

陇剑杯Writeup (部分)

原创

The True H00HA 于 2021-09-15 16:40:23 发布 1533 收藏

文章标签: web安全 安全架构 安全 系统安全

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/s1mplelife/article/details/120310801>

版权



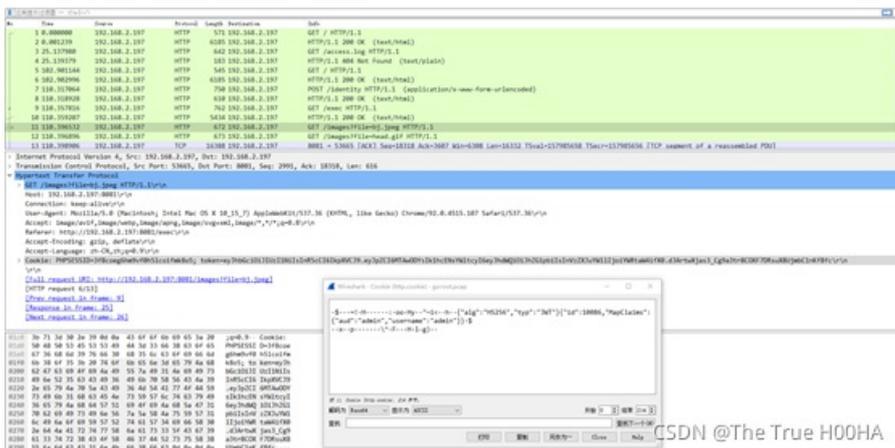
1、签到

No.	Time	Source	Protocol	Length	Destination	Info
20066	122.686290	192.168.241.1		82	192.168.241.255	49676 - 1947 Len=0
7517	76.073677	192.168.241.1	UDP	82	192.168.241.255	49676 - 1947 Len=0
5550	29.432833	192.168.241.1	UDP	82	192.168.241.255	49676 - 1947 Len=0
7035	44.739304	180.163.151.162	TLSv1.2	127	192.168.241.152	Application Data
5052	24.088134	192.168.241.152	TLSv1	571	172.217.160.106	Client Hello
5046	24.065341	192.168.241.152	TLSv1	571	172.217.160.106	Client Hello
5039	23.819897	192.168.241.152	TLSv1	571	172.217.160.106	Client Hello
21542	136.771844	180.163.150.161	TCP	60	192.168.241.152	[TCP Keep-Alive ACK] 80 - 52689 [ACK] Seq=430 Ack=834 Win=64240 Len=0
21541	136.770874	192.168.241.152	TCP	55	180.163.150.161	[TCP Keep-Alive] 52689 - 80 [ACK] Seq=833 Ack=430 Win=63382 Len=1
21528	132.145695	180.163.150.33	TCP	60	192.168.241.152	[TCP Keep-Alive ACK] 443 - 62398 [ACK] Seq=1 Ack=2 Win=64240 Len=0
21527	132.145587	192.168.241.152	TCP	55	180.163.150.33	[TCP Keep-Alive] 62398 - 443 [ACK] Seq=1 Ack=1 Win=64240 Len=1
21526	130.047080	192.168.241.152	TCP	54	192.168.241.147	56501 - 80 [ACK] Seq=21 Ack=541 Win=2101760 Len=0
21525	130.047040	192.168.241.147	TCP	60	192.168.241.152	80 - 56501 [FIN, ACK] Seq=540 Ack=21 Win=2102272 Len=0
21523	129.991154	192.168.241.152	TCP	54	192.168.241.147	56500 - 80 [ACK] Seq=21 Ack=541 Win=2101760 Len=0
21522	129.991146	192.168.241.147	TCP	60	192.168.241.152	80 - 56500 [FIN, ACK] Seq=540 Ack=21 Win=2102272 Len=0
21520	129.990256	192.168.241.152	TCP	54	192.168.241.147	56499 - 80 [ACK] Seq=21 Ack=541 Win=2101760 Len=0
21519	129.990249	192.168.241.147	TCP	60	192.168.241.152	80 - 56499 [FIN, ACK] Seq=540 Ack=21 Win=2102272 Len=0
21517	129.989543	192.168.241.152	TCP	54	192.168.241.147	56498 - 80 [ACK] Seq=21 Ack=541 Win=2101760 Len=0
21516	129.989537	192.168.241.147	TCP	60	192.168.241.152	80 - 56498 [FIN, ACK] Seq=540 Ack=21 Win=2102272 Len=0
21514	129.988852	192.168.241.152	TCP	54	192.168.241.147	56497 - 80 [ACK] Seq=21 Ack=541 Win=2101760 Len=0
21513	129.988829	192.168.241.147	TCP	60	192.168.241.152	80 - 56497 [FIN, ACK] Seq=540 Ack=21 Win=2102272 Len=0
21511	129.988185	192.168.241.152	TCP	54	192.168.241.147	56496 - 80 [ACK] Seq=21 Ack=541 Win=2101760 Len=0

