

# CTF流量分析题

原创

进一寸有一寸的欢喜077 于 2021-05-03 21:47:57 发布 941 收藏 7

分类专栏: [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/m0\\_37442062/article/details/116378287](https://blog.csdn.net/m0_37442062/article/details/116378287)

版权



[ctf](#) 专栏收录该内容

11 篇文章 1 订阅

订阅专栏

1.flag被盗了, [pcap](#) (gnnl)

尝试http过滤, get或者post追踪tcp流即可, 这里是post.

No.	Time	Source address	Source port	Destination	Destination port	Protocol	Length	Info
27	2017-09-12 12:14:16	192.168.228.1	52711	192.168.228.1...	80	HTTP	430	GET /shell.php HTTP/1.1
29	2017-09-12 12:14:16	192.168.228.135	80	192.168.228.1	52711	HTTP	257	HTTP/1.1 200 OK
34	2017-09-12 12:14:17	192.168.228.1	52711	192.168.228.1...	80	HTTP	430	GET /shell.php HTTP/1.1
36	2017-09-12 12:14:17	192.168.228.135	80	192.168.228.1	52711	HTTP	256	HTTP/1.1 200 OK
90	2017-09-12 12:14:31	192.168.228.1	52713	192.168.228.1...	80	HTTP	841	POST /shell.php HTTP/1.1 (application/x-www-form-urlencoded)
93	2017-09-12 12:14:31	192.168.228.135	80	192.168.228.1	52713	HTTP	301	HTTP/1.1 200 OK (text/html)
103	2017-09-12 12:14:33	192.168.228.1	52713	192.168.228.1...	80	HTTP	847	POST /shell.php HTTP/1.1 (application/x-www-form-urlencoded)
105	2017-09-12 12:14:33	192.168.228.135	80	192.168.228.1	52713	HTTP	251	HTTP/1.1 200 OK (text/html)
110	2017-09-12 12:14:34	192.168.228.1	52713	192.168.228.1...	80	HTTP	839	POST /shell.php HTTP/1.1 (application/x-www-form-urlencoded)
112	2017-09-12 12:14:34	192.168.228.135	80	192.168.228.1	52713	HTTP	239	HTTP/1.1 200 OK (text/html)
127	2017-09-12 12:14:43	192.168.228.1	52716	192.168.228.1...	80	HTTP	513	GET / HTTP/1.1
132	2017-09-12 12:14:43	192.168.228.135	80	192.168.228.1	52716	HTTP	659	HTTP/1.1 200 OK (text/html)
133	2017-09-12 12:14:43	192.168.228.1	52716	192.168.228.1...	80	HTTP	472	GET /icons/ubuntu-Logo.png HTTP/1.1
135	2017-09-12 12:14:43	192.168.228.135	80	192.168.228.1	52716	HTTP	234	HTTP/1.1 304 Not Modified

```
X@Yflag{This_is_a_f10g}
[S]
/var/www/html
[E]
X@YPOST /shell.php HTTP/1.1
X-Forwarded-For: 44.146.238.198
Referer: http://192.168.228.135/
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (compatible; Baiduspider/2.0; +http
https://blog.csdn.net/m0_37442062
```

flag{This\_is\_a\_f10g}

2.这么多数据包找找吧, 先找到getshell的流[pcap](#) (vn78)

过滤tcp

	Source address	Source port	Destination	Destination port	Protocol	Length	Info
:45:22	192.168.116.138	4444	192.168.116.1...	1040	TCP	60	4444 → 1040 [ACK] Seq=1207282 Ack=24509 Win=64240 Len=0
:45:22	192.168.116.159	1040	192.168.116.1...	4444	TLSv1	256	Application Data, Application Data
:45:22	192.168.116.138	4444	192.168.116.1...	1040	TCP	60	4444 → 1040 [ACK] Seq=1207282 Ack=24771 Win=64240 Len=0
:45:26	192.168.116.138	35880	192.168.116.1...	1234	TCP	74	35880 → 1234 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1661501 TSecr=0
:45:26	192.168.116.159	1234	192.168.116.1...	35880	TCP	78	1234 → 35880 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 TSval=1661501 TSecr=0
:45:26	192.168.116.138	35880	192.168.116.1...	1234	TCP	66	35880 → 1234 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=1661501 TSecr=0
:45:26	192.168.116.159	1234	192.168.116.1...	35880	TCP	154	1234 → 35880 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=88 TSval=30042 TSecr=0

