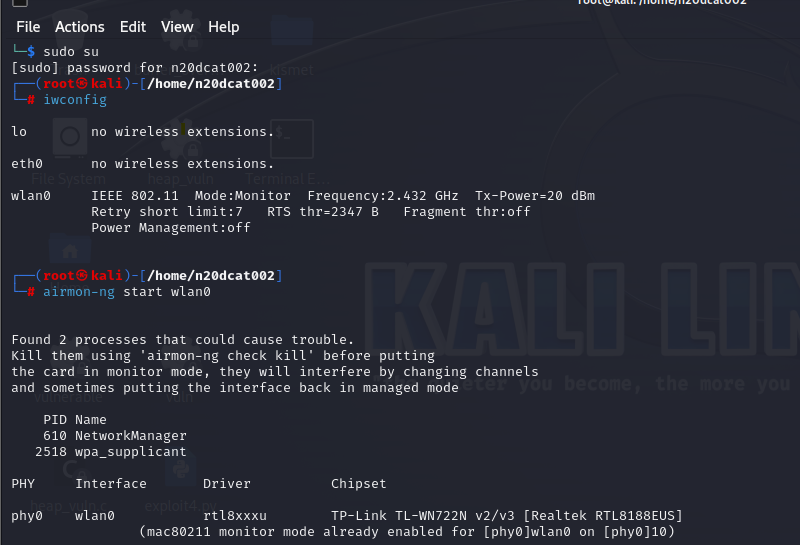
Khi một client muốn kết nối đến Router được cài đặt chuẩn bảo mật WPA/WPA2 để truy cập internet nó cần có PSK (Pre-shared Key) mà ta hay gọi là password. Client cần có cách để chứng minh với Router rằng nó biết password mà không trực tiếp gửi password qua Router (để tránh có kẻ  thứ 3 bắt được gói tin này và thu được password). Quá trình xác thực trải qua 4 bước (4-way handshake – giao thức bắt tay 4 bước):

1. Client dò mạng và thấy sóng public của Router, trong sóng này có cái mã Random là ANonce.
2. Client lấy cái ANonce, qua quá trình tính toán tính ra được cái mã SNonce, và gửi đi SNonce cùng một số thông tin đã được mã hóa như tao là ai, tao có password wifi nè, … cho Router.
3. Router nhận được SNonce, nó bảo: à há, thằng này biết password wifi nè, cho nó kết nối thôi. Nó hăm hở gửi lại cho client 1 cái mã khóa chung gọi là GTK (Group Temporary Key) và bảo rằng, ê thằng đệ, lấy cái Key này về mà mã hóa dữ liệu gửi cho tao, tao sẽ biết đường mã giải mã.
4. Client nhận được cái GTK sẽ lưu lại (Installation), liền dùng nó mã hóa 1 cái thư gửi lại cho Router với nội dung ACK thông báo cho Router rằng tao nhận được khóa rồi, vui quá mày ơi. Từ đó 2 thằng dùng cái mã khóa chung này để gửi và nhận dữ liệu.

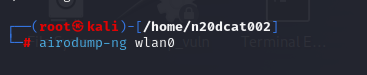
Card wireless có 2 chế độ, chế độ mặc định là Managed, card mạng sẽ chỉ thu nhận những gói dữ liệu (packets) được gửi đi trong không khí mà có địa chỉ nhận là máy của ta. Chế độ còn lại là Monitor, lúc này card mạng sẽ thu nhận tất cả các packets được gửi đi từ các card wireless khác trong phạm vi bắt sóng, bất kể địa chỉ nhận là gì.

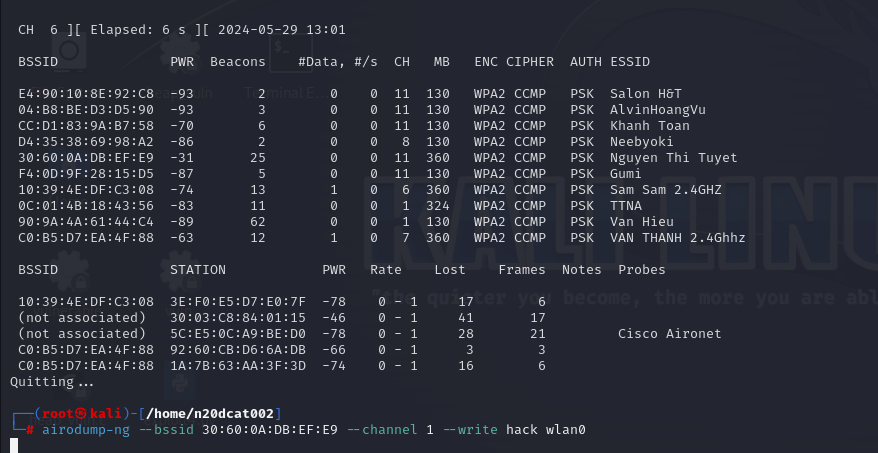
Để chuyển sang chế độ Monitor , gõ lệnh

airmon-ng start wlan0

Ta gõ tiếp lệnh sau để card mạng thăm dò các packets trong không khí nhằm xác định các AP (Access Point) và các client kết nối đến chúng.

