南開大學

恶意代码分析与防治技术课程实验报告

实验二

学院：网络空间安全学院
专业：信息安全
学号：2113997
姓名：齐明杰
班级：信安2班

1 实验目的

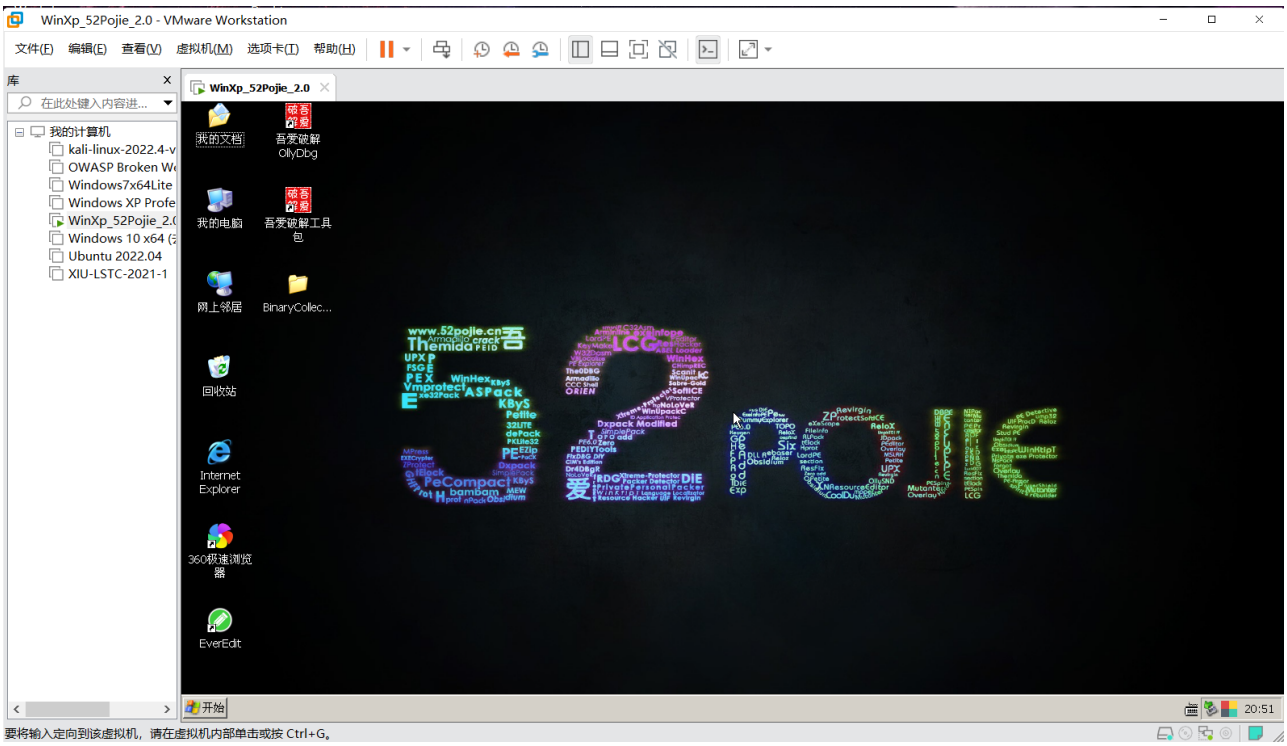
配置病毒分析VMware 虚拟机，使用Windows XP操作系统，并在虚拟机中安装静态分析工具和动态分析工具。通过这个实验，我们将学会如何设置一个合适的分析环境，以便对恶意代码进行研究和分析。

