

# 攻防世界 Misc simple\_transfer

原创

==Microsoft== 于 2022-02-26 12:20:43 发布 110 收藏

分类专栏: [Misc](#) 文章标签: [ctf misc](#)

迷心兔

本文链接: <https://blog.csdn.net/MrTreebook/article/details/123148008>

版权



[Misc](#) 专栏收录该内容

50 篇文章 0 订阅

订阅专栏

## 攻防世界 Misc simple\_transfer

- 1.binwalk分析
- 2.foremost分解
- 3.flag

### 1.binwalk分析

binwalk simple\_transfer.pcap

```
(root@kali)-[~/mss/桌面]
└─# binwalk simple_transfer.pcap
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	Libcap capture file, little-endian, version 2.4, Ethernet, snaplen : 262144
339380	0x52DB4	PDF document, version: "1.5"
339454	0x52DFE	Zlib compressed data, default compression
340171	0x530CB	Zlib compressed data, default compression
6380104	0x615A48	Zlib compressed data, default compression
6385002	0x616D6A	Zlib compressed data, default compression

CSDN @==Microsoft==

- 发现有一个pdf document
- 直接想到foremost分解

### 2.foremost分解

foremost simple\_transfer.pcap

```
(root@kali)-[~/mss/桌面]
└─# foremost simple_transfer.pcap
Processing: simple_transfer.pcap
|*|
```

目录下会生成一个output文件

打开看一下



打开这个pdf文件看一下

得到flag

### 3.flag

