BÁO CÁO BÀI TẬP

**Môn học: An toàn Mạng không dây và di động**

**Kỳ báo cáo: Buổi 03 (Session 03)**

**Tên chủ đề: VƯỢT QUA XÁC THỰC MẠNG WLAN**

**Bypassing WLAN Authentication**

*GV: Lê Đức Thịnh*

*Ngày báo cáo: 24/4/2023*

**Nhóm: 802.11**

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT330.N21.ANTT.1

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Lâm Thiệu Ân | 20521047 | 20521047@gm.uit.edu.vn |
| 2 | Bùi Đức Hoàng | 20520514 | 20520514@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Yêu cầu 1 | 100% |
| 2 | Yêu cầu 2 | 100% |
| 3 | Yêu cầu 3 | 100% |
| 4 | Yêu cầu 4 | 100% |
| 5 | Yêu cầu 5 | 100% |
| 6 | Yêu cầu 6 | 100% |
| 7 | Yêu cầu 7 | 100% |
| 8 | Yêu cầu 8 | 100% |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

## Yêu cầu 1: Theo cách trên có thể gửi broadcast deauthentication đến tất cả các client. Tìm hiểu công cụ aireplay-ng để deauthentication acttack có chọn lọc client.

* Để gửi gói deauthentication đến một client nhất định, ta tiến hành thêm option

-c <Client’s MAC Address>

Graphical user interface, text

Description automatically generated

* Sau khi tấn công.

Text

Description automatically generated

* Trên máy Client lúc này đã bị disconnect.

Graphical user interface, application

Description automatically generated

## Yêu cầu 2: Thực hiện lại mục C2

* Thông tin gói Beacon

A picture containing calendar

Description automatically generated

* Thông tin gói Beacon bị ẩn thông tin.