http协议网络攻击

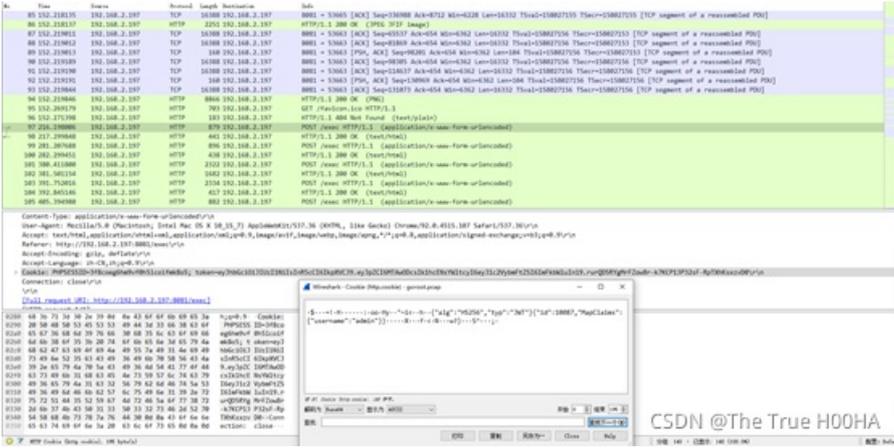
2 JWT

2.1



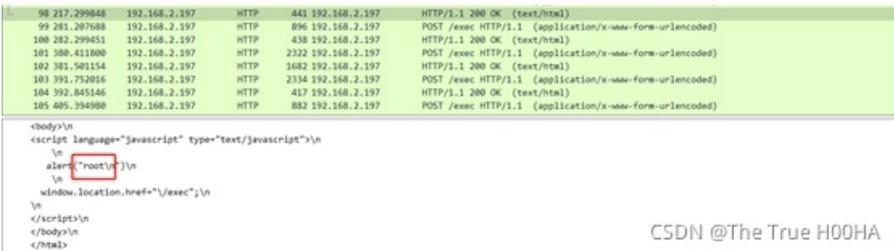
该网站使用了_JWT_认证方式。

2.2



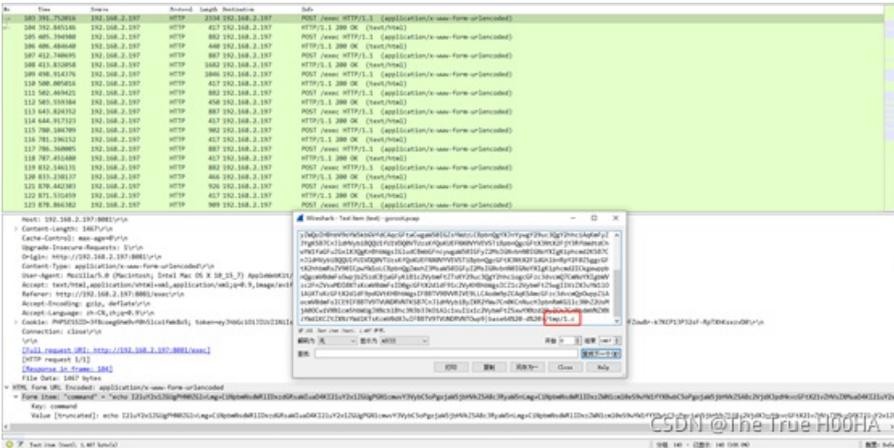
黑客绕过验证使用的jwt中，id和username是_10087#admin_。

