攻防世界杂项(misc)--新手练习区(详解十二道题完结,附件做题过程中使用到的各种工具和网站)

原创

 DBINGSEC
 ● ± 2021-10-07 15:57:50 发布
 ● 1066 ★ 收藏 6

 分类专栏:
 CTF合集 文章标签: 其他 经验分享

 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_56607768/article/details/120636729

 版权



CTF合集 专栏收录该内容

6 篇文章 1 订阅 订阅专栏

攻防世界杂项(misc)-新手练习区(详解)

第一题: this_is_flag

题目描述: Most flags are in the form flag{xxx}, for example:flag{th1s_!s_a_d4m0_4la9}

根据题目描述确定flag为: flag{th1s_!s_a_d4m0_4la9}

第二题: pdf

题目描述:菜猫给了菜狗一张图,说图下面什么都没有



根据题目描述:图片下面什么都没有,那么图片猜测flag就这图片下面,于是用ctrl+a全选粘到文本文档中,果然flag出现了: flag{security_through_obscurity}

第三题:如来十三掌

题目描述:菜狗为了打败菜猫,学了一套如来十三掌。



夜哆悉諳多苦奢陀奢諦冥神哆盧穆皤三侄三即諸諳即冥迦冥隸數顛耶迦奢若吉怯陀諳怖奢智侄諸若奢數菩奢集遠俱老竟寫明奢若 梵等盧皤豆蒙密離怯婆皤礙他哆提哆多缽以南哆心曰姪罰蒙呐神。舍切真怯勝呐得俱沙罰娑是怯遠得呐數罰輸哆遠薩得槃漫夢盧 皤亦醯呐娑皤瑟輸諳尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿皤沙蘇輸奢恐豆侄得罰提哆伽諳沙楞缽三死怯摩大蘇者數一遮

根据题目描述:菜狗为了打败菜猫,学了一套如来十三掌。然后依照文件中的内容,那么猜测是与佛论禅密码

与佛论禅密码加解密网站

AmanCTF - 与佛论禅密码

在线与佛论禅加密/解密

夜哆悉諳多苦奢陀奢諦冥神哆盧穆皤三侄三即諸諳即冥迦冥隸數顛耶迦奢若吉怯陀諳怖奢智侄諸若奢數菩奢集遠俱 盧皤豆蒙密離怯婆皤礙他哆提哆多缽以南哆心曰姪罰蒙呐神。舍切真怯勝呐得俱沙罰娑是怯遠得呐數罰輸哆遠薩得 娑皤瑟輸諳尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿皤沙蘇輸奢恐豆侄得罰提哆伽諳沙楞缽三死怯摩大蘇者數	老竟寫明奢若梵等 槃漫夢盧皤亦醯呐 一遮
	li.
加密解密	
MzkuM3gvMUAwnzuvn3cgozMIMTuvqzAenJchMUAeqzWenzEmLJW9	CSDN @seven-BING

MzkuM3gvMUAwnzuvn3cgozMIMTuvqzAenJchMUAeqzWenzEmLJW9

得到后感觉还不是flag,首先想到base64解密,但是不对,后来想到如来十三掌,那么猜测可能是rot13加密

rot13加解密网站

xhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ	9

ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9

然后我进行base64解密得到flag: flag{bdscjhbkzmnfrdhbvckijndskvbkjdsab}

gamma optomizyz	GnidmivravvpuZHiv	rdmJramRzYWJ9	
Reta			

第四题: give_you_flag

题目描述: 菜狗找到了文件中的彩蛋很开心, 给菜猫发了个表情包

r give_you_flag 107 最佳Writeup由testtestzrs提供	┓ ■ WP ● 建议
难度系数:	
题目来源:暂无	
题日细述:梁列战到了又件中的彩蛋很开心,结实通及了个表情也 题目场景: 暂无	
题目附件: 附件1	
	>
	CSDN @seven-BING

打开文件是一个gif动态图:



于是我用stegsolve工具进行动态图片分离

工具链接:stegsolve工具

1.首先我点击file



2.点击下好的附件,打开

▲ 打开	\times
查找(!): □第四题 🔽 🖾 🗂 🗄	0: D— 0: D—
4b0799f9a4d649f09a882b6b1130bb70.gif	
文件名(1):	
文件类型(I): Images	-
	<mark>见消</mark> enr-BINC

3.点击分析



4.翻到第五十张的时候出现二维码,点击保存



看到是一个缺少定位符的二维码,在网上找一个定位点图,用3d画图修改图片即可。得到以下图片



QR Research	- 🗆 X
文件(F) 工具(T) 帮助(H)	
in the second se	
	纠错等级 H(30%) ▼ Auto ▼ Auto ▼ 4 ÷
	< -
已解码数据 1:	^
位置:(308.2,301.2)-(379.8,301.8)-(308.0,372.1)-(3 颜色正常,正像 版本:5 纠错等级:H,掩码:6 内容: flag{e7d478cf6b915f50ab1277f78502a2c5}	79.8,372.6)
	CSDN @seven-BING

工具链接:CQR二维码扫描工具

第五题: stegano

题目描述:菜狗收到了图后很开心,玩起了pdf提交格式为flag{xxx},解密字符需小写

Stegano de 478 最佳Writeup由LK-TEAM • 来自南方的羊提供	📃 WP 🛛 🔮 建议
难度系数: ◆ ★★★★ 4.0	
题目来源: CONFidence-DS-CTF-Teaser	
题目描述:菜狗收到了图后很开心,玩起了pdf提交格式为flag{xxx},解密字符需小写	
题目场景:暂无	
题目附件: 附件1	
	CSDN @seven-BING

打开是一个: pdf文件, 并提示flag不在这里



然后我ctrl+a全选文章,复制到文本文档中,发现一串AB。

Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, ^ Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec f scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tort Your flag is not here]olestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tel sollicitudin a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum Duis gravida semper dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus nulla, eu interdum in.Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut metus vu magna volutpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed sem fauc diam orci, convallis vitae auctor vehicula, interdum ut mi. Maecenas nec urna at dolor mattis dictu Mauris condimentum adipiscing erat nec feugiat. Curabitur scelerisque varius ligula, iaculis adipis ullamcorper arcu. In facilisis et tortor commodo aliquam. Nulla feugiat, sem eu molestie bibendum, massa, id accumsan sapien libero id tellus. In enim lacus, sollicitudin a felis quis, blandit porta egestas, tristique mauris eu, rutrum justo. Nulla facilisi. Duis gravida semper dui laoreet vulputa orci. Cras placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit amet, consect elit. Cras faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu p Vestibulum suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, Maecenas nec urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec f scelerisque varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tort feugiat, sem eu molestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. I a felis quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum justo. Nulla semper dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus nulla, eu bibendum metu placerat lectus nulla, eu bibendum metus interdum in.Lorem ipsum dolor sit amet, consectetur adipis faucibus odio ut metus vulputate, id laoreet magna volutpat. Integer nec enim vel arcu porttitor eg suscipit lorem sed sem faucibus rutrum. Nunc diam orci, convallis vitae auctor vehicula, interdum u urna at dolor mattis dictum sit amet at orci. Mauris condimentum adipiscing erat nec feugiat. Curab varius ligula, iaculis adipiscing dui. Duis eget ullamcorper arcu. In facilisis et tortor commodo a sem eu molestie bibendum, leo nisi porttitor massa, id accumsan sapien libero id tellus. In enim la quis, blandit porta ipsum. Donec sed nibh egestas, tristique mauris eu, rutrum justo. Nulla facilis <u>dui laoreet vulputate. Aenean quis tempor orci. Cras placerat lectus nulla, eu hibendum metus inter</u> BABA BBB BA BBA ABA AB B AAB ABAA AB B AA BBB BA AAA BBAABB AABA ABAA AB BBA BBBAAA ABBBB BA AAAB A Close - but still not here ! < CSDN @seven-BING:

根据密文猜测是摩斯密码,这里使用到B站一位UP主(风二西)的工具(CTF编码转化工具):

根据密文想到A替换成摩斯的. B替换成摩斯-

	编码转换工具v1.0 By:风二西 2020.1	2.1	- 🗆 X
【编码转换】 【Base系列】 【注	抄转换】		
主界面 记事本			
	替换内容:		
	B 恭饶为。		
			记A省狭风. D狭风-
	全部替按		
			v
輸出			
congratulations, flag: lnv151b	13m3654g3	FLAG	^
			~
輸出复制到输入 替挑	倒序 转换大写	转换小写 输出复制到证	事本 CSDN @seven-BING

得到的flag: flag{1nv151bl3m3554g3}

第六题:坚持60s

题目描述: 菜狗发现最近菜猫不爱理他,反而迷上了菜鸡



打开文件是一个后缀为: jar



方法一:坚持60s即可得到flag

方法二: 使用逆向简单工具jd-gui 工具链接





flag{RGFqaURhbGlfSmlud2FuQ2hpamk=}

通过尝试上传flag后发现不对,那么一看加密方式为base64进行解密,在线加解密网站: https://www.qqxiuzi.cn/bianma/base64.htm

	ホ汁ド大功同/月剛 反火茶*尤近ド私 資料!	↓现同/月刚反观涂*无效下轨仅田参与	
	基恩士	打开 >	
RGFqaURhbGlfSmlud2FuQ2hpamk=			
清空 加密 解密 口解密为UTF-8字节流 DajiDali_JinwanChiji			
复制			

CSDN @seven-BING

第七题:gif

题目描述:菜狗截获了一张菜鸡发给菜猫的动态图,却发现另有玄机

▲题用时: 1分4秒	
「gif 159 最佳Writeup由不要让我起名提供」	₩P 建议
难度系数: ◆ ★ ★ ★ ★ 4.0	
题目来源:暂无	
题目描述:菜狗截获了一张菜鸡发给菜猫的动态图,却发现另有玄机	
题目场景:暂无	
题目附件: 附件1	
	CSDN @seven-BING

解压后是一组图片:



打开文件出现多个黑白,让人联想到二进制,白色图片代表0,黑色图片代表1。01100110前八位二进制换算后为f证明思路正确。

方法一:手动将图片转化为01二进制,转化为

方法二:编写python脚本:

```
from PIL import Image
result=""
for num,i in enumerate(range(104)):
    img=Image.open(f"G:/Desktop/dbbc971bf4da461fb8939ed8fc9c4c9d/gif/{i}.jpg")
    im=img.convert("RGB")
    r,g,b=im.getpixel((1,1))
    if r!=255:
        result+="1"
    else:
        result+="0"
for i in range(0,len(result),8):
    byte=result[i:i+8]
    print(chr(int(byte,2)),end="")
```

1	from PIL import Image	🛦 17 🗶 1 🔺 🗸
2	result=""	_
3 Ę	for num,i in enumerate(range(104)):	-
4	<pre>img=Image.open(f"G:/Desktop/dbbc971bf4da461fb8939ed8fc9c4c9d/gif/{i}.jpg")</pre>	
5	<pre>im=img.convert("RGB")</pre>	-
	r,g,b=im.getpixel((1,1))	-
7	<i>if</i> r <u>!=</u> 255:	
8	result+="1"	1
9	else:	_
10 👔	result+="0"	1
11	for i in range(0,len(result),8):	
12	byte=result[i:i+8]	
13 🗈	<pre>print(chr(int(byte,2)),end="")</pre>	
	for num,i in enumerate(range(10	
	🝦 test 🗵	\$ -
	D:\python3.9.4\python3.9.exe D:/python3.8.0/python代码练习/练习/test.py	
	flag{FuN_giF}	
	进程已结束,退出代码0	SDN @seven-BING

最后flag是: flag{FuN_giF}

第八题: 掀桌子

题目描述: 菜狗截获了一份报文如下

c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e9f3e4e3e8eaf9 eaf3e2e4e6f2, 生气地掀翻了桌子(╯°□°) ╯ ⌒ ┶━━┶



看题给字符串比较像十六进制,俩个一组,转化为十进制,减去128,再转字符串得到flag,有一点投机取巧。

str="c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e9f3e4e3e8eaf9e
af3e2e4e6f2"
strlen=len(str)
print(strlen)
for i in range(0,118,2):
<pre>byte=str[i:i+2]</pre>
s=int(byte,16)-128
<pre>print(chr(s),end="")</pre>



最后flag为: flag{hjzcydjzbjdcjkzkcugisdchjyjsbdfr}

第九题: ext3

题目描述:今天是菜狗的生日,他收到了一个linux系统光盘

返回 本题用时: 28秒	
F ext3 if 158 最佳Writeup由hackcat提供	₩P ● 建议
难度系数:	
题目来源: bugku	
题目描述:今天是菜狗的生日,他收到了一个linux系统光盘	
题目场景:暂无	
题目附件: 附件1	
	CSDN @seven-BING
MER AND A LEAR AND	CSDN @seven-BING

 1
 2021/10/6 22:13
 文件
 20,000 KB

方法一:首先放到010editor查看,搜素字符串flag,发现了如图的

010editor工具链接:

◎ 010 Editor - C:\比赛文件\攻防世界\misc新于区\第九题\1			- U X
文件(F) 编辑(E) 搜索(S) 视图(V) 格式(O) 脚本(I) 模板(L) 调试(D) 工具(T)	窗口(W) 帮助(H)		
ा 🗈 🗸 📂 🗸 🔜 🗊 🗐 🖿 🎓 1 🌭 📭 💼 🕫 🥬 🖓 1 🔎 🦗 🔶 1 Ag 🍡 нех	鄂 11		
起始页 1×		> ▽ 工作区	•
▼ 编辑方式: 十六进制(H) > 运行脚本 > 运行模板 >		🔚 ⊳ 打开的文件	:
0123456789ABCĎEF		<u>^</u> <u>1</u>	
68:03B0h: 00 00 00 00 00 00 00 00 00 00 00 00 00		📂 收藏的文件	
68:03C0h: 00 00 00 00 00 00 00 00 00 00 00 00 00		🍃 最近的文件	
68:03D0h: 00 00 00 00 00 00 00 00 00 00 00 00 00		📄 images.g	gif C:\Useresktop'
68:03E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00		🛃 书签的文件	
68:03FUN: 00 00 00 00 00 00 00 00 00 00 00 00 00			
68:0400n: 62 30 56 49 4D 20 37 2E 34 00 00 00 00 10 00 00			
68:0410h: 00 00 00 00 00 00 00 00 E3 12 00 00 72 6F 6F 74			
68:0440h: 00 00 00 00 75 62 75 6F 74 75 00 00 00 00 00 00	ubuntu		
68:0450h: 00 00 00 00 00 00 00 00 00 00 00 00 00			
68:0460h: 00 00 00 00 00 00 00 00 00 00 00 00 7E 72 6F 6F	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	一 工作区 1	
68:0470h: 74 2F 44 65 73 6B 74 6F 70 2F 66 69 6C 65 2F 4F	t/Desktop/file/0	拉索理	- 风柳白生品
68:0480h: 37 61 76 5A 68 69 6B 67 4B 67 62 46 2F 66 6C 61	7avZhikgKgbF/fla	位宣益	
68:0490h: 67 2E 74 78 74 00 00 00 00 00 00 00 00 00 00 00 00	g.txt	※型 ※型	值
68:04A0h: 00 00 00 00 00 00 00 00 00 00 00 00 00		带符号字节	102
68:04B0h: 00 00 00 00 00 00 00 00 00 00 00 00 00		大符号字节	102
68:04C0h: 00 00 00 00 00 00 00 00 00 00 00 00 00		市付 <u>ち</u> 应空 无符是短刑	27750
68:04D0h: 00 00 00 00 00 00 00 00 00 00 00 00 00		带符号整型	1734437990
68:04E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00		无符号整型	1734437990
68:04F0h: 00 00 00 00 00 00 00 00 00 00 00 00 00		带符号 Int64	83925856482566749
68:0500h: 00 00 00 00 00 00 00 00 00 00 00 00 00		尤付号 INT64 巡占	83925856482566749
68:0510h: 00 00 00 00 00 00 00 00 00 00 00 00 00		双精度	1.1205295609968e+
68:0520h: 00 00 00 00 00 00 00 00 00 00 00 00 00		半浮点	4504
68:0530h: 00 00 00 00 00 00 00 00 00 00 00 00 00		✓ ▲ 检索四 ■	flag tyt
68:0540h: 00 00 00 00 00 00 00 00 00 00 00 00 00		- 位金器	■ 役重 📕 书签 캐 <
查找结果		6	eseven-enve-

