IT005

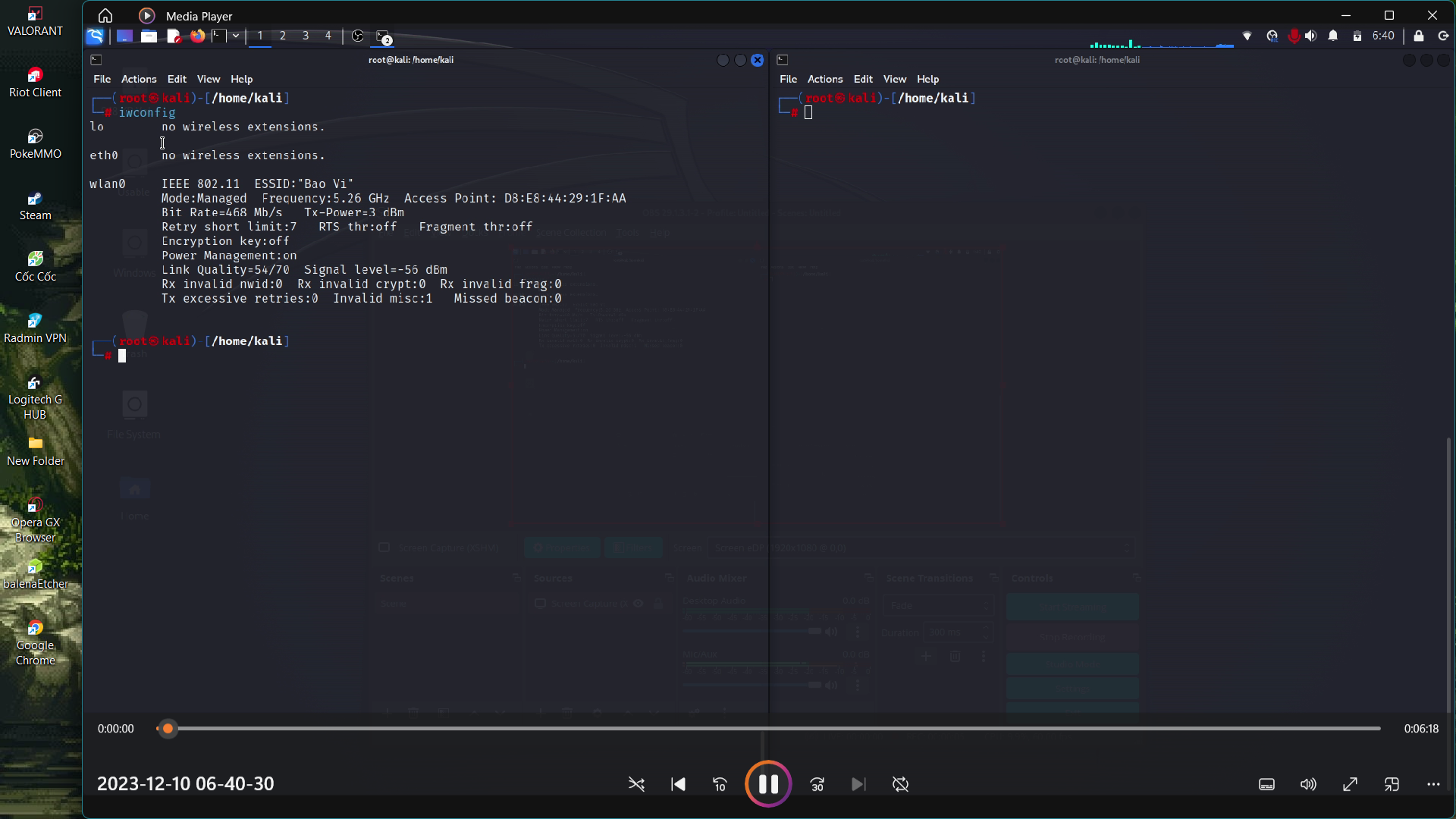
Nhập môn mạng máy tính

Báo cáo thực hành lab 6

|  |  |
| --- | --- |
| Họ tên | Nguyễn Gia Bảo |
| MSSV | 22520109 |
| Lớp | IT005.012 |
| GV HDTH | Nguyễn Thanh Nam |
| Link tới video | https://drive.google.com/drive/folders/1FyvbamaFSTLQcwYMxjmc-YiqGqVCklQe?usp=sharing |