TCP流通常是命令行操作

```

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is B03C-791A

Directory of C:\

04/14/2016  08:50 PM                0 AUTOEXEC.BAT
04/14/2016  08:50 PM                0 CONFIG.SYS

04/14/2016  08:52 PM   <DIR>                Documents and Settings
03/12/2012  10:24 PM   61,454 nc.exe
04/14/2016  08:54 PM   <DIR>                Program Files
04/14/2016  09:22 PM                36 s4cr4t.txt
04/14/2016  08:59 PM   <DIR>                WINDOWS
                4 File(s)                61,490 bytes
                3 Dir(s) 17,719,083,008 bytes free

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

```

[https://blog.csdn.net/m0\\_37442062](https://blog.csdn.net/m0_37442062)

Q0NURntkb195b3VfbGlrZV9zbmlmZmVyfQ==

解码: CCTF{do\_you\_like\_sniffer}

3.有一天皓宝宝没了流量只好手机来共享, 顺便又从手机发了点小秘密到电脑, 你能找到它吗? pcap (kbeg)

过滤obex

No.	Time	Source address	Source port	Destination	Destination port	Protocol	Length	Info
19389	2016-09-28 14:01:19	localhost ()		remote ()		OBEX	20	Sent Connect
19393	2016-09-28 14:01:19	remote ()		localhost ()		OBEX	26	Rcvd Success
19394	2016-09-28 14:01:19	localhost ()		remote ()		OBEX	670	Sent Put continue "secret.rar"
19401	2016-09-28 14:01:21	remote ()		localhost ()		OBEX	22	Rcvd Continue
19402	2016-09-28 14:01:21	localhost ()		remote ()		OBEX	19	Sent Put final
19404	2016-09-28 14:01:21	localhost ()		localhost ()		OBEX	25	Rcvd Success
19421	2016-09-28 14:01:28	localhost ()		remote ()		OBEX	21	Sent Disconnect
19423	2016-09-28 14:01:28	remote ()		localhost ()		OBEX	22	Rcvd Success
38018	2016-09-28 14:03:19	localhost ()		remote ()		OBEX	20	Sent Connect
38042	2016-09-28 14:03:19	remote ()		localhost ()		OBEX	26	Rcvd Success
38046	2016-09-28 14:03:19	localhost ()		remote ()		OBEX	184	Sent OBEX fragment
38048	2016-09-28 14:03:19	localhost ()		remote ()		OBEX	184	Sent OBEX fragment
38050	2016-09-28 14:03:19	localhost ()		remote ()		OBEX	184	Sent OBEX fragment
38054	2016-09-28 14:03:19	localhost ()		remote ()		OBEX	184	Sent OBEX fragment
38061	2016-09-28 14:03:19	localhost ()		remote ()		OBEX	184	Sent OBEX fragment
38066	2016-09-28 14:03:19	localhost ()		remote ()		OBEX	184	Sent OBEX fragment
38069	2016-09-28 14:03:19	localhost ()		remote ()		OBEX	184	Sent OBEX fragment
38075	2016-09-28 14:03:19	localhost ()		remote ()		OBEX	184	Sent OBEX fragment
38080	2016-09-28 14:03:19	localhost ()		remote ()		OBEX	184	Sent OBEX fragment
38084	2016-09-28 14:03:19	localhost ()		remote ()		OBEX	184	Sent OBEX fragment
38118	2016-09-28 14:03:19	localhost ()		remote ()		OBEX	184	Sent OBEX fragment
38127	2016-09-28 14:03:19	localhost ()		remote ()		OBEX	184	Sent OBEX fragment
38130	2016-09-28 14:03:19	localhost ()		remote ()		OBEX	736	Sent Put continue "-27b5cab3b6cc4b1e.jpg"
38945	2016-09-28 14:03:20	remote ()		localhost ()		OBEX	22	Rcvd Continue
38946	2016-09-28 14:03:20	localhost ()		remote ()		OBEX	19	Sent Put final
38968	2016-09-28 14:03:20	remote ()		localhost ()		OBEX	25	Rcvd Success
42015	2016-09-28 14:03:28	localhost ()		remote ()		OBEX	21	Sent Disconnect
42080	2016-09-28 14:03:28	remote ()		localhost ()		OBEX	22	Rcvd Success