然后我用7z工具打开,发现了一些文件夹,其中就有我们010editor看到的文件夹,点击查看,flag

02 C:\比赛文件\攻防世界	₹\misc新手区\	(第九题\1\								-		×
文件(F) 编辑(E) 查看(V	/) 书签(A)]	[具(T) 帮助(H)									
🕂 🖴 💎 📫	• 🗙 i											
添加 提取 测试 复制 移动	为删除 信息											
🤌 📋 C:\比赛文件\攻防	5世界\misc新手	戶区\第九题\1\										
名称	大小	压缩后大小	模式	修改时间	创建时间	访问时间	iNode	链接	链接	特征	用户	
Iost+found	0	0	drwx	2015-10-3		2015-10-3	11	2			0	
📜 LvuGM	0	0	drwxr-xr-x			2015-10-3	3358	2			0	
IWIRfzP	0	0	drwxr-xr-x			2015-10-3	3359	2			0	
📜 m	0	0	drwxr-xr-x			2015-10-3	3360	2			0	
📜 m9V0llaElz	0	0	drwxr-xr-x			2015-10-3	3361	2			0	
📜 MiU	0	0	drwxr-xr-x			2015-10-3	3362	2			0	
📜 Mnuc	0	0	drwxr-xr-x			2015-10-3	3363	2			0	
📕 n	0	0	drwxr-xr-x			2015-10-3	3364	2			0	- 1
📜 NgzQPW	957 094	1 041 408	drwxr-xr-x			2015-10-3	3365	8			0	
Nv Nv	0	0	drwxr-xr-x			2015-10-3	244	2			0	
0	0	0	drwxr-xr-x			2015-10-3	245	2			0	
O7avZhikgKgbF	53	1 024	drwxr-xr-x	2018-08-0		2015-10-3	247	2			0	
08	0	0	drwxr-xr-x	2018-08-0		2018-08-0	246	2			0	
📙 OOoOs	0	0	drwxr-xr-x			2015-10-3	248	2			0	
📕 orcA	0	0	drwxr-xr-x			2015-10-3	249	10			0	
<<	0	0	druve ve v			2015 10 2	ວດວ	Э		CSDN @s	even-BI	NØ

☑ C:\比赛文件\攻防世界\misc新手区\第九题\1\O7avZhikgKgbF\				_		\times
文件(F) 编辑(E) 查看(V) 书签(A) 工具(T) 帮助(H)						
d - − ∨ → ★ 1						
添加 提取 测试 复制 移动 删除 信息						
						\sim
名称 大小 压缩后大小 模式 修改时间 创建时	间访问时间	iNode	链接链接	特征	用户	:
flag.txt 53 1 024 -rw-rr- 2018-08-0	2018-08-0	571	1		0	•
flag.txt - 记事本		_				
文件(F) 编辑(F) 格式(O) 查看(V) 帮助(H)	-					
ZmxhZ3tzYWpiY21ienNrampjbmJoc2J2Y2pianN6Y3N6Ymt6an0=			~			
				CSDN	@seven-	BING

ZmxhZ3tzYWpiY2lienNrampjbmJoc2J2Y2pianN6Y3N6Ymt6an0=

看到这个就是用base64加密的: base64在线加解密网站

ZmxhZ3tzYWpiY21ienNrampjbmJoc2J2Y2pianN6Y3N6Ymt6an0=

清空 加密 解密 □解密为UTF-8字节流

 $\texttt{flag}\{\texttt{sajbcibzskjjcnbhsbvcjbjszcszbkzj}\}$

CSDN @seven-BING

最后得到的flag: flag{sajbcibzskjjcnbhsbvcjbjszcszbkzj}

方法二:用kali中binwalk -e 分离出文件,即可得到flag

						Shell No. 1		
0		文件(F) 动作(A) 编辑(E) 查看(V) 帮助(H)					
—		root@kali:~/桌面# binwalk 1						
文件系统	内存分析	DECIMAL HEXADECIMAL D	ESCRIPTION					
		0 0×0 L	inux EXT filesystem, bl	ocks count: 20000,	image size: 204	80000, rev 1.0, ext3 files	system data, UUID=cf6d7bff-c377-403f-84ae-956ce3c9e3c9	
		root@kali:~/桌面# binwalk -e 1						
十	第 单 日主八括	DECIMAL HEXADECIMAL D	ESCRIPTION					
主义针类	间半日志万竹	0 0×0 L	inux EXT filesystem, bl	ocks count: 20000,	image size: 204	80000, rev 1.0, ext3 files	system data, UUID=cf6d7bff-c377-403f-84ae-956ce3c9e3c9	
		root@kali:~/桌面# []						
	10 101 1010			ext-root - 文件管	理器	_ = ×		
zsteg			文件(F) 编辑(E) 视图(/) 转到(G) 帮助(H)				
			$\leftarrow \rightarrow \uparrow \uparrow$	/root/桌面/_1.extrail	:ted/ext-root/	G		
			警告,您正在使用超级帐	户,可能会损害您的系	统。			
1 10 101 1010			设备					
data.abr			♀ 文件系统					
				8RxQG4bvd	LG6F	NgzQPW		
			- root					
			2 回收站					
1.raw			×14	O7avZhikgKgbF	oiuy7Xdb	qkCN8		
			■ 音乐					
			□□ 图片			1 10 101		
			■ 优频	QQY3sE63w	rh7E1176a	02CdWGSxGPX bi		
_1.extracted			网络		ELLOY	n		
			■ 浏览网络				CSDN @seven-BIN	G

