bugku-ctf-Misc-ext3-WriteUp

原创

萌萌哒的baola 于 2020-05-23 17:31:39 发布 280 收藏

分类专栏： ctf题解

本文链接：https://blog.csdn.net/Claming_D/article/details/106063007

文章目录

ext3

题目分析

题目给了一个linux system file，这个linux file 正如题目所说是一个第三代扩展文件系统(Third extended filesystem，缩写为ext3)，是一个日志文件系统，用于Linux操作系统。它是很多Linux发行版的默认文件系统。对于这中文件系统，我们可以将其挂载到linux系统的某目录下，查看里面的内容。

Linux中的根目录以外的文件要想被访问，需要将其“关联”到根目录下的某个目录来实现，这种关联操作就是“挂载”，这个目录就是“挂载点”，解除次关联关系的过程称之为“卸载”。

```
[root@localhost ~]# mount [-t 文件系统] [-L 卷标名] [-o 特殊选项] \
设备文件名 挂载点
#\代表这一行没有写完，换行
选项：
    -t 文件系统：    加入文件系统类型来指定挂载的类型，可以 ext3、ext4、iso9660
                等文件系统。具体可以参考表 9-1
    -L 卷标名：      挂载指定卷标的分区，而不是安装设备文件名挂载
    -o 特殊选项：    可以指定挂载的额外选项，比如读写权限、同步异步等，如果不指定
                则默认值生效。具体的特殊选项，见表 9-4：
```

对于挂载不熟悉可以看一下这篇文章：Linux中挂载详解以及mount命令用法

执行挂载操作,挂载完后，我们可以看到有很多文件以及文件夹

```
root@kali:~# mount /root/Desktop/f1fc23f5c743425d9e0073887c846d23  /mnt/test
root@kali:~# cd /mnt/test/
root@kali:/mnt/test# 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          O7avZhikgKgbF RZTOGd
0wDq5            FinD        LG6F           o8           scripts
0Xs              fm          Lh             OOoOs        sdb.cramfs
1                g           LlC6Z0zrgy.bin orcA         sn
2X               gtj         LO0J8          oSx2p        SPaK8l2sYN
3                h           lost+found     OT           SrZznhSAj
3J               H           LvuGM          poiuy7Xdb    t
44aAm            H2Zj8FNbu   lWIRfzP        px6u         T
4A               hdi7        m              Q            TFGVOSwYd.txt
6JR3             hYuPvID     m9V0lIaElz     qkCN8
6wUaZE1vbsW      i           MiU            QmUY1d
7H7geLlS5        imgLDPt4BY  Mnuc           QQY3sF63w
root@kali:/mnt/test#
```


我们想要在这么多的文件和文件夹中找到flag，一个一个去看肯定不可取，我们可以使用 strings命令对这个ext3文件系统进行搜索有效信息，比如搜索flag，key之类的字眼，这也是解题套路。

```
root@kali:~# cd /root/Desktop/
root@kali:~/Desktop# strings f1fc23f5c743425d9e0073887c846d23 -f | grep flag
f1fc23f5c743425d9e0073887c846d23: .flag.txt.swp
f1fc23f5c743425d9e0073887c846d23: flag.txtt.swx
f1fc23f5c743425d9e0073887c846d23: ~root/Desktop/file/O7avZhikgKgbF/flag.txt
f1fc23f5c743425d9e0073887c846d23: .flag.txt.swp
f1fc23f5c743425d9e0073887c846d23: flag.txtt.swx
f1fc23f5c743425d9e0073887c846d23: .flag.txt.swp
f1fc23f5c743425d9e0073887c846d23: flag.txtt.swx
root@kali:~/Desktop#
```


找到一个flag.txt文件，用 -f 命令显示文件的路径，我们知道了flag.txt文件基本位置，接下来more一下这个文件

```
root@kali:/mnt/test# more ./O7avZhikgKgbF/flag.txt
ZmxhZ3tzYWpiY2lienNrampjbmJoc2J2Y2pianN6Y3N6Ymt6an0=
```

得到一个base64编码的字符串，base64解码方式有多种（在线，linux里面的base64
命令），这里我用python的base64库解码。

```
>>> import base64
>>> base64.b64decode("ZmxhZ3tzYWpiY2lienNrampjbmJoc2J2Y2pianN6Y3N6Ymt6an0=")
b'flag{sajbcibzskjjcnbhsbvcjbjszcszbkzj}'
>>>
```

其他思路：
1.直接将这个ext3文件放到winhex里面搜素flag，也能找到flag路径，然后用360压缩等压缩软件，打开ext3，根据路径找到flag.txt文件也可以得到flag。
2.直接搜索flag的base64编码：“ZmxhZ”，在winhex里直接得到flag的完整base64编码。

总结

这题主要考察给定linux某文件系统，如何快速地查找有效信息，在linux里面第一步就是要挂载这个文件，然后我们可以借助strings等命令查找敏感文件，得到敏感文件的路径，在挂载后的目录下找到该文件即可。当然其他的思路也是可以的。