MISC杂项签到——writeup

原创

iRudy 于 2016-11-27 14:56:49 发布 2176 收藏 3
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/iRudy/article/details/53364519
版权


CTF 专栏收录该内容
2 篇文章 0 订阅
订阅专栏

这里我们点开链接，下载了一个+_+.pcapng的文件

百度下.pcapng是什么文件，ok，我们知道了这是wireshark的抓包文件，直接用

No.	Time	Source	Destination	Protocol	Length	Info
4	5.193298045	192.168.1.13	192.168.1.111	TCP	74	57370→2333 [SYN] Seq=0 Win=29200 …
5	5.196570242	192.168.1.111	192.168.1.13	TCP	74	2333→57370 [SYN, ACK] Seq=0 Ack=1…
6	5.196689503	192.168.1.13	192.168.1.111	TCP	66	57370→2333 [ACK] Seq=1 Ack=1 Win=…
7	5.199680823	192.168.1.13	192.168.1.111	TCP	145	57370→2333 [PSH, ACK] Seq=1 Ack=1…
8	5.202249651	192.168.1.111	192.168.1.13	TCP	66	2333→57370 [ACK] Seq=1 Ack=80 Win…
9	5.202310224	192.168.1.13	192.168.1.111	TCP	101	57370→2333 [PSH, ACK] Seq=80 Ack=…
10	5.204414677	192.168.1.111	192.168.1.13	TCP	66	2333→57370 [ACK] Seq=1 Ack=115 Wi…
11	5.205558636	192.168.1.13	192.168.1.111	TCP	118	57370→2333 [PSH, ACK] Seq=115 Ack…
12	5.207653614	192.168.1.111	192.168.1.13	TCP	66	2333→57370 [ACK] Seq=1 Ack=167 Wi…
13	7.231511443	192.168.1.111	192.168.1.13	TCP	70	2333→57370 [PSH, ACK] Seq=1 Ack=1…
14	7.231665926	192.168.1.13	192.168.1.111	TCP	66	57370→2333 [ACK] Seq=167 Ack=5 Wi…
15	7.231756955	192.168.1.13	192.168.1.111	TCP	67	57370→2333 [PSH, ACK] Seq=167 Ack…
16	7.241139989	192.168.1.111	192.168.1.13	TCP	66	2333→57370 [ACK] Seq=5 Ack=168 Wi…
17	7.241222815	192.168.1.13	192.168.1.111	TCP	69	57370→2333 [PSH, ACK] Seq=168 Ack…
18	7.243150615	192.168.1.111	192.168.1.13	TCP	66	2333→57370 [ACK] Seq=5 Ack=171 Wi…
19	7.393595593	192.168.1.13	192.168.1.111	TCP	578	57370→2333 [PSH, ACK] Seq=171 Ack…
20	7.429809667	192.168.1.111	192.168.1.13	TCP	66	2333→57370 [ACK] Seq=5 Ack=683 Wi…

http://blog.csdn.net/

说实话，我对流量分析完全不会= =，可是既然它是签到题，那想来也不会太难，

```
bash: cannot set terminal process group (1778): Inappropriate ioctl for
device
bash: no job control in this shell
<test/something/welcome/web/upload_function/upload$ ]ls
]ls
No command ']ls' found, did you mean:
 Command 'ils' from package 'sleuthkit' (universe)
 Command 'als' from package 'atool' (universe)
 Command 'fls' from package 'sleuthkit' (universe)
 Command 'jls' from package 'sleuthkit' (universe)
 Command 'ls' from package 'coreutils' (main)
 Command 'ols' from package 'speech-tools' (universe)
 Command 'hls' from package 'hfsutils' (main)
 Command 'bls' from package 'bacula-sd' (universe)
 Command 'bls' from package 'bareos-tools' (universe)
]ls: command not found
<test/something/welcome/web/upload_function/upload$ ls
ls
c2hlbGw=.php
<test/something/welcome/web/upload_function/upload$ cd ..
cd ..
<lt/evaltest/something/welcome/web/upload_function$ cd ..
cd ..
www@cola:/home/wwwroot/default/evaltest/something/welcome/web$ cd ..
cd ..
www@cola:/home/wwwroot/default/evaltest/something/welcome$ ls
ls
```

一步步看下来，可以看到其中有个**python**的脚本文件，那运行这个文件应该就可

```
cat function.py
#!/usr/bin/env python
# coding:utf-8
__author__ = 'Aklis'

from Crypto import Random
from Crypto.Cipher import AES

import sys
import base64


def decrypt(encrypted, passphrase):
  IV = encrypted[:16]
  aes = AES.new(passphrase, AES.MODE_CBC, IV)
  return aes.decrypt(encrypted[16:])


def encrypt(message, passphrase):
  IV = message[:16]
  length = 16
  count = len(message)
  padding = length - (count % length)
  message = message + '\0' * padding
  aes = AES.new(passphrase, AES.MODE_CBC, IV)
  return aes.encrypt(message)


IV = 'YUFHJKVWFASDGODH'
```