方法三: 挂载到kali下

1.首先创建一个文件夹

命令: mkdir aa



2.挂载到刚刚创建的文件夹下面

命令: mount 1 aa



3.进入到aa 文件夹下 cd aa,并查看有哪些文件 ls

又1+(F) 动1F(A)	猵頖(E)	宣有(V) 帝田	IJ(H)			l l	l l			l i i i i i i i i i i i i i i i i i i i		
root@kali:~/桌面	# mkdir	aa										
root@kali:~/桌面	# mount	1 aa	一 讲入文	件夹								~
root@kali:~/桌面	t cd aa											
root@kali:~/桌面	/aa# ls		1	自有内容								
02CdWGSxGPX.bin	0wDq5	33	7H7geLlS5	8RxQG4bvd	h	i	jj	L00J8	m9V0lIaElz	NV	orcA	Q :
0GY1l	0Xs	44aAm	8A2MFawD4	FinD	Н	imgLDPt4BY	KxEQM	lost+found	MiU	0	oSx2p	qkCN8
0h3a5	1	4A	8DQFirm0D	fm	H2Zj8FNbu	ix1EMRHRpIc2	LG6F	LvuGM	Mnuc	07avZhikgKgbF	ОТ	QmUY1d
01	2X	6JR3	8HhWfV9nK1	g	hdi7	j6uLMX	Lh	lWIRfzP	n	08	poiuy7Xdb	QQY3sF6
0qsd	3	6wUaZE1vbsW	8nwg	gtj	hYuPvID	jE	LlC6Z0zrgy.bin	m	NgzQPW	00o0s	рхби	r
root@kali:~/桌面	/aa#											
										CCD	NI Gaaria	
										CSL	in @sever	I-BING

4.查看文件中是否存在flag文件,用 find -name flag*命令

文件(F) 动作(A)	编辑(E)	查看(V) 帮!	坊(H)								
root@kali:~/桌面 root@kali:~/桌面 root@kali:~/桌面 root@kali:~/桌面	<pre># mkdir # mount # cd aa /aa# ls</pre>	aa 1 aa									
02CdWGSxGPX.bin 0GY11 0h3a5 0l 0qsd	0wDq5 0Xs 1 2X 3	3J 44aAm 4A 6JR3 6wUaZE1vbsW	7H7geLlS5 8A2MFawD4 8DQFirm0D 8HhWfV9nK1 8nwg	8RxQG4bvd FinD fm g gtj	h H H2Zj8FNbu hdi7 hYuPvID	i imgLDPt4BY ix1EMRHRpIc2 j6uLMX jE	jj KxEQM LG6F Lh LlC6Z0zrgy.bin	LOØJ8 lost+found LvuGM lWIRfzP m	m9V0lIaElz MiU Mnuc n NgzQPW	Nv o O7avZhikgKgbF o8 OOoOs	orcA oSx2p OT poiuy7Xdt px6u
rootakal1:~/桌面 ./O7avZhikgKgbF, root@kal1:~/桌面	/flag.tx /aa#	t	*							CSDN @sever	1-BING

5.使用cat 查看里面的内容

							Sh	ell No. 1				
文件(F) 动作(A) 编辑(E)) 查看(V) 帮	助(H)									
root@kali:~/桌 root@kali:~/桌 root@kali:~/桌 root@kali:~/桌	面# mkdir 面# mount 面# cd aa 面/aa# ls	aa 1 aa										
02CdWGSxGPX.bi 0GY1l 0h3a5	n ØwDq5 ØXs 1	3J 44aAm 4A	7H7geLlS5 8A2MFawD4 8DQFirm0D	8RxQG4bvd FinD fm	h H H2Zj8FNbu	i imgLDPt4BY ix1EMRHRpIc2	jj KxEQM LG6F	LO0J8 lost+found LvuGM	m9V0lIaElz MiU Mnuc	Nv o O7avZhikgKgbF	orcA oSx2p OT	Q qkCN8 QmUY1d
0l 0qsd	2X 3	6JR3 6wUaZE1vbsW	8HhWfV9nK1 8nwg	g gtj	hdi7 hYuPvID	j6uLMX jE	Lh LlC6Z0zrgy.bin	lWIRfzP m	n NgzQPW	08 0000s	poiuy7Xdb px6u	QQY3sF6 r
root@kali:~/桌 ./07avZhikgKgb	面/aa# fi F/flag.tx	Ind -name flag	*									
root@kali:~/桌	面/aa# ca	it ./07avZhikg	KgbF/flag.tx	t								
zmxnz3tzfwp1fz root@kali:~/桌	tienNramp 面/aa#	JDmJoc2J242p1	annoyanoymico	anø=								
zsteg	i									CSD	N @sever	i-BING

ZmxhZ3tzYWpiY2lienNrampjbmJoc2J2Y2pianN6Y3N6Ymt6an0=

使用base64解密即可得到flag flag{sajbcibzskjjcnbhsbvcjbjszcszbkzj}

第十题: SimpleRAR

题目描述: 菜狗最近学会了拼图, 这是他刚拼好的, 可是却搞错了一块(ps:双图层)

	📑 WP
难度系数:	
题目来源: 08067CTF	
题目描述:菜狗最近学会了拼图,这是他刚拼好的,可是却搞错了一块(ps:双图层)	
题目场景:暂无	
题目附件: 附件1	CSDN @seven-BING

文件是一个压缩包

1.首先我解压,提示压缩包损坏,我在用7z打开,里面有一个flag.txt文件,但是打开说flag 不在这里

2.再用010editor打开,看见出一些端倪 010editor工具链接



Header CRC mismatch in Block #4

打开并提示:

压缩包被修改的。

rar 每个块的开头基本知识: (看到人家的writeup)

每—个块器	都是由以	下域开始的:【译者注:即每一个块的头部都是由以下域(西	可称之为头域)组成的】	
HEAD_CRC	2 bytes	CRC of total block or block part		
		整个块或者块某个部分的CRC(根据块类型而有不同)	
HEAD_TYPE	1 byte	Block type		
		块类型【译者注:也可以理解为块头部类型,因为不	同的块对应不同的块头部。	后文也经常混淆这两种概念。】
已经声明过	的块类型	包括:		
HEAD_TYPE=0	x72	marker block【译者注:有些文献里也称之为MARK_HEAD】		
		标志块【译者注: 一个固定为0x52 61 72 21 1A 07 00的7字节	「序列】	
HEAD_TYPE=0	x73	archive header【译者注:有些文献里也称之为MAIN_HEAD】		
		归档头部块		
HEAD_TYPE=0	x74	file header【译者注:有些文献里也称之为FILE_HEAD】		
		文件块【译者注: 直译为文件头部, 但是此处的类型应该指的	是整个块的类型,而非块头部	服结构的类型,因此感觉称之为文件块
更合适,]				
HEAD_TYPE=0	x75	old style comment header		
		老风格的 注释块【译者注:直译为注释头部,基于和文件块-	-样的原因,感觉称之为注释:	快更合适】
HEAD_TYPE=0	x76	old style authenticity information		
		老风格的 授权信息块/用户身份信息块		
HEAD_TYPE=0	x77	old style subblock		
		老风格的 子块		
HEAD_TYPE=0	x78	old style recovery record		
		老风格的 恢复记录块		
HEAD_TYPE=0	x79	old style authenticity information		
		老风格的 授权信息块/用户身份信息块		
HEAD_TYPE=0	x7a	subblock		
		子块		
HEAD_TYPE=0	x7b	end block	C	SDN @covon BING
		结束块【译者注: 一个固定为0xC4 3D 7B 00 40 07 00的7字	节序列】	Sold @Seven-DING