2.3



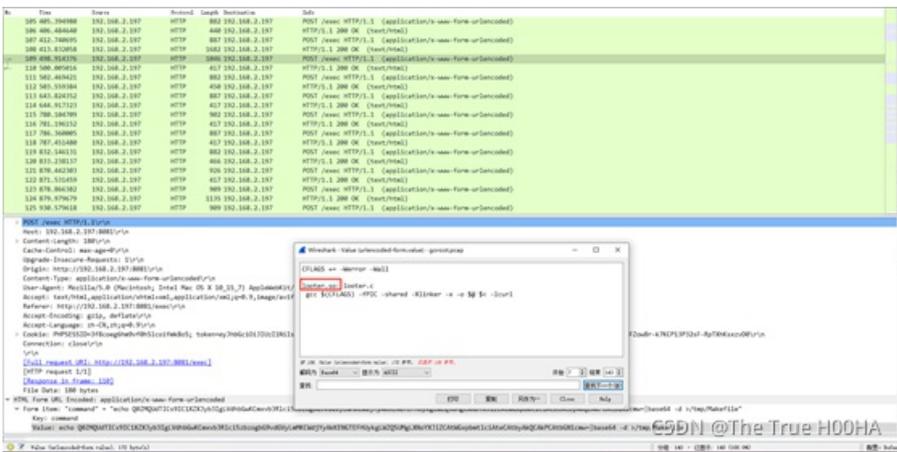
黑客获取webshell之后，权限是_root_?

2.4



黑客上传的恶意文件文件名是/tem/1.c_。

2.5



黑客在服务器上编译的恶意so文件，文件名是looter.so__。

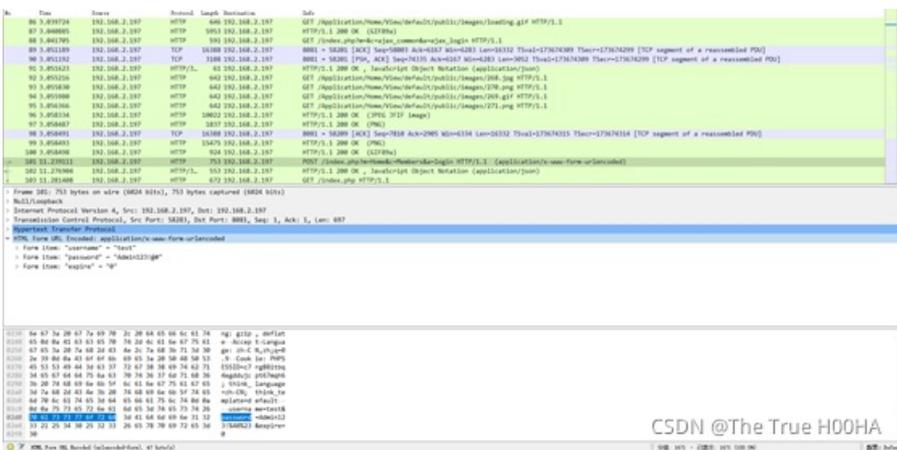
2.6



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_____。

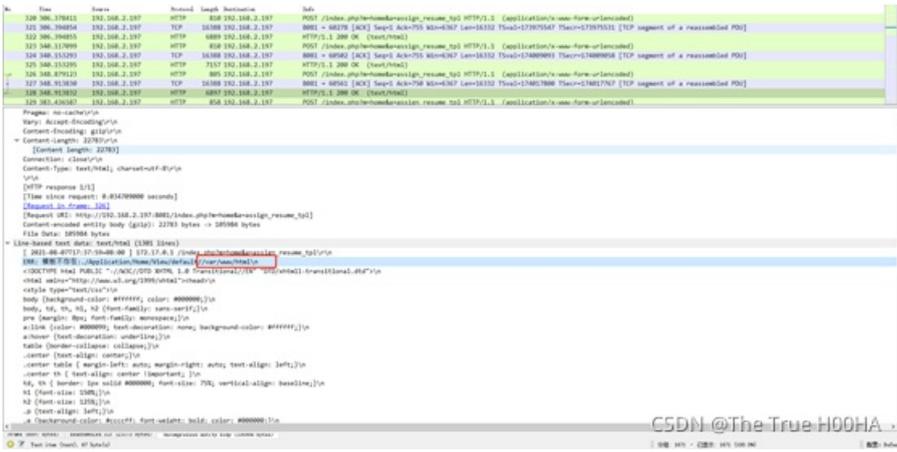
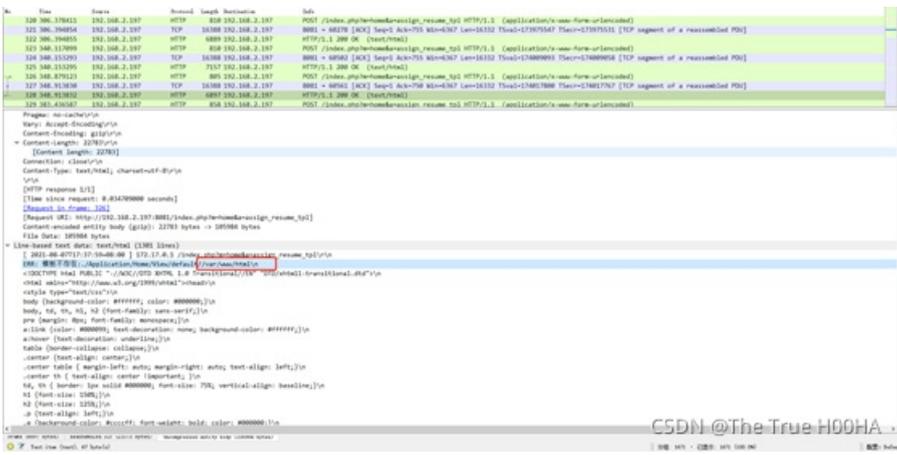
3 webshell