尝试导出分组字节流，无效

```

OBEX Protocol
  [Profile: Unknown (0)]
  [Current Path: /]
  .000 0010 = Opcode: Put (0x02)
  0... .... = Final Flag: False
  Packet Length: 656
  [Response in Frame: 19401]
  Headers
    > Connection Id: 1
    > Name: "secret.rar"
      > Header Id: Name (0x01)
        Length: 25
        Name: secret.rar
      > Length: 615
        > Header Id: Length (0xc3)
          Length: 615
      > Body
        > Header Id: Body (0x48)
          Length: 618
          Value: 526172211a0700cf907300000d000000000000015ae7400902d001f0200001f0200002...
0030 00 02 67 48 02 6a 52 61 72 21 1a 07 00 cf 90 73  ..gH·jRa r!.....s
0040 00 00 0d 00 00 00 00 00 00 00 15 ae 74 00 90 2d  .....t...
0050 00 1f 02 00 00 1f 02 00 00 02 03 2f 7c 6f d4 b0  .|.....|o..
0060 36 49 14 30 08 00 20 00 00 00 66 6c 61 67 2e 67  6I·0····flag.g
0070 69 66 00 b0 34 4b 19 47 49 46 38 39 61 b2 00 3f  if··4K·G IF89a··?
0080 00 80 00 00 00 00 00 ff ff ff 21 f9 04 00 00 00  .....!.....
0090 00 00 2c 00 00 00 00 b2 00 3f 00 00 02 ff 8c 8f  ..,.....?.....
00a0 a9 cb ed 0f a3 9c b4 da 8b b3 de bc fb 0f 86 e2  .....
00b0 48 96 e6 89 a6 ea ca b6 ee 0b c7 f2 4c d7 f6 8d  H.....L...
00c0 e7 fa ce f7 fe 0f 0c 0a 87 c4 a2 f1 88 4c 2a 97  .....L*
00d0 cc a6 f3 09 88 4a 0f 80 87 f4 fa 74 5e b1 81 a8  ....J...t^...
00e0 a2 da dd 4e 0d dc ec 10 cc 40 93 c1 ea 85 57 d2  ...N....@...W·
00f0 36 c7 e2 88 36 9a 5e a7 e0 e5 9e f8 96 ea a0 f6  6··6·^······
0100 d6 65 a5 07 43 b7 67 b3 27 18 78 97 17 68 f8 82  ·e·C·g·'x·h·
0110 f8 b3 f8 d8 c0 c6 08 39 91 68 32 e9 53 09 a8 69  .....9·h2·S·i
0120 57 b8 79 e8 46 79 69 99 16 96 c0 09 aa 0a 0b c1  W·y·Fyi······
0130 f9 75 fa 99 1a 7a 39 88 bb ca 1b 4b 56 31 db 5a  ·u··z9···KV1·Z
0140 db f3 4a 68 e5 47 3a bc 9b 56 96 db 2c 4c db c7  ··Jh·G:··V··,L·
0150 81 dc 1b 26 06 8d ed e6 27 e6 75 fd bb b6 f9 57  ··&····'u···W
0160 bd ac 11 9c 4c 8e 0e eb a9 dd 98 ed f8 9d 1c bc  ···L······
0170 3e 4d 9f dd 9a 38 1a cd 7e ab fa 6e 1c 1f 41 17  >M··8··~··n··A·
0180 bc 0d 63 a8 88 e3 86 70 cd 33 7c f6 06 ea 53 36  ··c···p·3|··S6
0190 d0 9f bc 74 f7 b8 e4 0b c5 4d a1 b7 8c f6 83 10  ···t····M····
01a0 be c9 e4 cb e1 bc 2f c5 22 e2 9a e8 90 19 46 7b  ·····/·"····F{
01b0 6c 1a 52 03 77 f1 e5 3f 8a 17 43 d2 7c 28 51 5c  l·R·w··?··C·|(Q\
01c0 34 6f ca 5a aa 13 f9 30 62 95 98 38 ef f1 4b 39  4o·Z···0 b·8··K9
01d0 13 62 2c 90 23 7d 15 f3 b9 0c 6a 4a 99 dd b0 51  ·b,·#}····jJ···Q
01e0 ad c3 d0 e9 39 97 96 9a a2 7b 0a f4 51 cd a9 58  ···9····{··Q··X