010editor 查看压缩包, rar 文件块的开头是 A8 3C 74 我们需要文件块而不是子块,于是更改 A8 3C 7A 为 A8 3C 74

		-						4	36	66	oc 6 3C 7)1 6 A 2	07 2 20 9	2 <mark>0 6</mark> 90 2	9 7 F 0)(
	ħ式:	+7	:讲:	(H)	~ (脚本	· ~ ,	运行	模板	ź: R	AR. b	t V	Þ			
	0		2		4	5		1	8	9		В		D			0123456789ABCDEF
h:			72	21	1A	07	00	CF			00	00	0D	00	00	00	Rar!1.s
h:	00	00	00	00			74	20	90	2D	00	10	00	00	00	10	
h:	00	00	00	02	C7	85	67	36	6D	BB	4E	4B	1D	30	08	00	Ç^g6m»NK.0
h:	20	00	00	00	66	6C	61	67	2E	74	78	74	00	в0	57	00	flag.txt.°W.
h:	43	66	60	61	-	20	69	73	20	6E	6F	74	20	68	65	72	Cflag is not her
h:	65				20	90	2F	00	3A	15	00	00	42	16	00	00	e ["] <t .="" .:b<="" td=""></t>
h:	02	BC	E9	8C	2F	6E	84	4F	4B	1D	33	0A	00	20	00	00	.¼éŒ/n"OK.3
h:	00	73	65	63	72	65	74	2E	70	6E	67	00	F0	40	AB	18	.secret.png.ð@«.
h:	11	C1	11	55	08	D1	55	80	0D	99	C4	90	87	93	22	19	.Á.U.ÑU€.™Ä.‡``".
h:	4C	58	DA	18	в1	A4	58	16	33	83	08	F4	3A	18	42	0B	LXÚ.±¤X.3f.ô:.B.
h:	04	05	85	96	21	AB	1A	43	08	66	EC	61	0F	A0	10	21	!«.C.fìa!
																	ČSDN @seven-BING

flag.txt	secret.png

打开图片有两张白色的图片,首先我看了一下文件的属性,发现没有任何东西,我先分别保存两张图片,于是我分别放到 stegsolve中,查看 。 stegsolve 工具链接

通过第一张图片得到半张二维码



同样进行第二张图片分析



于是3D将两张图片组合拼接,并把定位点拼接上,得到图片



使用CQR二维码扫描工具得到flag值: flag{yanji4n_bu_we1shi} CQR二维码工具链接



第十一题: base64stego

题目描述: 菜狗经过几天的学习, 终于发现了如来十三掌最后一步的精髓



得到的文件是一个压缩包: 我尝试解压,发现需要密码,于是我用7z打开,发现里面有一个文件,且里面的内容能够打开,说明 该压缩包是一个伪加密。7z工具链接

Ø	。 🌌 C:\比赛文件\攻	防世界\misc新	手区\第十一题\	a2eb7ceaf5al	o49f7acb33d	e2e7eed74a.zi	p\						~
2	品称	大小	压缩后大小	修改时间	创建时间	访问时间	属性	加密	注释		CRC	算法	特征
	stego.txt	7 093	3 561	2016-04-2				-			4B7D32FE	Deflate	Local
	/////////////////////////////////////	本 式(O) 查看(V)	帮助(H)						_		×		
	U3R1Z2Fub2dyYXE G1uZXMgb2YgYSBw JhcGhpYyB0cmFuc =ZiBIaXN0aWF1dy LiBUaGUgbWVzc2F cGhpY2FsbHkgc0= aW50ZXh0IiB3YXM	BoeSBpcyB0a wcm12YXR1IG 221pc3Npb+= KMsIHdobyBz FnZSBhbGx1Z ==cm9kdWN1Z MgaXRzZWxmI	GUgYXJ0IG x1dHR1ci41 =biBiZWNhd aGF2ZWQgdd 2VkbHkgY21 CBtaWNyb21 GVuY2+=ZG	FuZCBzY211 NCgOKVGh11(MXN1IG9mIH Gh1IGh1YWQ Fycm11ZCBh RvdHMgdG8g /kIGFuZCBn	omN1IG9mIH GFkdmFudGH RoZW1yIGxH gb2YgaG1z] IHdhem5pbn c2VuZCBpbn YXZ1IG1uZn	IdyaXRpbmcg PnZSBvZiBzd ncmd1IHNpem IG1vc3QgdHJ ncgdG8gR3J1 nZvcm1hdG1v n9ybWF0aW9u	aGlkZGVuIG1 GVnYW5vZ3Jh UuIEFzIB==Y 1c3R1ZCBzbG ZWN1IGFib5= biBiYWNrIGF IGFib3V0IHN	1c3NhZ2Vz1 cGh5LCBvdn SBzaW1wbGU F2ZSBhbmQg =dXQgUGVyc uZH==IGZvc oaXAgbW922	IG1uIF nVyIGN JgZXhF gdGF0d 21hbi 2nRoLi ZW11br	IN1Y2g NyeXBO nbXBsZ IG9vZW IBpbnZ IBNaWN nRzLF=	gYSB ^ b2dy SwgY QgYS hc21 yb2R =IGV		
E												CSDN	@seven-BINC

解决伪加密两种方法:

第一种直接用7z工具打开

第二种:用010editor打开,修改其密码位

zip的知识补充:

压缩源文件数据区		
50 4B 03 04	//数据区, 压缩包的文件头	
14 00	// 解压文件所需的pkware版本	
00 00	// 全局方式位标记 (有无加密)	
08 00	// 压缩方式	a start in the second
压缩源文件目录区		and the second second
50 4B 01 02	// 目录区, 目录中文件的文件头标记	A Come
3F 00	// 压缩使用的pkware版本	
14 00	// 解压文件所需的pkware版本	
00 00	// 全局方式位标记 (有无加密)	
08 00	// 压缩方式	
压缩文件目录结束标志		11 Barton
50 4B 05 06	// 目录结束标志	
		CSDN @seven-BING

常见压缩包格式分析

.zip																		
Offset	0	1	2	3	4	5	6	7	8	9	A	В	C	D	E	F	ANSI ASCII	
00000000	50	4B	03	04	14	00	00	60	08	00	E8	51	2D	4C	3D	51	PK èQ-L=Q	
00000010	6B	4D	05	00	00	00	03	00	00	00	05	00	00	00	31	2E	kM 1.	
00000020	74	78	74	33	34	34	04	00	50	4B	01	02	1F	00	14	00	txt344 PK	无加密
00000030	00	00	08	00	E8	51	2D	40	3D	51	6B	4D	05	00	00	00	èC-L=CkM	
00000040	03	00	00	00	05	00	24	00	00	00	00	00	00	00	20	00	S	
1.zip																		
Offset	0	1	2	3	4	5	6	7	8	9	A	В	С	D	E	F	ANSI ASCII	
00000000	50	4B	03	04	14	00	00	00	08	00	E8	51	2D	4C	3D	51	PK èQ-L=Q	
00000010	6B	4D	05	00	00	00	03	00	00	00	05	00	00	00	31	2E	kM 1.	
00000020	74	78	74	33	34	34	04	00	50	4B	01	02	1F	00	14	00	txt344 FK	伪加密
00000030	09	00	08	00	E8	51	2D	40	3D	51	6B	4D	05	00	00	00	èC-L=CkM	
00000040	03	00	00	00	05	00	24	00	00	00	00	00	00	00	20	00	s	
1.zip																		
Offset	0	1	2	3	4	5	6	7	8	9	A	В	С	D	E	F	ANSI ASCII	
00000000	50	48	03	04	14	00	09	00	63	00	E8	51	2D	4C	00	00	PK c èQ-L	
00000010	00	00	21	00	00	00	03	00	00	00	05	00	OB	00	31	2E	! 1.	
00000020	74	78	74	01	99	07	00	02	00	41	45	03	08	00	E5	4F	txt » AE åO	古加应
00000030	6E	3A	OE	2D	22	F2	D4	78	67	E8	CA	A4	00	12	DB	00	n: -"òÔxgèʤ Û	具加密
00000040	7E	55	17	EE	EB	53	47	FD	17	F7	DA	7C	49	9D	57	50	~U îëSGý ÷Ú I WP	
00000050	4B	07	08	00	00	00	00	21	00	00	00	03	00	00	00	50	K ! P	
00000060	48	01	. 02	11	00	14	00	09	00	63	00	E8	51	2D	4C	00	K c èQ-L	CON Group PI

