攻防世界misc 新手练习区 高手进阶区 wp

原创

OceanSec 于 2020-03-20 17:51:27 发布 8928 收藏 2
分类专栏： # CTF

本文链接：https://blog.csdn.net/q20010619/article/details/104995374

CTF 专栏收录该内容
66 篇文章 29 订阅
订阅专栏

misc：

新手练习区

this is flag：

直接get flag

pdf：

将pdf文档转换为word文档，移动图片显示下方隐藏的flag

如来十三章：

与佛论禅->rot13->base64

坚持60秒：

下载文件使用反编译工具xjad进行反编译，打开文件夹使用vscode打开PlaneGameFrame.java文件，找到flag，将内容base64进行解码得到真正的flag。

give your flag

使用stegslove打开文件使用flame模式发现残缺二维码使用ps补全
菜狗截获了一张菜鸡发给菜猫的动态图，却发现另有玄机
图片: https://uploader.shimo.im/f/wps4BdwghDUr9SxA.png图片: https://uploader.shimo.im/f/eGBFIRLoY5sHVKKe.png图片: https://uploader.shimo.im/f/kJ82hxku21Ml4T2X.png

掀桌子

图片: https://uploader.shimo.im/f/w5zLi3gYjvsln3xd.png
ext3

simpleRAR图片: https://uploader.shimo.im/f/hsIMAgQlCYwXvbIX.png

1.使用winrar打开rar文件，发现内含一个png文件，而文件头有误图片: https://uploader.shimo.im/f/XHmG0j18g3Mv0227.png
2.在010将7A改为74，提取出png图片
图片: https://uploader.shimo.im/f/ZWcktW9R4G0s9k5R.png
3.将文件后缀改为gif使用stegsolve查看文件发现隐藏损坏二维码，题目提示为：双图层使用ps打开，发现两个相似图层，分别保存，分别使用stegsolve打开发现两个残缺二维码，使用ps将其拼合并加上定位符号
4.使用QR research扫描
图片: https://uploader.shimo.im/f/A6tKYQbEwrcHbY5z.png
base64stego
使用010editor打开文件发现zip文件为伪加密，修改压缩源文件目录的标记为00打开文件
图片: https://uploader.shimo.im/f/qkWiLPbvLR82Klo8.png图片: https://uploader.shimo.im/f/GTibemTLjlMBqeQN.png
偶数未加密奇数加密
txt文件为base64的加密文件进行解密得到flag
图片: https://uploader.shimo.im/f/bbt28gy1pgwOB0ZC.png
功夫再高也怕菜刀
附件是一个流量包，使用foremost分离出一个有密码的压缩包，压缩包里的文件名为“flag.txt”，所以剩下的就是找解压密码
图片: https://uploader.shimo.im/f/fbJ9EzHM1DwpTg5l.png
在wireshark中图片: https://uploader.shimo.im/f/KtlsiLVst0oQsqOV.png选择第七个tcp流发现有个6666.jpg文件，使用TCP追踪流，复习下面蓝色部分。FFD8开头，FFD9结尾，并在中新建txt文件。在010图片: 中打开txt文件图片: https://uploader.shimo.im/f/AP4vAtMY61Eh8Eup.png图片: https://uploader.shimo.im/f/uxwBUKD3n9kYL8Mt.png
stegano

使用浏览器打开pdf文档，全选另存为txt文档，打开发现
图片: https://uploader.shimo.im/f/YXTlIFhoODQUxMxd.png
可以推测这是一个摩尔斯密码
将A用.替换 将B用-替换
图片: https://uploader.shimo.im/f/aAukq7Xf7pAbiAcJ.png
再放到在线解密工具中，得到flag图片: https://uploader.shimo.im/f/vvPgzvidRkgB82Or.png

高手进阶区

wireshark-1

使用wireshark打开流量包ctrl+f查找flag追踪包
Training-Stegano-1
010editor 直接打开

János-the-Ripper

1. 附件是个压缩包，解压之后得到 misc100
2. 用 010 分析发现是个压缩包，并且里面有 flag.txt
3. 用 foremost 提取压缩包
4. 这里解压要密码，要破解一下，这里用 ARCHPR