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

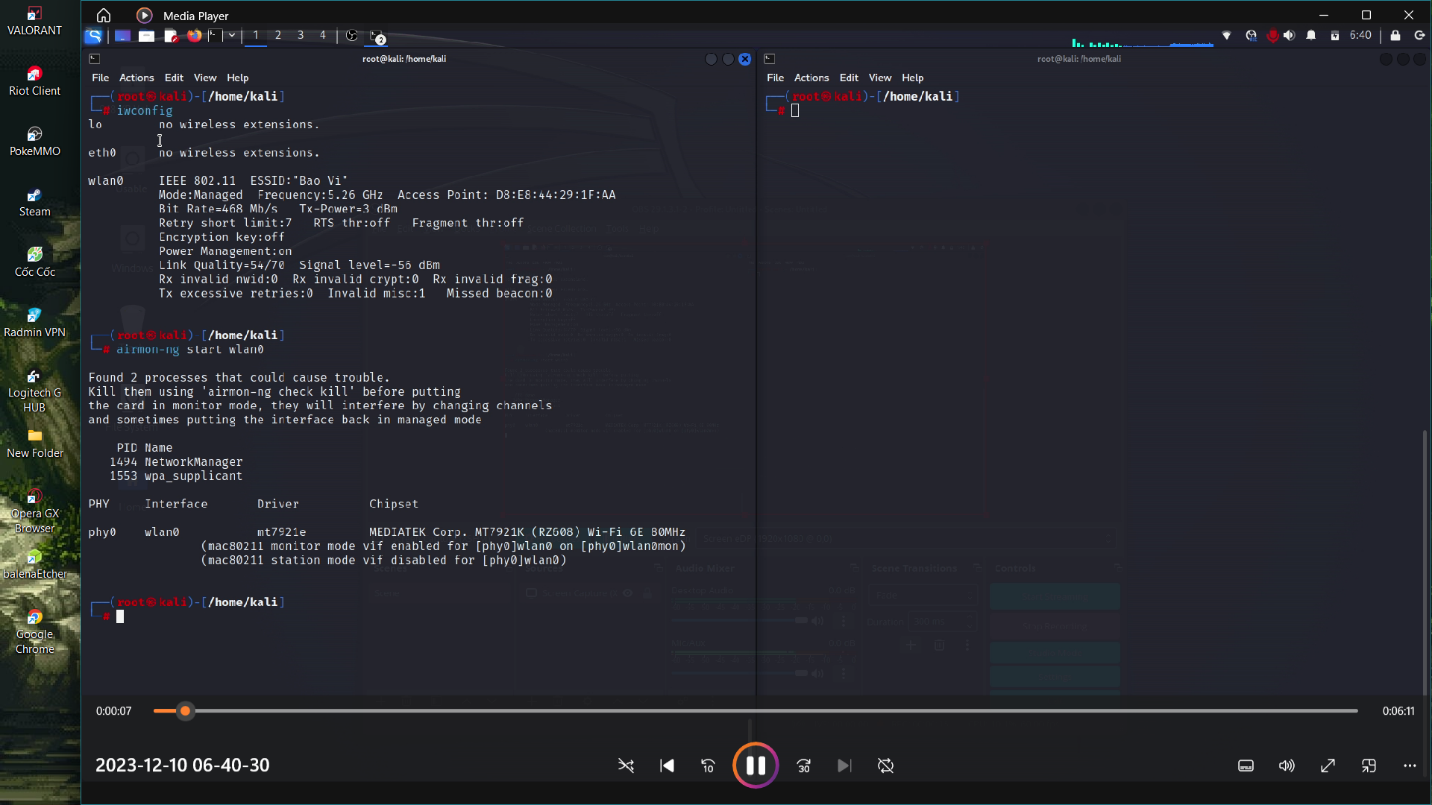
* Mở terminal và nhập câu lệnh “iwconfig” để kiểm tra tên card wireless đang sử dụng



