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 02: 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 | Tất cả các yêu cầu đều có sự đóng góp của cả 2 |
| Ý kiến *(nếu có)*  + Khó khăn  + Đề xuất, kiến nghị |  |

# BÁO CÁO CHI TIẾT

## Nội dung 1

***Khi sử dụng lênh ifconfig wlan0, làm sao để nhận biết wireless card đã up?***

Text

Description automatically generated

Khi sử dụng lệnh ifconfig wlan0 thì ta thấy dòng :

Flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

Thì ta biết rằng wireless card đã up

## Nội dung 2

### *Lệnh arp -a thể hiện điều gì?*

A screenshot of a computer

Description automatically generated with medium confidence

Lệnh arp -a cho phép được dùng để tìm ra địa chỉ phần cứng (địa chỉ MAC) của thiết bị từ một địa chỉ IP nguồn (wlan0)

## Nội dung 3

### *Hãy dùng một công cụ để Kali Linux kết nối mạng WPA/WPA2 như trên.*

\*Chú ý : ta phải dùng thiết bị di động , … để làm acesspoint với bảo mật wpa/wpa trước khi thực hiện các bước bên dưới

**B1** :Tìm các bộ điều hợp không dây có sẵn mà bạn có thể dễ dàng liệt kê tất cả bằng cách gõ lệnh sau : **iw dev ( iwconfig )**

Ta thấy bộ điều hợp duy nhất không có tên **wlan0** và được chỉ định là **phy#0**

**Mode** : **managed** (có nghĩa là thiết bị của ta là một trạm Wi-Fi hoặc là 1 client kết nối với một điểm truy cập - AP)

Và địa chỉ **MAC** là : **dc:8b:28:8a:f5:f2**

Text

Description automatically generated

**B2** : kiểm tra trạng thái thiết bị xem thiết bị không dây đang UP hay DOWN bằng cách gõ lệnh sau: **ip link show wlan0**

ip được sử dụng để hiển thị / thao tác định tuyến, thiết bị, policy routing và tunnels . Nó được sử dụng để bật / tắt thiết bị và giúp ta tìm thông tin mạng chung

A screenshot of a computer

Description automatically generated

**B3** : Sử dụng lệnh sau để chuyển trạng thái thiết bị sang **UP** :

**ip link set wlan0 up**



**B4 :** Kiểm tra trạng thái kết nối mạng WiFi bằng cách nhập “**iw wlan0 link**” để hiển thị tình trạng kết nối.

Tại thời điểm này chúng ta chưa kết nối .



**B5** : Scan tất cả các mạng WiFi gần bộ điều hợp bằng cách nhập lệnh sau:

**iw wlan0 scan**

Graphical user interface, text, application

Description automatically generated

**B6** : 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

## Nội dung 4

### *Có thể tạo nhiều interface ở mode monitor trên cùng một thiết bị vật lý. Dùng airmon-ng để làm điều đó.*

**B1** :

Chúng ta dùng lệnh :

**iw wlan0 interface add mon0 type monitor  
iw wlan0 interface add mon1 type monitor  
iw wlan0 interface add mon2 type monitor**

Graphical user interface, text, application

Description automatically generated

Thì ta sẽ có :  
mon0 (type monitor)  
mon1 (type monitor)  
mon2 (type monitor)

**B2** : Gõ **airmon-ng start mon0** để chạy qua **airmon-ng**

Text

Description automatically generated

**B3 :** Gõ **iwconfig** để hiển thị các interfaces

Text

Description automatically generated

## Nội dung 5

### *Nhìn các trường hãy chỉ ra các WLAN frame type.*

**B1**: Vào monitormode

**1**.Dùng công cu **airmon-ng** để card mạng vào chế độ monitor. Kiểm tra công cụ nhận thiết bị bằng lệnh airmon-ng.

Graphical user interface, application

Description automatically generated

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.