常见文件的识	文	• 0	:11:15		
jpeg(jpg)	FF	D8	FF		
png	89	50	4E	47	
bmp	42	4D	36	5D	
gif	47	49	46	38	
zip	50	4B	03	04	
rar	52	61	72	21	
wav	57	41	56 cs	45 DN @sev	en-BING

	~ 🗁	- ~		1		1	11	lo I		L د	9 (۱.,	•	8 🍃	• →	• 1	A ₁	Hex	🛱 ¶	
始	页	a26	eb7c	eaf	5ab4	19f7	acb	33de	e2e7	eed	74a.	zir	×							
纠	辑方	式:	+7	、进制	(H)	~	运行	脚本	Y	运行	F模板	į: Z	IP. b	t ~	⊳					
		0	1	-2	. .	4	-5-			2	ğ	A	B	Ċ	D	Ę	F	012	34567	8 9AE
00	h:	50	4B	03	04	14	03	00	00	08	00	68	BF	9B	48	FE	32	PK.		h;
10	h:	7D	4B	E9	0D	00	00	25	1B	00	00	09		00	00		74	}Ké	µ.	
20	h:	65	67	бF	2E	74	78	74	עז	ور	C9	76	E2	48	10	B¢	(-EB)		+ txt)	XÉvâ
30	h:	57	Eб	22	24	33	CF	1C	38	8C	68	83	C4	18	7A	00	A3	Wæ"	\$3Ï.8	ŒhfÄ
40	h•	ED	AA	C5	0F	01	12	30	ΠD	08	C4	ח7	4 F	44	56	09	68	í!Å	0	ÄxC
36	7A	C7	00	3A	B1	B6	F	-	A D	<u></u>	CC	FC	DB	F8	0F		6zÇ.	.:±¶õ	/-èIü	Uø.
50	4B	01	02	3F	03	14	03	09	00	- 28	00	68	BF	9B	48		PK.		h	: >H
FE	- 32	7D	4B	E9	UD	00	00	85	ΙB	70	00	09	00	24	00		þ2}I	Κé	μ	.ş.
00	00	00	00	00	00	20	80	ΕD		00	00	00	00		74			€		.st
65	67	6F	2E	74	78	74	A0	00	20	00	00	00	00	00	01		ego.	.txt.		
00	18	00	80	0B	49	BF	9D	A0	D1	01	80		42	38	В7		€		Ñ.€§	B8 ·
2 F	'D4	01	00		AA		в7	2F	D4	01	50	4B	05	06	00		/ô.	·· cr	(Â-BK	nunn
0.0	00	00		00	01	00	5B	00	00	00	10	0E	00	00	00			بردي	IN WS	even-

00000DE0	14	2D	DE	6A	EC	Β9	36	4F	18	ED	EC	71	DA	E5	FΒ	FA	-Þjì¹	60 í:	ìqUăûı	ú
00000DF0	B5	8E	01	5B	68	F9	8F	24	74	78	50	F 1	8E	Ε7	EЗ	OB	µ∎ [hù	. ŞtxI	Pñ∎çã	
00000E00	36	7A	C7	00	ЗA	B1	Β6	F5	2F	AD	E8	CC	FC	DB	F8	OF	6zÇ :±¶õ∕-èÌüÛø			
00000E10	50	4B	01	02	ЗF	03	14	03	00	00	08	00	68	BF	9B	48	PK ?		hċ∎ł	Н
00000E20	FE	32	7D	4B	Ε9	OD	00	00	B5	1B	00	00	09	00	24	00	þ2}Ké	μ	\$	
00000E30	00	00	00	00	00	00	20	80	ED	81	00	00	00	00	73	74		lí	st	t
00000E40	65	67	6F	2E	74	78	74	ΟA	00	20	00	00	00	00	00	01	ego.tx	t		
00000E50	00	18	00	80	ΟB	49	BF	9D	AO	D1	01	80	A7	42	38	B7	ΙI	ίÑ	I§B8	·
00000E60	2F	D4	01	00	11	AA	37	Β7	2F	D4	01	50	4B	05	06	00	∕Ô ª	7•∕Ô	PK	
00000E70	00	00	00	01	00	01	00	5B	00	00	00	10	0E	00	00	00		[
									11-2		_									
白柳									19CX	口舟	9			×	王			χ.	IN	
stego.txt									201	6/4/	27 2	23:5	9	文	本文	相	当 7 KB			KB

解压出来。

解压后发现是一堆base64加密的字符串,看题目来源是olympicCTF,这是俄罗斯2014年有道 misc 题是关于 Base64的隐写 题,那我们直接写解码,这里的思路是先循环解密base64字符串,提取出可以隐写的最后2-4位,再拼接最后转回ascii码flag就 出来了,下面是python2j脚本

```
#coding=utf-8
def get_base64_diff_value(s1, s2):
   base64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
   for i in xrange(len(s2)):
        if s1[i] != s2[i]:
            \label{eq:stars} return \ abs(base64chars.index(s1[i]) \ - \ base64chars.index(s2[i]))
   return res
def solve_stego():
   with open('G:/Desktop/1.txt', 'rb') as f:
        file_lines = f.readlines()
       bin_str = ''
        for line in file_lines:
            steg_line = line.replace('\n', '')
            norm_line = line.replace('\n', '').decode('base64').encode('base64').replace('\n', '')
            diff = get_base64_diff_value(steg_line, norm_line)
            print diff
            pads_num = steg_line.count('=')
            if diff:
                bin_str += bin(diff)[2:].zfill(pads_num * 2)
            else:
                bin_str += '0' * pads_num * 2
            print goflag(bin_str)
def goflag(bin_str):
   res_str = ''
    for i in xrange(0, len(bin_str), 8):
        res_str += chr(int(bin_str[i:i + 8], 2))
   return res_str
if __name__ == '__main__':
   solve_stego()
```

1 1	ა		Daseo4cnars = ^Abluer6hijKlmnuFQK5iuVWXYZADCaerghijKlmnopqrstuVWXYZ@123456789+/	A 5 √ 4 ∧
۰.	4		res = 0	
	5		for i in xrange(len(s2)):	
	6		<i>if</i> s1[i] != s2[i]:	
	7	φ.	<pre>return abs(base64chars.index(s1[i]) - base64chars.index(s2[i]))</pre>	
	8	- d 💿	return res	
		Ē		
1	0	def	solve stego():	
1	1	Å	with open('G:/Desktop/1.txt'. 'rb') as f:	
F	Run	at teo	et X	Å
-				
		↑ Ba	nse sixty four point fiv0	
1		↓ 4		
-		= Ba	use sixty four noint five	
	-	0		
	*	<u>탄</u> 역 Ra	se sixty four noint five	
		a 🦉	196-217(Å-1001-h011(f-1146	
<u>s</u>			and the four estat fine	
影:7		Ba	ise_sixty_four_point_five	
		0		
		Ba	ise_sixty_four_point_five	
を調			CSDN	@seven-BING

