CTF Wireshark Test-flag-please-ignore

原创

艺博东 于 2020-10-06 17:59:31 发布 9552 收藏 6

分类专栏： 网络攻防 文章标签： CTF

本文链接：https://blog.csdn.net/HYD696/article/details/108905997

网络攻防 专栏收录该内容

24 篇文章 17 订阅

订阅专栏

文章目录

一、Wireshark

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)

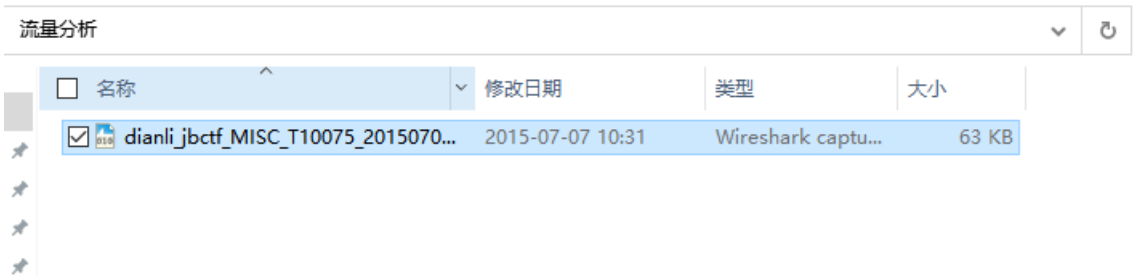
题目附件： 附件1

1、 附件1

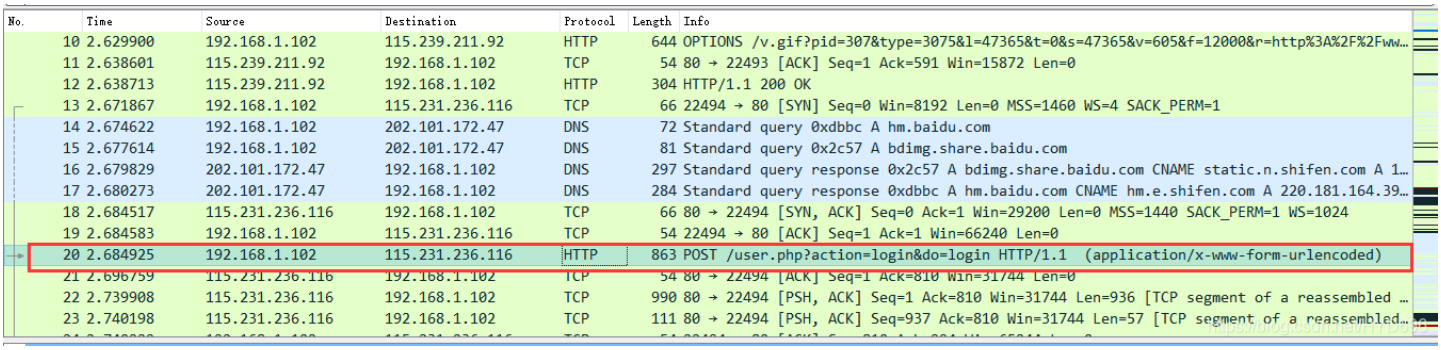
链接：https://pan.baidu.com/s/1fD_SHM1d1_EFc7tx7KVmow

