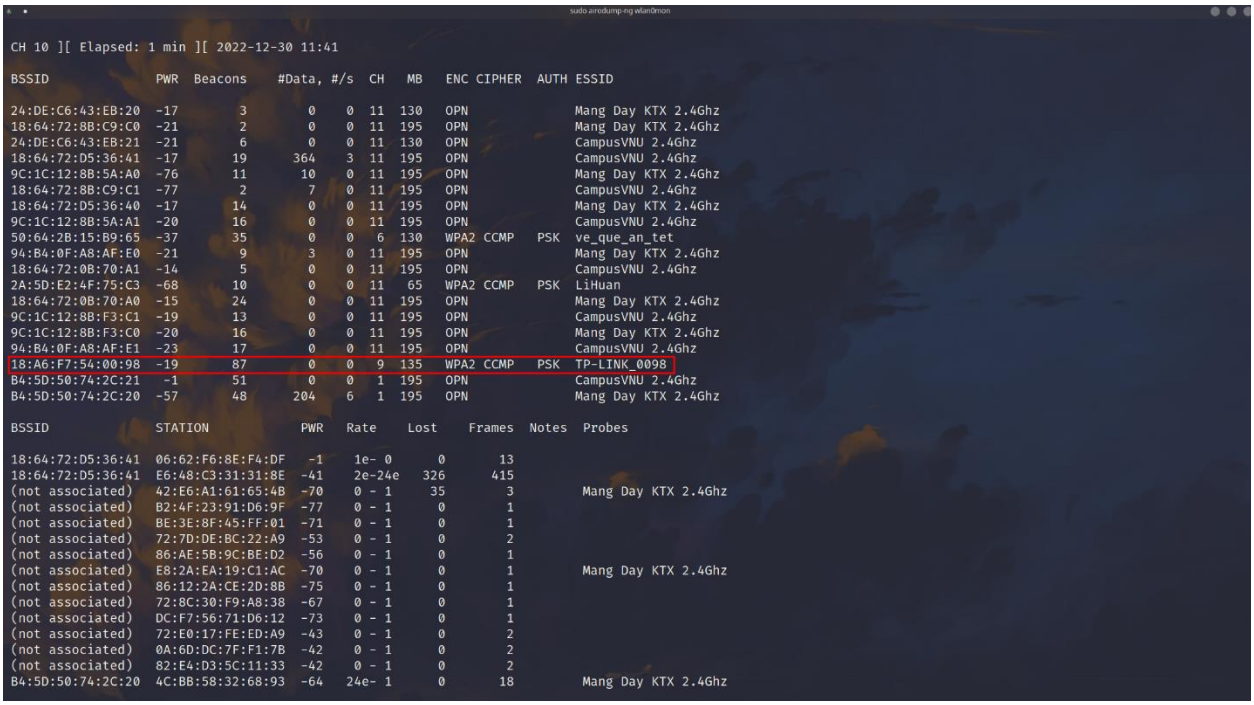
Hình 3

Card wifi mà máy đang sử dụng là năm ở interface **wlan0**. Sau đi xác định được interface của card wifi ta tiến hành chuyển card wifi sang chế độ monitor bằng lệnh **airmon-ng**. Kết quả và lệnh đã nhập chi tiết ở Hình 4.



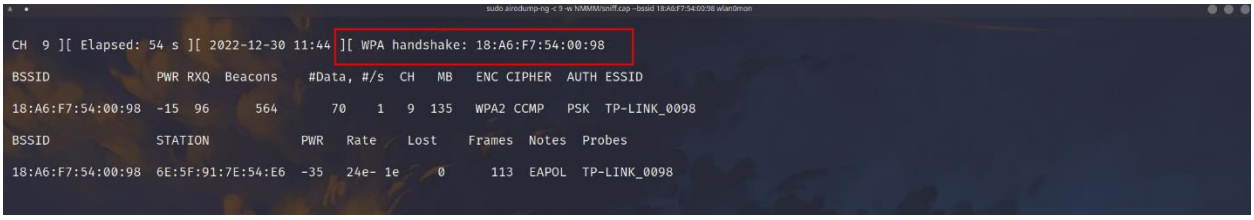
Hình 4

Sử dụng **airodump** để theo dõi hoạt động các mạng wifi hiện tại qua card **wlan0mon**. Và xác định mạng wifi muốn tấn công là **TP-Link_0098** và nằm ở **Channel 9**. Chi tiết ở Hình 5



