bugku writeup(misc_1)

原创

Time-s_up 于 2017-10-01 08:53:29 发布 17151 收藏
分类专栏： ctf writeups 文章标签： CTF writeup misc bugku

题目网址：http://123.206.31.85/challenges

先大体梳理一下图片隐写的一般思路：

1.查看图片属性中的详细信息，2.用notepad打开查看内容，3.binwalk检查图片里是否存在其他文件，4.使用winhex观察或提取信息，5.stegsolve观察图片

分析流量包的一般思路：

1.追踪数据流，2.直接导出文件

1.这是一张单纯的图片？？

30

http://120.24.86.145:8002/misc/1.jpg

FLAG在哪里？？

打开网址，保存图片。用notepad打开发现底部的一串字符

key{you are righ

在线unicode解码 http://tool.chinaz.com/Tools/Unicode.aspx

得key{you are right}

2.

隐写**2**

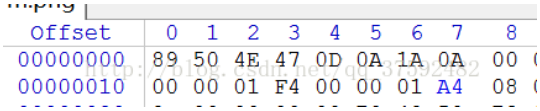
40

下载rar文件，打开得到一张图片。

尝试各种方法后无果。

最后从图片格式入手，更改其高度得到flag

http://blog.csdn.net/bisword/article/details/2777121



Offset	0	1	2	3	4	5	6	7	8
00000000	89	50	4E	47	0D	0A	1A	0A	00
00000010	00	00	01	F4	00	00	01	A4	08

将A4改为F4

BUGKU{a1e5aSA}

3.

telnet

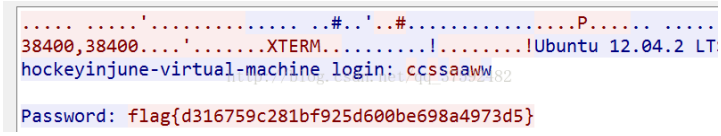
50

http://120.24.86.145:8002/misc/telnet/1.zip

key格式flag{xxxxxxxxxxxxxxxxxxxxxxxxxxxx}

下载文件，打开得到一个流量包，拖进wireshark里面分析。

题目提示telnet，直接右键追踪第一个telnet协议数据包的tcp流得到



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

Password: flag{d316759c281bf925d600be698a4973d5}
```

flag{d316759c281bf925d600be698a4973d5}

4.

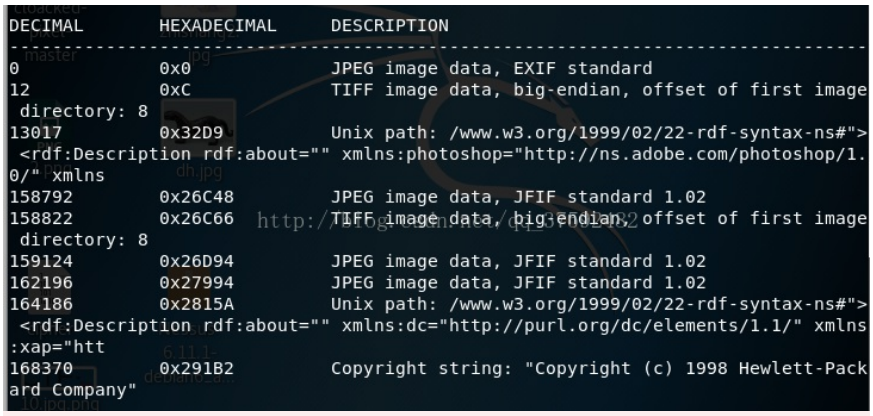
又一张图片，还单纯吗？？

60

http://120.24.86.145:8002/misc/2.jpg

好像和上一个有点不一样

下载图片，binwalk分析后发现里面藏了jpg文件，首地址为0x26C48。用winhex将图片进行手工分离，



```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, EXIF standard
12            0xC             TIFF image data, big-endian, offset of first image
 directory: 8
13017         0x32D9          Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#">
 <rdf:Description rdf:about="" xmlns:photoshop="http://ns.adobe.com/photoshop/1.
0/" xmlns
158792        0x26C48         JPEG image data, JFIF standard 1.02
158822        0x26C66         TIFF image data, big-endian, offset of first image
 directory: 8
159124        0x26D94         JPEG image data, JFIF standard 1.02
162196        0x27994         JPEG image data, JFIF standard 1.02
164186        0x2815A         Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#">
 <rdf:Description rdf:about="" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns
:xap="htt
168370        0x291B2         Copyright string: "Copyright (c) 1998 Hewlett-Pack
ard Company"
```

得到 falg{NSCTF_e6532a34928a3d1dadd0b049d5a3cc57}

falg{NSCTF_e6532a34928a3d1dadd0b049d5a3cc57}

5.

多种方法解决

60

在做题过程中你会得到一个二维码图片

http://120.24.86.145:8002/misc/3.zip

下载文件，得到一个exe的文件。用notepad打开得到一串base64的编码，使用在线base64编码转图片
http://imgbase64.duoshitong.com/

得到二维码

在线扫码 http://jiema.wwei.cn/

得KEY{dca57f966e4e4e31fd5b15417da63269}

6.

猜？

60

http://120.24.86.145:8002/misc/cai/QQ20170221-132626.png

flag格式key{某人名字全拼}

下载图片，根据提示，直接百度识图。图中大美女为刘亦菲。

key{liuyifei}

7.

宽带信息泄露

60

flag格式：
flag{宽带用户名}

下载文件，得到一个conf.bin文件。
使用routerpassview打开该文件，搜索关键字username得到

flag{053700357621}

8.

linux ??????

80

http://120.24.86.145:8002/misc/1.tar.gz

linux基础问题哟

下载文件，解压后得到一个flag文件，直接用notepad打开，搜索关键字key
得到key{feb81d3834e2423c9903f4755464060b}

9.

中国菜刀，不再web里？

80

国产神器
http://120.24.86.145:8002/misc/caidao.zip

下载文件，得到一个流量包，拖进wireshark里面分析，

根据提示是菜刀链接，筛选http协议。

在第三个握手包里发现了包含加密的flag

```
X@Y... w.pW ...Y
.0.....+......['|.
..w..A........CHnrd..a./.T....p..{...D.t.>..v....=.u...i.[9...Y..z.G../o..pN..G..r..:
.}....?.s..w.....c.....R....?..Y.N..*.me...j$)$...f,.i....M.            x..y..S (  X@Y
```

右键显示分组字节，去掉X@Y后压缩解密

```
flag/
000755  000765  000024  00000000000 12734163500 014133  5
ustar 00zhangjianxiang                  staff                           000000  000000
flag/flag.txt
000644  000765  000024  00000000045 12734157617 015620  0
ustar 00zhangjianxiang                  staff                           000000  000000
key{8769fe393f2b998fa6a11afe2bfcd65e}
```

得到

10.

这么多数据包

80

这么多数据包找找吧，先找到getshell的流

用wireshark打开pcapng文件

根据提示，首先找到从104开始，为端口扫描。

继续往下，找到攻击机通过3389端口远程连接目标机，以及smb协议的包

（被用于Web连接和客户端与服务器之间的信息沟通）

从5542开始已经getshell，追踪流后得到字符串。

```
C:\>type s4cr4t.txt
type s4cr4t.txt
Q0NURntkb195b3VfbGlrZV9zbmlmZmVyfQ==
```

base64解密得

CCTF{do_you_like_sniffer}

感想：win10自带的照片查看器，视频播放器真心不好使，导致走了很多弯路，浪费了很多时间。还有360解压缩。。

剩下的过会儿再写。。困了。。