3.1



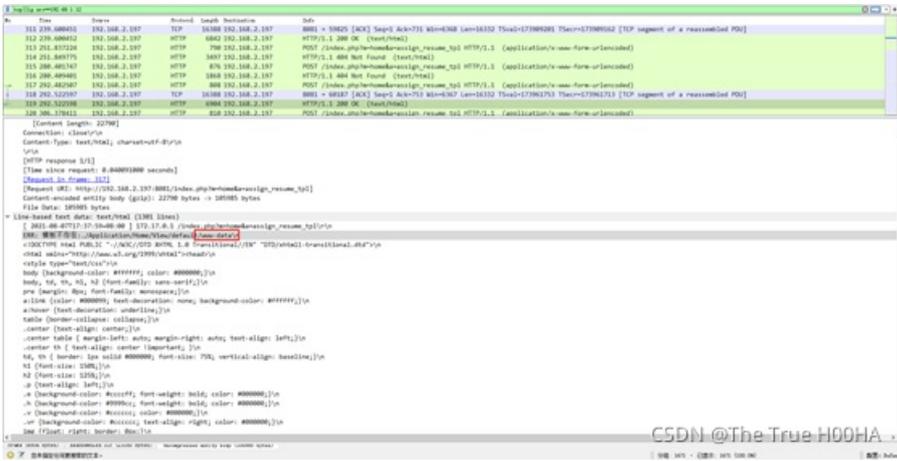
黑客登录系统使用的密码是__Admin123!@#_。

3.2



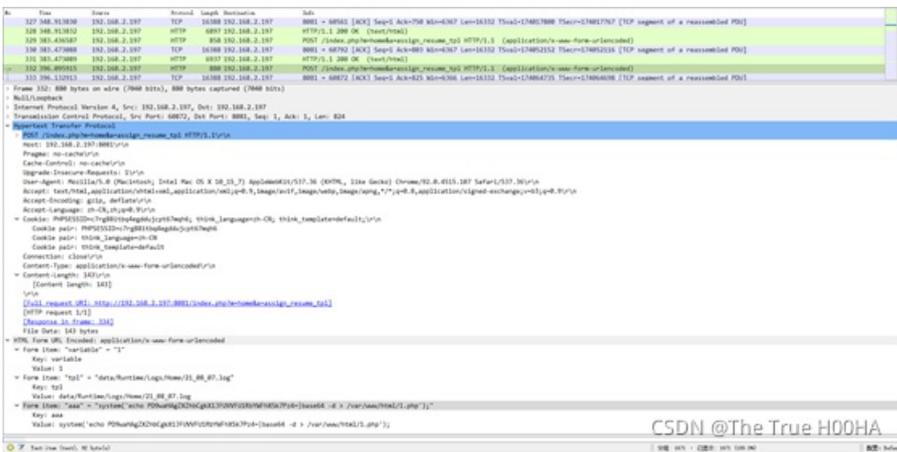
黑客修改了一个日志文件，文件的绝对路径为/var/www/html/data/Runtime/Logs/Home/21_08_07.log_____。

