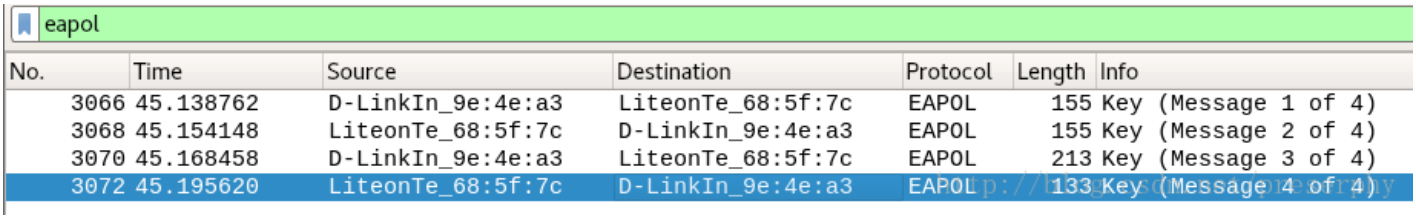
【BugKu-CTF论坛writeup(杂项)】想蹭网先解开密码

原创

Kingyo12 于 2018-03-05 20:28:39 发布
分类专栏： BugKu-CTF论坛writeup(杂项)

提示WIFI密码为手机号。下载下来是一个cap包，用wireshark打开。

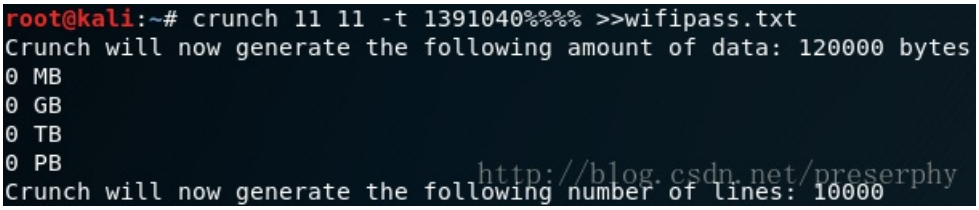
WIFI连接认证的重点在WPA的四次握手包，也就是eapol协议的包，过滤一下——



eapol

No.	Time	Source	Destination	Protocol	Length	Info
3066	45.138762	D-LinkIn_9e:4e:a3	LiteonTe_68:5f:7c	EAPOL	155	Key (Message 1 of 4)
3068	45.154148	LiteonTe_68:5f:7c	D-LinkIn_9e:4e:a3	EAPOL	155	Key (Message 2 of 4)
3070	45.168458	D-LinkIn_9e:4e:a3	LiteonTe_68:5f:7c	EAPOL	213	Key (Message 3 of 4)
3072	45.195620	LiteonTe_68:5f:7c	D-LinkIn_9e:4e:a3	EAPOL	133	Key (Message 4 of 4)

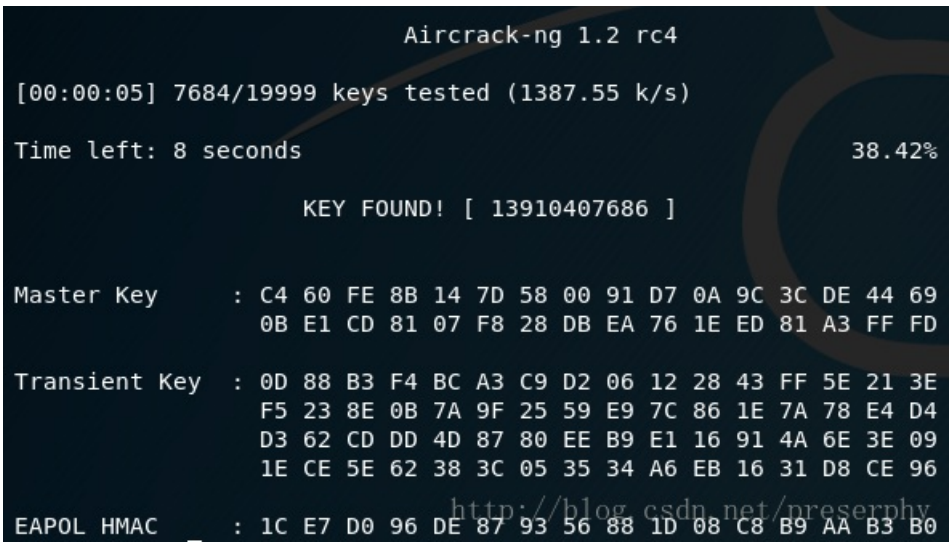
正好四个包，接下来就是破解密码了，因为已经给了11位手机号的前七位，使用crunch生成一个密码字典，然后进行破解



```
root@kali:~# crunch 11 11 -t 1391040%%%% >>wifipass.txt
Crunch will now generate the following amount of data: 120000 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 10000
```


因为实际上只有四位数的排列，所以很快就生成好了。

使用命令 `aircrack-ng -w wifipass.txt wifi.cap` 进行破解，得到密码了~



```
                          Aircrack-ng 1.2 rc4

[00:00:05] 7684/19999 keys tested (1387.55 k/s)

Time left: 8 seconds                                      38.42%

                      KEY FOUND! [ 13910407686 ]


Master Key     : C4 60 FE 8B 14 7D 58 00 91 D7 0A 9C 3C DE 44 69
                 0B E1 CD 81 07 F8 28 DB EA 76 1E ED 81 A3 FF FD

Transient Key  : 0D 88 B3 F4 BC A3 C9 D2 06 12 28 43 FF 5E 21 3E
                 F5 23 8E 0B 7A 9F 25 59 E9 7C 86 1E 7A 78 E4 D4
                 D3 62 CD DD 4D 87 80 EE B9 E1 16 91 4A 6E 3E 09
                 1E CE 5E 62 38 3C 05 35 34 A6 EB 16 31 D8 CE 96

EAPOL HMAC     : 1C E7 D0 96 DE 87 93 56 88 1D 08 C8 B9 AA B3 B0
```


所以flag就是flag{13910407686}