2021年中国工业互联网安全大赛核能行业赛道writeup之wifi破解近源攻击

原创

苦行僧(csdn) 于 2021-11-07 11:03:55 发布 55 收藏
分类专栏： 信息安全 文章标签： aircrack-ng wifi dict 字典

本文链接：https://blog.csdn.net/qpeity/article/details/121188660

信息安全 专栏收录该内容

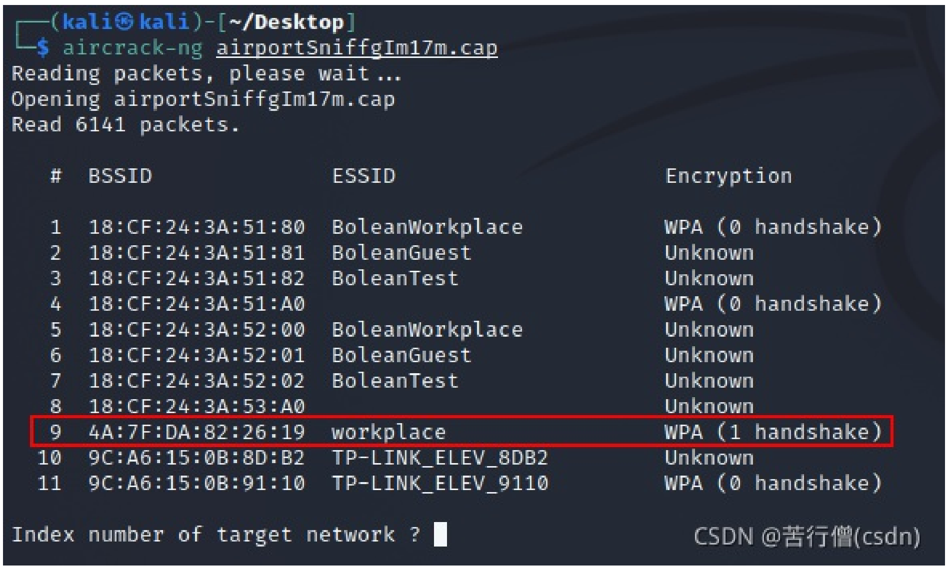
附件题：wifi破解——近源攻击

题目描述：

> 近源攻击，在攻防演练期间，攻击队队员使用无人机悬停监听技术，成功抓取到了某核电办公网络的Wifi握手包，现在正在进行紧张的破解，你能破解该密码吗？ 据得到的信息显示，该办公室设置的密码比较简单，可能是wifi名字和弱口令的组合。flag格式： flag{} + 密码 例如： flag{12345678}

附件下载：

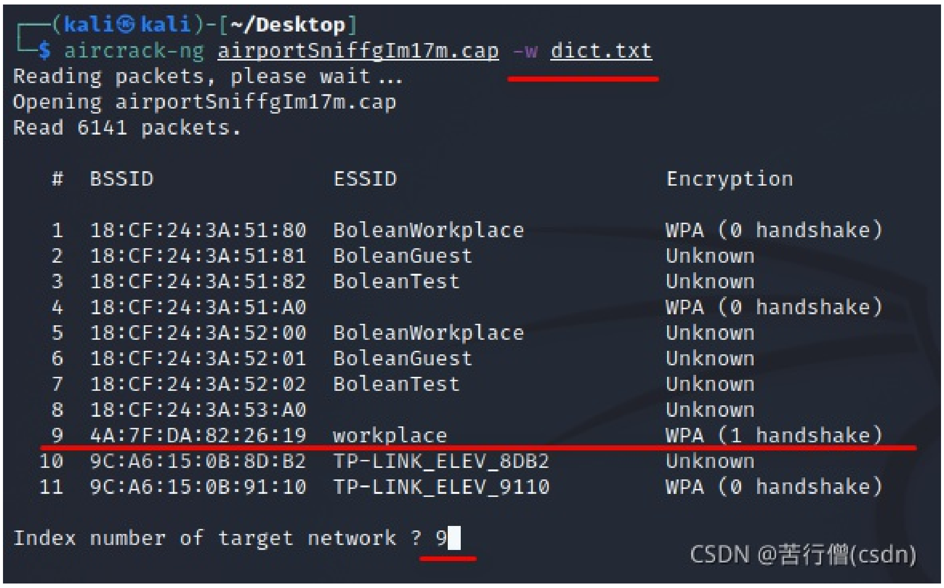
2021-10-12T15_39_04.258808+00_00airportSniffglm17m.cap.zip-网络攻防文档类资源-CSDN下载wifi破解——近源攻击近源攻击，在攻防演练期间，攻击队队员使用无人机悬停监听技术，成功抓取到了某更多下载资源、学习资料请访问CSDN下载频道.https://download.csdn.net/download/qpeity/37959291先用aircrack-ng工具，看看哪个wifi有可能突破。发现有一个名为workplace的wifi有握手，那么就这个了。



```
┌──(kali㉿kali)-[~/Desktop]
└─$ aircrack-ng airportSniffgIm17m.cap
Reading packets, please wait ...
Opening airportSniffgIm17m.cap
Read 6141 packets.

   #  BSSID              ESSID                     Encryption

   1  18:CF:24:3A:51:80  BoleanWorkplace           WPA (0 handshake)
   2  18:CF:24:3A:51:81  BoleanGuest               Unknown
   3  18:CF:24:3A:51:82  BoleanTest                Unknown
   4  18:CF:24:3A:51:A0                            WPA (0 handshake)
   5  18:CF:24:3A:52:00  BoleanWorkplace           Unknown
   6  18:CF:24:3A:52:01  BoleanGuest               Unknown
   7  18:CF:24:3A:52:02  BoleanTest                Unknown
   8  18:CF:24:3A:53:A0                            Unknown
   9  4A:7F:DA:82:26:19  workplace                 WPA (1 handshake)
  10  9C:A6:15:0B:8D:B2  TP-LINK_ELEV_8DB2         Unknown
  11  9C:A6:15:0B:91:10  TP-LINK_ELEV_9110         WPA (0 handshake)

Index number of target network ?
```

根据提□，该wifi密码为wifi名字和弱□令的组合，那可以使□字典□成器来任意□成0-4,5,6……位的字符来测试。目前我还没有掌握字典生成器，先用python脚本生成字典，先生成workplace+4位数字的字典。如果4位的不行，再尝试5,6……位数字的。

```
#!/usr/bin/bash

f = open('dict.txt', 'w')
for i in range(1, 10000):
    f.write('workplace' + str(i) + '\n')
f.close()
```



flag是 flag{workplace1014}