

攻防世界misc文件格式化分析

原创

MIGENKING 于 2019-09-19 00:25:58 发布 700 收藏

分类专栏: [做题](#)

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/MIGENKING/article/details/98759238>

版权



[做题](#) 专栏收录该内容

23 篇文章 0 订阅

订阅专栏

ext3:

The screenshot shows a challenge card for 'ext3'. It includes a difficulty rating of 1.0 (one star), the source 'bugku', a description in Chinese: '今天是菜狗的生日, 他收到了一个linux系统光盘', a live scenario of 'N/A', and an attachment named 'Enclosure1'. The URL 'https://blog.csdn.net/MIGENKING' is visible at the bottom right of the card.

题目提示! ext3文件

是一种Linux日志文件, 所以在Linux系统下用:

法一用kali虚拟机:

strings 文件名 |grep flag 查看文件中含有flag的文件;

```
root@WFL:~/桌面# strings linux |grep flag
.flag.txt.swp
flag.txtt.swx
~root/Desktop/file/O7avZhikgKgbF/flag.txt
.flag.txt.swp
flag.txtt.swx
.flag.txt.swp
flag.txtt.swx
```

发现一个含有“~root/Desktop/file/O7avZhikgKgbF/flag.txt”内含有flag.txt, 于是使用“mount” (mount可将指定设备中指定的文件系统加载到Linux目录下 (也就是装载点)):

```
~root/Desktop/file/07avZhikgKgbF/flag.txt
.flag.txt.swp
flag.txttt.swx
.flag.txt.swp
flag.txttt.swx
root@WFL:~/桌面# mount linux /mnt
root@WFL:~/桌面# cd /mnt
root@WFL:/mnt# ls
02CdWGSxGPX.bin  8A2MFawD4  ix1EMRHRpIc2  n  r
0GY1l            8DQFirm0D  j6uLMX        NgzQPW  Raf3SYj
0h3a5            8HhWfV9nK1  jE            Nv      rhZE1LZ6g
0l              8nwg        jj            o       Ruc9
0qsd            8RxQG4bvd  KxEQM        07avZhikgKgbF  RZTOGd
0wDq5           FinD        LG6F         o8      scripts
0Xs            fm          Lh           00o0s  sdb.cramfs
1              g           LlC6Z0zrgy.bin  orcA   sn
2X             gtj         L00J8        oSx2p  SPaK8l2sYN
3              h           lost+found   OT      SrZznhsAj
3J            H           LvuGM        poiuy7Xdb  t
44aAm         H2Zj8FNbu  lWIRfzP     px6u   T
4A            hdi7       m            Q       TFGV0SwYd.txt
6JR3         hYuPvID    m9V0lIaElz  qkCN8  https://blog.csdn.net/MIGENKING
6uHc7F1ybcH   i          MiH         QmUY1d
```

```
root@WFL:/mnt# cd 07avZhikgKgbF/
root@WFL:/mnt/07avZhikgKgbF# vim flag.txt
[1]+ 已停止          vim flag.txt
```

