# 攻防世界Misc赛题记录

原创

Bit0_ 于 2021-10-14 11:23:33 发布 68 收藏
文章标签： 经验分享 网络安全


**János-the-Ripper**

题目：

https://adworld.xctf.org.cn/task/answer?type=misc&number=1&grade=1&id=4756&page=1

知识点：

1.010查看文件，PK开头为zip文件标志。

2.zip压缩包若非伪加密（09 00），密码可尝试爆破（Advanced Archive Password Recovery）

**hit-the-core**

题目：

https://adworld.xctf.org.cn/task/answer?type=misc&number=1&grade=1&id=5024&page=1

知识点：

1.kali中strings文件，字符串中存在栅栏密码（隔几个字符取一个字符）

**Ditf**

题目：

https://adworld.xctf.org.cn/task/answer?type=misc&number=1&grade=1&id=5562&page=2

知识点：

1.修改图片高度CTF 图片隐写之修改图片高宽_D-R0s1的博客-CSDN博客_ctf修改图片高度

2.流量包中搜索pdf字段，追踪http流

**stage1**

题目：

https://adworld.xctf.org.cn/task/answer?type=misc&number=1&grade=1&id=4878&page=2

Writeup：

攻防世界_MISC进阶区_stage 1_RuoLi_s的博客-CSDN博客

知识点：

1.二维码扫描器：QR reserch 更万能，很多在线扫描扫不出的也能扫

2.一串类似十六进制的文件源码，03F30D0A开头是pyc文件，复制到winhex中，用ASCII hex，另存为.pyc文件，使用Easy Python Decompiler反编译，得到文件改为.py运行。

**Miscellaneous-200**

题目：

https://adworld.xctf.org.cn/task/answer?type=misc&number=1&grade=1&id=4901&page=2

Writeup：

攻防世界 Misc高手进阶区 3分题 Miscellaneous-200_闵行小鱼塘-CSDN博客

知识点：

1.多组三个三位数字组成数据，可能为像素点，使用python代码画出。

**Hear-with-your-Eyes**

题目：

https://adworld.xctf.org.cn/task/answer?type=misc&number=1&grade=1&id=4904&page=2

知识点：

1.音频文件，尝试用Audacity打开，看频谱图。

**Hidden-Message**

题目：

https://adworld.xctf.org.cn/task/answer?type=misc&number=1&grade=1&id=4905&page=2

知识点：

1.端口隐写，有01规律，8位二进制为一组，可利用ASCII转换为字符，但因为是1开头，大于ASCII对应最大二进制数（最大为01111111），故考虑将01互换，得到答案。

**Recover-Deleted-File**

题目：

https://adworld.xctf.org.cn/task/answer?type=misc&number=1&grade=1&id=4906&page=2

知识点:

1.修复误删文件磁盘

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

2.齿轮图标文件，可尝试执行。

**就在其中**

题目：

https://adworld.xctf.org.cn/task/answer?type=misc&number=1&grade=1&id=4925&page=2

Writeup：

攻防世界misc——就在其中_CNS-Enterprise BCC-1701-J-CSDN博客

知识点：

1.流量包字段搜索：key，或逐个TCP流追踪检查可疑项。

2.BEGIN RSA PRIVATE KEY为私钥，需要全部复制（包括首尾标识）保存到.key文件使用。

3.txt文件乱码，可能需要用私钥解密，openssl命令：

```
openssl rsautl -decrypt -in key.txt -inkey psa.key -out flag.txt
```

**再见李华**

题目：

https://adworld.xctf.org.cn/task/answer?type=misc&number=1&grade=1&id=4927&page=2

知识点：

1.注意题目提示，对数字敏感，进制转换。本题“不少于1000字”暗示密码不少于8位（0x1000=8），根据提示进行爆破。

**MISCall**

题目：

https://adworld.xctf.org.cn/task/answer?type=misc&number=1&grade=1&id=4937&page=2

Writeup：

攻防世界——MISCall_Sylvia_j的博客-CSDN博客

知识点：

1. binwalk 查看文件类型

2. tar xjvf 解压bzip2文件

3. git stash命令 `git stash show` 显示做了哪些改动

    git stash 用法总结和注意点 - 加个小鸡腿 - 博客园

**flag_universe**

题目：

https://adworld.xctf.org.cn/task/answer?type=misc&number=1&grade=1&id=5458&page=2

Writeup：

记录下做攻防世界的misc题 - Paddling - 博客园

知识点：

1.WireShark查看流量包的追踪流时，右下角可切换流序号，方便切换。

2.查看TCP流时，红色是客户端分组，蓝色是服务器分组，可能在此做提示。

3.在TCP流中发现图片ASCII源码时，切换为显示原始数据，复制后粘贴到Winhex新建文件，以ASCII Hex格式传入，保存为相应格式即可。

4.zsteg工具可破解LSB隐写中的flag。