Table

Description automatically generated with low confidence

* Thông tin gói Deauthentication

Graphical user interface, text, application

Description automatically generated

* Thông tin gói Authentication

Graphical user interface, text, application

Description automatically generated

* Station của MAC

A picture containing text

Description automatically generated

A picture containing calendar

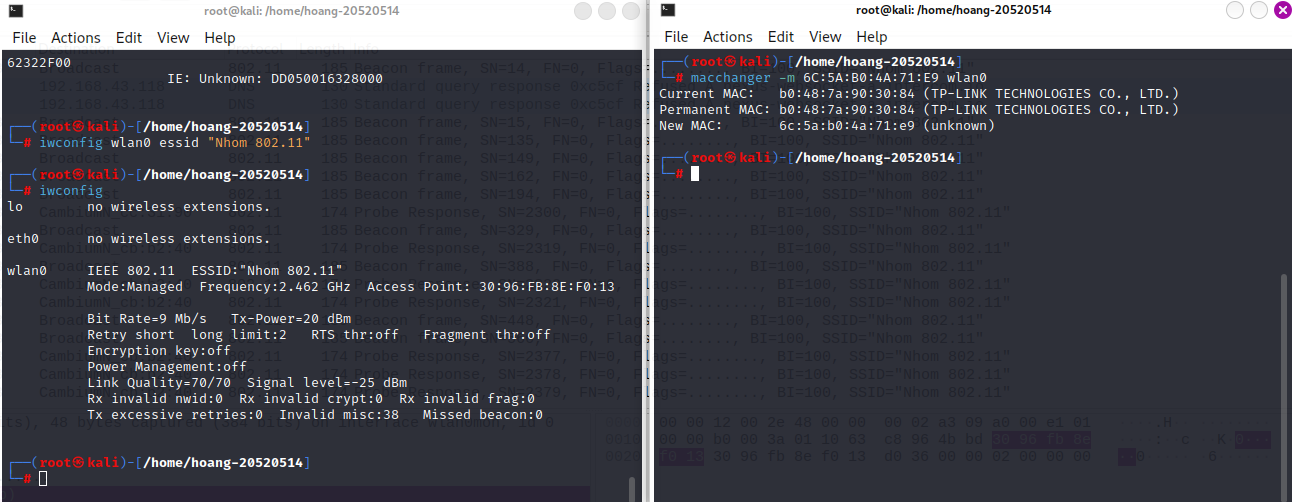
Description automatically generated

* MAC changer

Text

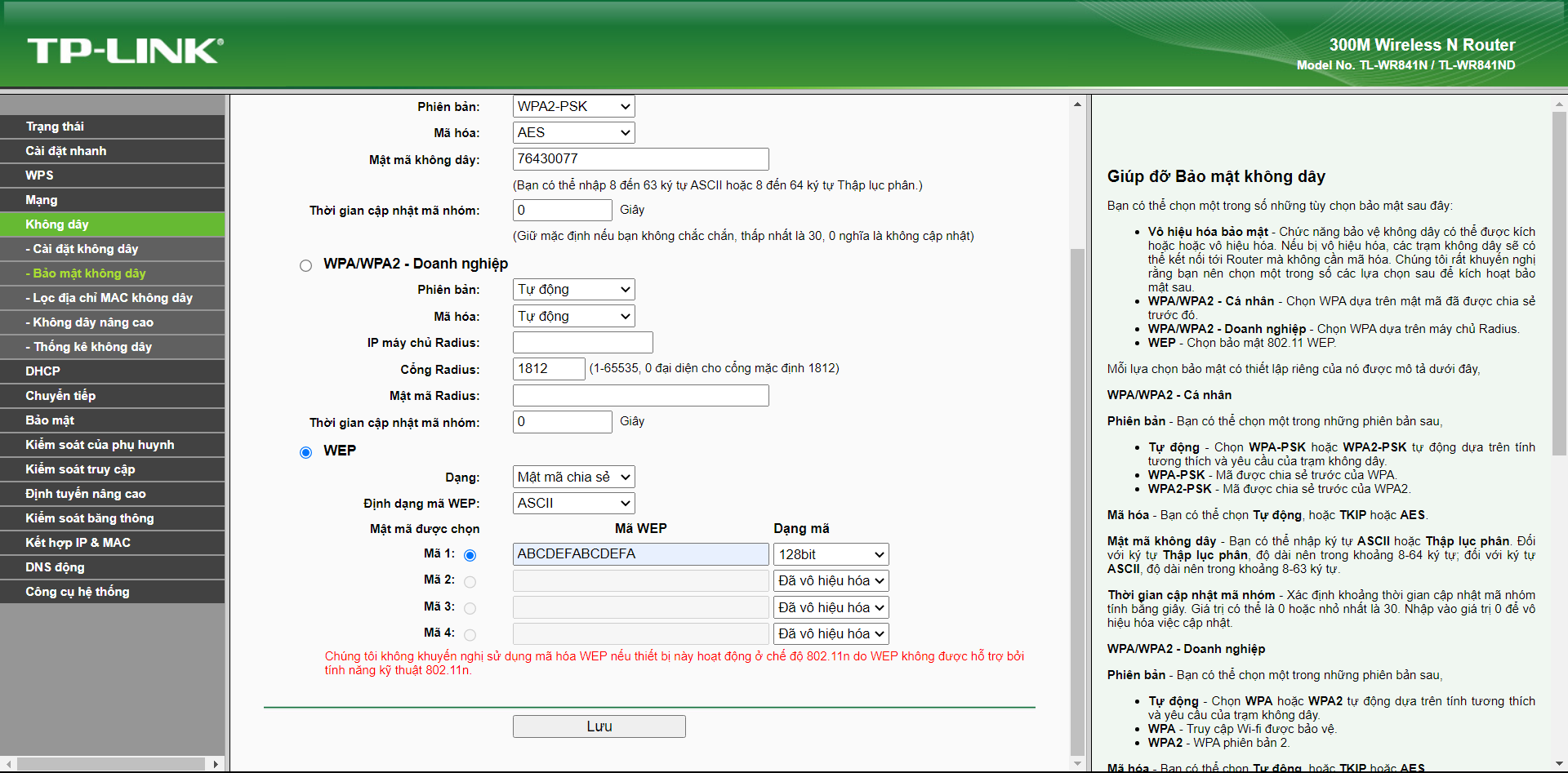
Description automatically generated

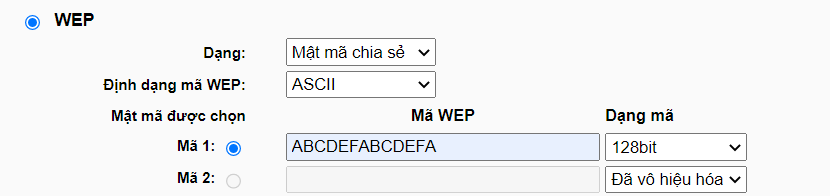
* Đã bypass được.



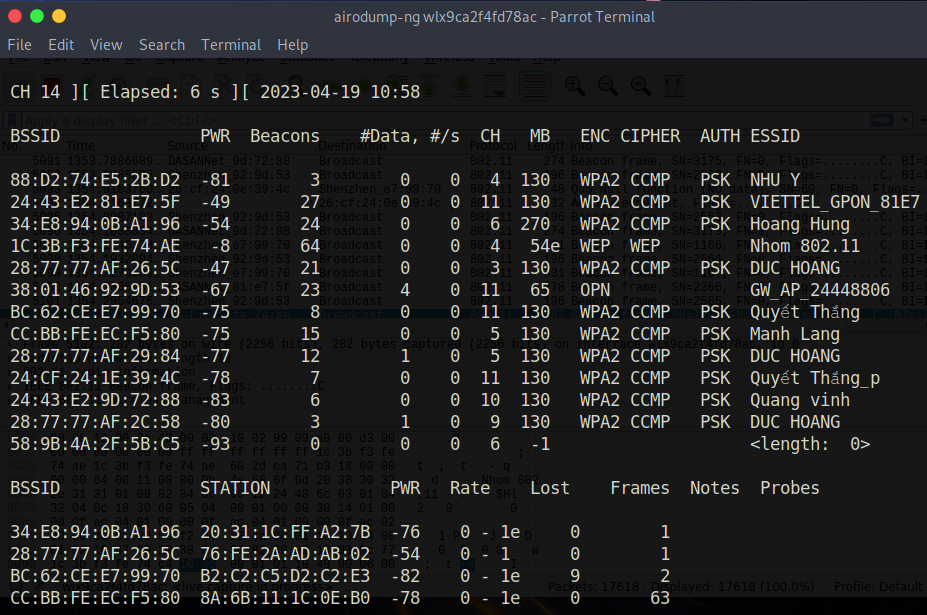
## Yêu cầu 3: Xác định gói đầu tiên, yêu cầu xác thực được gửi bởi aireplay-ng đến AP.