2 实验原理

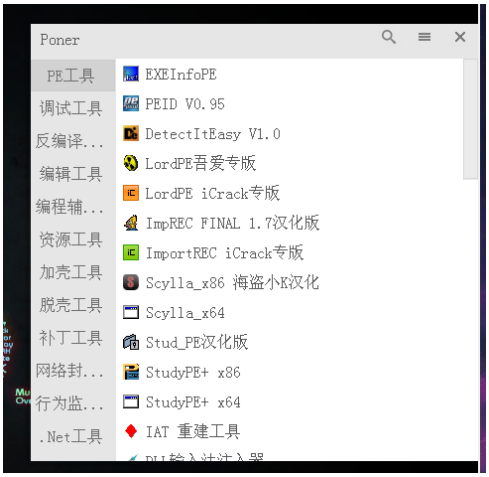
在这个实验中，我们使用了虚拟化软件（如VMware）来创建一个虚拟机。虚拟机是一个隔离的操作系统环境，可以在其中运行另一个操作系统（如Windows XP）。这使得我们可以在同一物理计算机上同时运行多个独立的操作系统实例，以便进行安全的恶意代码分析。

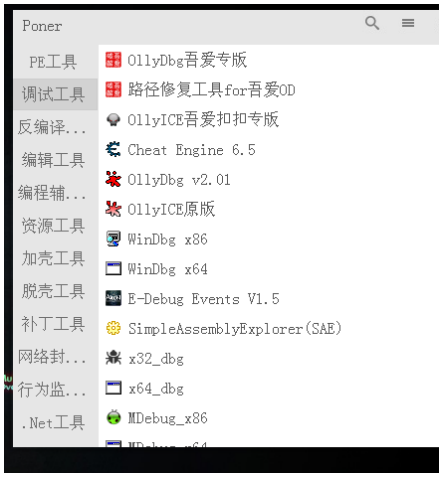
3 实验过程

我在**吾爱破解论坛**上下载了其提供的专门用于逆向分析用途的**XP虚拟机**(下载地址: https://www.52pojie.cn/thread-661779-1-1.html)，如下图所示：



其中**工具包齐全**，`ollydbg`，`IDA PRO`等必要工具均已下载，如下图所示：





因此我***不再重新安装***已有的工具，下面将分述介绍此虚拟机**工具包**含有的**各项工具及其功能**:

3.1 PE工具

- **PEview**

PEview 是一个用于查看和分析可执行文件 (PE 文件) 的工具。它提供了有关文件的各种信息，如文件头、节表、导入和导出函数等

- **EXEInfoPE**

EXEInfoPE 用于识别未知可执行文件的类型。它可以检测文件的编译器、包装器、是否加壳等信息。

- **PEID V0.95**

PEiD 用于检测可执行文件的包装器（加壳器）。它可以帮助我们确定一个文件是否经过加壳，以及可能的加壳器类型。

- **LordPE吾爱专版**

LordPE 是一个强大的 PE 文件编辑工具，它允许我们查看和编辑 PE 文件的各个部分，包括节表、导入表、导出表等。

- **ImpoREC FINAL 1.7**

ImpoREC 用于修复被加壳的可执行文件的导入表，以便进行静态和动态分析。

- **StudyPE+ x86**

StudyPE+ 是一个用于学习 PE 文件结构的工具，它可以帮助我们深入了解 PE 文件的各个组成部分。

- **DetectItEasy V1.0**

DetectItEasy 用于检测可执行文件的编译器和加壳器信息，帮助我们确定文件的特征和类型。

3.2 调试工具

- **OllyDbg吾爱专版**

OllyDbg 是一个流行的动态分析工具，用于分析可执行文件的运行时行为。吾爱专版包含一些自定义插件和特性，使其更适用于逆向工程。

- **Cheat Engine 6.5**

Cheat Engine 是一个内存编辑和调试工具，通常用于游戏修改，但也可以用于分析可执行文件的运行时数据。

- **OllyDbg V2.01**

OllyDbg 的另一个版本，提供更多的功能和改进。

- **WinDbg x86 & x64**

WinDbg 是微软的调试器，用于 Windows 操作系统内核和应用程序的调试。x86 和 x64 版本适用于不同的位数的应用程序。

- **E-Debug Events V1.5**

E-Debug Events 是一个用于监视和分析 Windows 事件的工具，有助于跟踪系统和应用程序的行为。

- **x64dbg & x32dbg**

x64dbg 和 x32dbg 是开源的调试器，支持 32 位和 64 位应用程序的动态分析。

3.3 反编译工具

- **IDA Pro v6.8 x86 & x64**

IDA Pro 是一款强大的静态分析工具，用于反汇编和反编译可执行文件，以便查看和理解其代码结构和逻辑。

- **DarkDe4**

DarkDe4 是一个专用的反编译工具，用于处理特定类型的文件或任务。

- **DelphiDecompiler**

DelphiDecompiler 用于反编译 Delphi 编写的应用程序，以还原其源代码。

3.4 资源工具

- **ResourceHacker**

ResourceHacker 用于查看、编辑和提取可执行文件中的资源，如图标、字符串、位图等。

- **ResEdit x86 & x64**

ResEdit 是另一个资源编辑工具，用于修改 PE 文件中的资源数据。

- **ResScope 1.96**

ResScope 是一个资源查看器，用于浏览和分析 PE 文件的资源内容。

3.5 加壳工具

- **ACProtect2.1.1**

ACProtect 是一个加壳工具，用于保护可执行文件免受逆向工程的威胁。

- **ASPack v2.1.2**

ASPack 是一个可执行文件压缩和加壳工具，可以减小文件大小并提高安全性。

- **ASProtect**

ASProtect 是另一个加壳工具，用于保护应用程序的代码免受未经授权的访问。

- **Enigma Protector v3.8**

Enigma Protector 是一个功能强大的可执行文件保护工具，用于防止恶意破解。

- **Obsidium v1.3.6.4**

Obsidium 是一个软件保护系统，用于加固应用程序的安全性。

- **FSG 2.0**

FSG 是一个可执行文件加壳工具，用于保护程序的代码。

- **Themida v2.3.7 x64 & x86**

Themida 是一个高级的软件保护工具，用于防止逆向工程和破解。

- **UPX Shell 3.4**

UPX Shell 是 UPX (Ultimate Packer for eXecutables) 的图形界面版本，用于压缩和加壳可执行文件。

- **VMProtect v2.08**

VMProtect 是一个虚拟化保护工具，用于保护应用程序的代码免受逆向分析。

- **WinLicense v2.3.7**

WinLicense 是一个软件保护工具，用于加密和保护可执行文件。

3.6 脱壳工具

- **ASPack UnPacker**

ASPack UnPacker 用于脱去使用 ASPack 加壳的可执行文件的保护。

- **ASProtect Unpacker**

ASProtect Unpacker 用于脱去使用 ASProtect 加壳的可执行文件的保护。

- **UnFSG 2.0**

UnFSG 用于解除使用 FSG 加壳的文件的保护。

- **UPX Unpacker**

UPX Unpacker 用于解压使用 UPX 压缩的可执行文件。

3.7 补丁工具

- **PYG-内存补丁制作工具**

PYG 是一个内存补丁制作工具，用于修改运行时内存中的程序数据。

- **DUP v2.26 汉化版**

DUP 是一个用于制作和应用补丁的工具，允许我们修改可执行文件的行为。

- **樱花补丁制作工具 正式版 2.74**

樱花补丁制作工具是一个用于创建自定义补丁的工具。

- **KeyMake V2.0 修改版**

KeyMake 用于生成许可证密钥和序列号，通常用于破解软件保护。

3.8 网络封包工具

- **Fiddler**

Fiddler 是一个用于拦截和分析网络流量的工具，可用于查看应用程序与服务器之间的通信。

- **Wireshark 便携版**

Wireshark 是一款流行的网络协议分析工具，用于捕获和分析网络数据包。

- **HTTPDebugger**

HTTPDebugger 用于监视和分析 HTTP 请求和响应，有助于理解应用程序的网络行为。

3.9 .Net工具

- **de4dot x64 & x86**

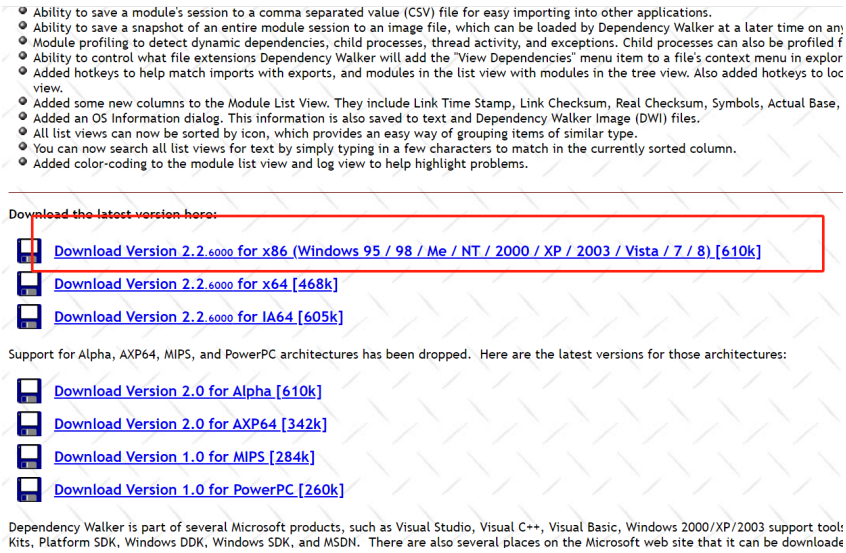
de4dot 是一个用于去除 .NET 反编译保护的工具，可以还原被混淆的 .NET 程序。

- **dnSpy x64 & x86**

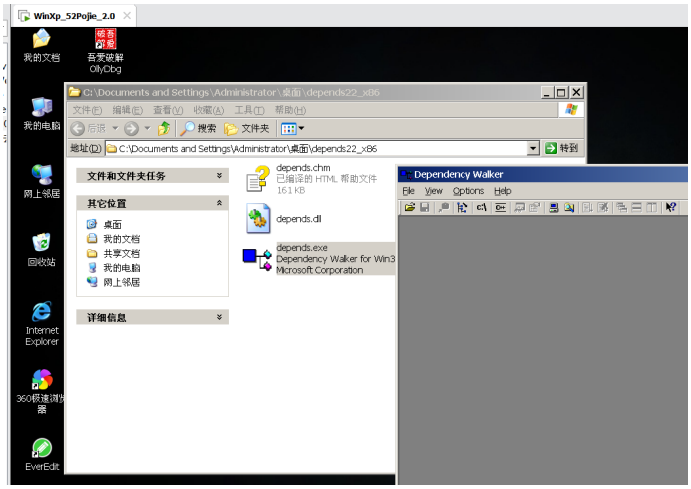
dnSpy 是一个 .NET 程序的反编译和调试工具，用于查看和编辑 .NET 程序的源代码和 IL 代码。