提取码：f20n

2、文件



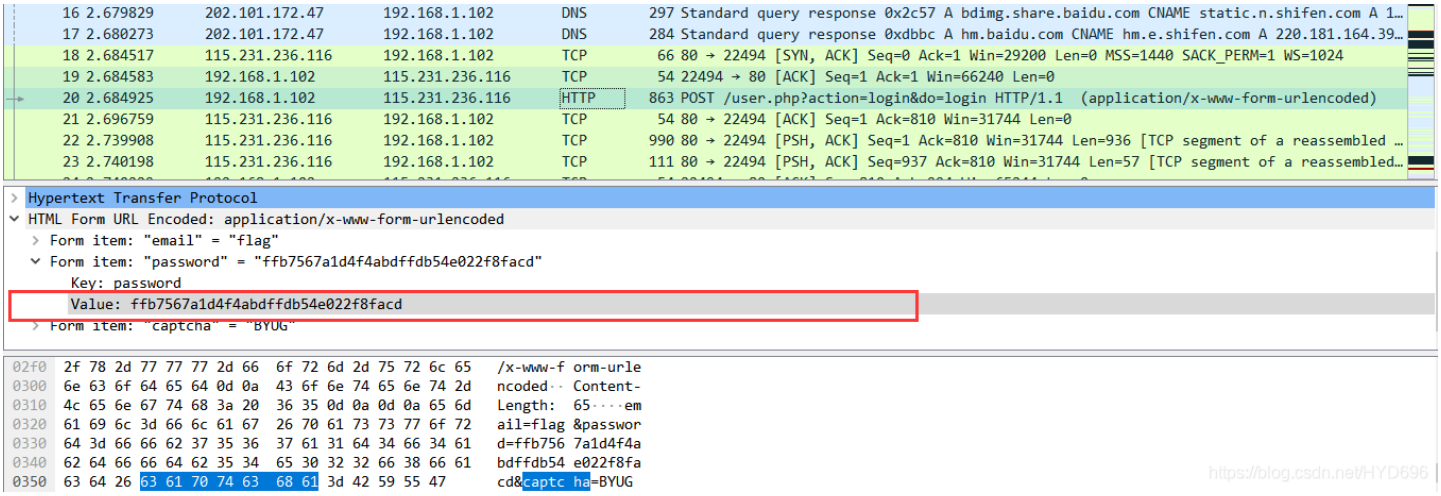
3、用“Wireshark”软件打开



No.	Time	Source	Destination	Protocol	Length	Info
10	2.629900	192.168.1.102	115.239.211.92	HTTP	644	OPTIONS /v.gif?pid=307&type=3075&l=47365&t=0&s=47365&v=605&f=12000&r=http%3A%2F%2Fww…
11	2.638601	115.239.211.92	192.168.1.102	TCP	54	80 → 22493 [ACK] Seq=1 Ack=591 Win=15872 Len=0
12	2.638713	115.239.211.92	192.168.1.102	HTTP	304	HTTP/1.1 200 OK
13	2.671867	192.168.1.102	115.231.236.116	TCP	66	22494 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
14	2.674622	192.168.1.102	202.101.172.47	DNS	72	Standard query 0xdbbc A hm.baidu.com
15	2.677614	192.168.1.102	202.101.172.47	DNS	81	Standard query 0x2c57 A bdimg.share.baidu.com
16	2.679829	202.101.172.47	192.168.1.102	DNS	297	Standard query response 0x2c57 A bdimg.share.baidu.com CNAME static.n.shifen.com A 1…
17	2.680273	202.101.172.47	192.168.1.102	DNS	284	Standard query response 0xdbbc A hm.baidu.com CNAME hm.e.shifen.com A 220.181.164.39…
18	2.684517	115.231.236.116	192.168.1.102	TCP	66	80 → 22494 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM=1 WS=1024
19	2.684583	192.168.1.102	115.231.236.116	TCP	54	22494 → 80 [ACK] Seq=1 Ack=1 Win=66240 Len=0
20	2.684925	192.168.1.102	115.231.236.116	HTTP	863	POST /user.php?action=login&do=login HTTP/1.1 (application/x-www-form-urlencoded)
21	2.696759	115.231.236.116	192.168.1.102	TCP	54	80 → 22494 [ACK] Seq=1 Ack=810 Win=31744 Len=0
22	2.739908	115.231.236.116	192.168.1.102	TCP	990	80 → 22494 [PSH, ACK] Seq=1 Ack=810 Win=31744 Len=936 [TCP segment of a reassembled …
23	2.740198	115.231.236.116	192.168.1.102	TCP	111	80 → 22494 [PSH, ACK] Seq=937 Ack=810 Win=31744 Len=57 [TCP segment of a reassembled…

