

【WP】攻防世界新手Misc writeup

原创

Tiumo 于 2019-07-18 20:52:00 发布 65 收藏

文章标签: [python](#) [linux](#) [信息安全](#) [base64](#) [wireshark](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/y320284/article/details/108646692>

版权

ext3

- 在Linux, 使用root账户挂载linux文件, 打开后使用 `find *|grep flag` 查找到一个flag.txt, 打开后是base64编码, 解码获得flag。

give_you_flag

- gif图片, 使用stegsolve提取帧, 修复二维码的三个定位符。
- 修复定位: https://blog.csdn.net/hk_5788/article/details/50839790

pdf

- 直接pdf编辑器打开, 移开图片, 获得flag

simpleRAR

- 16进制编辑器打开, 发现有有一个图片文件的HEAD_TYPE域类型错误, 更改后提取出图片文件, 查看文件头, 是一张gif, 把两帧提取出来, stegsolve从灰度通道提取出两张破碎的二维码, 拼在一起再修复一下定位点。

坚持60s

- jar包反汇编, jd: <http://www.iitshare.com/wp-content/uploads/2013/07/jd-gui-0.3.6.rar>

gif

- 把黑白图片转换成0和1获得二进制串, 转换成字符串

如来十三掌

- 与佛论禅解码, 再rot13。

掀桌子

- 减去128, 按十六进制转字符串。

功夫再高也怕菜刀

- foremost分离文件, 得到一个加密的压缩包, wireshark打开下载的文件, 搜索flag关键字, 在某一个包中找到6666.jpg, 追踪TCP流, 获得jpg的十六进制码, 使用十六进制编辑器保存为jpg获得压缩包的密码。

stegano

- 直接福昕编辑器打开, 删除水印后, 在上方超出可视范围的地方有一串AB字符, 加空格, 把A替换成., 把B替换成-, 用莫尔斯码翻译。
- 一开始直接把翻译出来的东西当flag提交了, 后来发现真正的flag在最后面一截。

base64stegano

- 一个伪加密的zip，从ctf-wiki上可以找到解决办法，得到txt是一堆base64编码，这里是base64隐写，参考这篇：<https://www.tr0y.wang/2017/06/14/Base64steg/index.html>