

i春秋网鼎杯网络安全大赛clip题目writeup

原创

iqiqiya 于 2018-08-21 19:51:23 发布 10139 收藏 3

分类专栏: [我的CTF之路 -----2018春秋网鼎杯](#) [我的CTF进阶之路](#) 文章标签: [网鼎杯网络安全大赛clip题目writeup](#) [clip](#) [writeup](#) [MISC](#)

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/xiangshangbashaonian/article/details/81906161>

版权



[我的CTF之路](#) 同时被 3 个专栏收录

92 篇文章 5 订阅

订阅专栏



[-----2018春秋网鼎杯](#)

6 篇文章 0 订阅

订阅专栏

[我的CTF进阶之路](#)

108 篇文章 18 订阅

订阅专栏

题目信息:

下载下来是一个压缩包 解压之后可以得到两个文件

18 > clip_66ebb848ff3221cd09ff6006972f9a73

名称	修改日期	类型	大小
damaged.disk	2018/8/18 13:46	DISK 文件	2,570 KB
desc.txt	2018/8/18 13:38	文本文档	1 KB

<https://blog.csdn.net/xiangshangbashaonian>

下载链接: <https://pan.baidu.com/s/1k4UXTq8hYpwGLVzNa9lVEg> 密码: 9was

先查看desc.txt的内容并翻译

检测到英语 ⇌ 中文 翻译 人工翻译

Horse Clip-Clop
A strange filesystem is recovered from a damaged old hard disk.

马夹
从损坏的旧硬盘中恢复一个奇怪的文件系统。
<https://blog.csdn.net/xiangshangbashaonian>

可以看出damaged.disk是一个磁盘文件

那么里边肯定有东西!

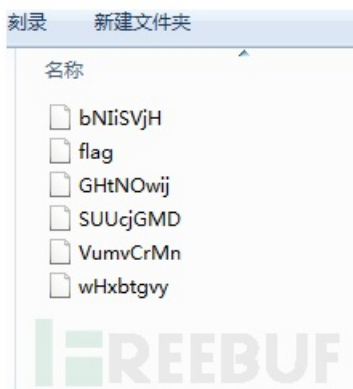
尝试将其放进kali linux用binwalk分析 foremost提取都无果。。。

各种百度damaged Boken

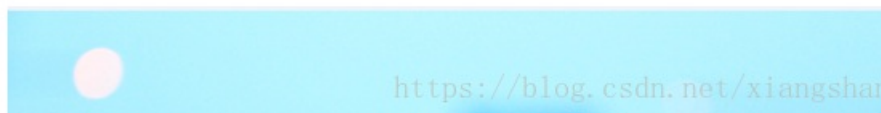
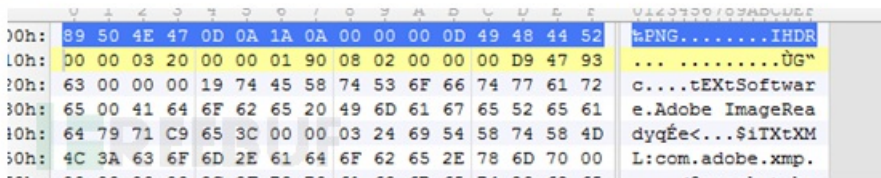
找到一篇[类似题目](#)(强网杯的)

