攻防世界-misc进阶 Recover-Deleted-File

原创

vientof 于 2020-07-20 18:01:06 发布

分类专栏： 攻防世界 文章标签： ctf misc 攻防世界

攻防世界-misc进阶 Recover-Deleted-File

攻防世界全misc进阶（Github）

- 工具

> scalpel
> 扫描整个镜像文件，根据配置文件寻找相关文件类型的文件头和文件尾，正常找到后将这段内容雕刻出来；当找到了文件的头部，但是在它附近没有找到文件尾标志的时候，scalpel提供两种处理方式，一是放弃对该文件的雕刻，二是根据自定义的各类文件的最大长度进行雕刻。

> https://github.com/sleuthkit/scalpel

方法一

- 解压出文件， binwalk查看文件

```
$ binwalk disk-image
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Linux EXT filesystem, rev 1.0 ext3 filesystem data, UUID=bc6c2b24-106a-4570-bc4f-a
e09abbdabbd
65536         0x10000         Linux EXT filesystem, rev 1.0 ext3 filesystem data, UUID=bc6c2b24-106a-4570-bc4f-a
e09abbdabbd
72704         0x11C00         Linux EXT filesystem, rev 1.0 ext3 filesystem data, UUID=bc6c2b24-106a-4570-bc4f-a
e09abbdabbd
1113088       0x10FC00        ELF 64-bit LSB executable, AMD x86-64, version 1 (SYSV)
1116896       0x110AE0        LZMA compressed data, properties: 0x89, dictionary size: 16777216 bytes, uncompres
sed size: 100663296 bytes
1117024       0x110B60        LZMA compressed data, properties: 0x9A, dictionary size: 16777216 bytes, uncompres
sed size: 100663296 bytes
1117216       0x110C20        LZMA compressed data, properties: 0xB6, dictionary size: 16777216 bytes, uncompres
sed size: 33554432 bytes
1117408       0x110CE0        LZMA compressed data, properties: 0xD8, dictionary size: 16777216 bytes, uncompres
sed size: 50331648 byt
```

- 我们用自己写的scalpel的config 文件执行

```
# scalpel.conf
elf     y       1000000 \x7F\x45\x4C\x46
```

```
$ scalpel -c scalpel.conf disk-image
[...]
$ tree scalpel-output
scalpel-output/
├── audit.txt
└── elf-0-0
    └── 00000000.elf

    1 directory, 2 files
```

- 查看执行了什么

```
$ chmod u+x ./scalpel-output/elf-0-0/00000000.elf && ./scalpel-output/elf-0-0/00000000.elf
your flag is:
de6838252f95d3b9e803b28df33b4baa
```

方法二

- 使用命令

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

生成文件夹 RECOVERED_FILES

运行 flag 文件

得到 flag

> de6838252f95d3b9e803b28df33b4baa