

[网络安全自学篇] 六十二.PE文件逆向之PE文件解析、PE编辑工具使用和PE结构修改（三）

原创

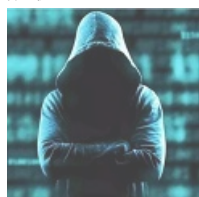
Eastmount 于 2020-03-25 21:11:33 发布 9024 收藏 40

分类专栏: [网络安全自学篇](#)

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/Eastmount/article/details/105080804>

版权



[网络安全自学篇](#) 专栏收录该内容

107 篇文章 2590 订阅 ¥19.90 ¥99.00

订阅专栏

本系列虽然叫“网络安全自学篇”, 但由于系统安全、软件安全与网络安全息息相关, 作者同样会分享一些系统安全案例及基础工具用法, 也是记录自己的成长史, 希望大家喜欢, 一起进步。前文分享了数字签名, 采用Signtool工具对EXE文件进行签名, 接着利用Asn1View、PEVie、010Editor等工具进行数据提取和分析。本文将详细介绍PE文件格式, 熟悉各种PE编辑查看工具, 针对目标EXE程序新增对话框等, 这也为后续PE病毒和恶意代码的攻防打下坚实基础。希望这篇基础文章对您有所帮助~

使用工具:

- PEView、Stud_PE
 - UltraEdit、010Editor
 - Ollydbg、x64dbg
 - exeScope
- 待分析程序:
- hello-2.5.exe

文章目录

一.PE文件基础

二.PE文件格式解析

1.010Editor解析PE文件

2.Ollydbg动态调试程序

3.仅弹出第二个窗口

三.熟悉并分析PE文件的引出表

1.PEView和Stud_PE查看文件

2.寻找函数MessageBoxA的地址

四.PE文件