* Đầu tiên, ta vào trang cấu hình của thiết bị AP để thực hiện đổi Authentication Type sang Shared Key.



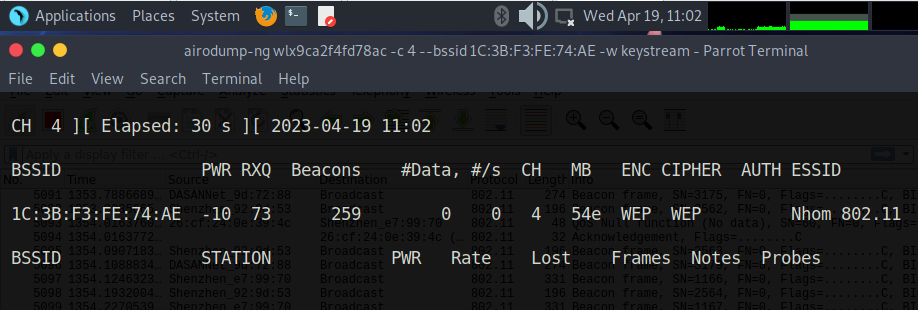


* Tiếp đó, ta chạy lệnh *airodump-ng wlan0* để tìm địa chỉ MAC cũng như channel hiện tại của Nhom 802.11

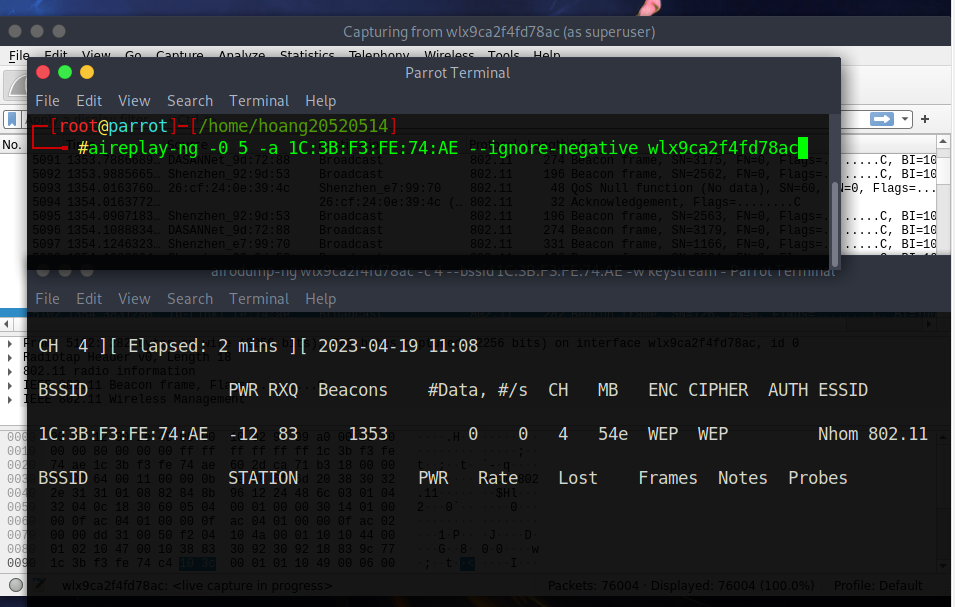


* Ở đây do bị lỗi monitor mode nên nhóm em chuyển sang ParrotOS thay vì Kali, vì USB Wifi của nhóm không chạy monitor mode trên Kali được do không hỗ trợ driver.
* Chạy lệnh airodump-ng wlan0mon -c <channel> --bssid <mac AP> -w keystream để sniff các gói tin trao đổi giữa client và AP.