图片: https://uploader.shimo.im/f/c5PigT4P31cLmdWE.png

Test-flag-please-ignore
无加密
图片: https://uploader.shimo.im/f/PW8nBKJJVPAEleRG.png
What-is-this
解压文件，是一个没有后缀的文件，放进winhex中审查一下，发现有几个文件名，目测这是一个压缩包，把后缀给为zip后解压，
图片: https://uploader.shimo.im/f/RNgHMrWDSh0AElDW.png
两张图片，正常思路：1，图片拼接 2，盲水印 3，各有一部分flag
先试一下 图片拼接，用stegsolve把两张图片合成一下：
直接提交
图片: https://uploader.shimo.im/f/RsslmJM6UNQ4CEyX.png图片: https://uploader.shimo.im/f/dQRxoUMBTFYwArtF.png
base64÷4
图片: https://uploader.shimo.im/f/YYDJB3X55vEV5bZ4.png
embarrass
放入wireshark搜索即可
图片: https://uploader.shimo.im/f/g2PpuwBB5v0v8qoD.png
神奇的Modbus
flag为sctf{Modbus}
图片: https://uploader.shimo.im/f/6lM8P29k2gQwmc22.png
MISCall（为解决）
miscmisc（搬运）

明文攻击

图片: https://uploader.shimo.im/f/uOUi1TqNDa0L3s1Q.png

【原理】
LSB图片隐写
【目的】
明文攻击 关于LSB图片隐写的解法 word字符隐藏显示 zip加密文件破解
【环境】
windows
【工具】
winhex、Advanced Zip Password Recover 、StegSolve
【步骤】
打开后下载附件buguoruci.png，是一个.png后缀的图片，看到图片二话不说直接梭，拖到HXD里面，直接搜索 flag，用F3查找下一处。
图片: https://uploader.shimo.im/f/uPvnzrOa7J4Ro0jb.png
用winhex分析，我们会看到falg.zip字段，同时也可以看到 50 4B 03 04 的数字，.zip文件头是50 4B 03 04
这么多的zip格式文件，为啥不直接把源文件改成.zip格式那，直接梭，改完后成了一个.zip格式的压缩包，很惊喜，打开压缩包后，有如以下两个包
图片: https://uploader.shimo.im/f/AwlCvn3Ou8QMbXnU.png
打开压缩文件 chadian.zip 。会看到一个加密的flag.zip文件和一个加密的flag.txt文本。。。这时候会想到用爆破软件Advanced Zip Password Recover 暴力破解.zip压缩包，可是暴力破解了半天，没出来密码。。 我们来看buguoruci.zip下的 chayidian.jpg ，如下
图片: https://uploader.shimo.im/f/Cz15GcmMpusmDVHz.png
又来张图片 ，老规矩先放到HXD里看一下 ，同样搜索 flag ，会看到flag.txt 字段，往上扫一眼，惊喜万分又看到了 .zip文件开头 50 4B 03 04 字样，直接把jpg格式改为.zip格式。发现可以解压，得到一个 flag.txt 文件，咦，，，，，刚才解压chayidian.zip文件时，目录下也有一个flag.txt 文件，查看两个文件的CRC32 可知两个文件一样，很明显这是一个明文攻击，又已知是.zip加密，上工具 Advanced Zip Password Recover。
图片: https://uploader.shimo.im/f/hjppDvlCSv4siaGy.png
在这里我跑出密码 z$^58a4w
图片: https://uploader.shimo.im/f/Ue5yhe80XDgSwllj.png
拿着密码将加密文件 flag.zip解压，得到如下几个文件：
图片: https://uploader.shimo.im/f/P38OgL96gEEnyhyE.png
（1）打开whoami.zip文件，发现有个加密文本，需要密码，猜想flag就在里面。
图片: https://uploader.shimo.im/f/Lt47Sx6ZSu0mf1HZ.png
（2）打开world.doc文件，只有简单几个字。
图片: https://uploader.shimo.im/f/T3LdmNW5BIolEZ7S.png
（3）打开 world/media/task/writeup/cn/miscmisc/1.png图片。
图片: https://uploader.shimo.im/f/T3HcUGWJjMEooRlD.png
发现有提示： pass in world. 此时想到密码可能与 此图片还有world.doc文件有关。既然是图片隐写， （1）放到HXD里面分析一下，发现没收获，再用经常使用的工具 StegSolve
打开图片然后试探各种通道，在LSB BGR条件下发现pass，所以这是LSB信息隐写。得到pass：z^ea，去解压文件 发现不行。
（2）根据提示 pass in world 猜想 world.doc 文件里不可能那么简单 可能还会有隐藏文字，百度一下，ctrl+A 全选，右击—字体—取消勾选隐藏。果不其然，发现了隐藏字符。
图片: https://uploader.shimo.im/f/OE9KoLO7tm8UZYRX.png
（3）到此为止，我们从world/media/task/writeup/cn/miscmisc/1.png中得到 pass：z^ea 在world.doc文件中得到隐藏字符串。
（4）出题人真不要脸，最后来了一个脑筋急转弯，谁会想到最后的密码是 pass内容+world里每行字符串的最后一个字符
（5）用密码解压加密文本，在这里插入图片描述
得到flag ：flag{12sad7eaf46a84fe9q4fasf48e6q4f6as4f864q9e48f9q4fa6sf6f48}