Broken

什么都是坏的，找了个正常的引导区直接winhex覆盖头，发现启动不了，通过vmware在windows下挂载软盘镜像或者直接winhex打开，可以找到几个文件：



Flag文件拿下来，补上png的文件头：





开脑洞，调大长度，拿到flag：



<https://blog.csdn.net/xiangshangbashaonian>

那么上winhex分析

根据PNG文件格式中的数据块格式

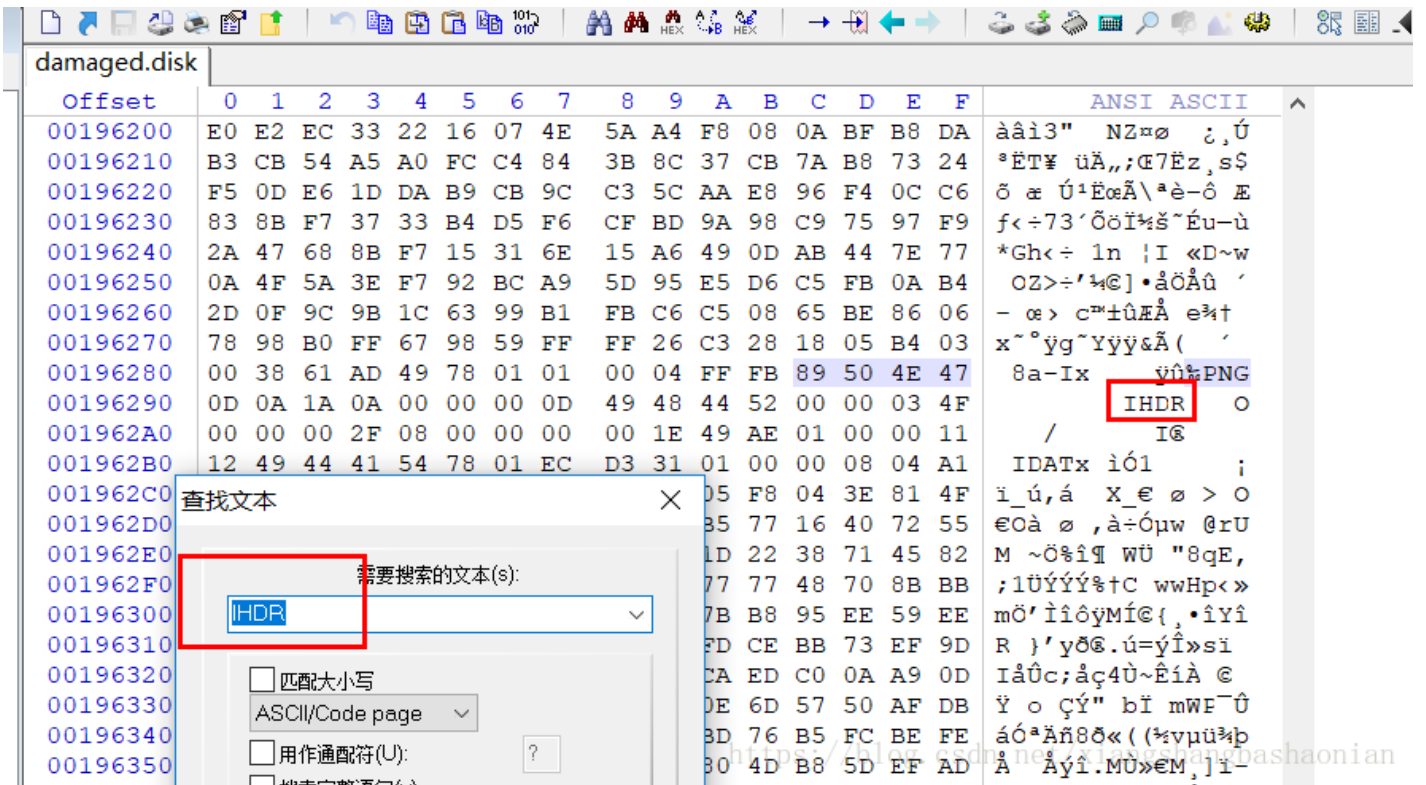
PNG文件格式中的数据块				
数据块符号	数据块名称	多数据块	可选否	位置限制
IHDR	文件头数据块	否	否	第一块

PNG图片文件头和文件尾格式

PNG (png), 文件头: 89504E47 <https://blog.csdn.net/xiangshangbashaonian> 文件尾: AE 42 60 82

