M1n3 / 2018-01-12 13:29:00 / 浏览数 9849 安全技术 CTF 顶(1) 踩(0)

# 实验简介

音频、视频等多媒体也是我们生活经常看到的文件格式。我们上网听音乐,看视频,都离不开多媒体,一方面多媒体文件一般比单独的图片文件大,这是否也意味着能存储。

## 实验内容

实验内容主要针对音频文件以及视频文件为载体的隐写分类

- 一、音频
  - 众所周知的摩尔斯电码
  - 利用MP3stego进行的数据隐写
  - 频谱图
- 二、视频
  - 通过分离视频文件

## 实验环境

- 操作机: Windows XP
  - 实验工具:
    - Adobe Auditon之后暂且简称AU
    - · mp3stego
    - foremost for windows
       下面进行实验 音频隐写

# 第一部分 音频隐写

## 众所周知的摩尔斯电码

背景知识

摩尔斯电码(又译为摩斯密码, Morse

code)是一种时通时断的信号代码,通过不同的排列顺序来表达不同的英文字母、数字和标点符号。在过去它以电报的形式来发送消息,如今当听到这样的电报你还能解出

摩尔斯电码对照表

# 实验

实验:

- ------

- BERNARD Auditon

- **BERNESSES**flag

- ■■■flag■ xianzhi.aliyun.com

当我们确认是摩尔斯电报之后,我先用Adobe Auditon打开目标文件,并观察波形

以长的代表代表横线,短的代表点,大的间隔是空格,抄写下摩尔斯电码

对照上图,将摩尔斯电码抄写下来是:

-..- .. .- -. --.. .... .. .-.-. .- .-. .. -.-- ..- -. .-.- -.- ---

按照上文中的摩尔斯电码对照表翻译

最后翻译出来的结果是 xianzhi.aliyun.com

当然,我们也可以利用一些! $\underline{\text{在线的工具}}$ 翻译摩尔斯电码,也可以利用JPK这样的工具进行翻译。如下图的操作:

#### 思考与实践

1. 利用lakey这个软件给制作一个自己ID的摩尔斯电文吧。

# 利用MP3stego进行的数据隐写

## MP3stego介绍

MP3stego是著名的音频数据隐写工具,支持常见的压缩音频文件格式如mp3的数据嵌入,它采用的是一种特殊的量化方法,并且将数据隐藏在MP3文件的奇偶校验块中。 使用方法

MP3Stego

■■■encode -E ■■■■ -P ■■ wav■■ mp3■■

■■■decode -X -P ■■ mp3■■

## 实验

实验:

小明想和小红告白,在一个首歌中藏了一个txt文件,可是小红却不知道怎么找到mp3文件中的隐藏信息,你能帮帮她吗? hit: password: love

- -----
- **IIIIIIIII**mp3stego**IIIIIIIIIIIIIIIIIIII**

首先先将目标文件复制到MP3stego这个工具的目录下

在CMD下使用Decode.exe程序进行提取

最后打开目录下的love.mp3.txt文件就能看到隐写内容了

## 思考与实践

1. 最后小明表白成功了,你是否也可以尝试去做一个MP3隐写呢

## 频谱图的音频隐写

#### 背景知识

频谱是频率谱密度的简称,是频率的分布曲线。复杂振荡分解为振幅不同和频率不同的谐振荡,这些谐振荡的幅值按频率排列的图形叫做频谱。在CTF中,我们可以单独只对一个声道中,隐写进信息

## 实验

- 实验:
- -----
- MANAGEMENT Adobe Aud ton
- -
- **BERNESSEE** flag flag (CTF\_i5\_really\_funny!)

## 直接进入正题吧

使用AU打开目标文件,

调整到频谱图,并调整频谱图大小,直到能看清flag

有必要只得一提的是,我们会发现只有一个音轨有隐写信息,那是因为我只对一个通道隐写进了信息,一般人也不会去分析这个wav文件的频谱吧。

## 思考与实践

如何做一个音频隐写?

