2017年陕西省网络空间安全技术大赛——一维码——Writeup

转载

baikeng3674 于 2017-04-21 09:07:00 发布 59 收藏
原文链接：http://www.cnblogs.com/WangAoBo/p/6741826.html

<!doctype html>

2017年陕西省网络空间安全技术大赛——一维码——Writeup

先判断下载的文件**flag.png**确实是png格式的图片后（binwalk， file命令均可判断），很自然的一个想法是先扫描这个条形码，得到的结果如下图：

发现**keyword:hydan**,百度了一下hydan，可以发现这是一种**elf隐写格式**

再根据题目的提示，发现是LSB隐写

> 参考资料：
>
> http://www.2cto.com/article/201502/377052.html
>
> http://www.bugbank.cn/pwn/detail/57a4be7196c5ece11fccbed8.html

于是用图片隐写神器**stegsolve**打开图片，根据LSB选择*Analyse -> Data Extract* ,选择RGB的最低位，Preview结果如下：

（这个题我在windows下preview没有结果，在ubuntu下才发现elf文件的标志，不知道是不是姿势有问题）

看到了elf文件标志，再结合**hydan**的提示，这个题的思路就很明显了，先*save bin*保存这个elf

再安装**hydan**,根据hydan的使用教程即可得到flag

```
wust_ao@ubuntu:~/hydan$ ./hydan-decode 0.so
Password:
Segmentation fault (core dumped)
wust_ao@ubuntu:~/hydan$ ./hydan-decode 0.so
Password:
flag{good4y0u}
```


> hydan安装和使用
>
> http://www.cnblogs.com/pcat/p/6716502.html

hydan只支持32位系统，而我在32位deepin上又一直没安装成功，最后一张图就直接拿了别人博客里的

转载于:https://www.cnblogs.com/WangAoBo/p/6741826.html