3.3



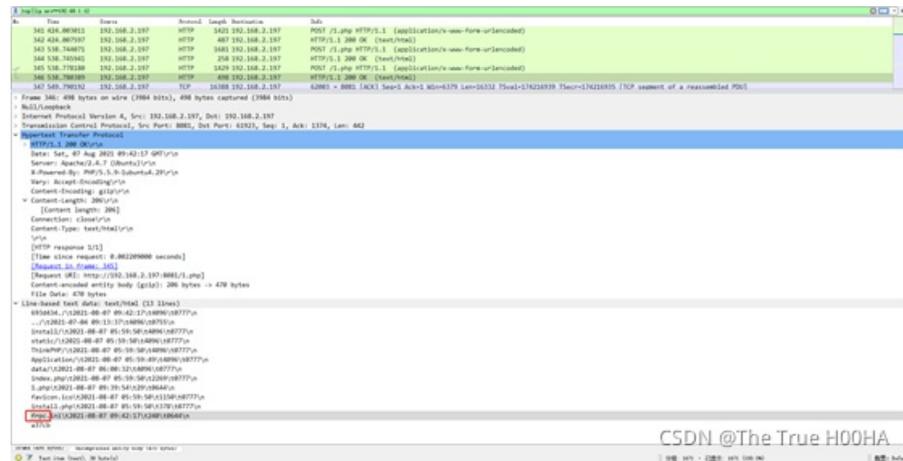
黑客获取webshell之后，权限是_<code>www-data</code>?

3.4



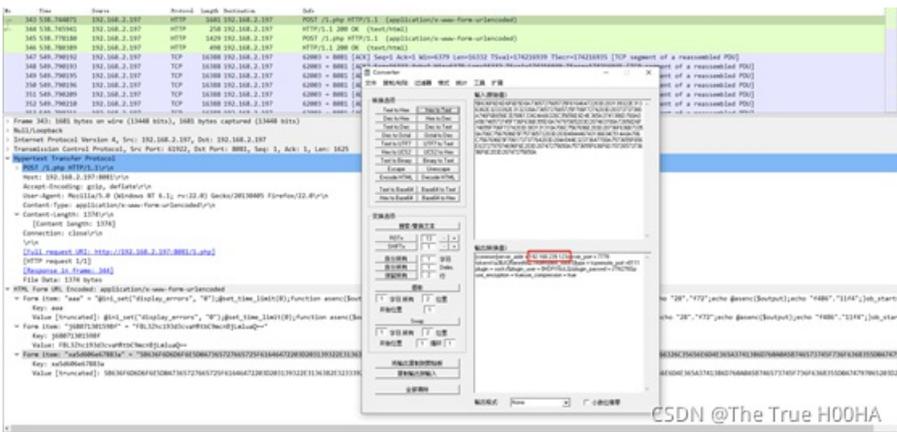
黑客写入的webshell文件名是1.php_____。

3.5



黑客上传的代理工具客户端名字是__frpc__。

3.6



黑客代理工具的回连服务端IP是__192.168.239.123__。

3.7


```
i%3A%22%2Fflag%22%3Bs%3A13%3A%22SpIFileObject%22%3B%7D HTTP/1.1" 302 879 "-" "python-  
i%3A%22%2Fflag%22%3Bs%3A13%3A%22SpIFileObject%22%3B%7D HTTP/1.1" 302 879 "-" "python-  
CSDN @The True H00HA
```

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

6.1

```
Volatility 2.6_win64_standalone.exe -f .\Target.vmem --profile=Win7SP1x64 lsadump  
DefaultPassword  
0x00000000 48 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.O...  
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.....  
CSDN @The True H00HA
```

虚拟机的密码是flag{W31C0M3 T0 THiS 34SY FOR3NSiCX} _____。

6.2

vol镜像 die逆向文件

exe导出后是个自动解压的，获得文件夹

华为备份加密使用工具

<https://github.com/RealityNet/kobackupdec>

```
python .\kobackupdec.py -  
vvv W31C0M3_T0_THiS_34SY_F0R3NSiCX "C:\Users\Snowywar\Desktop\HUAWEI P40_2021-aa-  
bb xx.yy.zz" ./HUAWEI
```