最后得到flag为: flag{Base_sixty_four_point_five }

第十二题: 功夫再高也怕菜刀

题目描述: 菜狗决定用菜刀和菜鸡决一死战

▲题用时: 32秒	
功夫再高也怕菜刀 1 53 最佳Writeup由B301 • dals提	
难度系数:	
题目来源: 安恒杯	
题目描述:菜狗决定用菜刀和菜鸡决一死战	
题目场景:暂无	
题目附件: 附件1	
	CSDN @seven-BING

打开文件是一个流量包、

acfff53ce3fa4e2bbe8654284dfc18e1.... 2021/10/7 14:15 Wireshark captu... 2,310 KB

	acfff53ce3fa4e2bbe8654284dfc18e1.pcapng
--	---

文件(F)	编辑(E)	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)
	-	10.00	0	A			00			

-		N 👻 👻 🚍 🛣 🔽 🖃	- ~ ~ ~ <u>-</u>						
	http							表达式…	+
	分组子节演 > 寛祥	▶ 🗌 区分大	小写 字符串	∨ flag			查找	取消	
No	. Time	Source	Destination		Frotocol	Length Thfo			^
	184 8.282759602	192.168.25.128	192.168.43.8	3	ТСР	54 47844 → 80 [ACK] Seq=912 Ack=346 Win=30016 Len=0			
	185 8.484945747	192.168.25.128	192.168.43.8	3	ТСР	290 47844 → 80 [PSH, ACK] Seq=912 Ack=346 Win=30016 Len=236 [TCP segment of a	a reasser	nbled 🖡	
	186 8.486681298	192.168.43.83	192.168.25.1	28	ТСР	60 80 → 47844 [ACK] Seq=346 Ack=1148 Win=64240 Len=0			
	187 8.486797464	192.168.25.128	192.168.43.8	3	HTTP	779 POST /upload/1.php HTTP/1.1 (application/x-www-form-urlencoded)			-
	188 8.488527592	192.168.43.83	192.168.25.1	28	тср	60 80 → 47844 [ACK] Seq=346 Ack=1873 Win=64240 Len=0			
e	189 8.491449977	192.168.43.83	192.168.25.1	28	HTTP	474 HTTP/1.1 200 OK (text/html)			
	190 8.491488677	192.168.25.128	192.168.43.8	3	тср	54 47844 → 80 [ACK] Seq=1873 Ack=766 Win=31088 Len=0			- ~
<								>	
>	Frame 189: 474 bytes	on wire (3792 bits)	, 474 bytes ca	ptured (3792 bits) on interface 0			
>	Ethernet II, Src: Vm	ware_f5:c2:5f (00:50	:56:f5:c2:5f),	Dst: Vm	ware_21:b	8:f4 (00:50:56:21:b8:f4)			
>	Internet Protocol Ve	ersion 4, Src: 192.16	8.43.83, Dst:	192.168.2	25.128				
>	Transmission Control	Protocol, Src Port:	80, Dst Port:	47844, 9	Seq: 346,	Ack: 1873, Len: 420			
>	Hypertext Transfer P	rotocol							
~	Line-based text data	: text/html (6 lines	.)						
	-> ./\t2017-12-08	11:38:58\t0\t0777\n							
	/\t2017-12-08 1	1:39:10\t4096\t0777\ı	n						
	1.php\t2017-12-08	11:33:16\t33\t0666\	n						
	<pre>flag.txt\t2017-12</pre>	-08 11:35:29\t17\t06	66\n						
	hello.zip\t2017-1	2-08 09:32:36\t224\t	0666\n						
	<-								
0	180 31 36 09 33 33 0	09 30 36 36 36 0a 66	5 6c 61 67 2e	16.33.0	6 66·flag				^
0	190 74 78 74 09 32	30 31 37 2d 31 32 2d	30 38 20 31	txt 201	7 -12-08	1			
0	1a0 31 3a 33 35 3a 3	32 39 09 31 37 09 30	0 36 36 36 0a	1:35:29	· 17·0666	5,			
0	1b0 68 65 6c 6c 6f 2	2e 7a 69 70 09 32 30) 31 37 2d 31	hello.z	i p•2017-	1	CSDN @s	seven-BIN	JG.

提示里面包含一个flag.txt文件,于是再kali里面先用binwalk查看一下,也可以用windows中binwalk工具链接

422689	0×15B561	Zip archive data, encrypted at least v2.0 to extract, compressed size: 52, uncompressed size: 40, name: flag.txt	
root@kali:~/桌	面‡ binwalk acf	fff53ce3fa4e2bbe8654284dfc18e1.pcapng	
DECIMAL	HEXADECIMAL	DESCRIPTION	
63085 64045 12025 14001 238637 .240937 .391563 .393067 406647 412887	0×A1E2D 0×A21ED 0×C63F9 0×C68B1 0×12E66D 0×12EF69 0×153BCB 0×154AB 0×1576B7 0×158F17	xz compressed data xz compressed data	
.422689 'oot@kali:~/桌	0×158561 面 #	Zip archive data, encrypted at least v2.0 to extract, compressed size: 52, uncompressed size: 40, name flag.txt	CSDN @seven-BING

说明存在flag.txt,使用kali 中foremost进行分离。也可以用windows中foremost工具链接



用7z工具打开,需要密码:

C:\比赛文件\攻防世界\mis	sc新手区\	第十二题\out	file\zip\00002	778.zip\			_	
文件(F) 编辑(E) 查看(V) 书	签(A) I	[具(T) 帮助(H	H)					
🕂 🚥 💙 🕩 🏓 🎽 添加 提取 测试 复制 移动 删	】 〕 除 信息							
🦻 🔛 C:\比赛文件\攻防世界	\misc新手	⊑区\第十二题\	outfile\zip\00	002778.zip\				
名称	大小	压缩后大小	修改时间	创建时间	访问时间	属性	加密 注释	٦ - ٦
flag.txt	40	52	2017-12-0	2017-12-0	2017-12-0	А	+	
						CS	DN @seven	-BING

