恶意代码分析与防治技术实验报告

Lab2

网络空间安全学院 信息安全专业

2112492 刘修铭 1063

一、实验目的

1. 配置病毒分析虚拟机，为后续实验奠定基础；
2. 安装病毒分析工具，了解并熟悉其功能。

二、实验原理

（一）Vmware

Vmware是一款虚拟机集成软件，能够将光盘映像加载为虚拟机，并实现相关功能。

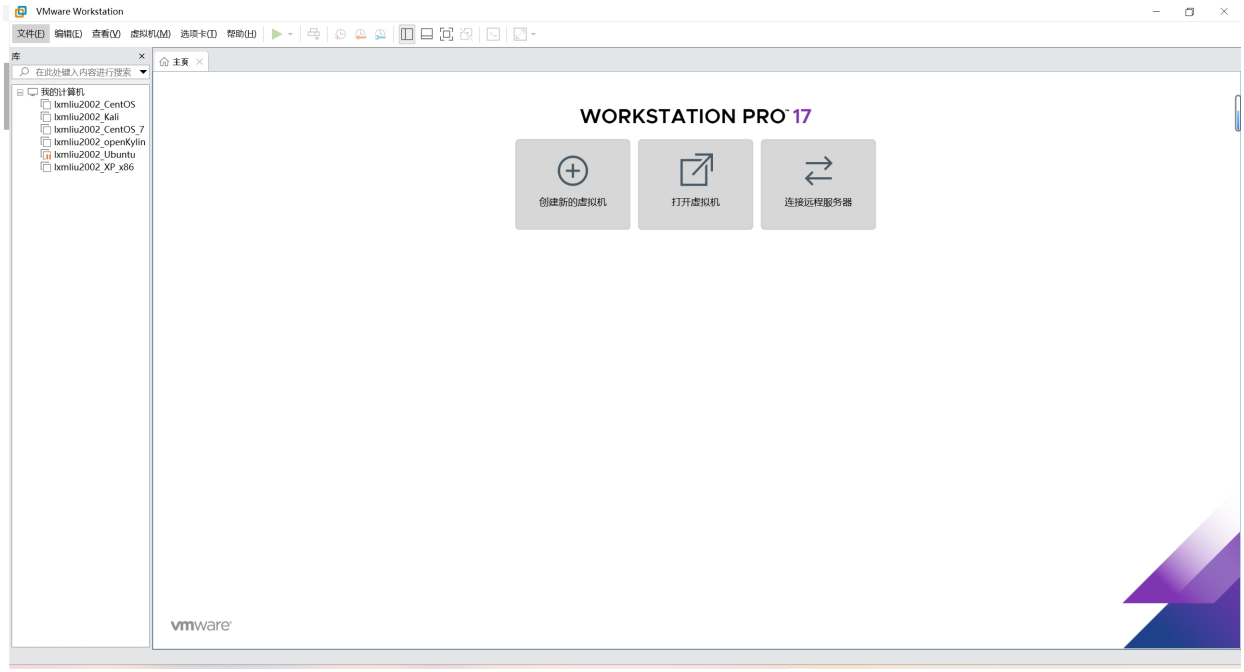
（二）实验环境

Windows11

三、实验过程

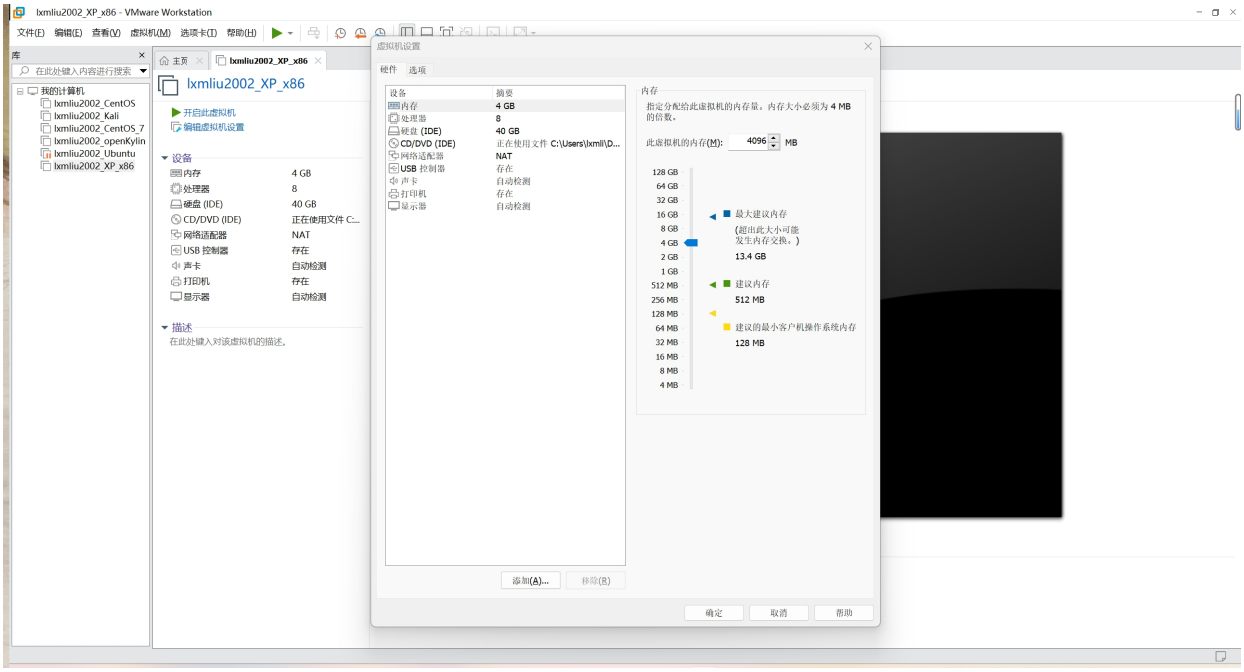
（一）安装Vmware

借助https://blog.csdn.net/leah126/article/details/131450225教程，我完成了VMware Workstation Pro的安装，版本为17.0.0。



（二）安装XP操作系统

从网络上下载好XP光盘映像，导入VMware虚拟机中，完成好相关配置设置，即可实现XP操作系统的安装。

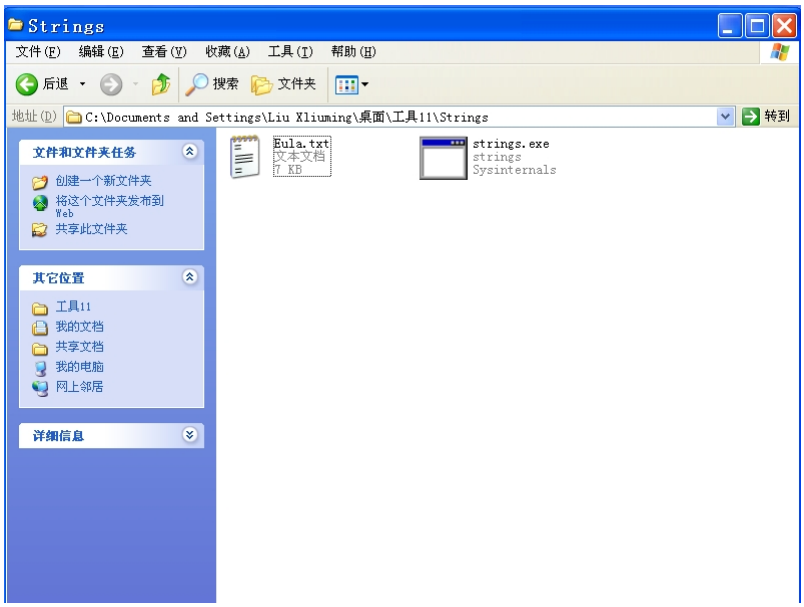


（三）安装静态分析工具

打开已经创建好的XP虚拟机，完成安装操作。已经给定分析工具的安装包，直接解压即可安装，或是按照安装引导一步一步安装即可，文中不过多赘述，仅展示根目录的文件内容或工具的运行截图。

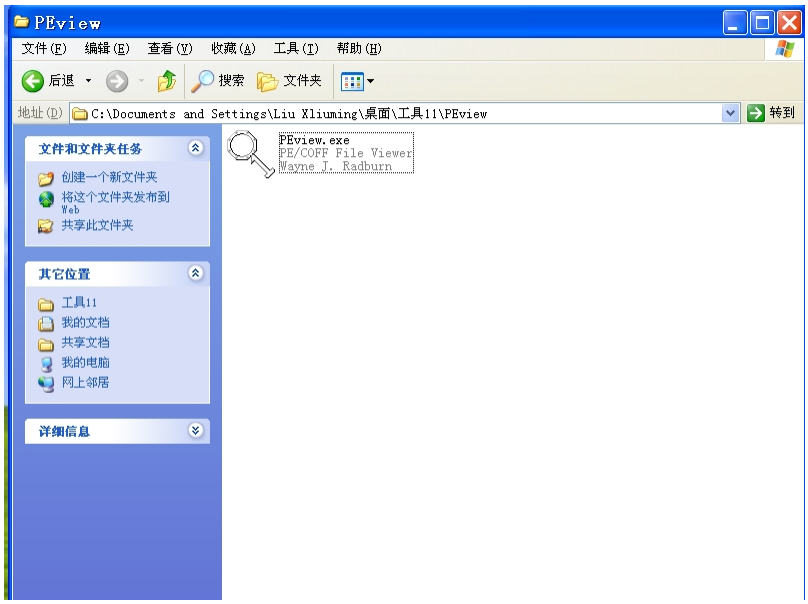
1. string.exe

   扫描传递给它的文件中的UNICODE字符串，常被用来查找可执行文件、动态链接库或静态链接库中的特定字符串。



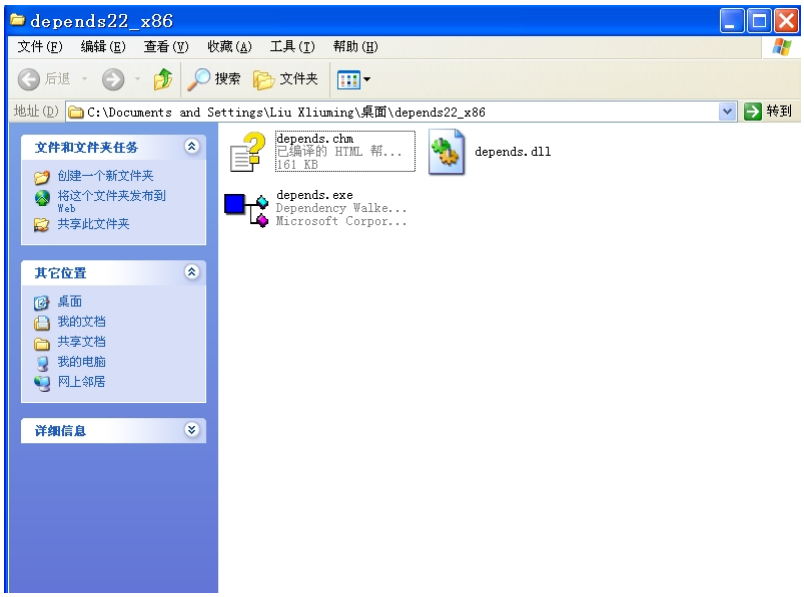
2. PEView

是一款使用C/C++开发实现的命令行交互式Windows PE文件解析器，可以快速轻松地查看32位Portable Executable (PE)和Component Object File Format (COFF)文件的结构和内容，可以显示EXE、DLL、OBJ、LIB、DBG和其他文件类型中的头部、区段、目录、导入表、导出表和资源信息，内置有各种结构查询转换等功能。



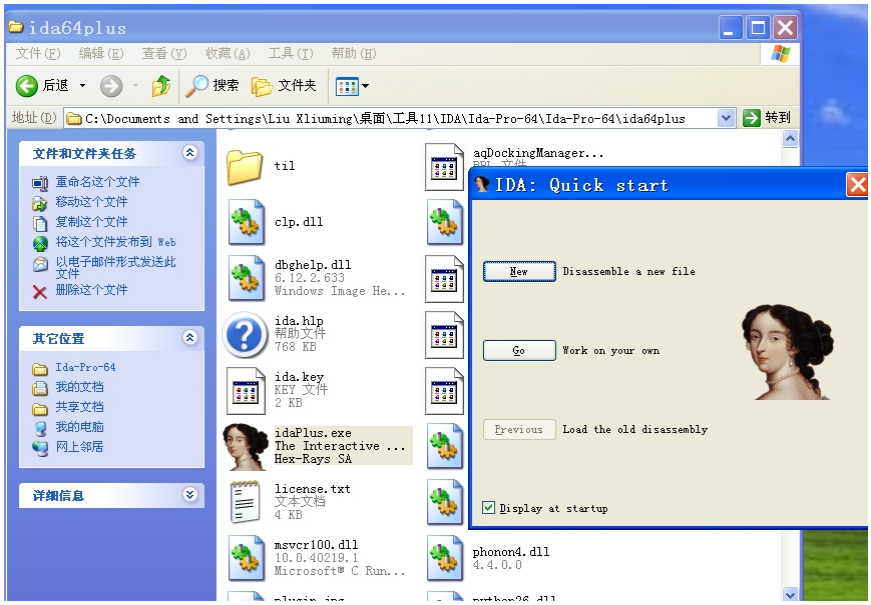
3. dependency walker

它可以扫描任何32位或64位Windows模块（EXE，DLL，OCX，SYS等），并建立所有相关模块的分层树形图。对于每个找到的模块，它列出了该模块导出的所有函数，以及哪些函数实际上被其他模块调用，对于排除加载和执行模块故障错误非常有用，可以处理所有类型的模块依赖关系，包括隐式、显式（动态/运行时）、转发、延迟加载和注入，此外，它还可以显示最小的必需文件集，以及每个文件的详细信息，包括文件的完整路径、基地址、版本号、机器类型、调试信息等。在病毒分析中，Dependency Walker可以帮助理解恶意软件的行为和功能。



4. IDA

   是一款交互式反汇编工具，具有交互式、可编程、可扩展、多处理器等特点，可以通过Windows或Linux、MacOS平台来分析程序，支持数十种CPU指令集其中包括Intel x86、x64、MIPS、PowerPC、ARM、Z80、68000、c8051等等。在病毒分析中，IDA Pro被广泛应用于病毒木马等样本的解包分析工作。它可以解析32/64位可执行程序的绝大部分通用参数，并内置有各种结构查询转换等功能。

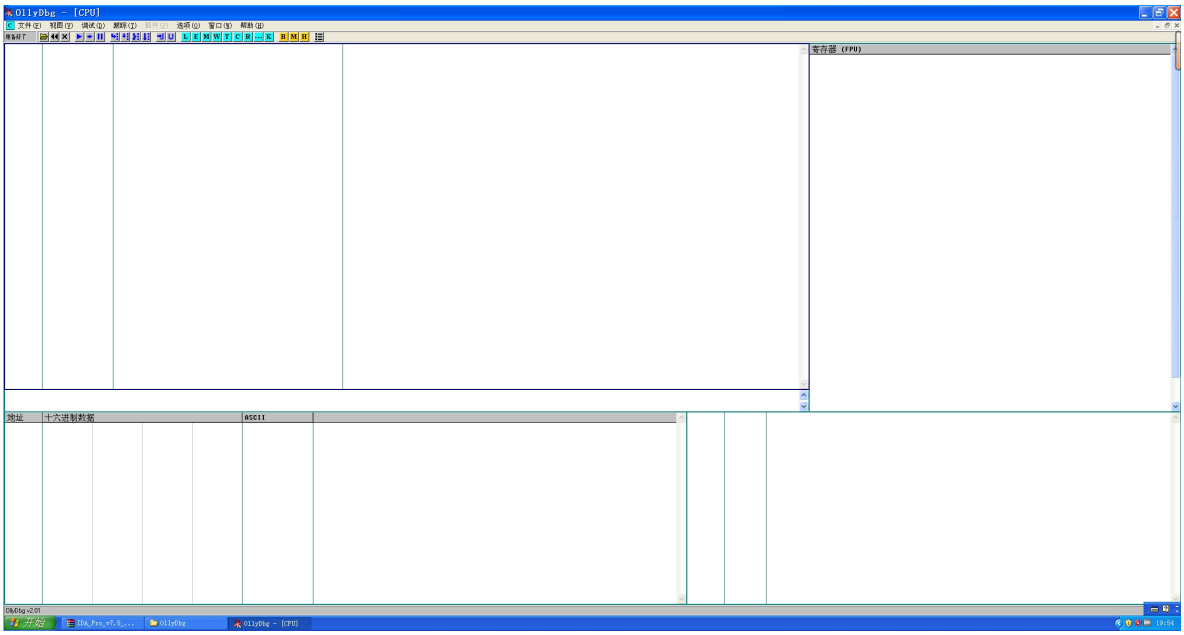


（四）安装动态分析工具

打开已经创建好的XP虚拟机，完成安装操作。已经给定分析工具的安装包，直接解压即可安装，或是按照安装引导一步一步安装即可，文中不过多赘述，仅展示根目录的文件内容或工具的运行截图。

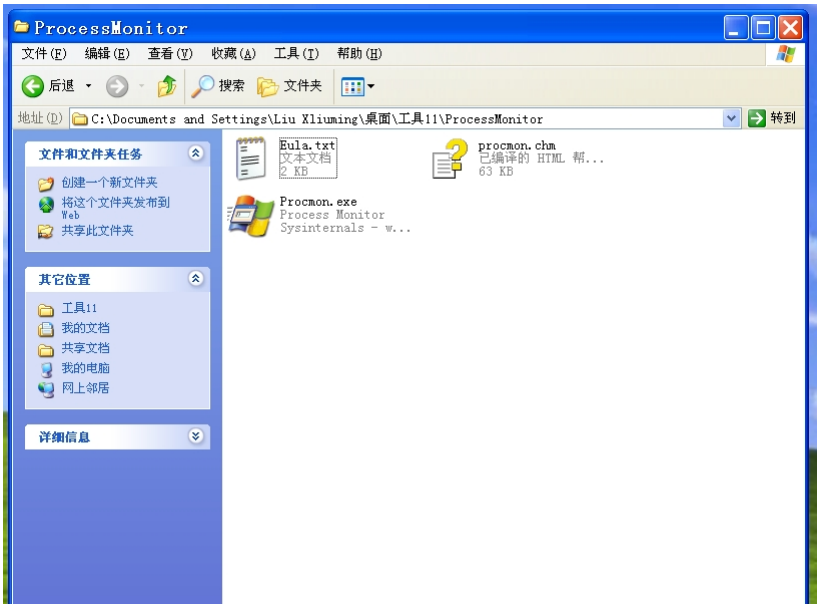
1. OllyDBG

   OllyDbg是一款新的动态追踪工具，Ring 3级调试器，支持插件扩展功能，OllyDbg的界面包括反汇编窗口、寄存器窗口、信息窗口、数据窗口、堆栈窗口。在病毒分析中，OllyDbg被广泛应用于病毒木马等样本的解包分析工作。它可以解析32/64位可执行程序的绝大部分通用参数，并内置有各种结构查询转换等功能。



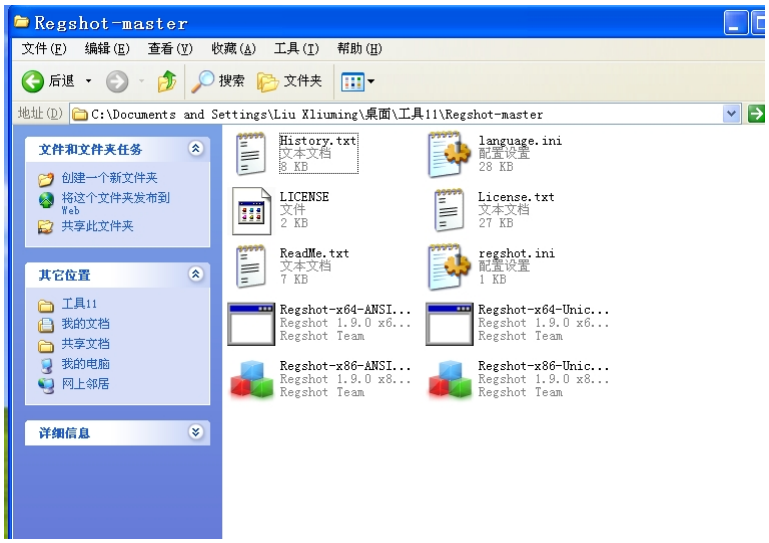
2. Process Monitor

是一个高级的监控工具，用于显示Windows的实时文件系统、注册表和进程/线程活动。它结合了两个传统的Sysinternals实用程序（Filemon和Regmon）的功能，并添加了一系列增强功能，包括丰富且非破坏性的过滤、全面的事件属性（如会话ID和用户名）、可靠的进程信息、每个操作的完整线程堆栈（带有集成符号支持）、同时记录到文件等。在恶意代码分析中，Process Monitor常常被用作查找可执行文件、动态链接库或静态链接库中的特定字符串等。



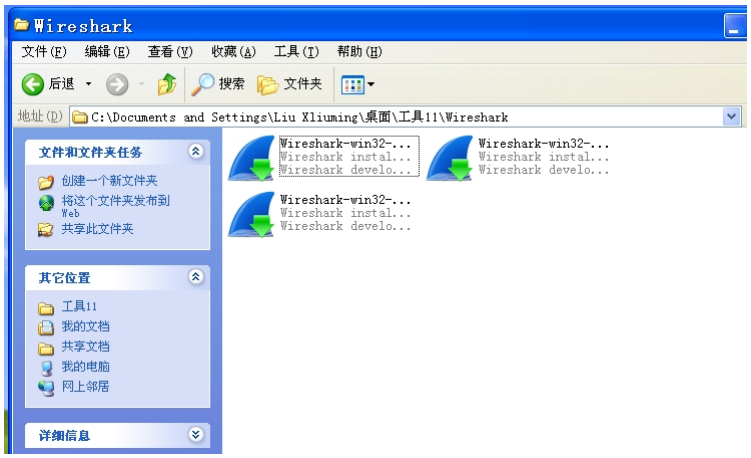
3. Process Explorer

Windows系统和应用程序监视工具，结合了文件监视和注册表监视两个工具的功能，还增加了多项重要的增强功能，此工具支持64位Windows系统。可以显示Windows的实时文件系统、注册表和进程/线程活动，所有相关模块的分层树形图。对于每个找到的模块，它列出了该模块导出的所有函数，以及哪些函数实际上被其他模块调用。对于排除加载和执行模块故障错误非常有用。它可以处理所有类型的模块依赖关系，包括隐式、显式（动态/运行时）、转发、延迟加载和注入。此外，它还可以显示最小的必需文件集，以及每个文件的详细信息，包括文件的完整路径、基地址、版本号、机器类型、调试信息等。



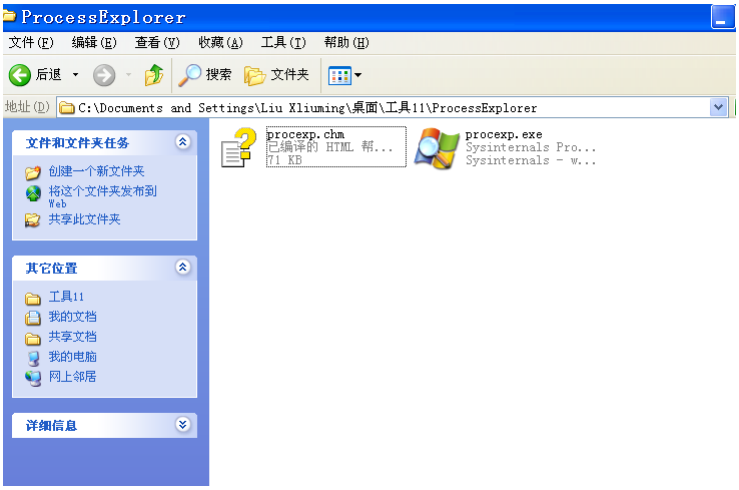
4. RegShot

是一款用于动态恶意软件分析的工具，它可以在执行某个操作之前和之后对注册表和文件系统进行快照，然后比较这两个快照，从而找出在执行该操作期间发生的所有注册表和文件系统的更改。



5. WireShark

Wireshark是一款网络协议分析器，也被称为数据包嗅探器。它可以捕获网络连接中的数据包，并自动解析数据包，为用户显示数据包的详细信息，供用户对数据包进行分析。它可以运行在Windows和Linux操作系统上。



四、实验结论及心得

1. 对于虚拟机有了一个初步的认识。
2. 创建了自己的病毒分析环境，为以后实验打下基础。
3. 了解并安装了若干静态与动态的分析工具，为以后分析病毒提供了工具包。