171221 杂项-i春秋【迎圣诞】（可恶的黑客、流量分析）

原创

奈沙夜影 于 2017-12-22 13:59:50 发布 2074 收藏 1

分类专栏： CTF

本文链接：https://blog.csdn.net/whklhhhh/article/details/78872613

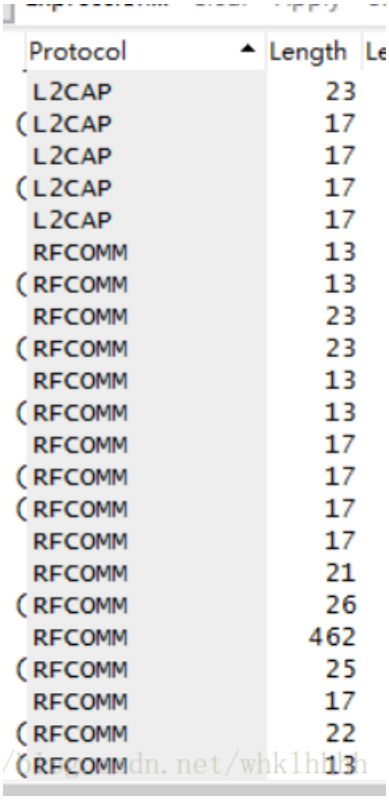
1625-5 王子昂 总结《2017年12月21日》 【连续第447天总结】

A. i春秋【迎圣诞】（可恶的黑客、流量分析）

B.

流量分析

题目给了2个文件，分别是web和蓝牙的数据包
查找资料得知，蓝牙的协议分为命令、数据和事件3种
由于我们的目标是flag，因此可以忽略命令和事件，也就是协议为'HCI_CMD'和'HCI_EVT'的
按照协议分类，扫剩下的数据包时发现有一个长度异常的



Protocol	Length	Le
L2CAP	23	
(L2CAP	17	
L2CAP	17	
(L2CAP	17	
L2CAP	17	
RFCOMM	13	
(RFCOMM	13	
RFCOMM	23	
(RFCOMM	23	
RFCOMM	13	
(RFCOMM	13	
RFCOMM	17	
(RFCOMM	17	
(RFCOMM	17	
RFCOMM	17	
RFCOMM	21	
(RFCOMM	26	
RFCOMM	462	
(RFCOMM	25	
RFCOMM	17	
(RFCOMM	22	
(RFCOMM	13	

点进去查看数据发现Data中出现了很多可见字符，并且包括一个secret头
Dump下来，以十六进制查看：

```
0000 52 61 72 21 1A 07 00 CE 99 73 80 00 0D 00 00 00 Rar!...蟮sÇ.....
0010 00 00 00 00 75 8E EE 95 D1 3D B8 28 86 7E C1 46 ....u廇曆=?吵罠
0020 24 89 2B DE 8D E9 CB A1 A4 DF 5D 31 0B B0 05 98 $?迪樗·谖1.??
0030 90 AC C6 F1 C6 AC 82 C0 E2 39 41 AA 3C 43 1A 16 滤岂片俦?A?C..
0040 0D 27 A0 D2 FC 54 2C A5 75 F3 D1 7B DB C8 F8 A9 .'鼾黔,  笱<又_
0050 ED BA 55 15 5F 8E F7 24 16 65 6E 61 9C 1A 63 B6 砗U._廇$.ena?c?
0060 DB 1A C9 FB BC AA E0 DC 74 14 EE 39 BA 01 D4 4E ?甥吉嘬t.??訃
0070 BD 63 25 E3 8D 50 7E 6F 51 F7 85 FC 37 2A 3A DD 绾%銎P~oQ鲋?*:?
0080 2F 3C 67 41 E7 AC 6F 64 E4 79 24 39 75 8E EE 95 /<gA绗od鄒$9u廇?
0090 D1 3D B8 28 32 D0 48 E0 2F 32 9F 08 E9 09 5A 52 ???蠼?2??ZR
00A0 93 7E 52 6B 00                                  “~Rk
```

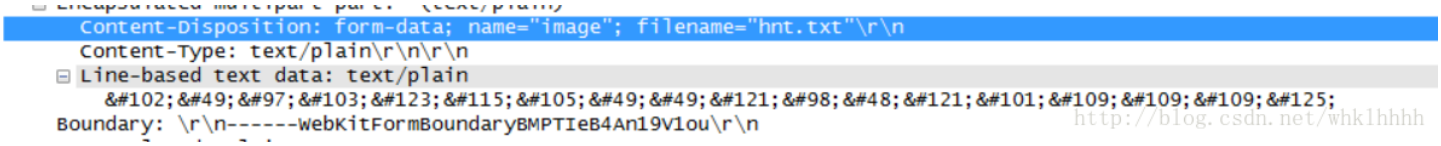

很明显是一个rar压缩包，保存后发现需要密码

手里还有一个pcapng数据包没看，拿来分析
导出为HTTP对象发现大部分都是baidu和sougo的干扰流量
除此以外有两个paste.ubuntu.com的，点开分析发现post参数中有jsfuck，放到控制台里运行就弹出了密码

打开压缩包得到flag

可恶的黑客

查看内容，发现是与黑客的交易对话内容
提示放在hnt.txt里，尝试搜索



找到这里，里面的txt很明显是ASCII
遂转码得到flag