# 音频隐写小结

音频文件的隐写,现如今除了通过频谱以外,还有一种是在时域中进行的信息隐写,在PCTF中,或者汪神的OJ中有几个挺经典例子,大家可以尝试去做看看。 另一方面,音频还有高级随机化技术的LSB嵌入技术,但是这还是不是很成熟。

## CSAW CTF 2016 Quals: Watchword为例

目前在CTF赛事中较为常出现的视频隐写,一般都是将一场带有隐写信息的图片,嵌入视频中,我们所需要做的就是将这个图片从视频分离出来,然后在分析我们分离出来的

另一方面,我们分离文件,如果单独对视频来说ffmpeg是一个很好的工具,这里我使用的是foremost

,一款linux下的命令行工具,当然我们也可以使用binwalk或者dd等工具,正如我们图片隐写中教大家分离图片所用的方法一样。 区别是,ffmpeg将视频分解成一张一张的图片,foremost是一个基于文件头和尾部信息以及文件的内建数据结构恢复文件的命令行工具。

#### 实验环境

- 操作机: linux
  - 实验工具:
    - foremost
      - · stegohide

#### 实验

- 实验:
- -----
- ----
- flag{We are fsociety, we are finally free, we are finally awake!}

#### 首先用foremost分离图片

foremost powpow.mp4

## 在output目录下找到分离出来的图片

使用命令 steghide extract -sf thing.jpg -p password提取图片隐写内容内容

#### 对提取出来的隐写内容进行解码

```
cat base64.txt
python3
>>> import base64
>>> base64.b85decode(b'W^7?+dsk&3VRB_4W^-?2X=QYIEFgDfAYpQ4AZBT9VQg%9AZBu9Wh@|fWgua4Wgup0ZeeU}c_3kTVQXa}eE')
b'flag{We are fsociety, we are finally free, we are finally awake!}'
```

#### 最终的flag是

\*\*完整操作命令flag{We are fsociety, we are finally free, we are finally awake!}

```
foremost powpow.mp4
stepic -i output/png/00001069.png -d > thing
steghide extract -sf thing.jpg -p password
cat base64.txt
python3
>>> import base64
>>> base64.b85decode(b'W^7?+dsk&3VRB_4W^-?2X=QYIEFgDfAYpQ4AZBT9VQg%9AZBu9Wh@|fWgua4Wgup0ZeeU}c_3kTVQXa}eE')
b'flag{We are fsociety, we are finally free, we are finally awake!}'
```

## 小结

一般的MISC题目都不是简简单单的一个隐写就能解决的,正常都包含了密码,编码,隐写甚至更多的计算机网络知识。

到这里,隐写的内容基本结束了,希望大家能学到东西,也不要拘束于我写的内容,毕竟这是一个天高任鸟飞的领域,并不是所有的内容我都能包含进来的。

#### 点击收藏 | 1 关注 | 2

上一篇:浅淡高级威胁情报对于安全建设的意义... 下一篇: DNS外带查询怎么防。。。

1. 1条追加内容

追加于 2018年1月12日 13:59

# 1. 4条回复



<u>老锥</u> 2018-01-25 15:20:37

支持

0 回复Ta



<u>1815837370479554</u> 2018-05-29 14:00:57

支持 支持

0 回复Ta



<u>相视一笑似路人</u> 2019-01-14 11:05:18



<u>相视一笑似路人</u> 2019-01-18 15:12:34

@相视一笑似路人

这几天研究了一下,视频文件素材是将视频和图片分别用二进制编辑器(我用的010editor)打开后,复制图片所有内容追加到视频的结尾处,然后保存即可,可以追加感谢楼主的分享~

0 回复Ta

登录 后跟帖

先知社区

# 现在登录

热门节点

# 技术文章

社区小黑板

目录

RSS <u>关于社区</u> <u>友情链接</u> <u>社区小黑板</u>