入门知识

前言

与音频相关的 CTF 题目主要使用了隐写的策略，主要分为 MP3 隐写，LSB 隐写，波形隐写，频谱隐写等等。

常见手段

通过 binwalk 以及 strings 可以发现的信息不再详述。

MP3 隐写

MP3 隐写主要是使用 Mp3Stego 工具进行隐写，其基本介绍及使用方法如下

```
# MP3Stego will hide information in MP3 files during the compression process. The data is first compressed, encrypted and then hidden in the MP3 bit stream.
encode -E hidden_text.txt -P pass svega.wav svega_stego.mp3
decode -X -P pass svega_stego.mp3
```

波形

通常来说，波形方向的题，在观察到异常后，使用相关软件（Audacity, Adobe Audition 等）观察波形规律，将波形进一步转化为 01 字符串等，从而提取转化出最终的 flag。

频谱

音频中的频谱隐写是将字符串隐藏在频谱中，此类音频通常会有一个较明显的特征，听起来是一段杂音或者比较刺耳。

LSB 音频隐写

类似于图片隐写中的 LSB 隐写，音频中也有对应的 LSB 隐写。主要可以使用 Silenteye 工具，其介绍如下：

```
# SilentEye is a cross-platform application design for an easy use of steganography, in this case hiding messages into pictures or sounds. It provides a pretty nice interface and an easy integration of new steganography algorithm and cryptography process by using a plug-ins system.
```

常用工具

- binwalk
- MP3Stego
- Adobe Audition
- silenteye

实战案例

把东西藏到音频里 - 常见音频隐写的实现方法

参考资料

CTFer成长之路-Nu1L战队-Misc部分