直接搜在线python编程网站，ok，把脚本扔进去。得到了这个flag is hctf{*******

```python
def encrypt(message, passphrase):
    IV = message[:16]
    length = 16
    count = len(message)
    padding = length - (count % length)
    message = message + '\0' * padding
    aes = AES.new(passphrase, AES.MODE_CBC, IV)
    return aes.encrypt(message)


IV = 'YUFHJKVWEASDGQDH'

message = IV + 'flag is hctf{xxxxxxxxxxxxxxx}'


print len(message)

example = encrypt(message, 'Qq4wdrhhyEWe4qBF')
print example
example = decrypt(example, 'Qq4wdrhhyEWe4qBF')
print example
```

http://blog.csdn.net/

run (ctrl+r) copy 分享当前代码 出现故障，请使用这个点击这里

文本方式显示 html方式显示

```
45
h   Y  6:  r  w   su/  >TGf2pi    tm
flag is hctf{xxxxxxxxxxxxxxx}
```

既然这个脚本运行出不了结果，接着找呗。看到这句话，secrect(秘密)：祝贺你

```
<ng/welcome/secret/important_secret/very_important$ cat se
cat secrect
Congratulations on your being cheated.<ng/welcome/secret/
```

http://blog.csdn.net/

接着看，又发现了这个，这很熟悉啊，不就是base64加密吗，扔到在线解密网站

```
cat flag
mbZoEMrhAO0WWeugNjqNw3U6Tt2C+rwpgpbdWRZgfQI3MAh0sZ9qjnziUKkV90XhAOkIs/
OXoYVw5uQDjVvgNA==<mething/welcome/secret/not_important_secret/trash$ ls
```

http://blog.csdn.net/

可是解密之后完全乱码啊= =，之后我就完全没头绪了，尝试了各种解密方法。。

```
mbZoEMrhAO0WWeugNjqNw3U6Tt2C+rwpgpbdWRZgfQI3MAh0sZ9qjnziUKkV90XhAOkIs/OXoYVw5uQDj
VvgNA==
```

编码 解码 解码结果以16进制显示

http://blog.csdn.net/

Base64编码或解码结果：

```
h2  :ð:N)70{ tj| E  p
```

吃饭休息了一会，接着看呗，慢慢的我觉得这个python应该是有用的吧，否则放一句一句翻译呗。首先，它构造了两个函数，encrypt（加密），decrypt（解密），貌似前面的flag不就是经过了加密的吗，ok,又有点思路了，看来这个python脚本还是很重要的。我们注意到，脚本最后的两句：把message加密后赋值给example,再把example解密输出。ok，我们只要把前面一长串的base64的代码放到decrypt()后面的参数里，解密输出不就行了吗。

```
example = encrypt(message, 'Qq4wdrhhyEWe4qBF')
print example
example = decrypt(example, 'Qq4wdrhhyEWe4qBF')
print example
```

http://blog.csdn.net/

那我们就修改下代码，什么鬼，还报错了= =，这个签到题有毒。看看报错信息，貌

```
34
35  example = encrypt(message, 'Qq4wdrhhyEWe4qBF')
36  print example
37  code='mbZoEMrhAO0WWeugNjqNw3U6Tt2C+rwpgpbdWRZgfQI3MAh0sZ9qjnziUKkV90XhAOkIs/OXoYVw5uQDjVvgNA=='
38  example = decrypt(code, 'Qq4wdrhhyEWe4qBF')
39  print example
```

run (ctrl+r) | copy | 分享当前代码 出现故障，请使用这个点击这里

文本方式显示 html方式显示

```
45
??h???Y??6:??r??w???su?/??>TGf?2pi????tm
Traceback (most recent call last):
  File "code", line 38, in <module>
    example = decrypt(code, 'Qq4wdrhhyEWe4qBF')
  File "code", line 15, in decrypt
    return aes.decrypt(encrypted[16:])
  File "/usr/local/lib/python2.7/dist-packages/Crypto/Cipher/blockalgo.py", line 295, in decrypt
    return self._cipher.decrypt(ciphertext)
ValueError: Input strings must be a multiple of 16 in length
```

http://blog.csdn.net/

没思路啊，先干点别的事再来。接着开干的时候，我才想到flag加密后是不是又经过了base64加密= =很有可能啊。那就先用base64解密，再丢进脚本解密啊。然后。。。flag就出来了= =卧槽啊，一道签到题用了我一天时间，还是要努力啊！！！

```
33  print len(message)
34
35  example = encrypt(message, 'Qq4wdrhhyEWe4qBF')
36  print example
37  code='mbZoEMrhAO0WWeugNjqNw3U6Tt2C+rwpgpbdWRZgfQI3MAh0sZ9qjnziUKkV90XhAOkIs/OXoYVw5uQDjVvgNA=='
38  code=base64.b64decode(code)
39  example = decrypt(code, 'Qq4wdrhhyEWe4qBF')
40  print example
```

run (ctrl+r) | copy | 分享当前代码 出现故障，请使用这个点击这里

http://blog.csdn.net/

文本方式显示 html方式显示

```
45
??h???Y??6:??r??w???su?/??>TGf?2pi????tm
flag is hctf{n0w_U_w111_n0t_f1nd_me}
```