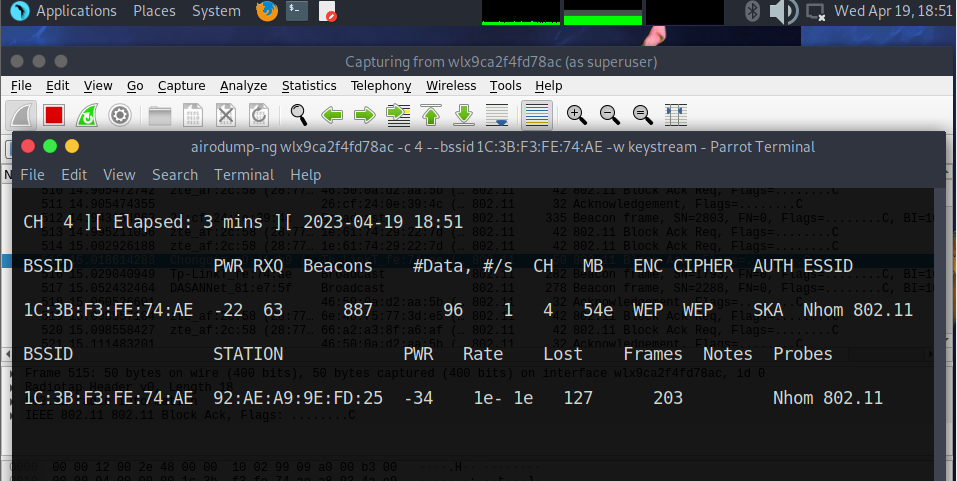


* Dùng kĩ thuật tấn công Deauthentication để ngắt kết nối của Client, bắt Client phải kết nối lại.

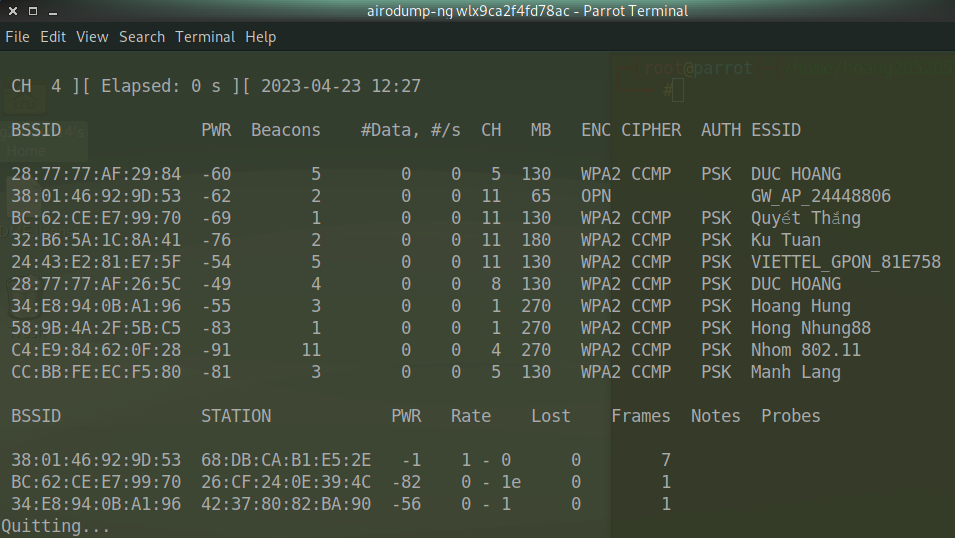




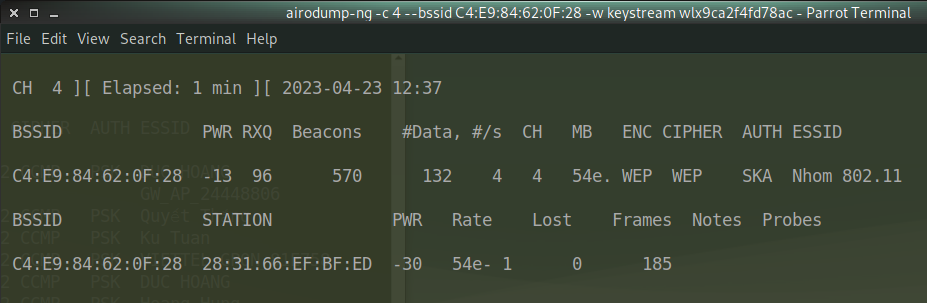
* Sau đó, ta thấy khi Client kết nối lại thì đã xuất hiện SKA ở cột AUTH, lúc này ta sẽ ngắt kết nối và thực hiện fake SKA.



* Ở đây do em thực hiện bắt gói .xor không được, em cũng thực hiện tấn công chopchop nhưng vẫn không được, nên em đổi qua thiết bị router khác, có địa chỉ MAC là C4:E9:84:62:0F:28, và thiết bị kết nối có địa chỉ MAC là 28:31:66:EF:BF:ED.

