xctf攻防世界 MISC高手进阶区 Recover-Deleted-File

原创

l8947943 于 2022-01-15 19:33:19 发布 5779 收藏

分类专栏： 攻防世界misc之路 文章标签： linux 运维 服务器 misc

本文链接：https://blog.csdn.net/l8947943/article/details/122514473

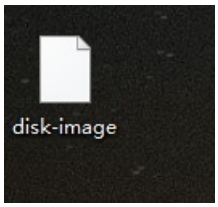
攻防世界misc之路 专栏收录该内容

68 篇文章 2 订阅

订阅专栏

1. 进入环境，下载附件

解压后发现是个无后缀的disk-image文件：



题目给的给的提示 `恢复磁盘并且找到FLAG.`

2. 问题分析

1. **扔进kali恢复**
   这个工具没怎么使用过，参考网上的命令：extundelete恢复文件。如何使用，参考链接：
   https://blog.csdn.net/liucc09/article/details/51644173

先安装extundelete工具

```
$ sudo apt install extundelete
```

fls列出图像中的文件和目录名，并可以显示使用给定名称的目录最近删除的文件的文件名：

```
$ fls disk-image
```

可以看到有个flag东东，搞起

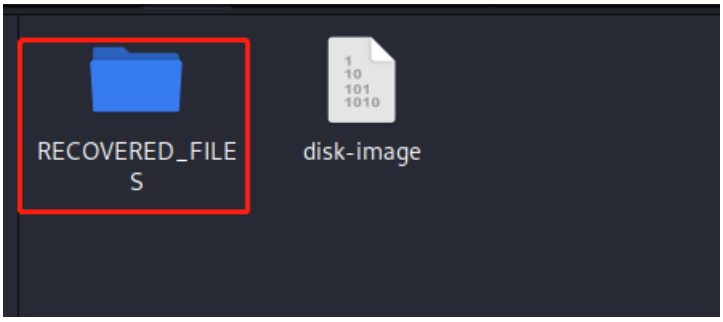
接着恢复文件：

```
$ extundelete --restore-all disk-image
```

如图：

```
┌──(zhangfa㉿kali)-[~/下载]
└─$ extundelete --restore-all disk-image
NOTICE: Extended attributes are not restored.
Loading filesystem metadata ... 1 groups loaded.
Loading journal descriptors ... 17 descriptors loaded.
Searching for recoverable inodes in directory / ...
1 recoverable inodes found.
Looking through the directory structure for deleted files ...
0 recoverable inodes still lost.
```

出来个恢复文件



2. **尝试打开**

   打开flag后一堆乱码，我还以为在文件中找，TM的，这是个可执行文件。。。麻了！

修改文件权限可执行：

```
chmod +x flag
```

然后执行它：

```
┌──(zhangfa㉿kali)-[~/下载/RECOVERED_FILES]
└─$ ./flag
your flag is:
de6838252f95d3b9e803b28df33b4baa
```

最终答案为：`de6838252f95d3b9e803b28df33b4baa`