airodump-ng wlan0mon





Trong đó:

* 30:60:0A:DB:EF:E9 là địa chỉ MAC của AP
* -c 11 là channel mà AP phát sóng
* -w hack là tên file mà ta muốn viết
* wlan0 là tên card wifi ở chế độ monitor

Lệnh trên sẽ bắt các gói tin đi và đến AP có địa chỉ MAC: 30:60:0A:DB:EF:E9 trên channel … và ghi lại các gói tin bắt được vào file .cap có tên bắt đầu là hack…

Lúc này ta sẽ chờ đợi khi có client nào connect đến AP nó sẽ bắt được quá trình 4-way handshake và dòng chữ WPA Hanshake sẽ hiện ở góc trên phải của terminal. File hack…cap sẽ được lưu trong /root.

Để đảm bảo quá trình nghe lén này thành công ta mở 1 terminal khác và gõ lệnh sau để ngắt kết nối các client đang kết nối với AP. Khi đó client sẽ thực hiện lại 4-way handshake và ta sẽ bắt được gói tin cần thiết.

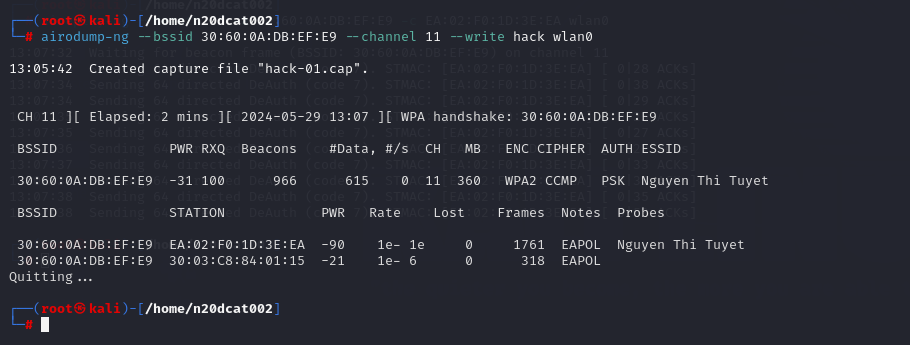
A screen shot of a computer

Description automatically generated

Trong đó:

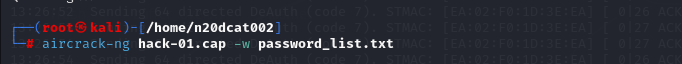
* –deauth 0: thực hiện tấn công ngắt kết nối liên tục đến các client của mạng này.
* -a 30:60:0A:DB:EF:E9là địa chỉ MAC của AP.
* wlan0 là tên card wireless ở chế độ monitor.

Quan sát cửa sổ đang chạy lệnh airodump-ng, đến khi hiện chữ “WPA Handshake” thì coi như đã hoàn thành bước 1: bắt gói tin. Ta có thể Ctrl + C tại các cửa sổ để dừng lệnh lại.



Bước tiếp theo trong quá trình tấn công là tiến hành wordlist attack. Ta cần có một bộ từ điển tốt để hack.  
Một cách khác khá hay để tạo wordlist là chương trình cupp viết bằng python, tạo wordlist dựa trên thông tin về đối tượng cần hack như: họ tên, ngày sinh, tên người yêu, tên thú nuôi, … Tìm hiểu thêm tại đây:

<https://hackingvision.com/2017/12/13/cupp-target-specific-wordlist-generator/>



Lệnh này sẽ tiến hành tạo mã hash cho mỗi password trong wordlist và tiến hành so sánh với password đã hash bắt được trong file hack-01.cap. Kết quả test trên máy tác giả:

A screenshot of a computer screen

Description automatically generated

Kismet:

Kismet là một hệ thống phát hiện mạng, dò gói và phát hiện xâm nhập cho các mạng LAN không dây 802.11. Kismet sẽ hoạt động với bất kỳ thẻ không dây nào hỗ trợ chế độ giám sát thô và có thể đánh giá lưu lượng 802.11a, 802.11b, 802.11g và 802.11n. Chương trình chạy trên Linux, FreeBSD, NetBSD, OpenBSD và Mac OS X.

A screenshot of a computer screen

Description automatically generated

Sử dụng kismet để phát hiện tấn công Dos và wifi:

