CTF-REVERSE练习之病毒分析

原创

ChuMeng1999 于 2021-11-29 17:04:24 发布 2613 收藏 1

分类专栏： CTF特训营：技术详解、解题方法与竞赛技巧 # CTF之Reverse 文章标签： windows 安全 web安全

本文链接：https://blog.csdn.net/ChuMeng1999/article/details/121613878

目录

预备知识

相关实验

本实验要求您已经认真学习和完成了《CTF REVERSE练习之逆向初探》。

7Zip

7-Zip是一款开源软件。我们可以在任何一台计算机上使用7-Zip，包括用在商业用途的计算机。7-Zip适用于Windows 7/Vista/XP/2008/2003/2000/NT/ME/98。并且有面向Mac OS X、Linux、Unix平台的命令行版本。
7zip使用起来十分方便，通过添加的右键菜单，可以尝试对任意文件进行解压缩操作。7zip支持的文件格式十分丰富，其中压缩包括：7z，XZ，BZIP2，GZIP，TAR，ZIP and WIM等格式，解压缩包括：
ARJ，CAB，CHM，CPIO，CramFS，DEB，DMG，FAT，HFS，ISO，LZH，LZMA，MBR，MSI，NSIS，NTFS，RAR，RPM，SquashFS，UDF，VHD，WIM，XAR，Z等格式。
在一些CTF逆向分析的题目中，我们可以尝试使用7zip对其进行解压缩操作，可能就会有意想不到的效果，可以大大加快我们的分析过程。

在线沙箱

网上有许多公开的在线沙箱，使用这些沙箱提供的服务，我们可以方便的观察一个程序的详细行为报告，进而判断一个程序大致的内部逻辑。
在线沙箱通常用于大致判定一个程序的行为是否安全，在逆向分析中，我们可以通过提交一个文件给沙箱程序来判断程序内部的大致逻辑，通过对沙箱报告的分析，有时候可以有效加快我们的逆向分析进程。
常见的在线沙箱包括但不限于：
VirusTotal：https://www.virustotal.com/gui/
VirSCAN：https://virscan.org/
微步云沙箱：https://s.threatbook.cn/
Joe Sandbox Cloud Basic：https://www.joesandbox.com/#windows
布谷鸟沙盒：https://sandbox.pikker.ee/
OPSWAT MetaDefender：https://metadefender.opswat.com/?lang=en

实验目的

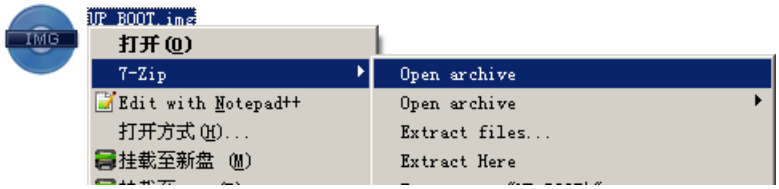
1）了解CTF比赛中逆向分析的目的。
2）掌握7zip工具的使用。
3）掌握在线沙箱的基本使用方法。

实验环境

服务器：Windows XP，IP地址：随机分配
辅助工具：7Zip，Ollydbg

实验步骤一

题目描述：
某日，一小学生弄了个U盘到打印店打印文件，U盘往计算机上一插，发现机子死机了，高明的打印店老板为了防止此类事件，特意设置了霸王键，可一键备份，随后老板把U盘备份了交给小王，小王想要知道U盘里到底被感染了什么你能帮帮他吗？
主机C:\Reverse\8目录下提供了这个UP_BOOT.img文件，请对该文件进行逆向分析，找到题目过关的Flag。
考察意图：
主要考察对病毒程序的逆向分析操作，以及对在线分析沙箱的一些基本使用方法。通过一些常用的工具如7zip以及在线分析沙箱提供的报告来加速我们的分析进程。
病毒特征分析：
病毒程序是一个IMG文件，这种文件不是可执行文件，因此无法直接运行。我们使用7zip打开这个文件，看看里面是不是附加了什么东西。选中UP_BOOT.img文件后，单击鼠标右键，在弹出的右键菜单中选择“7Zip”——“Open archive”，如图所示：