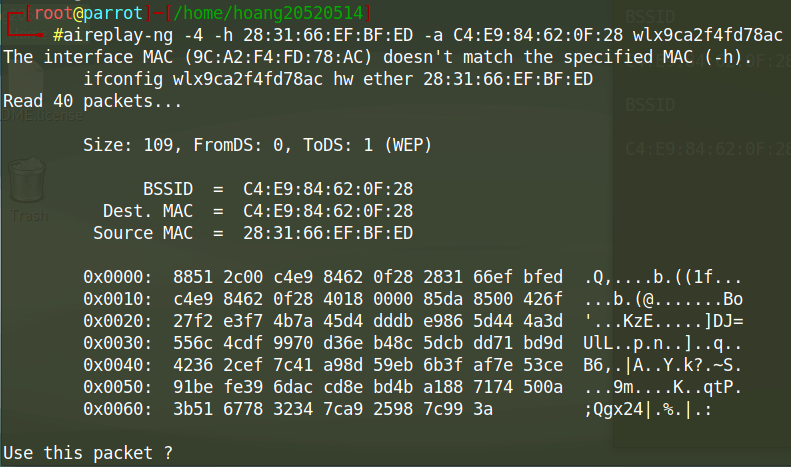


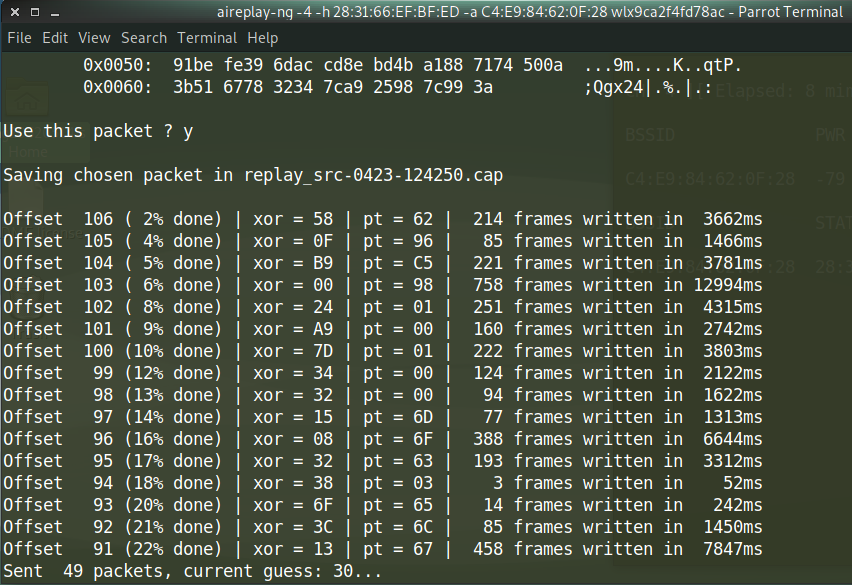
* Ta lấy thiết bị kết nối với AP, ta thấy ở cột AUTH đã xuất hiện SKA.

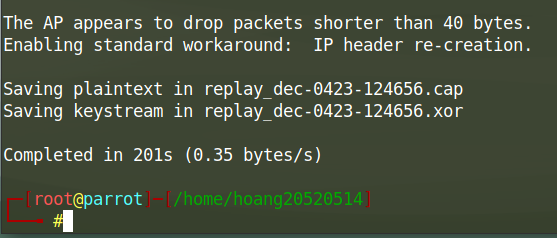


* Nhưng ở dòng đầu tiên vẫn chưa xuất hiện đoạn keystream, do đó theo hướng dẫn trong tài liệu tham khảo “Packt - Kali Linux Wireless Penetration Testing Beginners Guide 2017 3rd Edition.pdf”, ta sẽ thực hiện tấn công chopchop để tạo ra gói .xor