### Tên card wireless đang sử dụng “wlan0”

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

|  |
| --- |
| airmon-ng start wlan0 |



### Terminal trả về sau khi chuyển card wifi sang monitor mode

* 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 |

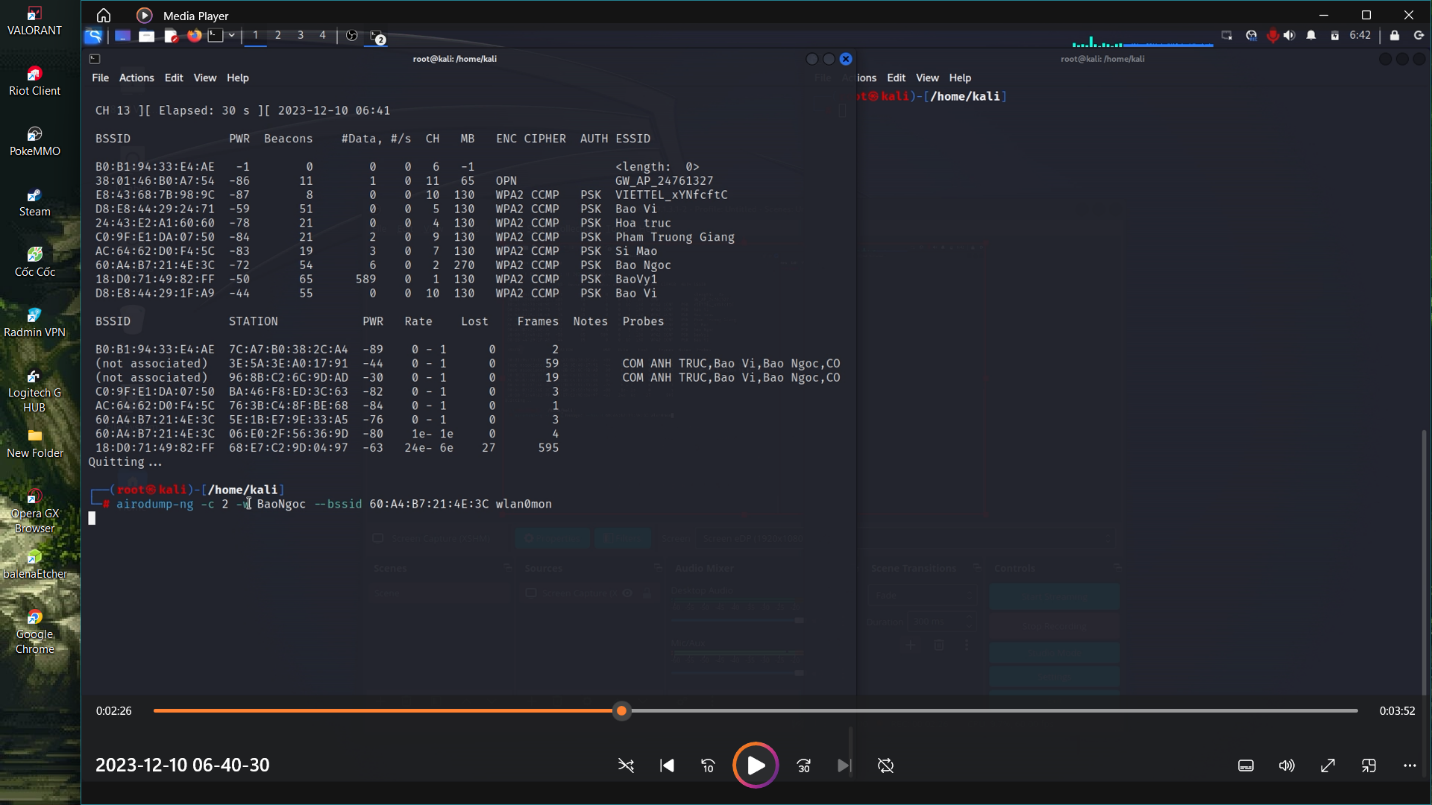
### Hoạt động của các mạng wifi có sẵn sau khi dùng lệnh “airodump-ng wlan0mon”

