MISC总结

原创

南昌十七 于 2019-07-17 23:03:22 发布 4320 收藏 10
分类专栏： 新知识


新知识 专栏收录该内容
11 篇文章 1 订阅
订阅专栏

流量分析

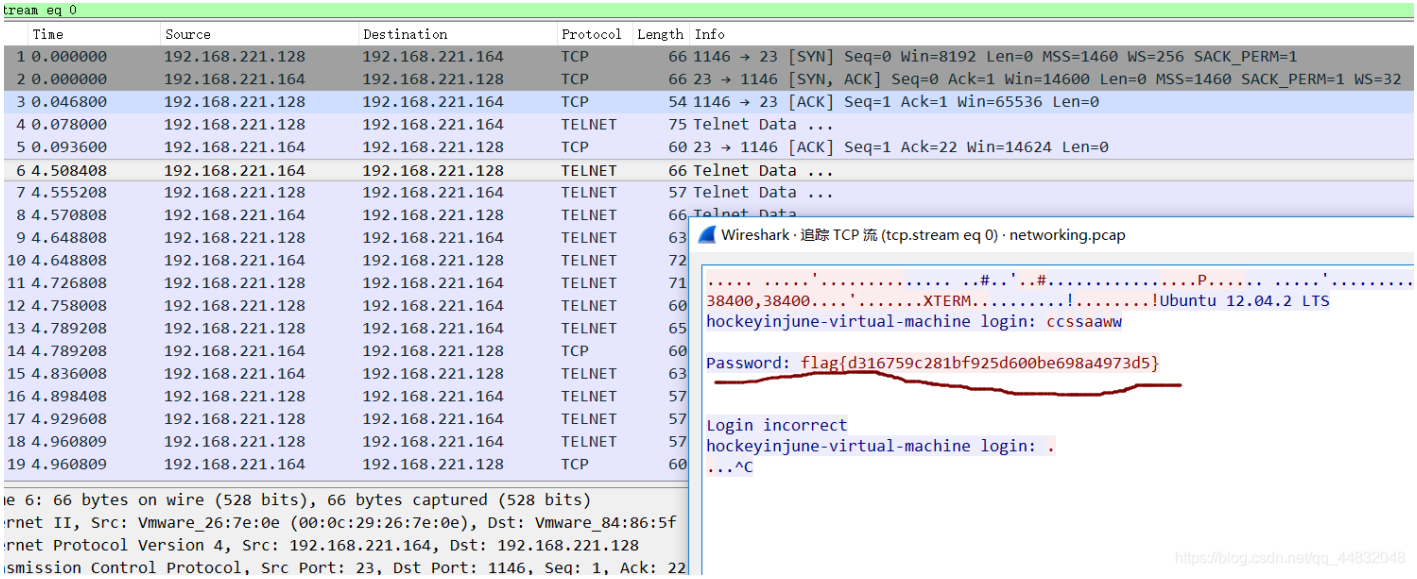
IP过滤

ip.src ==192.168.1.102,显示源地址为192.168.1.102；
ip.dst==192.168.1.102, 显示目标地址为192.168.1.102；
ip.addr == 192.168.1.102,包括源地址和目标地址

bugku-networking.pcap

使用wireshark

telnet是一个远程连接协议，协议端口号为23。
它的特性为明文传输用户和密码。
首先过滤，只查看”telent流”，然后选取一行，右键打开，追踪”TCP流“



题目二

一大段的Len=0,所以我们直接拉到后面，然后追踪数据流，发现了返回了一段加密后的编码，推测可能是base64加密，解密之后得到flag

```
C:\>type s4cr4t.txt
type s4cr4t.txt
Q0NURntkb195b3VfbGlrZV9zbmlmZmVyfQ==
C:\>shutdown -r -t 100 -m "Stupid Manager!"
shutdown -r -t 100 -m "Stupid Manager!"
```

文件格式分析

追踪流后发现有返回的信息中有flag文件，
放在linux下使用binwalk分析提取出来
解压后便可以发现flag

```
up/      2015-06-08 00:36:02     0       0777
uploads/        2015-06-08 00:36:11     0       0777
wcms/    2016-01-17 05:56:46     0       0777
webshop5/       2015-06-08 08:04:59     0       0777
XiaoCms_20140710/       2015-06-03 11:53:31     0       0777
xss/     2016-01-28 06:48:07     0       0777
Z/       2015-06-03 11:53:31     0       0777
1.php    2016-01-28 08:54:46     1740    0666
3.php    2016-06-01 03:36:25     27      0666
flag.tar.gz      2016-06-27 08:45:38     203     0666
log.txt 2015-06-03 12:18:46     1502    0666
news.asp        2014-06-27 03:44:24     365     0666
SaveFile.asp    2014-06-27 05:45:08     822     0666
testNull.php    2014-07-17 08:06:14     16      0666
upload.html     2014-06-27 05:27:46     364     0666
webshell.php    2014-07-21 05:52:36     18      0666
```


