

CTF i春秋从0刷题 MISC

原创

XY 44 于 2018-07-13 15:24:57 发布 2073 收藏 1

分类专栏: [ctf](#) 文章标签: [CTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/XY_44/article/details/81032216

版权



[ctf](#) 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

1、分值: 20分 类型: MiscStego 题目名称: A

shipin.cap 2016/8/22 14:56 看图片 CAP 图片... 546 KB

题目是一个.cap文件。根据提示

和wireshark分析一下需要查dns。扔到kali里爆破密码。过程不赘述, 直接上截图。

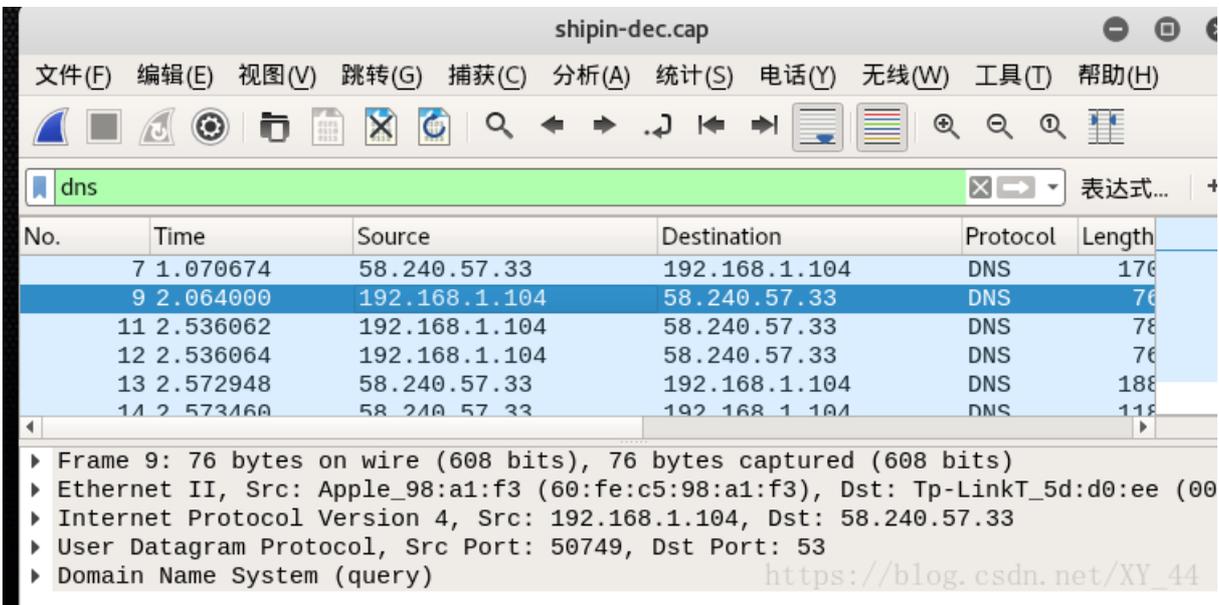
```
root@kali:~# aircrack-ng "Desktop/2/shipin.cap"
Opening Desktop/2/shipin.cap
Read 16664 packets.
# BSSID      ESSID      Encryption
1 00:1D:0F:5D:D0:EE 0719      WPA (1 handshake)
Choosing first network as target.
Opening Desktop/2/shipin.cap
Please specify a dictionary (option -w).
```

```
root@kali:~# aircrack-ng -a2 -b 00:1D:0F:5D:D0:EE -w Desktop/1.txt Desktop/2/shipin.cap
Opening Desktop/2/shipin.cap
Reading packets, please wait...
Aircrack-ng 1.2 rc4
[00:00:00] 2/2 keys tested (303.17k/s)
Time left: 0 seconds 100.00%
KEY FOUND! [ 88888888 ]
```

这里看题目分值应该是纯数字, 所以找了个纯数字字典很快就出来了。

```
root@kali:~# airdecap-ng "Desktop/2/shipin.cap" -e 0719 -p 88888888
Total number of packets read      16664
Total number of WEP data packets   0
Total number of WPA data packets   27
Number of plaintext data packets   0
Number of decrypted WEP packets    0
```

得到dec。dns过滤。



这里居然不是第一个google。提示却是第一个网站。辣鸡提示！