* Dừng việc quan sát các hoạt động của các mạng wifi (Ctrl + C). 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 -c [channel] -w [Tên tệp tin] –bssid [BSSID của mạng mục tiêu] wlan0mon |

Trong đó:

|  |  |  |
| --- | --- | --- |
| **Giá trị** | **Giải thích** | **Giá trị trong video** |
| channel | giá trị channel của mạng (màu đỏ) | 2 |
| Tên tệp tin | Tên tệp tin sẽ lưu các gói tin bắt được khi quan sát hoạt động của mạng (xanh lam) | BaoNgoc |
| BSSID của mạng mục tiêu | BSSID của mạng cần dò (vàng) | 60:A4:B7:21:4E:3C |



### Xác định mục tiêu là mạng “Bao Ngoc” và dùng lệnh airodump-ng để tập trung quan sát mục tiêu

* Sử dụng câu lệnh “aireplay-ng” để tạo tín hiệu deauth, nhằm kích các người dùng đang sử dụng thoát ra và đăng nhập lại để bắt được gói tin bắt tay WPA handshake.

|  |
| --- |
| aireplay-ng --deauth [số lệnh deauth] -a [BSSID của mạng] wlan0mon |

Trong đó

|  |  |  |
| --- | --- | --- |
| **Giá trị** | **Giải thích** | **Giá trị trong video** |
| Số lệnh deauth | Số lệnh deauth muốn gửi tới wifi, đặt thành 0 để gửi vô hạn lệnh deauth | 0 |
| BSSID của mạng mục tiêu | BSSID của mạng cần dò | 60:A4:B7:21:4E:3C |