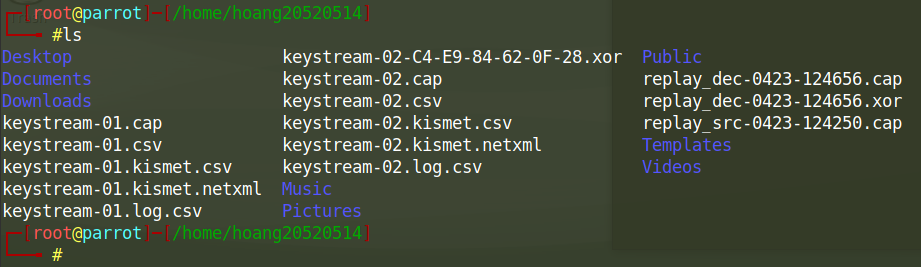




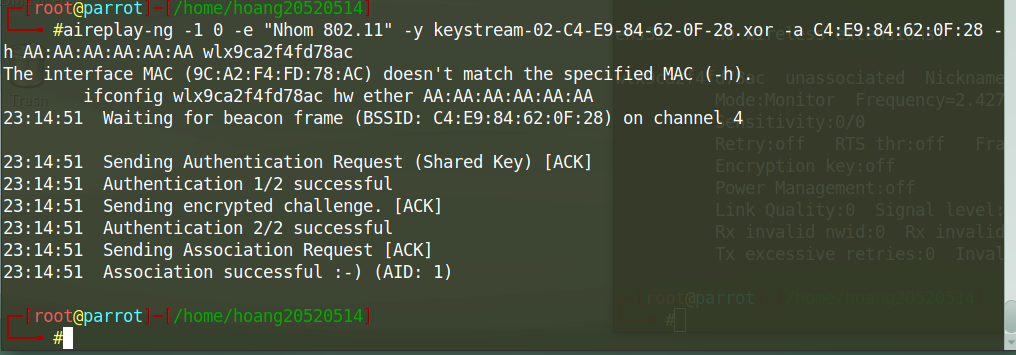




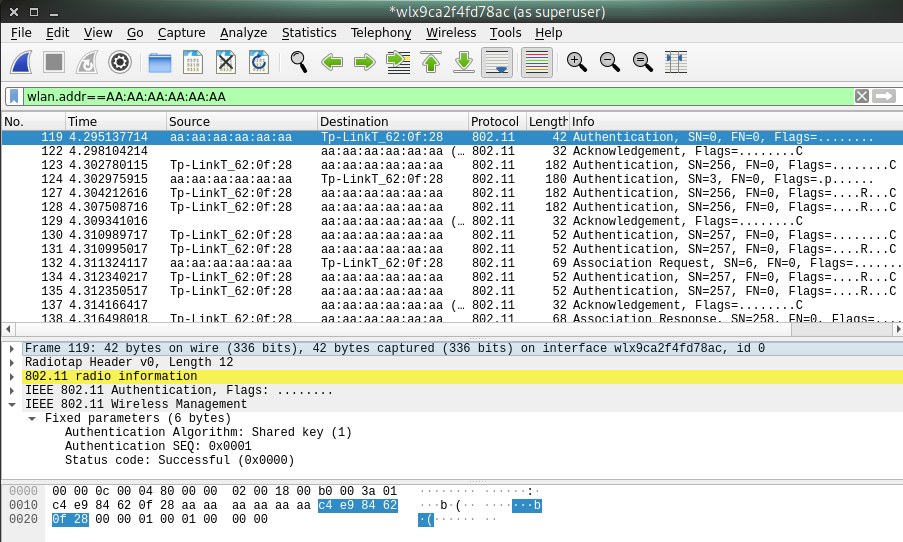
* Khi ta thực hiện lệnh ls, ta sẽ thấy gói keystream<AP’s MAC>.xor đã xuất hiện.



* Thực hiện fake SKA.

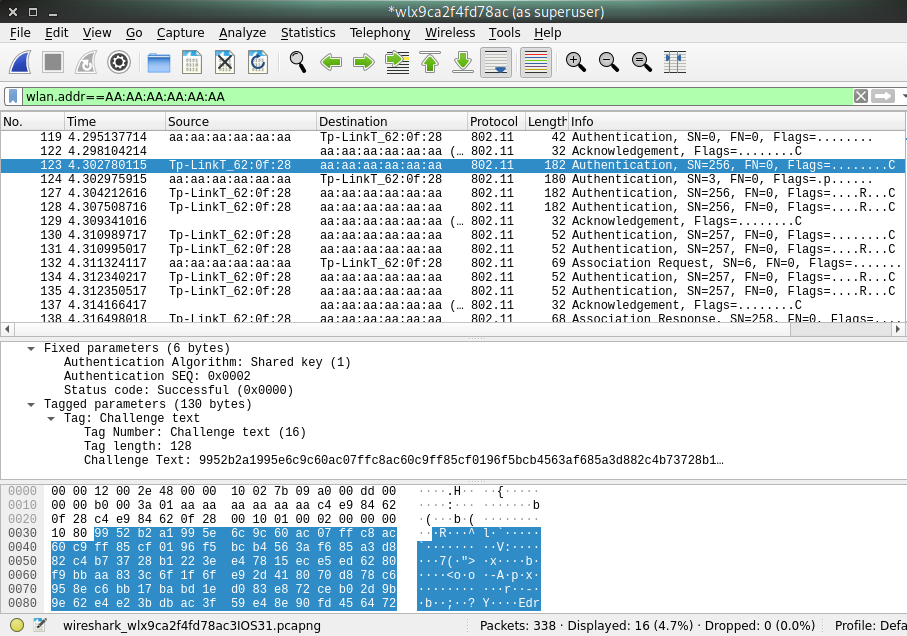


* Gói đầu tiên bắt được là authentication request được gửi bởi aireplay-tool tới AP.