bugku隐写2

zip压缩文件。
果然内含zip文件。用dd命令提取。

```
root@cyc:~# binwalk -e Welcome_.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
30            0x1E            TIFF image data, big-endian, offset of first image
 directory: 8
52516         0xCD24          Zip archive data, at least v1.0 to extract, compre
ssed size: 6732, uncompressed size: 6732, name: flag.rar
59264         0xE780          End of Zip archive, footer length: 22
147852        0x2418C         End of Zip archive, footer length: 22

root@cyc:~# dd if=welcome_.jpg of=2.zip skip=52516 bs=1
dd: 打开'welcome_.jpg'失败：没有那个文件或目录
root@cyc:~# dd if=Welcome_.jpg of=2.zip skip=52516 bs=1
记录了95358+0 的读入
记录了95358+0 的写出
95358 bytes (95 kB, 93 KiB) copied, 0.182277 s, 523 kB/s
root@cyc:~# ls
2.zip  视频  下载  deets.txt  todolist.txt            wp-config.php
公共   图片  音乐  Desktop    Welcome_.jpg
模板   文档  桌面  Downloads  _Welcome_.jpg.extracted
```


解压2.zip之后有两个文件。

，一开始以为是rar压缩包，用rar的破解工具提示格式不正确。

然后用file命令一检查，发现是zip压缩文件。

```
root@cyc:~# ls
2.zip  视频  下载  deets.txt  flag.rar      _Welcome_.jpg.extr
公共   图片  音乐  Desktop    todolist.txt  wp-config.php
模板   文档  桌面  Downloads  Welcome_.jpg
root@cyc:~# file flag.rar
flag.rar: Zip archive data, at least v2.0 to extract
```

fcrackzip -b -l 3-3 -c1 -v flag.zip
放到Kali Linux中用fcrackzip工具破解。

flag.rar的密码是三位数。直接暴力破解

```
root@cyc:~# fcrackzip -b -l 3-3 -c1 -v flag.zip
found file '3.jpg', (size cp/uc   6588/  6769, flags 801, chk 102c)
possible pw found: 035 ()
possible pw found: 337 ()
possible pw found: 728 ()
possible pw found: 871 ()
```

得到密码871

解压flag.zip

然后又是一个图片，用16进制跑一下，文件尾处发现flag。

题目一

一个压缩文件，解压后得到一个word文档，打开里面并没有我们想要的，用HxD打开，发现它的文件头是504B0304，文件尾是504B，发现这又是一个压缩文件，加上后缀.zip另存打开在里面的document.xml发现flag。

```
      - <w:rPr>
            <w:rFonts w:hint="eastAsia"/>
            <w:vanish/>
        </w:rPr>
    </w:pPr>
  - <w:r w:rsidRPr="002B3D8D">
      - <w:rPr>
            <w:vanish/>
        </w:rPr>
        <w:t>flag{F1@g}</w:t>
    </w:r>
    <w:bookmarkStart w:name="_GoBack" w:id="0"/>
    <w:bookmarkEnd w:id="0"/>
  </w:p>
- <w:sectPr w:rsidR="002B3D8D" w:rsidRPr="002B3D8D">
    <w:pgSz w:w="11906" w:h="16838"/>
    <w:pgMar w:gutter="0" w:footer="992" w:header="851"
    <w:cols w:space="425"/>
    <w:docGrid w:linePitch="312" w:type="lines"/>
```

无法运行的exe

用HXD打开，看到了一长串base64，尝试了base64解密没成功，用base64图片解密，上传几张png格式的图像，发现它们的头都是一样的，都是iVBORw0KGgoAAAANSUhEUgAAA然后发现原文件里面的和它有的不一样，将A改成o在用base转图片得到了一个二维码，得到flag。

文件分离

通过binwalk我们可以看到这个png文件中还包含着一个zip文件

Binwalk提取文件

命令 binwalk -e+file；

“-e”和“–extract”用于按照定义的配置文件中的提取方法从固件中提取探测到的文件系统

若提取成功则会生成一个_文件名_extracted的目录，目录中存放的就是提取出的文件

使用***dd命令***分离文件格式如下：
dd if=源文件名 of=输出文件名 skip=开始分离的字节数 bs=1；
参数说明：
if=file #输入文件名，缺省为标准输入。
of=file #输出文件名，缺省为标准输出。
bs=bytes #同时设置读写块的大小为 bytes ，可代替 ibs 和 obs 。
skip=blocks #从输入文件开头跳过 blocks 个块后再开始复制。

1、jpg　　jpg图片是经过有损的压缩；
2、png　 png是无损的压缩；
3、gif　　gif可以存放动态的帧；
4、bmp　 bmp是将数据原样储存；

图片隐写

倒立屋

lsb图片隐写；

用stegsolve打开图片，观察发现red、green、blue在最低色度时都看不清，点Data Extract

（:数据抽取，图片中隐藏数据的抽取），勾选Red、Green、Blue颜色的最低位信道然后Preview，然后看到了flag，倒过来就OK。

题目二

Windows下查看下图片的属性

WE1BTntVNWU=base64解码得到XMAN{U5e 可以明显的感觉到是半个flag，

尝试使用16进制编辑器打开查看找到完整的base64 flag加密后的信息，最后解密即可得到flag