

# THỰC HÀNH NHẬP MÔN MẠNG MÁY TÍNH

## Lab 6 - Scanning WPA\_WPA2 Passwords

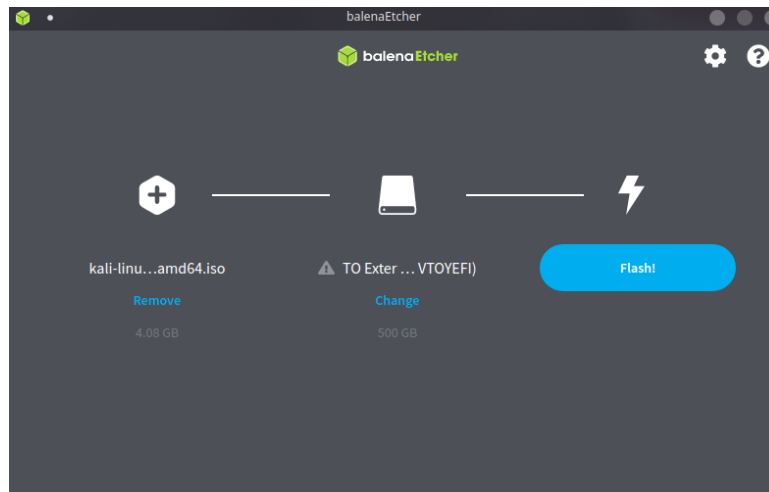
**Họ và Tên:** Lê Hoàng Khánh

**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

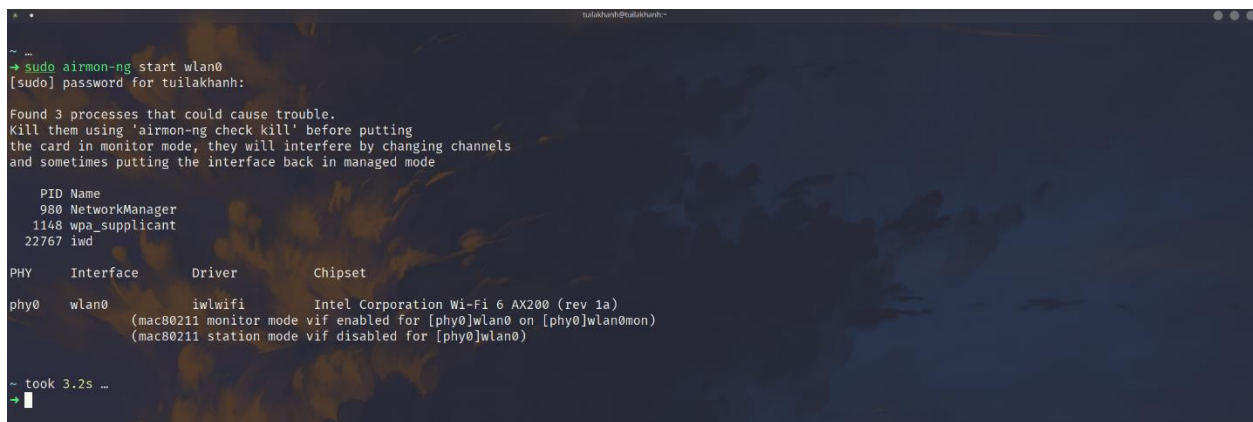
## II. Dò tìm mật khẩu với bộ công cụ Aircrack-NG