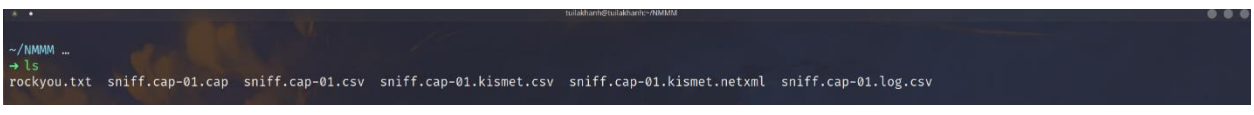
Hình 5

Sử dụng airodump để bắt gói tin và chỉ theo dõi Wifi muốn tấn công xác định từ bước ở trên. Wifi muốn tấn công có BSSID là **18:A6:F7:54:00:98** và nằm ***ở* Channel 9**. Sau đó lưu kết quả vào file **Sniff.cap** nằm ở folder NMMM. Sau một khoảng thời giàn đã có đăng nhập vào mạng và chúng ta thu thập được gói tin **WPA handshake**. Kết quả chi tiết ở Hình 6.



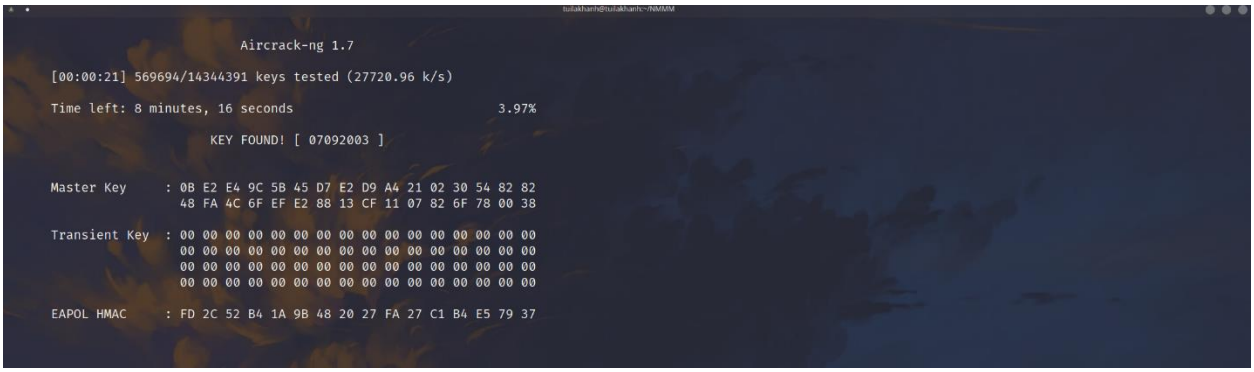
Hình 6

Sử dụng phương pháp **Worldlist** để dò tìm mật khẩu, **Worldlist** được cung cấp bởi file **rockyou.txt** mà mình đã chuẩn bị sẵn, chúng ta sẽ dò tìm mật khẩu từ file **sniff.cap** đã được thu thập từ các bước ở trên. Chi tiết ở Hình 7.



Hình 7

Sử dụng **aircrack-ng** để do tìm mật khẩu bằng từ điển và file **sniff.cap** đã được thu thập từ các bước ở trên. Vì mật khẩu rất dễ dò là ngày tháng năm sinh và có nằm trong từ điển **rockyou.txt** nên sau một khoảng thời gian chạy thì chúng ta đã dò tim ra mật khẩu. Chi tiết ở Hình 8.



Hình 8

HẾT