于是,转头又分析流量包,发现刚刚找flag时候出现的6666.jpg有点可疑。

右击,点击追踪流,点击tcp流

acfff53ce3fa4e2bbe8654284df	fc18e1.pcapng			-		×
文件(F) 编辑(E) 视图(V) 跳转(C		Shift+Right	工具(T) 帮助(H)			
🖉 🔳 🖉 💿 📕 🛅 🕱 🍯 🤇	折叠子树	Shift+Left				
📕 tcp.stream eq 1	展开全部(E)	Ctrl+Right		× -> -	表达式…	+
分组字节流 ∨ 宽窄	收起全部(A)	Ctrl+Left	flag	查找	取消	
No. Time S	应用为列	Ctrl+Shift+I	Protocol Length Info			^
183 8.282453099 184 8.28275960 185 8.484945747 185 8.484945747 186 8.486681298 187 8.486797464 188 8.488527592 ≤ > Frame 189: 474 bytes €	作为过滤器应用 准备过滤器 列试过滤器 用过滤器着色 過始流 复制 显示分组字节	, Ctrl+shift+O	HTTP 399 HT1P/1.1 200 OK (Textr/ntml) TCP 54 47844 >80 [ACK] Seq=912 Ack=346 Win=30016 Len=0 TCP 290 47844 >80 [PSH, ACK] Seq=912 Ack=346 Win=30016 Len=236 [TCP segment of TCP 60 80 + 47844 [ACK] Seq=346 Ack=1148 Win=66240 Len=0 HTTP 770 POST /upload/1.php HTTP/1.1 (application/x-www-form-urlencoded) TCP % Ctrl+Alt+Shift+T UDP % Ctrl+Alt+Shift+S HTTP% Ctrl+Alt+Shift+S HTTP% Ctrl+Alt+Shift+S	a reasser	mbled F	•
 > Ethernet II, Src: Vmwa > Internet Protocol Vers > Transmission Control F > Hypertext Transfer Pro 	导出分组字节流(B) Wiki协议页面 过滤器字段参考 协议首选项	Ctrl+Shitt+X	st: Vmware_21:b8:f4 (00:50:56:21:b8:f4) 2.168.25.128 7844, Seq: 346, Ack: 1873, Len: 420			
✓ Line-based text data: _>\/\+2017_12_08_1	解码为(A)					
/\t2017-12-08 11:	转到链接的分组(L) 在新窗口由显示已链接的分	2 8				
1.php\t2017-12-08 1	1:33:16\t33\t0666\n	<u> </u>]			
flag.txt\t2017-12-04 hello.zip\t2017-12-0 <-	3 11:35:29\t17\t0666\n 08 09:32:36\t224\t0666	\n				
0160 30 39 36 09 30 37 0170 30 31 37 2d 31 32 0180 31 36 09 33 33 09 0190 74 78 74 09 32 30	37 37 0a 31 2e 70 68 2d 30 38 20 31 31 3a 30 36 36 36 0a 66 6c 31 37 2d 31 32 2d 30	70 09 32 0 33 33 3a 61 67 2e 38 20 31	96•0777 •1.php•2 17-12-0 8 11:33: .6·33·06 66·flag. xt·2017 -12-08 1			^
01a0 31 3a 33 35 3a 32	39 09 31 37 09 30 36	36 36 0a 1	:35:29. 17.0666.			
Text item (text) 34 文	2 共		分组・2129 ・ 戸見示・43 (2.0%)		敬罟:Def	∨ •ult
					15:09	aur -
搜索 Web 朻 Windo		_ []]		-CSDN@6	老い202日41	d,G

当流到第七个的时候,出现了可疑的数据流。

Wireshark · 追踪 TCP 流 (tcp.stream eq 7) · acfff53ce3fa4e2bbe8654284dfc18e1.pcapng — [<
ntent-Length: 204999		^
lase64_decode(\$_POSI[action]));&action=QG1uaV92ZXQ01mkpc3B5YX1tZXJVB3JZ11W1MC1pO0BZZXRtdG1tZV95aW1pdCg	NKITA	
VOXZ1NZ21JX3F103K1C19ydM50aW11KDAp02VJaG80110%2BFC1p0ZsKZJ11YXNINJKFZGVJDZRIKCKFUE9IVFS1EJE1X5K/JGM9J	-9011	
JWYJ6MIJAUYKJPXNOCI9YZXBSYWNIKCJCCIISIISJGMPOYKJPXNOCI9YZXBSYWNIKCJCDIISIISJGMPOYKIAW91117ZM9YKCRPP	IA/JG	
<pre>3c3RybGVukCkJklskass9MikkYnVmLj11cmxkZwNvZGU011U1LnN1YnN0c1gkYywkaswyksk/ZwNobynAzndyaxRikGZvCGVukCkmli magy a start w start w start w start w start w start w start w start w start start w start w sta</pre>	03311	
JGJIZIK%2FIJEIOIIWIIK/OZVJAG8OINW8LSIPOZRPZSGPOW%3D%3D%ZI=RDpcd2FtCDY0XHd3d1X1cGXVYWRCNJY2N15qCGc%3D&	Z2=FF	
3FFE000104A4649460001010100/800/80000FFDB0043000101010101010101010101010101010101	10101	
10101010101010101010101010101010101010	10101	
.01010101010101010101010101010101010101	01108	
l3901E203012200021101031101FFC4001F00000105010101010101000000000000000	20002	
l0303020403050504040000017D01020300041105122131410613516107227114328191A1082342B1C11552D1F024336272820	90A16	
[/] 18191A25262728292A3435363738393A434445464748494A535455565758595A636465666768696A737475767778797A83848	58687	
3898A92939495969798999AA2A3A4A5A6A7A8A9AAB2B3B4B5B6B7B8B9BAC2C3C4C5C6C7C8C9CAD2D3D4D5D6D7D8D9DAE1E2E3E	4E5E6	
7E8E9EAF1F2F3F4F5F6F7F8F9FAFFC4001F01000301010101010101010100000000000	10002	
102040403040705040400010277000102031104052131061241510761711322328108144291A1B1C109233352F0156272D10A10000000000000000000000000000000000	62434	
L25F11718191A262728292A35363738393A43445464748494A535455565758595A636465666768696A737475767778797A828	38485	
38788898A92939495969798999AA2A3A4A5A6A7A8A9AAB2B3B4B5B6B7B8B9BAC2C3C4C5C6C7C8C9CAD2D3D4D5D6D7D8D9DAE2E	3E4E5	
52728E9EAF2F3F4F5F6F7F8F9FAFFDA000C03010002110311003F00FC18823DB907E62481211D6493F86143D914E012BCF5E30	056C4	
l0192E7D0CC40EFFC30478E3B0DFF00FD8F352DA3DBB0AF0769F2C1FF00964839699CF3866C9C11CF719E33AD6F1B7C840EB93	0AB71	
372D7327B0C1D99EC0632179FF49A8C75F376FF002FB9DFAD9BE65D66EDFE56D79EFADBB3D9AB5BE4AC95FB69D5455EDC28724	C9C70	
D238D89FC30A1F523AE3D4F6539D88632E4EE013080CA57FE58C5FC31A7FD34933F377E7DCD54B78F714DA0B00711038F9DC7	DF9DF	
)95E703FA6EAD98101D8A83702FF20FF9ED3779187FCF34391CF5F539AF568C36EFDF7BAD36F5BBDBBE9F146DE3D79F4DDAFBA	FA2F9	
)1EFA2B35B4657B90A6428036314F7C5BC1F967CC7DDCF7391D0B1C6CDBA6D0BB70A4292B9FF963177918FF00CF47E3033B88C	6324A	
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	6FF00	
7D3F357B745A42FE4566B5F3EFADB656B3F5B5B4FCDABD465BB78CFC85540620B421B811A1FBD7327FB47036F4F5F47DD4AD7B	78F73	
A1E2AEEA856EE73EBC8003B0C6D2573C63D81354E14C06DDE32EE5E30071EBC006365B45D72A300311C71E8A2B6A353021B10	EBCE6	
E151F72DA3C74E061B6F4C73F74E7D6A11DB4ED7B697DBEE4ADD3E1B69750478D5A5ABD6FA7E76F4BEEBD6FAD9CED1B70A9F90	047F3	~
客户端 分组, 0 服务器 分组, 0 turn(s).		
个对话(206 kB)	流 7	*
戈: 2011 2011 2011 2011 2011 2011 2011 201	(h	D
·海道州·法 打印 Sarra acm 近回 Classered		



发现就是jpg,然后把这些十六进制,复制到010editor中





点击另存为1.jpg

图片就出来



CSDN @seven-BING

第一次猜测这个是flag,但是输入进去不对,那么猜测就是压缩包密码: Th1s_1s_p4sswd_!!!

