

Wifi 干扰:

准备一块网卡，要能用的到 kali 上的一些工具，这里用的是 kali 实体机，加上某宝上网的一个 kali linux 专用的网卡，目前理解应该是和网卡芯片能够支持的协议的版本有关，攻击流程如下：

开启网卡的混杂模式：

```
root@kali: ~
File Edit View Search Terminal Help
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 10 bytes 2364 (2.3 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# airmon-ng start wlan0

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

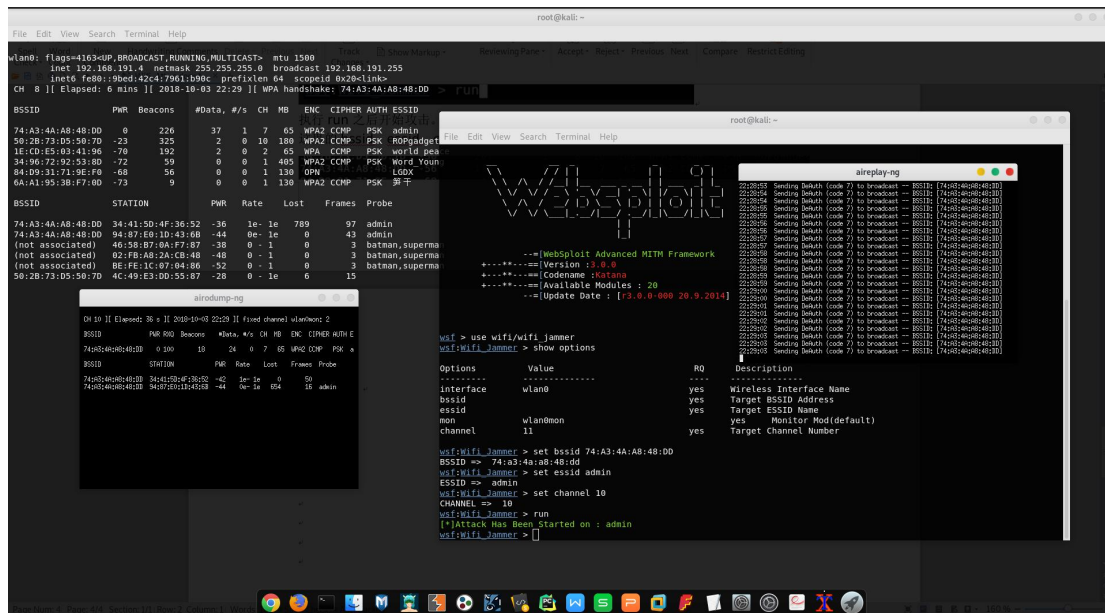
PID Name
402 NetworkManager
953 wpa_supplicant
11339 dhclient

PHY Interface Driver Chipset
phy3 wlan0 rt2800usb Ralink Technology, Corp. RT2870/RT3070
0mon) (mac80211 monitor mode vif enabled for [phy3]wlan0 on [phy3]wlan0
(mac80211 station mode vif disabled for [phy3]wlan0)
root@kali:~# airmon-ng start wlan0
root@kali:~#
```

开始监听，嗅探 wifi 热点信息：

```
root@kali:~/Desktop/WIFIattcker# airodump-ng wlan0mon
```

开启 websploit:



以下攻击方式没有列出具体攻击方式使用什么软件，有待后期完善：

Access Point Overloaded——接入点过载

Authentication Flood——身份验证泛洪攻击

Authentication Failure——身份验证失败泛洪

Deauthentication Flood——取消身份验证泛洪攻击

Association Flood——关联泛洪

Disassociation Flood——取消关联泛洪攻击

Duration Attack——持续时间攻击

Wireless Adapter Driver Buffer OverFlow——无线网卡驱动溢出攻击

WiFi DEnum——网卡漏洞检测工具

WVE——<http://www.wirelessve.org> 无线漏洞及攻击代码的软件

AusCERT——<http://www.auscert.org.au> 无线漏洞公告及讨论区

RF Jamming——RF 干扰（完全干扰，不分敌我）