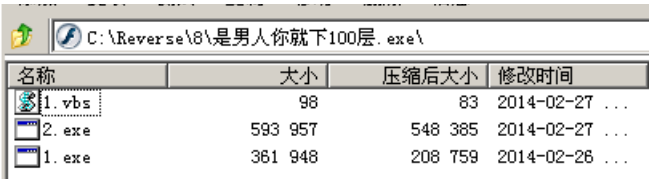
打开文件后我们发现里面有两个文件，将其解压出来：

我们发现一个autorun.inf文件，文件内容为：

你真厉害都到这了，看看这个游戏你肯定会喜欢的，但是据说这个游戏是被加了后门的，找到后门操作的文件的内容，取文件内容的16位md5值作为key！祝你好运……

提示游戏“是男人你就下100层.exe”被加了后门，双击运行程序，发现弹出了一个游戏，游戏还是很难玩的，如下图所示：

再次尝试使用7Zip打开“是男人你就下100层.exe”这个文件，我们发现里面有三个文件，分别为1.vbs、1.exe、2.exe，如下图所示：



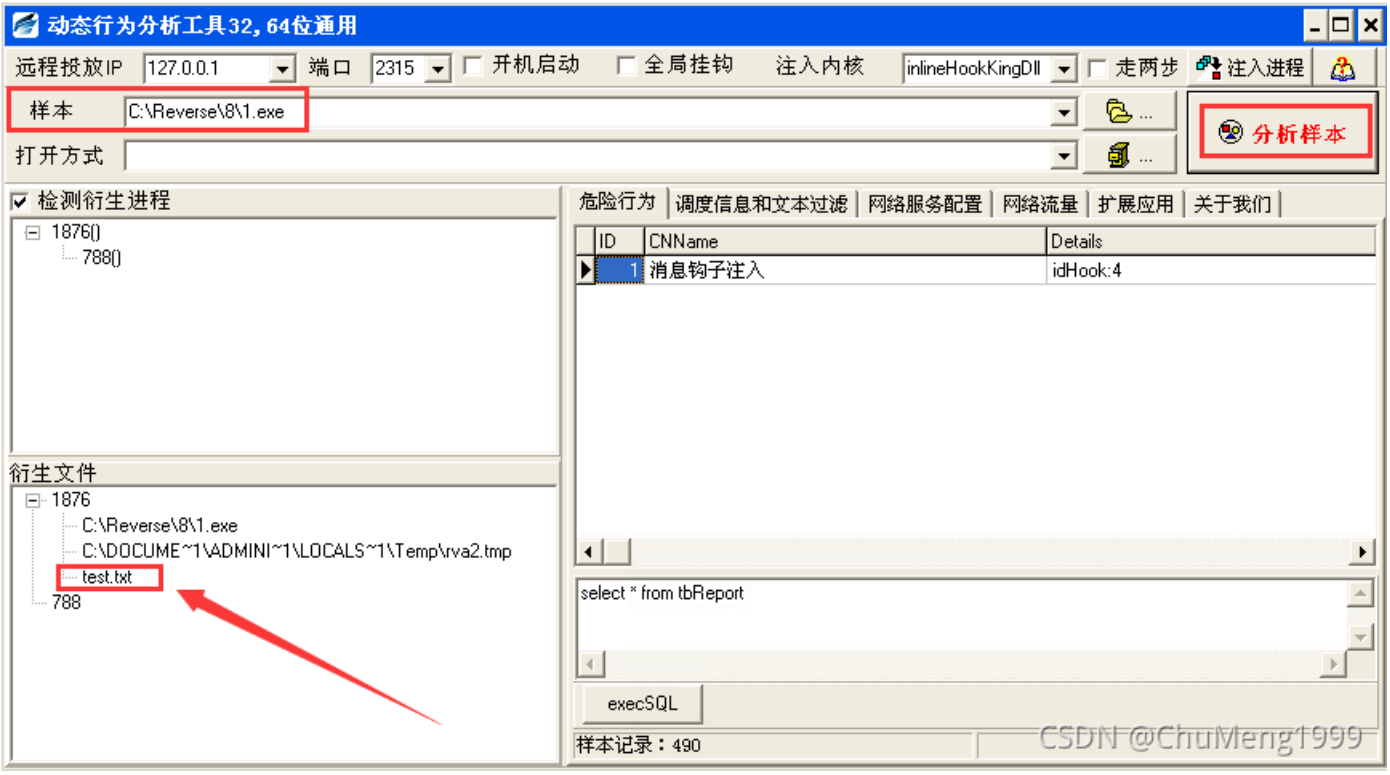
实验步骤二

使用沙箱分析病毒程序：

运行释放的1.exe文件，除了一个一闪而过的黑框之外，我们看不到任何其他行为。现在我们需要使用在线沙箱分析来加快我们的分析流程，看看1.exe都有哪些行为特征。

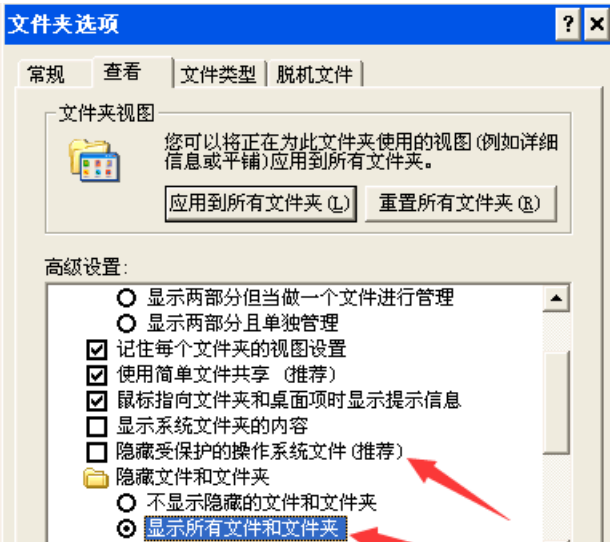
浏览器访问http://tools.hetianlab.com/tools/ActionScope.rar下载动态行为分析工具，解压并运行install.exe。

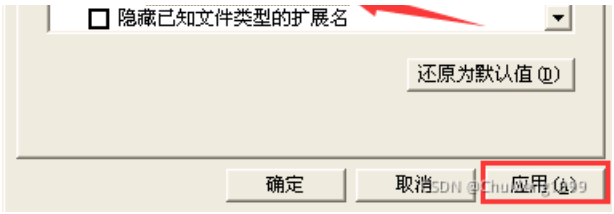
样本选择1.exe，点击【分析样本】：



可以看到1.exe释放了一个test.txt文件，而且把test.txt的文件属性设置为系统和隐藏，因此我们看不到文件夹里面多了一个txt文件。

回到目录C:\Reverse\8，打开【工具】→【文件夹选项】→【查看】，进行下面的设置：





可以看到test.txt文件了。
现在使用记事本打开这个test.txt文件，文件内容为
（WdubQ4IGEzAG54NfATJTNhl4TLIvPvENyTLLWb3YCNBeK5wad5XCgrSQNOih1F），如图所示：

实验步骤三

计算Flag信息：
这就是我们所要找的文件，使用MD5计算工具，算出这个字符串的16位MD5值，为a4620ba0298017b2，这就是我们要找的flag了，如图所示：