A screenshot of a computer

Description automatically generated

**B2** :

Trên Kali Linux mở công cụ Wireshark. Vào **Capture** - > **Options**.

Chọn capture packet từ interface **wlan0mon**, sau đó chọn **Start**. Wireshark sẽ bắt đầu capture nên có thể thấy các packet.

A screenshot of a computer

Description automatically generated

Trong trường hợp này là **Beacon frame**

## Nội dung 6

### *Chọn filter (wlan.bssid == <mac>) && (wlan.fc.type\_subtype == 0x20)*

### *và bắt đầu bắt gói trên Wireshark trên interface wlan0mon. Từ máy client truy*

### *cập đến giao diện quản ký của AP (như trong bài thực hành là 192.168.2.1).*

### *Wireshark bắt được những gói tin data như thế nào?*

**B1: Vào monitormode**

Y như B1 của yêu cầu 5

**B2** : **Truy cập đến giao diện quản ký của AP bằng cách ping đến default gateway của AP**

Tiến hành bắt gói tin của AP tự tạo không xác thực có **SSID** là **113115**.

1. 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 sniff 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. Giá trị tần số Frequency: 2.447 GHz tương ứng với channel 6

### Text Description automatically generated

**B3** :Bật Wireshark sniff trên interface **wlan0mon**.

Chọn filter **(wlan.bssid == <mac>) && (wlan.fc.type\_subtype == 0x20)**

A screenshot of a computer

Description automatically generated

Trong trường hợp 1: bắt được gói **SSDP : Simple Service Discovery Protocol**

A screenshot of a computer

Description automatically generated

Trường hợp 2 : Bắt được các gói **ARP**

(Test 2 lần)

## Nội dung 7

### *Cài đặt thiết bị client quên AP và tiến hành kết nối lại. Phân tích các tin ARP sau khi client yêu cầu DHCP request và DHCP server phản hồi.*

Graphical user interface

Description automatically generated

Ta nhận đc info :

Who has **192.168.253.119** ? Tell **192.168.253.1**

**192.168.253.119** is at **fa:f1:e6:d0:e5**

Giải thích :

Máy chủ có địa chỉ IP **192.168.253.1** muốn gửi một số dữ liệu. Nó biết nó phải gửi dữ liệu này đến **192.168.253.119**, nhưng nó không biết địa chỉ MAC để gửi, vì vậy nó đã gửi một yêu cầu **Address Resolution Protocol (ARP)** để tìm ra thông tin đó. **ARP** là viết tắt của "Giao thức phân giải địa chỉ", và 42 là số byte bao gồm gói ARP này. Và vì 42 ít hơn số byte tối thiểu cho một khung Ethernet, điều đó cũng có nghĩa là đang bắt gói tin trên cùng một máy đã gửi yêu cầu ARP, trong trường hợp này là **192.168.253.1**

## Nội dung 8

### *Hãy chỉ ra các packet injection mà aireplay-ng sinh ra.*

* Làm từ đầu đến hết **B2** của yêu cầu 6
* Để tiến hành inject gói tin, bật Wireshark chọn interface **wlan0mon** và chọn filter sau:

**(wlan.bssid == < FA:F1:E6:D0:0F:E5>)** **&& !(wlan.fc.type\_subtype == 0x08)**. Filter này giúp ta loại bớt các gói beacon.

* Gõ lệnh **aireplay-ng -9 -e <113115> -a <FA:F1:E6:D0:0F:E5> wlan0mon**

Text

Description automatically generated

* Ta sẽ thấy thông báo **Injection is working !**

A screenshot of a computer

Description automatically generated with medium confidence

# QoS Null: Cho biết QoS frame không mang bất kỳ dữ liệu nào.

***Các trường hợp khác :***

# Dữ liệu QoS + CF-ACK: Cho biết khung QoS mang dữ liệu.

# Dữ liệu QoS + CF-Poll: Cho biết khung QoS mang dữ liệu.

# TÀI LIỆU THAM KHẢO