另外，由于虚拟机没有`string.exe`和`dependency walker`，现进行安装：

从官网下载`dependency walker`：



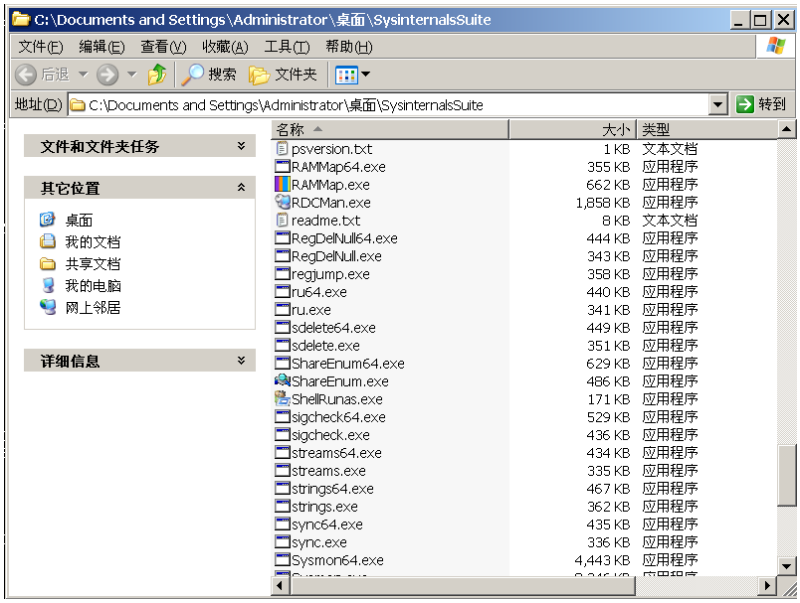
下载后移到虚拟机中解压即可使用，如下图：



Dependency Walker 是一个用于分析可执行文件的依赖关系的工具。它可以显示一个可执行文件所依赖的动态链接库（DLL）和其他模块，以及它们之间的关系。以下是 Dependency Walker 的主要用途：

1. **查找依赖项**: Dependency Walker 可以列出一个可执行文件所依赖的所有 DLL 文件。这对于理解程序的运行时行为和资源需求非常重要。
2. **检测缺失的依赖项**: 工具可以标识出程序缺失的依赖项，这有助于解决程序无法正常运行的问题。
3. **查看导出函数**: 我们可以查看 DLL 文件中导出的函数列表，这有助于理解程序如何与外部模块进行交互。
4. **检查依赖项的完整性**: Dependency Walker 还可以检查 DLL 文件的完整性，以确保它们没有被篡改或损坏。
5. **分析依赖项路径**: 工具可以显示每个依赖项的文件路径，帮助我们了解程序在运行时从哪里加载这些模块。

下载`string.exe`同理，文件夹内容如下：



string.exe 是一个用于提取和显示可执行文件中的字符串的命令行工具。它的主要功能是在二进制文件中搜索并提取ASCII和Unicode字符串，这些字符串可能包含在程序中用于各种目的，如错误消息、文件路径、URL等。

以下是 string.exe 的主要用途:

1. **查找隐藏的信息**: String.exe 可以帮助我们查找可执行文件中隐藏的文本信息，这些信息可能包含恶意软件的指示或标识。
2. **分析文件功能**: 通过查看提取的字符串，我们可以初步了解程序的功能和行为，以及它可能与文件系统、网络通信或注册表交互的方式。
3. **识别常见字符串**: String.exe 可以帮助我们识别常见的恶意代码字符串，如URL、IP地址、加密密钥等，这些信息对于进一步的分析非常有用。
4. **辅助反汇编工作**: 在进行静态分析时，提取的字符串可以帮助我们在反汇编中识别和理解代码的不同部分。

至此该虚拟机必要软件均已齐全。

4 实验结论及心得体会

实验结论:

通过完成这个实验，我成功地配置了一个用于恶意代码分析的虚拟机环境，并了解了其中重要的静态和动态分析工具。这些工具将帮助我们在安全的环境中分析恶意代码，从而更好地理解其行为和功能。

心得体会:

在这个实验中，我学会了如何设置一个用于恶意代码分析的虚拟机环境，并了解了多种有用的分析工具。这些工具对于理解恶意代码的工作原理和危害非常重要。同时，我也明白了安全性在恶意代码分析中的重要性，虚拟机环境可以提供一个安全的隔离环境，以防止恶意代码对真实系统造成损害。

通过这个实验，我对恶意代码分析有了更深入的了解，并且掌握了一些实用工具的使用技巧。这将有助于我在未来的研究和工作中更好地应对恶意代码和网络安全问题。