ZmxhZ3tzYWpiY2lienNrampbmJoc2J2Y2pianN6Y3N6Ymt6an0

“=”是base64密码的标志

rsacrack

VMwareTools-10.2.0-7259539.tar.gz

vmware-tools-distrib

shell.php

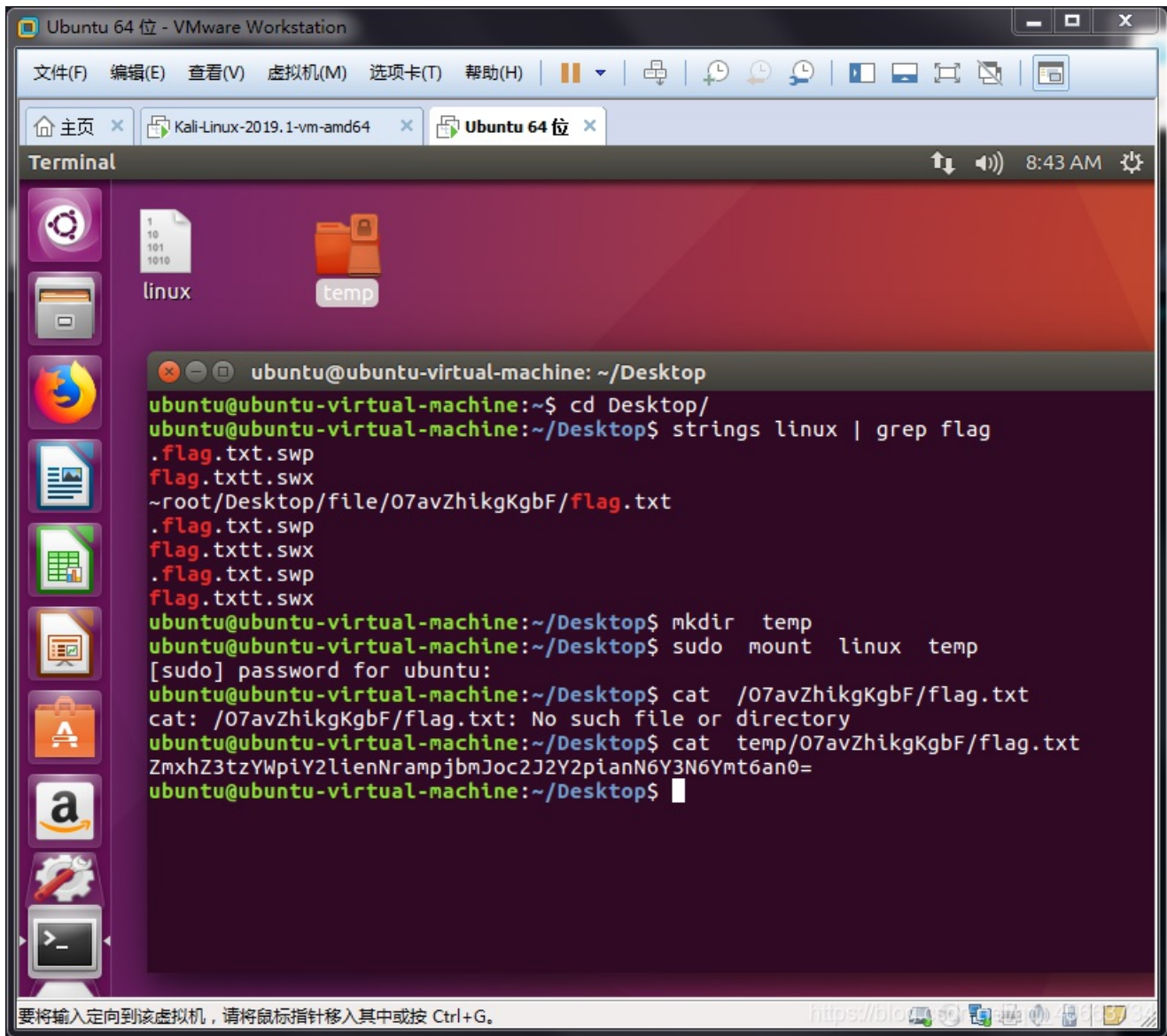
1,52 全部

https://blog.csdn.net/MIGENKING

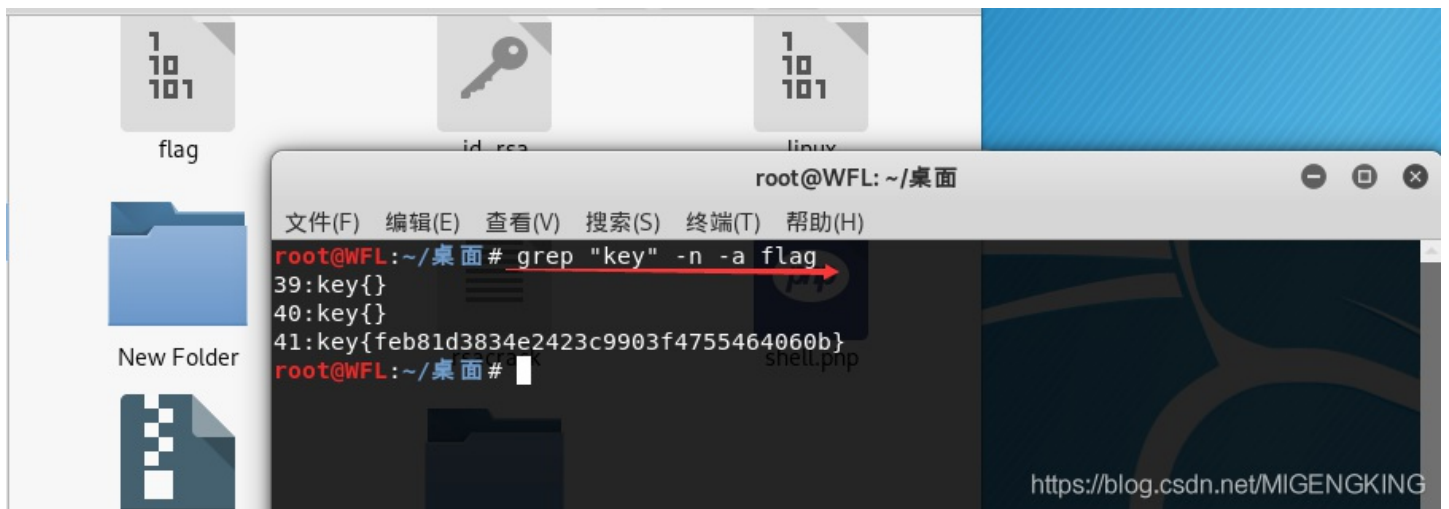
然后直接base64 (-d, --decode 解码数据) 解码得到flag:

```
root@WFL:/mnt/07avZhikgKgbF# base64 -d flag.txt
flag{sajbcibzskjjcnbhsbvcjbjszcszbkzj}root@WFL:/mnt/07avZhikgKgbF#
```

法二：用Ubuntu虚拟机：



而bugku上的MISC的Linux题目解法差不多（不过命令行才熟练）：



也可以用Notepad++来查找，首先查找flag，不过找不到，后面用key来找：

33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61

查找 x

查找 替换 文件查找 标记

查找目标(F): key 查找下一个

选取范围内(I) 计数(T)

反向查找 查找所有打开文件(O)

全词匹配(W) 在当前文件中查找

匹配大小写(C) 取消

循环查找(P)

查找模式

普通(N) 透明度(Y)

扩展(X) (\n, \r, \t, \0, \x...)

正则表达式(G) . 匹配新行 失去焦点后

始终

[Progress Bar]

```
key{ }  
key{ feb81d3834e2423c9903f4755464060b1 }  
key{ }
```