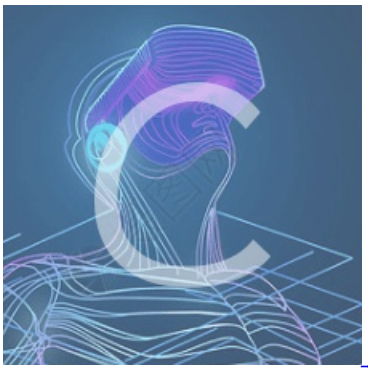
Bugku--杂项一（签到题------猜）

原创

gclome 于 2019-11-16 21:26:12 发布 488 收藏

分类专栏： # CTF

本文链接：https://blog.csdn.net/qq_44108455/article/details/103099666



签到题

傻瓜化操作，直接关注微信公众号，就会把flag发过来

这是一张单纯的图片

我点开链接是这样的，点击右键，将图片下载下来，打开

点击右键，将图片下载下来，打开

用notepad++打开，最后显示了一串编码，解码后得flag

key{you are right}

隐写

打开图片

把图片放到HxD里，根据图片格式，我们发现图片的宽与高有矛盾,更改不合尺寸,把此处的A4改为F4，将图片保存，

2.png

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	对应文本
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG.....IHDR
00000010	00	00	01	F4	00	00	01	F4	08	06	00	00	00	CB	D6	DF	...ô...ô.....ËÖß
00000020	8A	00	00	00	09	70	48	59	73	00	00	12	74	00	00	12	Š....pHYs...t...
00000030	74	01	DE	66	1F	78	00	00	0A	4D	69	43	43	50	50	68	t.Þf.x...MiCCPPh
00000040	6F	74	6F	73	68	6F	70	20	49	43	43	20	70	72	6F	66	otoshop ICC prof
00000050	69	6C	65	00	00	78	DA	9D	53	77	58	93	F7	16	3E	DF	ile..xÚ.SwX"÷.>ß

