XCTF-REVERSE-指南

原创

ChengKaoAO 于 2017-10-17 16:02:35 发布 425 收藏

分类专栏： CTF CTF 文章标签： XCTF Reverse

本文链接：https://blog.csdn.net/ZmeiXuan/article/details/78261562

CTF 同时被 2 个专栏收录

5 篇文章 0 订阅

订阅专栏

CTF

11 篇文章 0 订阅

订阅专栏

XCTF-REVERSE-指南

首先介绍一下 linux和windows下一些常用命令和工具 **ELF反调试初探**

[http://www.freebuf.com/sectool/83509.html]

1. readelf
    1. 该命令是Linux下的分析ELF文件的命令，这个命令在分析ELF文件格式时非常有用
    2. 命令格式：readelf elf文件名
2. strings
    1. 可以打印出文件中所有列出的可打印字符串
    2. 格式：strings 文件名
3. file
    1. 用于检测文件类型
    2. 格式：file 文件名
4. gdb
    1. 用于调试linux下程序
    2. 命令参数太多，最简单：gdb 文件名
5. objdump
    1. 用于输出可执行文件的汇编代码
    2. 格式：objdump -D 可执行文件名 > out.asm