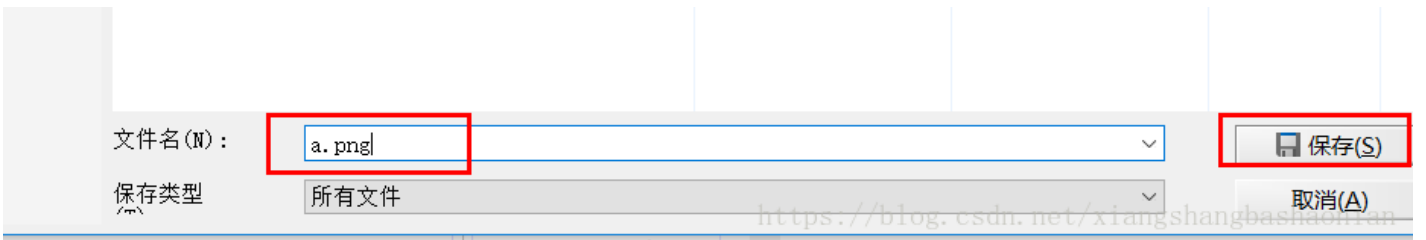
我们直接ctrl+F搜索文本IHDR

这是第一个图片



这里会出现搜索不到文件尾的情况 直接从89 50 4E 47选中到00197400这一行结尾就好

然后右键编辑à复制选块à至新文件à重命名保存



按F3继续向下搜索

找到第二张图片 但是PNG文件头不完整 补齐89 50 4E 47 0D

00198850	60 14 8C 54 00 00 04 00 00 01 78 5E 63 60 18 05	GT x^c`
00198860	A3 60 14 8C 54 00 00 04 00 00 01 78 5E 63 60 18	£` GT x^c`
00198870	05 A3 60 14 8C 54 00 00 04 00 00 01 78 5E 63 60	£` GT x^c`
00198880	18 05 A3 60 14 8C 54 00 00 04 00 00 01 78 5E 63	£` GT x^c`
00198890	60 18 05 A3 60 14 8C 54 00 00 04 00 00 01 78 01	£` GT x
001988A0	01 00 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48	%PNG IH
001988B0	44 52 00 00 03 4F 00 00 00 2F 08 00 00 00 00 1E	DR 0 /
001988C0	49 AE 01 00 00 11 12 49 44 41 54 78 01 EC D3 31	I@ IDATx ió1
001988D0	01 00 00 08 04 A1 EF 5F FA 2C E1 08 1D 58 5F 80	;i,ú,á X_e
001988E0	05 F8 04 3E 81 4F 3D 4F E0 13 E8 04 2C E0 F7 D3	ø > ceDà ø ,à÷ó
001988F0	B5 77 16 40 72 55 4D 1B 7E E6 25 EE B6 1B 37 DC	µw @rUM -ó%i¶ wÜ
00198900	1D 22 38 71 45 82 3B 31 DC DD DD DD 25 86 43 1C	"8qE,;1ÜÝÝ%+C
00198910	77 77 48 70 8B BB 6D D6 92 CC EE F4 FF 4D CD A9	wwHp«»mÖ' ìiôÿMí@
00198920	7B B8 95 EE 59 EE 52 7F 7D 92 79 F0 AE 2E FA 3D	{,•iYiR }'yð@.ú=
00198930	FD CE BB 73 EF 9D 49 E5 DB 63 3B E5 E7 34 D9 7E	ýÍ»si IáÛc;âç4Û~
00198940	CA ED C0 0A A9 0D 9F 0E 6F 9D C7 DD 22 09 62 CF	ÊiÀ @ Ý o ÇÝ" bÍ
00198950	0E 6D 57 50 AF DB E1 D3 AA C4 F1 38 F0 AB 28 28	mWF^Úáó^Añ8ð«((
00198960	BD 76 B5 FC BE FE C5 05 05 C5 FD EE 2E 4D D9 BB	~vuu%pA Äyi.MÜ»

按照上边的格式空8个位

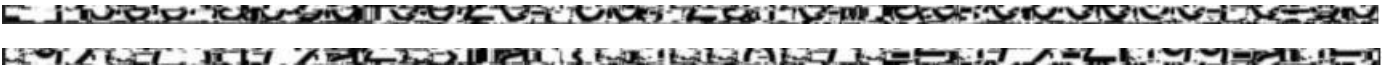
001999E0	9F CA B7 FF D6 7E DE 2C 95 57 FF EA B5 D0 A3 E3	ÝÊ·ÿÖ~Þ,•WÿèµÐÉä
001999F0	8B BB 8A CC 8E DB 2C F5 7C AE B9 3A F0 FC C9 47	<»ŠižŮ,ð @¹:ðúÉG
00199A00	0E 97 96 78 7E 9E FF FD F7 EE E5 9E 93 9F FD 67	--x~žÿÿ=iáž"Ýÿg
00199A10	78 FC 2F E3 49 55 E9 E1 34 06 20 F0 74 F5 73 99	xú/ãIUéá4 ðtðsÿ
00199A20	E7 94 D0 C4 30 0A 46 C1 10 04 00 A4 D9 A1 33 78	ç"ÐÄ0 FÁ µÜ;3x
00199A30	5E 63 60 18 05 A3 60 14 8C 54 00 00 04 00 00 01	£`cse£) £` GT /xiangshangbashaonian
00199A40	78 5E 63 60 18 05 A3 60 14 8C 54 00 00 04 00 00	x^c` £` GT

选中到这里结束就好 保存成b.png

接着对比两张图片



然后进行切图 拼图(ps大法好)



最后得到flag