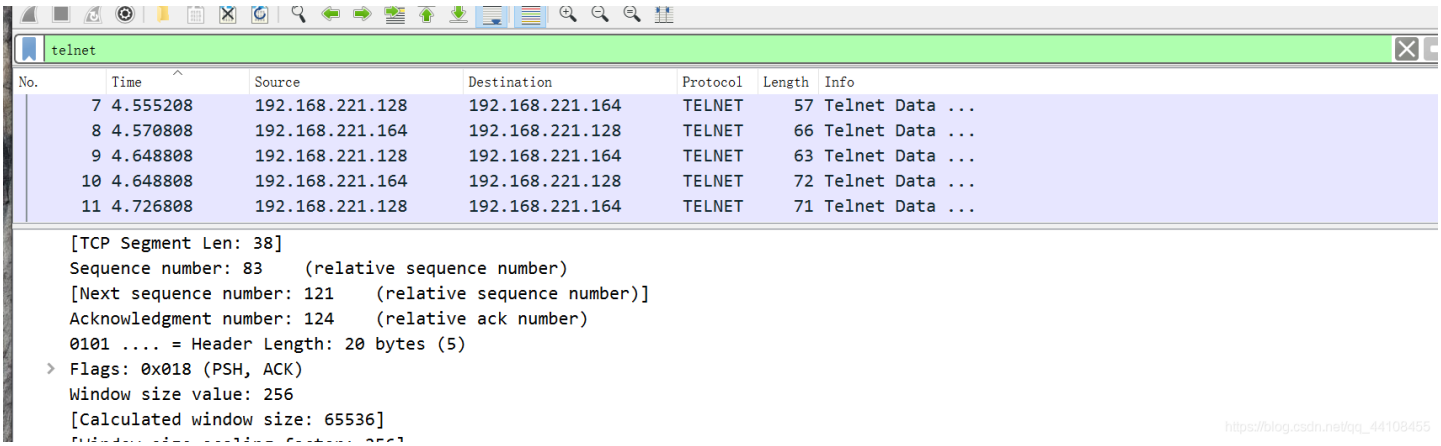
然后打开图片，得到flag

BUGKU{a1e5aSA}

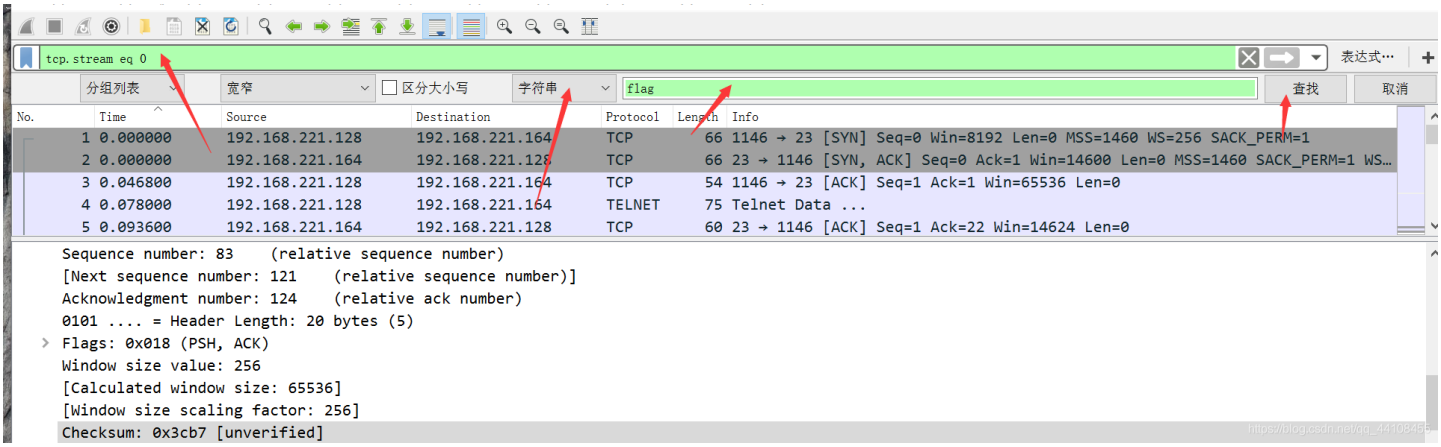
telnet

打开链接，下载了一个流量包

先查找telnet



查找flag



找到之后，追踪tcp流，然后找到了flag

Wireshark · 追踪 TCP 流 (tcp.stream eq 0) · networking.pcap

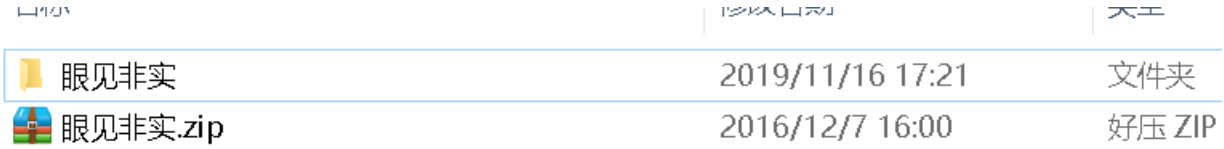
```
..... .....'.............. ..#..'..#.................P..... .....'.......... .
38400,38400....'.......XTERM..........!........!Ubuntu 12.04.2 LTS
hockeyinjune-virtual-machine login: ccssaaww

Password: flag{d316759c281bf925d600be698a4973d5}


Login incorrect
hockeyinjune-virtual-machine login: .
...^C
```

眼见非实(ISCCCTF)

下载下来是一个zip文件，解压得到一个word文档，但是并打不开，尝试修改后缀为txt，png，依旧无果。
看了别人的writeup，发现别人在这里打开了文档，但是乱码，下面出现了FK，然后猜测这是一个压缩包，于是将其后缀改为zip