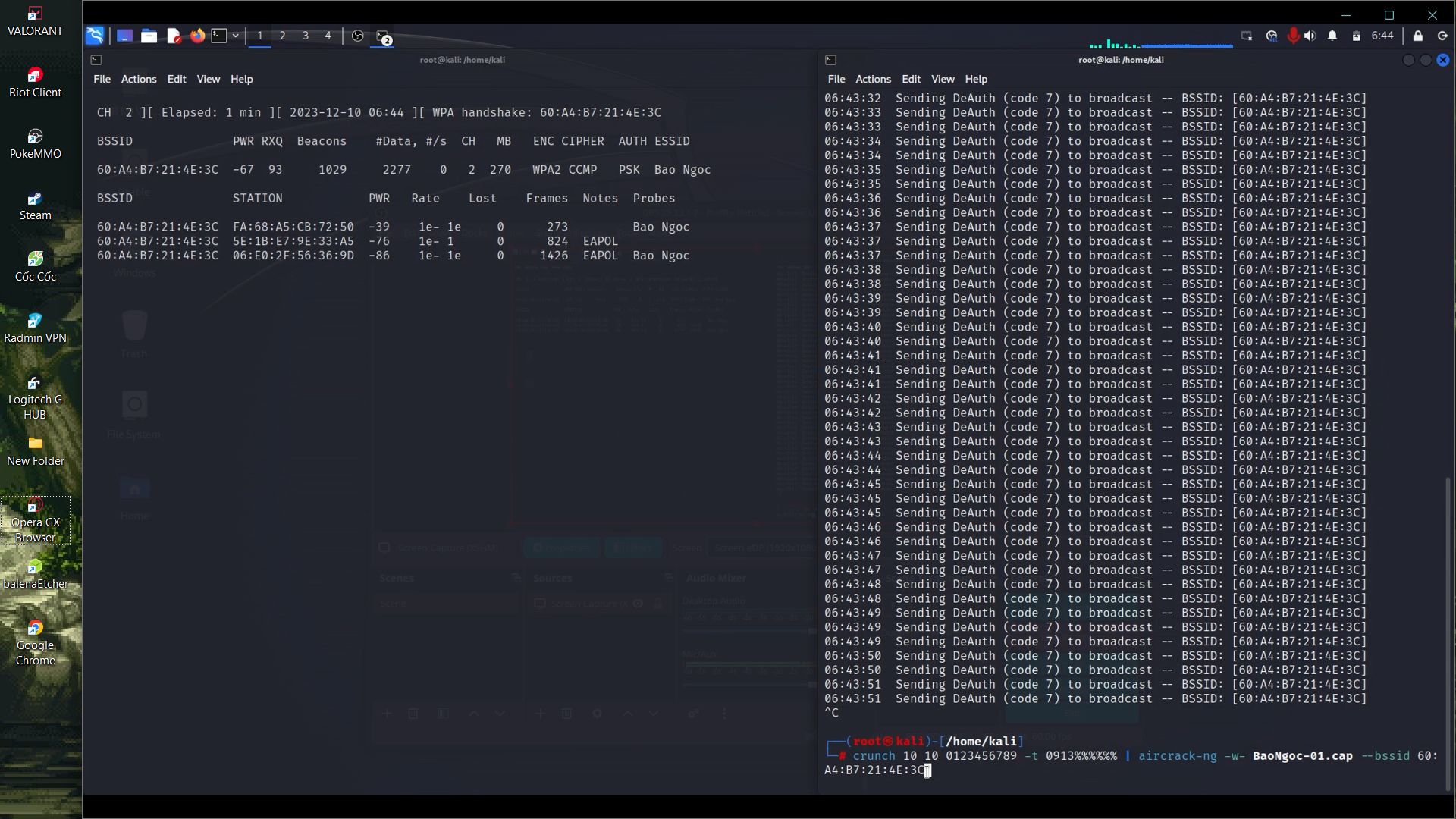
### Liên tục gửi các tín hiệu deauth cho tới khi bắt được gói tin WPA handshake

* Dừng việc gửi tín hiệu deauth (Ctrl + C), và bắt đầu việc crack password bằng phương pháp brute-force với lệnh:

|  |
| --- |
| crunch [min] [max] [danh sách ký tự] –t [mẫu định dạng mật khẩu] | aircrack-ng -w- [tập tin đã capture.cap] –bssid [địa chỉ MAC của mục tiêu] |

Trong đó:

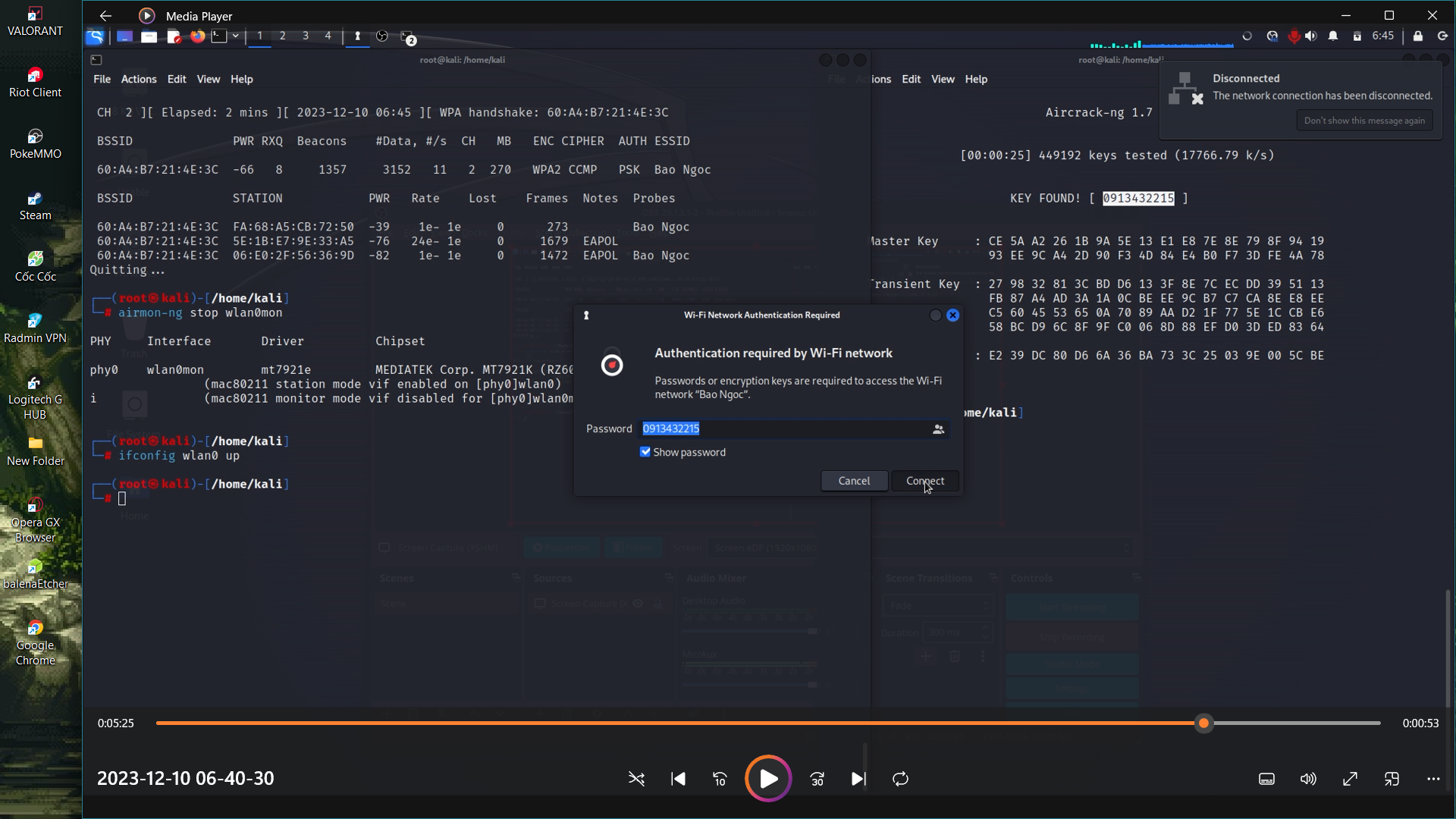
|  |  |  |
| --- | --- | --- |
| **Giá trị** | **Giải thích** | **Giá trị trong video** |
| Min | Độ dài tối thiểu của mật khẩu | 10 |
| Max | Độ dài tối đa | 10 |
| Danh sách ký tự | Danh sách các kí tự có thể xuất hiện trong mật khẩu | các chữ số từ 0 đến 9 |
| Mẫu định dạng password | Định dạng của mật khẩu, % là những kí tự chưa biết | Một số điện thoại bắt đầu bằng “0913” |
| Tên tập tin đã bắt được | Tên tệp tin đã bắt được khi bắt gói tin WPA handshake | BaoNgoc |
| Địa chỉ MAC của mục tiêu | Địa chỉ MAC của mạng wifi mục tiêu | 60:A4:B7:21:4E:3C |



### Sử dụng câu lệnh “crunch” để bắt đầu quá trình dò password

* Sau 1 khoảng thời gian chờ đợi thì kết quả dò được sẽ xuất hiện ở trên màn hình trong dòng “KEY FOUND”

### Password dò được là 0913432215

* Đăng nhập và sử dụng thử wifi (chi tiết trong video):

Kết thúc quá trình dò mật khẩu wifi.