

i春秋misc-可恶的黑客-150分

原创

萌萌哒的baola 于 2020-10-06 09:20:33 发布 254 收藏

分类专栏: [ctf题解](#)

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/Claming_D/article/details/108936227

版权



[ctf题解](#) 专栏收录该内容

20 篇文章 0 订阅

订阅专栏

i春秋misc-可恶的黑客-150分

题目链接: https://pan.baidu.com/s/1QmVISuLydb6Cf_UOr4LcRA 密码: 08bu

做题感受: 常规题, 一般思路即可。

题目分析

这题属于流量包分析, 应用层协议是http, 那么主要分析http就行。查看分析每一个tcp流, 分析第二道流的时候发现一个图片hack.png(想法: 可能是线索, 搞出来分析一波)

将图片复制出来, 分析无果。继续下一道流。

在分析过程中, 我们可以发现有两个人利用1.php(webshell)进行交易(留言)。根据谈话的内容我们知道交易的对象就是flag。14道流里面给出了线索, 根据线索继续查看流

```
Wireshark · Follow TCP Stream (tcp.stream eq 2) · 可恶的黑客.pcapng

GET /dirtrav/example2.php?file=/var/www/files/hacker.png HTTP/1.1
Host: 10.211.55.15
Connection: keep-alive
Accept: image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_5) AppleWebKit/603.2.4 (KHTML, like Gecko) Version/10.1.1 Safari/603.2.4
Accept-Language: zh-cn
Referer: http://10.211.55.15/
Accept-Encoding: gzip, deflate

HTTP/1.1 200 OK
Date: Wed, 09 Aug 2017 02:40:49 GMT
Server: Apache/2.2.16 (Debian)
X-Powered-By: PHP/5.3.3-7+squeeze15
Cache-Control: public
Content-Disposition: inline; filename="hacker.png";
```

```
Content-Transfer-Encoding: binary
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 24074
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html
```

```
.....=|.P.M.....%8....%H.....'.Cp'.].w.....{...US.5.....s....
(5.Y4dbd...&/'...@.w ..\1b...8!9.....(8..P..l...n.....0f.....$......$).....
(=m.l(.l.)e.....h.....y)q-.i....u....+AL...rrI9w.X]...} ...9.....9..NUp.[...>...
.n;.....r.....+..T.|V.f[y9.._BS.*....lS...[...>v...)..N.{m.\{..0.hj... (g...@=10.
(g.c8.....D.7.V./0...=P.^..d....I.....t.....c.x<.....
7.....x.....E.@..rrr...F.....X.....j...L.c.BK[[.8 ...S.....`S.....#Q..
4~.K.....?.....T..4.....Sp.....}.....
%.0.I.o.....Kp...l.R.@.~..."/.D}.c>...[.0*......'i...AZ.7'..Pk"..L .....7...d[...
```

Packet 28. 1 client pkt, 17 server pkts, 1 turn. Click to select.

Entire conversation (24 kB)

Show and save data as

ASCII

Stream

2

Find:

Find Next

Help

Filter Out This Stream

Print

Save as...

Back

Close

https://blog.csdn.net/Gaming_D

在16道流中发现 hnt.txt

```
.P..q.k!==.5.....6.{y1....4.9.....G.i.t...h.....v.....oq.
8;..&..]...e..K.>.....~.v?.._J....W..e... POST /upload/example1.php HTTP/1.1
Host: 10.211.55.15
Content-Type: multipart/form-data; boundary=-----WebKitFormBoundaryBMPTIeB4An19V1ou
Origin: http://10.211.55.15
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_5) AppleWebKit/603.2.4 (KHTML,
like Gecko) Version/10.1.1 Safari/603.2.4
Referer: http://10.211.55.15/upload/example1.php
Content-Length: 384
Accept-Language: zh-cn
```

```
-----WebKitFormBoundaryBMPTIeB4An19V1ou
Content-Disposition: form-data; name="image"; filename="hnt.txt"
Content-Type: text/plain
%102;%49;%97;%103;%123;%115;%105;%49;%49;%121;%98;%48;%121;%101;%109;%109;
%109;%125;
-----WebKitFormBoundaryBMPTIeB4An19V1ou
Content-Disposition: form-data; name="send"

Send file
-----WebKitFormBoundaryBMPTIeB4An19V1ou
HTTP/1.1 200 OK
Date: Wed, 09 Aug 2017 02:48:09 GMT
Server: Apache/2.2.16 (Debian)
X-Powered-By: PHP/5.3.3-7+squeeze15
```

Packet 458. 7 client pkts, 21 server pkts, 7 turns. Click to select.

Entire conversation (30 kB)

Show and save data as

ASCII

Stream

16

https://blog.csdn.net/Gaming_D

Connection: Keep-Alive
Content-Type: text/html

```
|ai,i don't want do this,just look look xml sql!|<
```

6 client pkts, 3 server pkts, 5 turns.

Entire conversation (3264 bytes) Show and save data as ASCII Stream 14

Find: 1 Find Next

Help Filter Out This Stream Print Save as... Back Close

https://blog.csdn.net/qq_36059314_2

发送的内容是Unicode编码的

```
&#102;&#49;&#97;&#103;&#123;&#115;&#105;&#49;&#49;&#121;&#98;&#48;&#121;&#101;&#109;&#109;&#125;
```

解码得到:

<pre>&#102;&#49;&#97;&#103;&#123;&#115;&#105;&#49;&#49;&#121;&#98;&#48;&#121;&#101;&#109;&#109;&#125;</pre>	<pre>flag{si11yb0yemmm}</pre>
---	-------------------------------

flag{si11yb0yemmm}

将1改为l即: flag{si11yb0yemmm}

总结

考察http协议内容的分析，出题类型比较常规。