flag{TH4NK Y0U FOR DECRYPTING MY DATA}

CSDN @The True H00HA

7 简单日志分析

7.1



黑客攻击的参数是 _user_。

7.2



黑客查看的秘密文件的绝对路径是 /Th4s_IS_VERY_Import_Fi1e_____。

7.3



黑客反弹shell的ip和端口是 192.168.2.197: 8888。

8、SQL注入

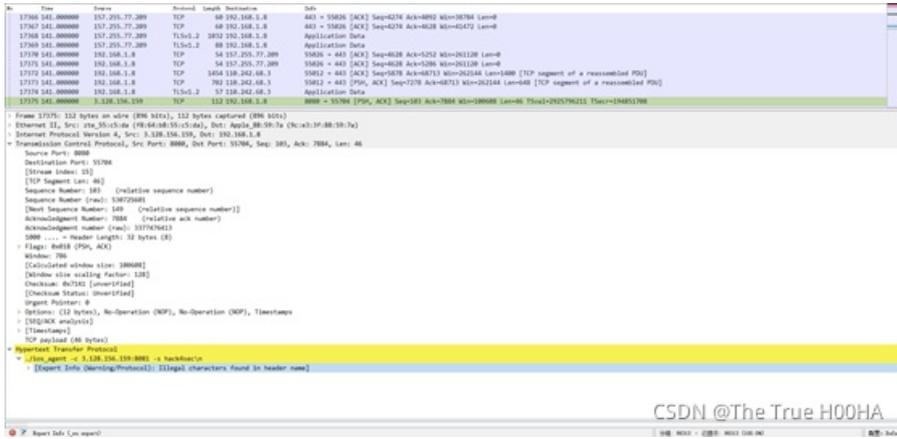
8.1

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

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

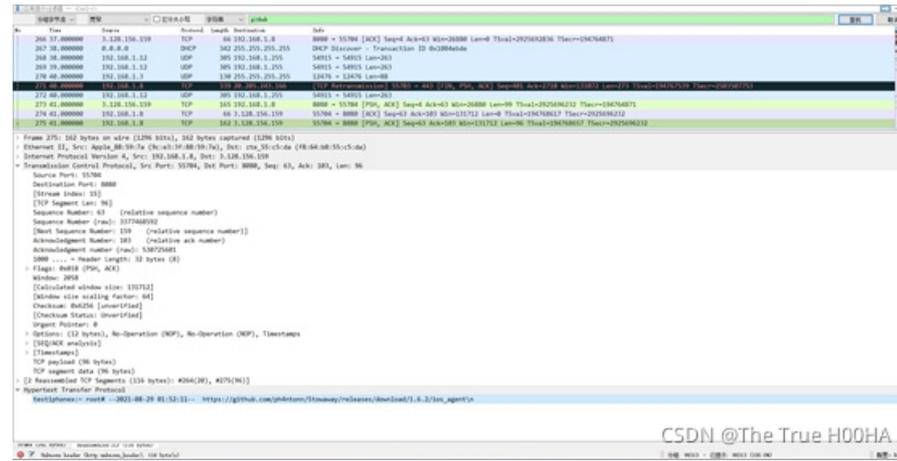
10、IOS

10.1



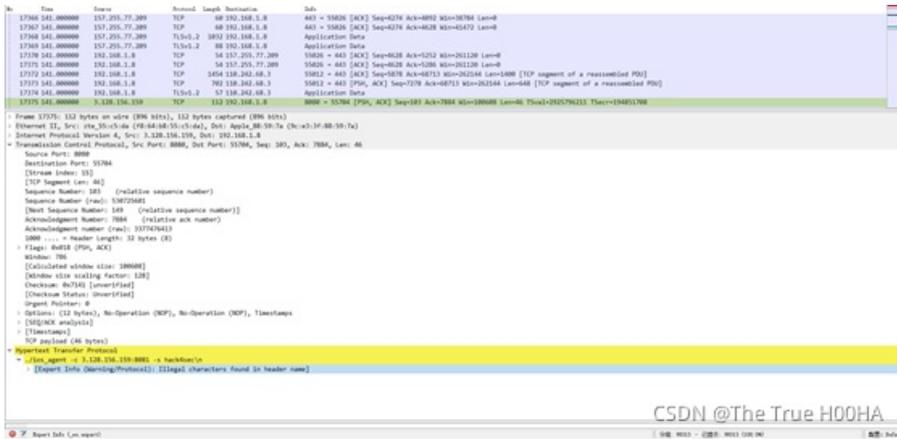
黑客所控制的C&C服务器IP是__3.128.156.159__。

10.2



黑客利用的Github开源项目的名字是__stowaway__。

10.3



通讯加密密钥的明文是__hack4sec__。

10.4