Tôi sẽ sử dụng Linux đã được cài sẵn trên máy thay vì sử dụng Kali Linux để thuận tiện 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 nằm 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

```
CH 10 [[ Elapsed: 1 min ]] 2022-12-30 11:41

BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
24:DE:C6:43:E8:20 -17 3 0 0 11 130 OPN Mang Day KTX 2.4Ghz
18:64:72:88:C9:C0 -21 2 0 0 11 195 OPN Mang Day KTX 2.4Ghz
24:DE:C6:43:E8:21 -21 6 0 0 11 130 OPN CampusVNU 2.4Ghz
18:64:72:D5:36:41 -17 19 364 3 11 195 OPN CampusVNU 2.4Ghz
9C:1C:12:88:5A:A0 -76 11 10 0 11 195 OPN Mang Day KTX 2.4Ghz
18:64:72:88:C9:C1 -77 2 7 0 11 195 OPN CampusVNU 2.4Ghz
18:64:72:D5:36:40 -17 14 0 0 11 195 OPN Mang Day KTX 2.4Ghz
9C:1C:12:88:5A:A1 -20 16 0 0 11 195 OPN CampusVNU 2.4Ghz
50:64:2B:15:B9:65 -37 35 0 0 6 130 WPA2 CCMP PSK ve_que_an_tet
94:B4:0F:A8:AF:E0 -21 9 3 0 11 195 OPN Mang Day KTX 2.4Ghz
18:64:72:08:70:A1 -14 5 0 0 11 195 OPN CampusVNU 2.4Ghz
2A:5D:E2:4F:75:C3 -68 10 0 0 11 65 WPA2 CCMP PSK LiHuan
18:64:72:08:70:A0 -15 24 0 0 11 195 OPN Mang Day KTX 2.4Ghz
9C:1C:12:88:F3:C1 -19 13 0 0 11 195 OPN CampusVNU 2.4Ghz
9C:1C:12:88:F3:C0 -20 16 0 0 11 195 OPN Mang Day KTX 2.4Ghz
94:B4:0F:A8:AF:E1 -23 17 0 0 11 195 OPN CampusVNU 2.4Ghz
18:A6:F7:54:00:98 -19 87 0 0 9 135 WPA2 CCMP PSK TP-LINK_0098
B4:5D:50:74:2C:21 -1 51 0 0 1 195 OPN CampusVNU 2.4Ghz
B4:5D:50:74:2C:20 -57 48 204 6 1 195 OPN Mang Day KTX 2.4Ghz

BSSID STATION PWR Rate Lost Frames Notes Probes
18:64:72:D5:36:41 06:62:F6:8E:F4:DF -1 1e- 0 0 13
18:64:72:D5:36:41 E6:48:C3:31:31:8E -41 2e-24e 326 415
(not associated) 42:E6:A1:61:65:4B -70 0 - 1 35 3 Mang Day KTX 2.4Ghz
(not associated) B2:4F:23:91:D6:9F -77 0 - 1 0 1
(not associated) BE:3E:8F:45:FF:01 -71 0 - 1 0 1
(not associated) 72:7D:DE:BC:22:A9 -53 0 - 1 0 2
(not associated) 86:AE:5B:9C:BE:D2 -56 0 - 1 0 1
(not associated) E8:2A:EA:19:C1:AC -70 0 - 1 0 1 Mang Day KTX 2.4Ghz
(not associated) 86:12:2A:CE:2D:8B -75 0 - 1 0 1
(not associated) 72:8C:30:F9:A8:38 -67 0 - 1 0 1
(not associated) DC:F7:56:71:D6:12 -73 0 - 1 0 1
(not associated) 72:E0:17:FE:ED:A9 -43 0 - 1 0 2
(not associated) 0A:6D:DC:7F:F1:7B -42 0 - 1 0 2
(not associated) 82:E4:D3:5C:11:33 -42 0 - 1 0 2
B4:5D:50:74:2C:20 4C:BB:58:32:68:93 -64 24e- 1 0 18 Mang Day KTX 2.4Ghz
```

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 gian đã có đăng nhập vào mạng và chúng ta thu thập được gói tin **WPA handshake**. Kết quả chi tiết ở Hình 6.

```
CH 9 [[ Elapsed: 54 s ]] 2022-12-30 11:44 [[ WPA handshake: 18:A6:F7:54:00:98 ]]

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
18:A6:F7:54:00:98 -15 96 564 70 1 9 135 WPA2 CCMP PSK TP-LINK_0098

BSSID STATION PWR Rate Lost Frames Notes Probes
18:A6:F7:54:00:98 6E:5F:91:7E:54:E6 -35 24e- 1e 0 113 EAPOL TP-LINK_0098
```

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.

```
~/NMMM ...
→ ls
rockyou.txt sniff.cap-01.cap sniff.cap-01.csv sniff.cap-01.kismet.csv sniff.cap-01.kismet.netxml sniff.cap-01.log.csv
```

Hình 7

Sử dụng **aircrack-ng** để dò 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 tìm ra mật khẩu. Chi tiết ở Hình 8.

```
Aircrack-ng 1.7

[00:00:21] 569694/14344391 keys tested (27720.96 k/s)

Time left: 8 minutes, 16 seconds          3.97%

KEY FOUND! [ 07092003 ]

Master Key   : 0B E2 E4 9C 5B 45 D7 E2 D9 A4 21 02 30 54 82 82
              48 FA 4C 6F EF E2 88 13 CF 11 07 82 6F 78 00 38

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   : FD 2C 52 B4 1A 9B 48 20 27 FA 27 C1 B4 E5 79 37
```

Hình 8

HẾT