Boston Key Party 2015 Heath Street 题解（Writeup）

转载

anrao3094 于 2017-04-30 23:44:00 发布 67 收藏
文章标签： 操作系统
原文链接：http://www.cnblogs.com/HacTF/p/6790769.html

Heath Street是Boston Key Party 2015的一道数字取证题目，我们得到了一个叫做“secretArchive.6303dd5dbddb15ca9c4307d0291f77f4”的文件，目标显然是将包含flag的文件恢复过来。

识别

首先我们使用file来确定文件类型

```
wiremask:~$  file  secretArchive.6303dd5dbddb15ca9c4307d0291f77f4
```

secretArchive.6303dd5dbddb15ca9c4307d0291f77f4: Linux rev 1.0 ext4 filesystem data, UUID=035b2734-be8c-46dd-af8f-1b3523dcd9d2 (extents) (huge files)

诱饵

文件看上去是一个linux文件系统，我们把他挂载到系统来检查其内容

```
wiremask:~$  mount  secretArchive.6303dd5dbddb15ca9c4307d0291f77f4  /mnt/tmp
```

里面包含了1986个文件，绝大部分是ASCII文本文件，都是《The Venona Story》里面的内容。“secret1337”文件看上去和其他不同，他是一个加密的ZIP文件，不幸的是他只是一个诱饵。

恢复文件

其实真正的目标是恢复删除过的文件，也许可以使用extundelete，他可以从ext4分区恢复删除的文件。

```
wiremask:~$ extundelete --restore-all secretArchive.6303dd5dbddb15ca9c4307d0291f77f4
```

这个命令产生了一个隐藏的新文件“.secret31337”，使用file命令查看后我们发现这是一个使用KGB Archiver 软件进行了3级压缩的文件

获取flag

最后一步是下载这个软件然后解压缩，最后我们获得了flag。