DOC隐写

原创

__N4c1__ 于 2019-07-26 20:32:32 发布 1836 收藏 6

分类专栏： ctf

本文链接：https://blog.csdn.net/qq_43504939/article/details/97416301


```
<p></p><h1 id="toc-0">实验简介</h1>
```

。这次我们以电子文档最为一个整体载体，继续介绍其他的隐写方法。电子文档，它主要包括电子文书、电子信件、电子报表、电子图纸、纸质文本文档的电子版本等等，是人们电脑办公中必不可少的文件。

实验内容

以文件格式来划分

- 在Word中隐藏数据
  - 利用隐藏文本功能进行隐写
  - word文档的xml转换
- PDF文件中的信息隐藏

实验环境

- 操作机：Windows XP
  - 实验工具：
    - Word 2003 或者WPS
    - wbStego4open
    - 7z等压缩包工具

下面进行实验 在Word文档中隐藏数据

第一部分 在Word文档中隐藏数据

微软的Word一直是文字处理软件中的佼佼者。微软的Word、Excel、PowerPoint提供了许多在文档中隐藏数据的方法，包括批注、个人信息、水印、不可见内容、隐藏文字和定制的XML数据。最简单，也是最奇妙的，也就是这里将提到的隐藏文本功能。

利用隐藏文本功能进行隐写

我这里使用的是WPS文字这个工具，当然方法使用Word2003 或者其他版本也是一样的。

> - 实验：

```
- 在实验机中找到隐写术目录，打开电子文档隐写，打开flag.doc
- 在菜单栏中选择，并单击File（文件）->Tool（工具）->Option（选项）
- 找到 隐藏文字 功能，选择这个功能，点击保存
- 最终flag{doc_stego_is_ez}
```

首先打开，flag.doc

打开flag.doc，能看到的文字内容只有`Flag in here。`,我们就可以猜测，flag是被隐藏起来了

开启隐藏文字显示功能，查看flag是否被隐写

在菜单栏中，找到文件，移动鼠标到工具一栏，选择选项功能。

在弹出来的菜单栏中，找到隐藏文字功能，选择使其打上对勾。

点击确定，回到文字编辑界面就能看到flag了。

思考

1. 尝试将文本中的 Flag in here。 也隐藏掉。
2. 尝试使用word自带的文档检查器检查是否又文字隐藏

word文档的xml转换

我们可以将word文档转换成xml格式，当然反过来我们也可以将xml转换成word文档，这导致了我们如果重新打包为word文档的过程中，有可能被隐藏进其他数据。

> - 实验：

```
- 在实验机中找到隐写术目录，打开电子文档隐写，打开file.docx
- 看到的内容是 This is not the flag you're looking for.
- 我们可以尝试分离word文档
- 发现，其中包含了一个flag.txt的文件，我们可以直接用7Z，使用zip的方法重新打开file.doc
- 打开flag.txt，最终flag{this_would_be_the_flag_you_are_looking_for}
```

首先，找到文件并打开文件查看

尝试分离文件内容

```
+bash-4.3$ file file.docx
```

```
file.docx: Zip archive data, at least v2.0 to extract
+bash-4.3$ 7z x file.docx -oout
```

7-Zip [64] 9.20 Copyright (c) 1999-2010 Igor Pavlov 2010-11-18
p7zip Version 9.20 (locale=utf8,Utf16=on,HugeFiles=on,8 CPUs)

Processing archive: file.docx

Extracting word/numbering.xml
Extracting word/settings.xml
Extracting word/fontTable.xml
Extracting word/styles.xml
Extracting word/document.xml
Extracting word/_rels/document.xml.rels
Extracting _rels/.rels
Extracting [Content_Types].xml
Extracting flag.txt

Everything is Ok

我们会发现又flag.txt的文件被打包在file.docx中，
直接用7z等压缩包工具打开file.docx

打开，flag.txt文件，就能看到flag了。

思考

1. 思考，如何制作这种隐写呢？
2. 试试能否用binwalk 或者strings等工具查看隐写痕迹。

第二部分 PDF文件中的信息隐藏

PDF隐写中，我们最常用，也是最熟知的工具就是wbStego4open,这是可以把文件隐藏到BMP，TXT,HTM和PDF文件中的工具，当然，这里我们只用他来最为以PDF为载体进行隐写的工具。

PDF隐写

> - 实验：

```
- 在实验机中找到隐写术目录，打开电子文档隐写，找到  stego.pdf文档
- 在工具目录中找到 wbStego4open，使用工具载入文档，
- 根据提示，一步一步完成隐藏信息的提取
- 最终flag{CTF_is_funny}
```

首先找到目标文件
在实验机中找到隐写术目录，打开电子文档隐写，找到 stego.pdf文档

其次，找到工具wbStego4open

在工具目录中找到 wbStego4open，使用工具载入文档，

Step 1 是文件介绍

Step 2 中，我们选择Decode，

Step 3 我们选择目标文件

Step 4 输入加密密码，这里我是空密码，直接跳过

Step 5 为保存文件为 flag.txt

最后打开保存后的文件，flag.txt

最后打开保存后的文件，flag.tx，就能得到flag了。

思考

1. 查阅其他资料，是否还要其他的PDF隐写方式，其原理又是什么？

```
        </div>
```