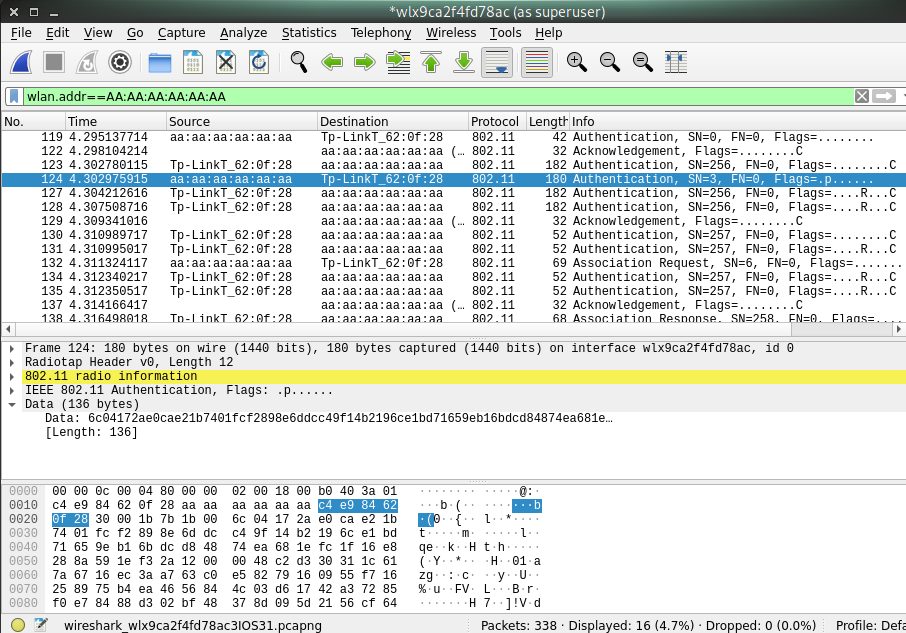


## Yêu cầu 4: Xác định gói thứ hai, chứa challenge mà AP gửi cho aireplay-ng.

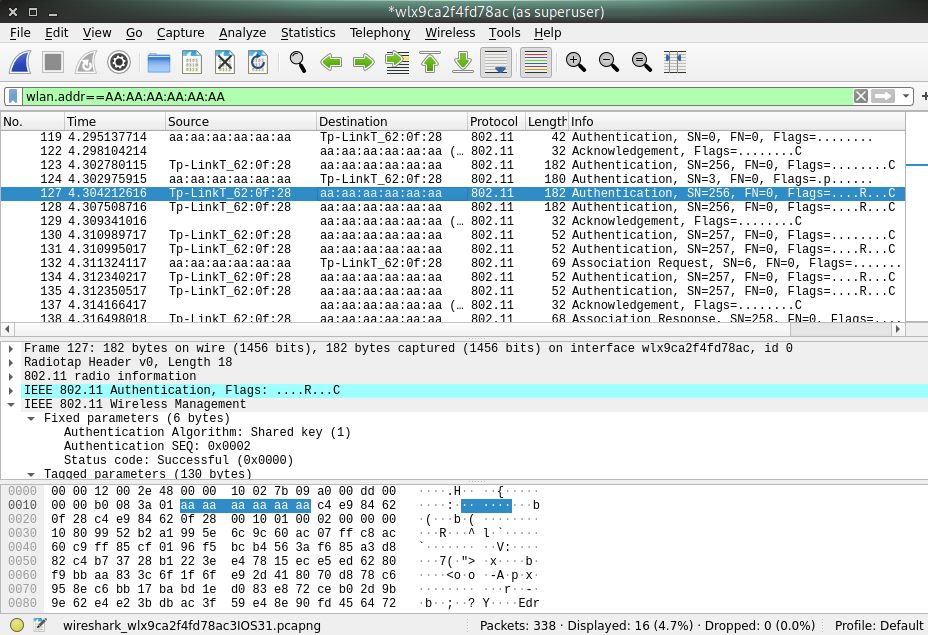
* Gói thứ hai bao gồm đoạn challenge text mà access point gửi cho client.



## Yêu cầu 5: Xác định gói thứ ba, aireplay-ng gửi challenge được mã hoá đến AP.



## Yêu cầu 6: Xác định gói thứ tư, thông báo AP gửi xác thực thành công.



## Yêu cầu 7: Sau khi xác thực thành công, vào giao diện quản trị của AP kiểm tra log truy cập.

Graphical user interface, text, application

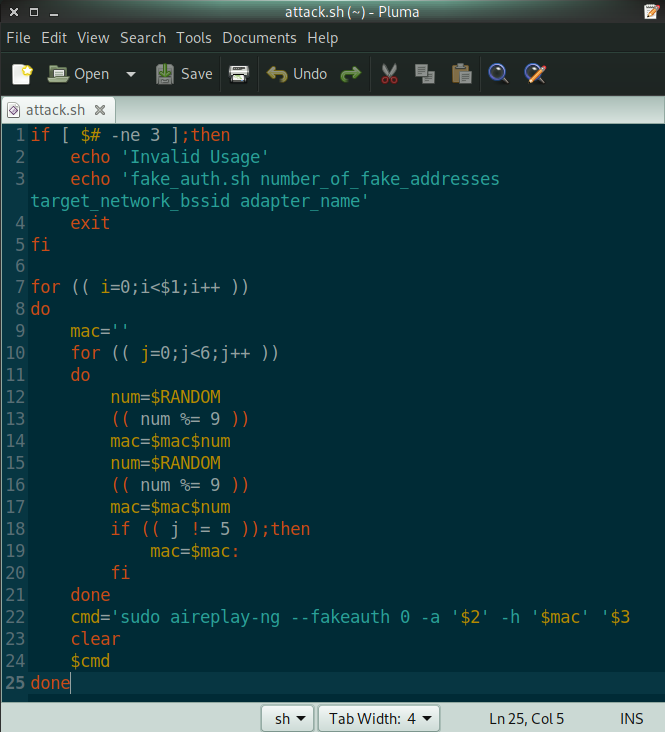
Description automatically generated

Graphical user interface, text, application

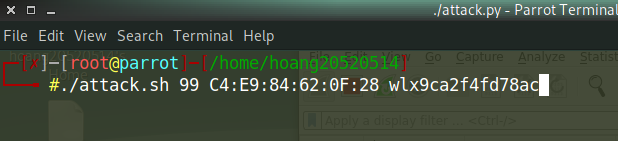
Description automatically generated

## Yêu cầu 8: AP chỉ chịu tải một số lượng client nhất định kết nối đến; viết một tool (gợi ý thư viện pyrcrack hoặc tìm hiểu được) để có thể kết nối đến với hàng trăm địa chỉ MAC ngẫu nhiên đến AP. Điều này sẽ làm cho AP ngưng chấp nhận kết nối khi đạt được lượt kết nối tối đa; đây được gọi là tấn công từ chối dịch vụ Denial of Service (DoS). Hãy xác minh điều này.