```

Bytes 54-668: Value (obex.header.value.byte\_sequence)

[https://blog.csdn.net/m0\\_3742062](https://blog.csdn.net/m0_3742062)

可以看到右侧有一个flag.gif

把选中部分粘贴到二进制编辑器中，保存为secret.rar，解压得到flag.gif。如下图



4.你能从截取的数据包中得到flag吗?

easycap 10 最佳Writeup由BinPr1me • zh\_cn提供

难度系数: 2.0

题目来源: bsidessf-ctf-2017

题目描述: 你能从截取的数据包中得到flag吗?

题目场景: 暂无

题目附件: 附件1

[https://blog.csdn.net/m0\\_37442062](https://blog.csdn.net/m0_37442062)

统计,发现tcp只有一条

Wireshark · Conversations · d5ba8f87969145059170a222f01e7883.pcap

Ethernet · 1 | IPv4 · 1 | IPv6 | TCP · 1 | UDP

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
172.31.98.199	46046	192.155.81.86	7890	82	5466	42	2818	40	2648

[https://blog.csdn.net/m0\\_37442062](https://blog.csdn.net/m0_37442062)

follow stream

FLAG:385b87afc8671dee07550290d16a8071

FLAG:385b87afc8671dee07550290d16a8071

5.黑客通过wireshark抓到管理员登陆网站的一段流量包（管理员的密码即是答案）。flag提交形式为flag{XXXX}

wireshark-1 12 最佳Writeup由admin提供

难度系数: ★ 1.0

题目来源: 广西首届网络安全选拔赛

题目描述: 黑客通过wireshark抓到管理员登陆网站的一段流量包（管理员的密码即是答案）。flag提交形式为flag{XXXX}

题目场景: 暂无

题目附件: 附件1

[https://blog.csdn.net/m0\\_37442062](https://blog.csdn.net/m0_37442062)

Filter: (http.request or ssl.handshaketype == 1) and !(udp.port eq 1900)