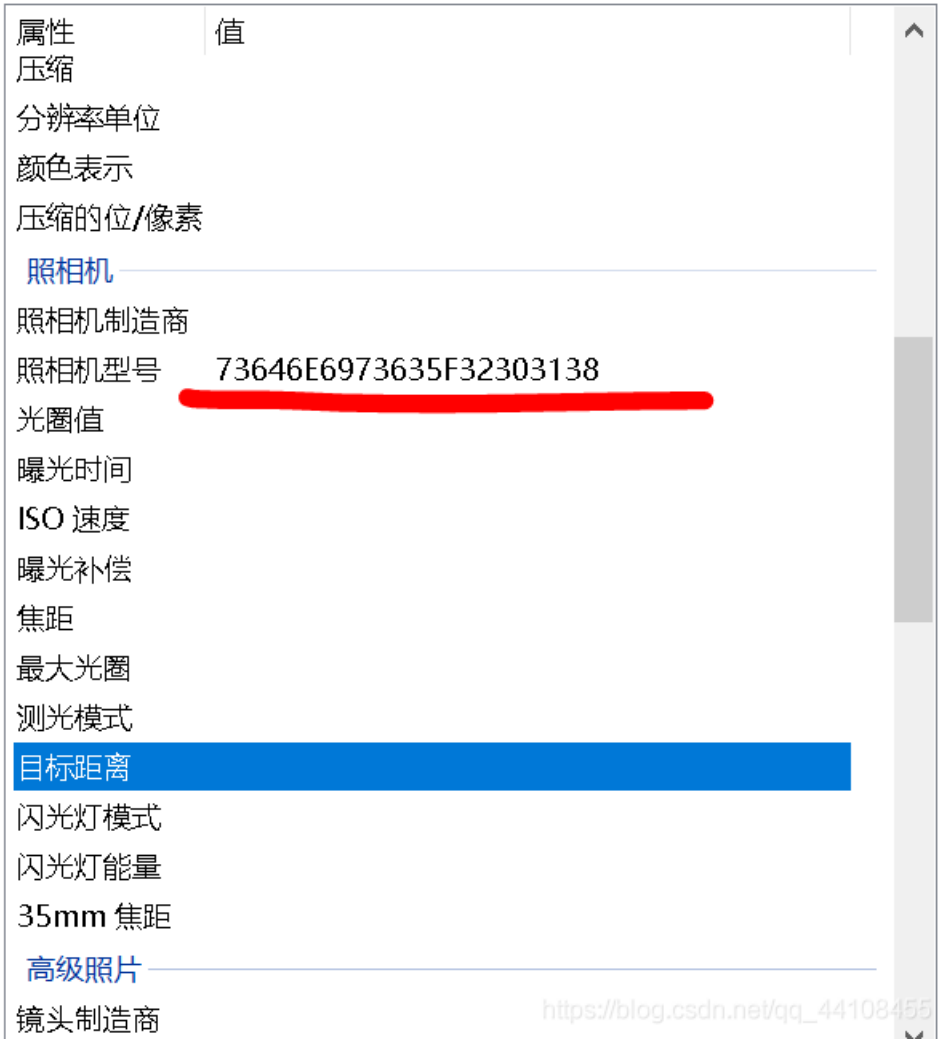
解压缩之后里面

有个document.xml文件，用记事本打开，然后“ctrl+F”，查找flag，就找到flag了。

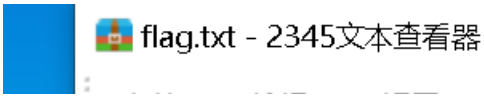
啊哒

下载下来是一张图

查看图片属性，有一串编码（后面有用），然后再无其他发现，



把图片放到notepad++里，这里看见大佬们的writeup里说是这是个压缩文件，(也不知道怎么看出来的),然后修改后缀为ada.zip,不过是加密的，输入上面那串编码ascll hex的`sdnisc_2018`
成功打开得到flag




文件(F) 编辑(E) 视图(V) 格式(M) 工具(T)
flag{3XiF_iNf0rM@ti0n}
https://blog.csdn.net/qq_44108455

又一张图片，还单纯吗

初练杂项，真的好多不会，看了别人的writeup，知道这道题要用binwalk（第一次用binwalk------瑟瑟发抖.jpg）。
写下我的笔记，打开链接一张程序猿

然后j将图片下载下来放到binwalk里
运行`binwalk -e /root/2.jpg`发现捆绑了好几张图片
运行`dd if=/root/2.jpg of=/root/1.jpg skip=158792 bs=1`查看其中一张图片

```
root@kali:~# binwalk -e /root/2.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, EXIF standard
12            0xC             TIFF image data, big-endian, offset of first image di
rectory: 8
158792        0x26C48         JPEG image data, JFIF standard 1.02
158822        0x26C66         TIFF image data, big-endian, offset of first image di
rectory: 8
159124        0x26D94         JPEG image data, JFIF standard 1.02
162196        0x27994         JPEG image data, JFIF standard 1.02
168370        0x291B2         Copyright string: "Copyright (c) 1998 Hewlett-Packard
 Company"

root@kali:~# dd if=/root/2.jpg of=/root/1.jpg skip=158792 bs=1
记录了27689+0 的读入
记录了27689+0 的写出
27689 bytes (28 kB, 27 KiB) copied, 0.128218 s, 216 kB/s
```

打开这张图片，

出现flag（真是学到了!!!），把flag一个个字母敲上去。。

猜

打开图片，是一个明星，只是不知道是谁，而flag就是这个人的名字全拼

于是百度识图哈哈哈，识别出来是刘亦菲，然后 成功了 。。 哈哈哈