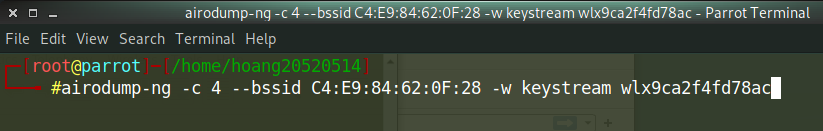
* Ở đây, ta tạo ra một shell script, ta sẽ random địa chỉ MAC và gửi các địa chỉ MAC đó kết nối với Access Point.
* Cấu trúc của shell script.



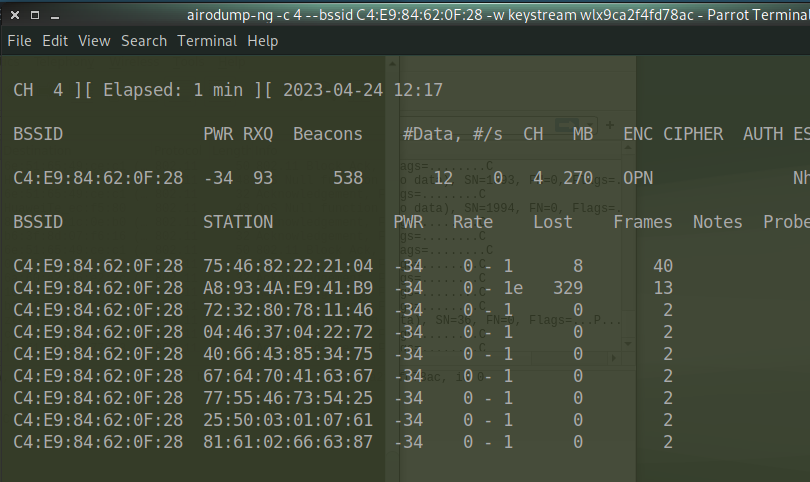
* Ta tiến hành chạy tấn công.



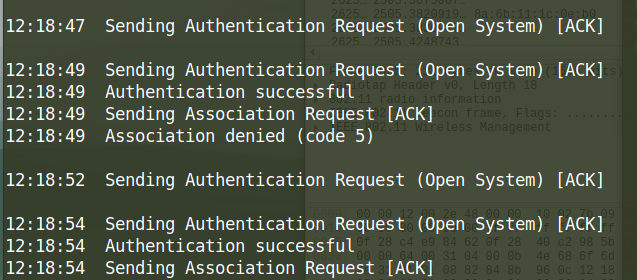
* Ở bên một Terminal khác, ta chạy lệnh airodump-ng để kiểm tra các kết nối.



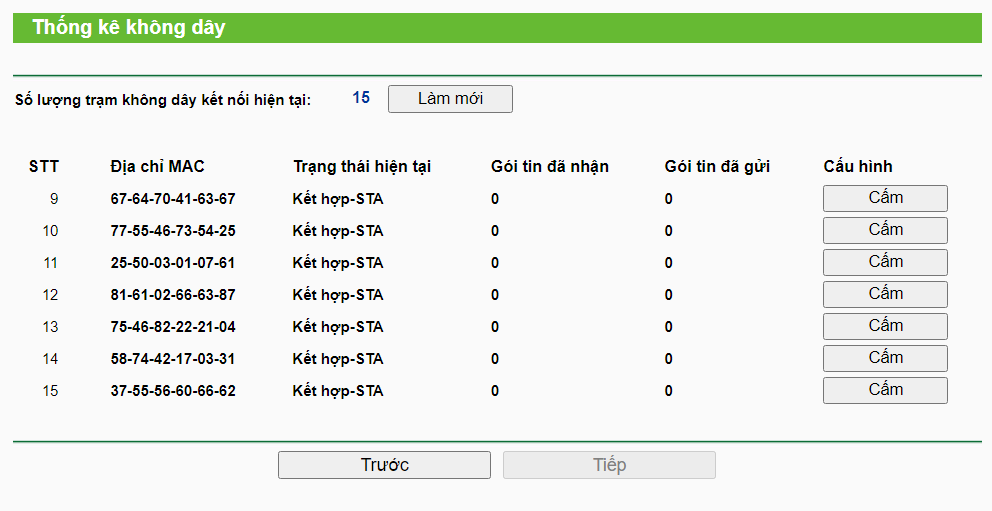
* Khi thực hiện tấn công.



* Sau một thời gian, AP đã từ chối truy cập do số lượng đã đạt đến giới hạn.



* Ở trên trang admin, ta thấy số lượng điểm truy cập đã đạt giới hạn là 15.



1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)