No.	Time	Source address	Source port	Destination	Destination port	Protocol	Length	Info
10	2015-06-29 15:10:22	192.168.1.102	22493	115.239.211.92	80	HTTP	644	OPTIONS /v.gif?pid=307&ty...=3075&l=47365&t=0&s
20	2015-06-29 15:10:22	192.168.1.102	22494	115.231.236.1...	80	HTTP	863	POST /user.php?action=login&do=login HTTP/1.1
33	2015-06-29 15:10:22	192.168.1.102	22495	220.181.57.241	80	HTTP	1094	GET /hm.gif?cc=1&ck=1&cl=4-bit&ds=1366x768&ep
48	2015-06-29 15:10:25	192.168.1.102	22494	115.231.236.1...	80	HTTP	676	GET /user.php?action=login&email=flag HTTP/1.1
64	2015-06-29 15:10:25	192.168.1.102	22494	115.231.236.1...	80	HTTP	690	GET /captcha.php HTTP/1.1
83	2015-06-29 15:10:25	192.168.1.102	22497	220.181.164.39	80	HTTP	938	GET /h.js?c12f88b5c1cd041a732dea597a5ec94c HTT
107	2015-06-29 15:10:25	192.168.1.102	22502	180.149.134.2...	80	HTTP	633	GET /b.gif?uid=&refer=www.wooyun.org&url=http%
108	2015-06-29 15:10:25	192.168.1.102	22495	220.181.57.241	80	HTTP	1163	GET /hm.gif?cc=1&ck=1&cl=24-bit&ds=1366x768&ep
122	2015-06-29 15:10:25	192.168.1.102	22504	220.181.57.241	80	HTTP	1045	GET /hm.gif?cc=1&ck=1&cl=24-bit&ds=1366x768&et
133	2015-06-29 15:10:26	192.168.1.102	22495	220.181.57.241	80	HTTP	1243	GET /hm.gif?cc=1&ck=1&cl=24-bit&ds=1366x768&ep=%

Source Address: 192.168.1.102  
Destination Address: 115.231.236.116  
Transmission Control Protocol, Src Port: 22494, Dst Port: 80, Seq: 810, Ack: 1550, Len: 622  
Source Port: 22494  
Destination Port: 80

```
POST /user.php?action=login&do=login HTTP/1.1
Host: www.wooyun.org
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://www.wooyun.org/user.php?action=login
Cookie: __cfduid=d473db479254a41d53bd0aae31cb7dc3b1433775400; Hm_lvt_c12f88b5c1cd041a732dea597a5ec94c=1434891316,143528:bdshare_firsttime=1433775454650; wy_uid=-1; PHPSESSID=h8i10mi6rdc8l9coc708otq661; Hm_lpvt_c12f88b5c1cd041a732dea597a5ec94c=143528
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 65

email=flag&password=ffb7567a1d4f4abdfdb54e022f8facd&captcha=BYUGHTTP/1.1 200 OK
Date: Mon, 29 Jun 2015 15:09:10 GMT
```

flag{ffb7567a1d4f4abdfdb54e022f8facd}

6.



先找到了get语句

Destination port	Protocol	Length	Info	Host
81	HTTP	286	GET /?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),1,1))=32%23	localhost:81
81	HTTP	286	GET /?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),1,1))=33%23	localhost:81
81	HTTP	286	GET /?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),1,1))=34%23	localhost:81
81	HTTP	286	GET /?id=1'%20and%20ascii(substring((select%20keyid%20from%20flag%20limit%200,1),1,1))=35%23	localhost:81

substring函数是取字符串的特定位置，此处参考[攻防世界 Misc高手进阶区 7分题 流量分析](#)

```
import re

with open("/Users/yueting/下载/4d7c14206a5c4b74a0af595992bbf439.pcapng", "rb") as f:
    contents = f.read()
    res = re.compile(r'0,1\\),(\d+),1\\)\)=(\d+)%23').findall(str(contents))
    dic = {}
    #取a对应b的最大值
    for a, b in res:
        if a in dic:
            if int(b) > dic[a]:
                dic[a] = int(b)
        else:
            dic[a] = int(b)
    flag = ""
    for i in range(1,39):
        flag += chr(dic[str(i)])
    print(flag)
```

flag{c2bbf9cecdaf656cf524d014c5bf046c}

8.

traffic 最佳Writeup由皓月123456提供

难度系数: 7.0

题目来源: 厦门邀请赛

题目描述: 暂无

题目场景: 暂无

题目附件: 附件1

[https://blog.csdn.net/m0\\_37442062](https://blog.csdn.net/m0_37442062)

明天再来吧