发现有一个HTTP的POST请求包

4、查看HTTP的POST请求包



No.	Time	Source	Destination	Protocol	Length	Info
16	2.679829	202.101.172.47	192.168.1.102	DNS	297	Standard query response 0x2c57 A bdimg.share.baidu.com CNAME static.n.shifen.com A 1…
17	2.680273	202.101.172.47	192.168.1.102	DNS	284	Standard query response 0xdbbc A hm.baidu.com CNAME hm.e.shifen.com A 220.181.164.39…
18	2.684517	115.231.236.116	192.168.1.102	TCP	66	80 → 22494 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM=1 WS=1024
19	2.684583	192.168.1.102	115.231.236.116	TCP	54	22494 → 80 [ACK] Seq=1 Ack=1 Win=66240 Len=0
20	2.684925	192.168.1.102	115.231.236.116	HTTP	863	POST /user.php?action=login&do=login HTTP/1.1 (application/x-www-form-urlencoded)
21	2.696759	115.231.236.116	192.168.1.102	TCP	54	80 → 22494 [ACK] Seq=1 Ack=810 Win=31744 Len=0
22	2.739908	115.231.236.116	192.168.1.102	TCP	990	80 → 22494 [PSH, ACK] Seq=1 Ack=810 Win=31744 Len=936 [TCP segment of a reassembled …
23	2.740198	115.231.236.116	192.168.1.102	TCP	111	80 → 22494 [PSH, ACK] Seq=937 Ack=810 Win=31744 Len=57 [TCP segment of a reassembled…

```
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "email" = "flag"
  v Form item: "password" = "ffb7567a1d4f4abdffdb54e022f8facd"
      Key: password
      Value: ffb7567a1d4f4abdffdb54e022f8facd
  > Form item: "captcha" = "BYUG"
```

```
02f0  2f 78 2d 77 77 77 2d 66  6f 72 6d 2d 75 72 6c 65   /x-www-f orm-urle
0300  6e 63 6f 64 65 64 0d 0a  43 6f 6e 74 65 6e 74 2d   ncoded·· Content-
0310  4c 65 6e 67 74 68 3a 20  36 35 0d 0a 0d 0a 65 6d   Length:  65····em
0320  61 69 6c 3d 66 6c 61 67  26 70 61 73 73 77 6f 72   ail=flag &passwor
0330  64 3d 66 66 62 37 35 36  37 61 31 64 34 66 34 61   d=ffb756 7a1d4f4a
0340  62 64 66 66 64 62 35 34  65 30 32 32 66 38 66 61   bdffdb54 e022f8fa
0350  63 64 26 63 61 70 74 63  68 61 3d 42 59 55 47      cd&captc ha=BYUG
```


5、OK

ffb7567a1d4f4abdffdb54e022f8facd

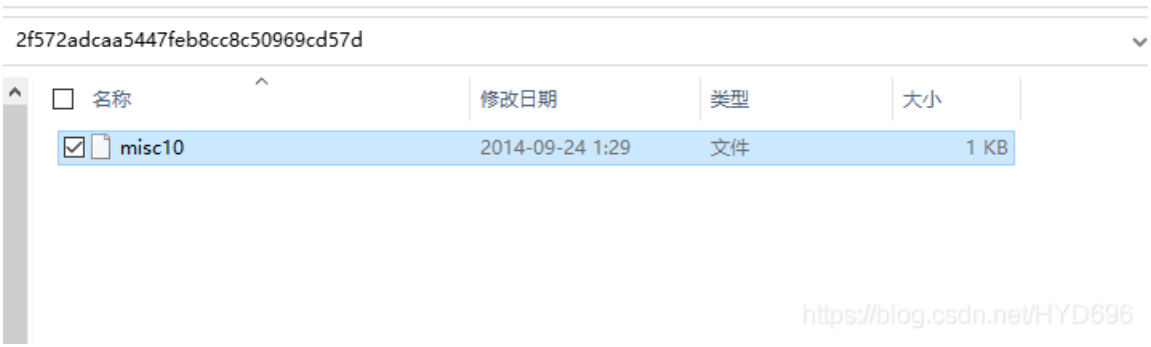
二、Test-flag-please-ignore

题目附件： 附件1

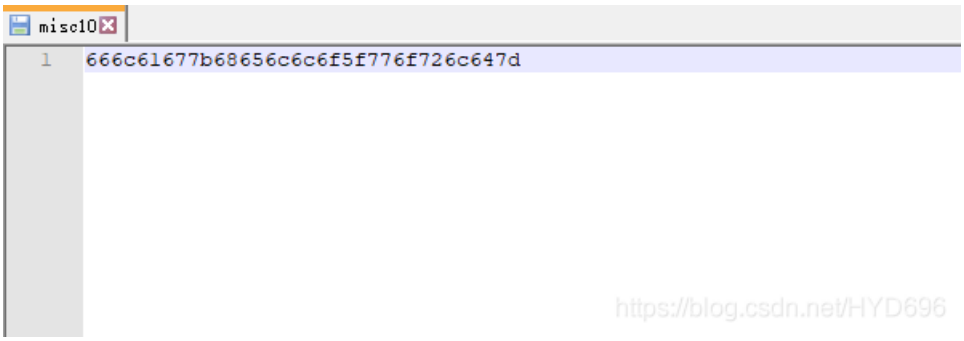
1、 附件1

链接：https://pan.baidu.com/s/1wHzTvsX3W2nHgqObyeT1vg
提取码：jtbs

2、文件



3、用“Notepad”打开misc10文件



十六进制：

666c61677b68656c6c6f5f776f726c647d

4、16进制转换文本

在线，十六制进制转换文本：https://www.sojson.com/hexadecimal.html

5、OK

flag{hello_world}