

**恶意代码分析实验报告**

**实验二：虚拟机技术实验**

****

学 院 网安

专 业 信安

学 号 2113662

姓 名 张丛

班 级 信安一班

1. **实验目的**

1配置病毒分析虚拟机

VMware 虚拟机或其它的虚拟机软件

Windows XP操作系统

2 虚拟机中安装静态分析工具

string.exe、PEView、dependency walker、IDA等工具

3 虚拟机中安装动态分析工具

预习教材chapter 3：basic dynamic analysis

OllyDBG、Process Monitor、Process Explorer、RegShot、WireShark等工具

1. **实验原理**

虚拟机技术，分析工具安装

1. **实验过程**

1.VM Pro安装，下载win\_XP镜像iso文件，新建虚拟机，如下：



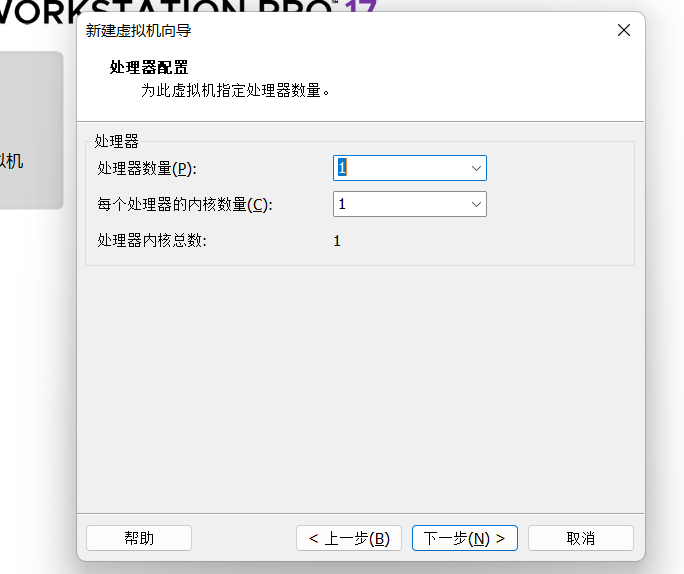
配置：

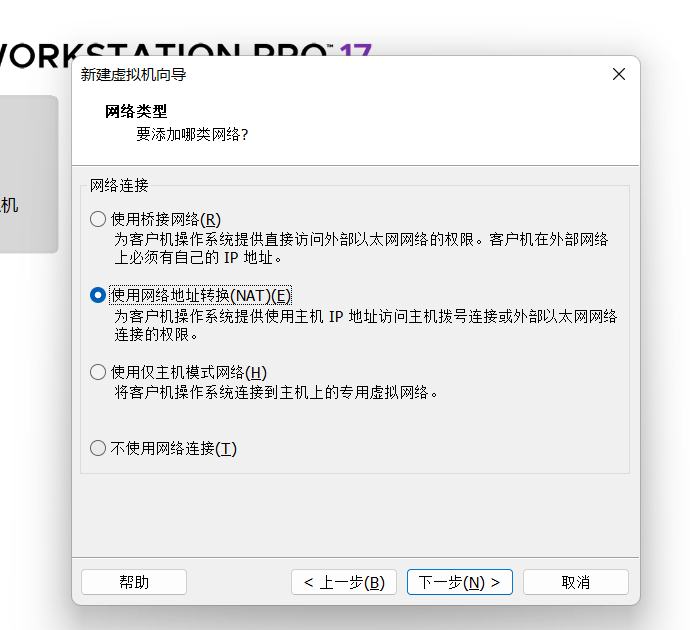
处理器：1

内存：512MB

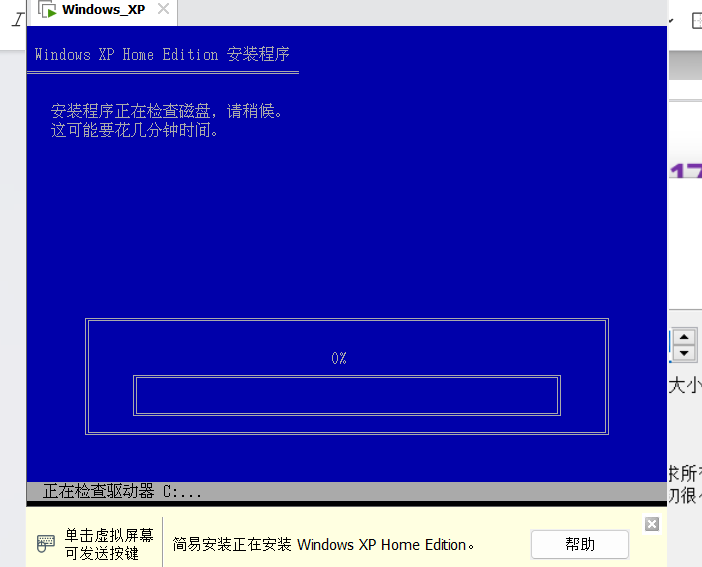
网络类型：NAT

磁盘：40GB





2.XP的安装与激活





安装完成后，虽然之前已经输入了密钥但还是会提示30天的激活时间，，，再去翻阅网上的资料，可以使用激活工具



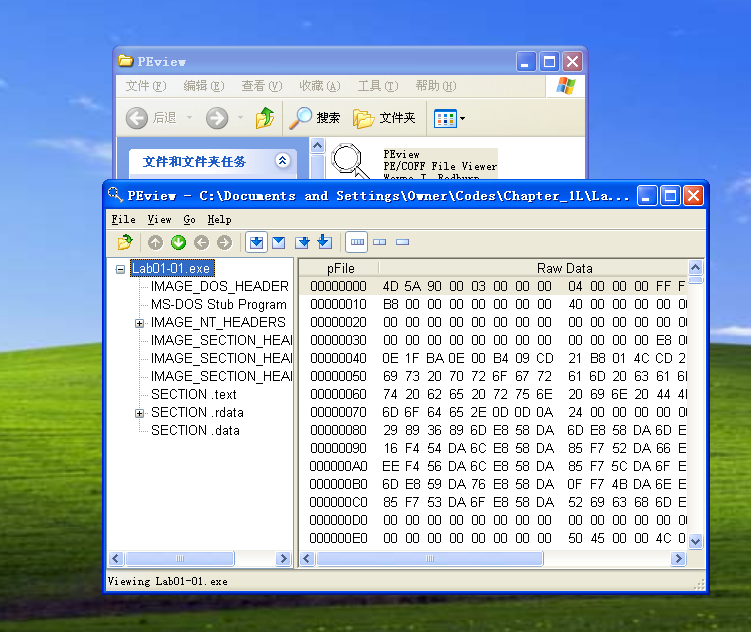
最后激活成功。

1. 静态分析工具安装（工具的功能分析放在最后），以Peview和Depandency Walker为例：

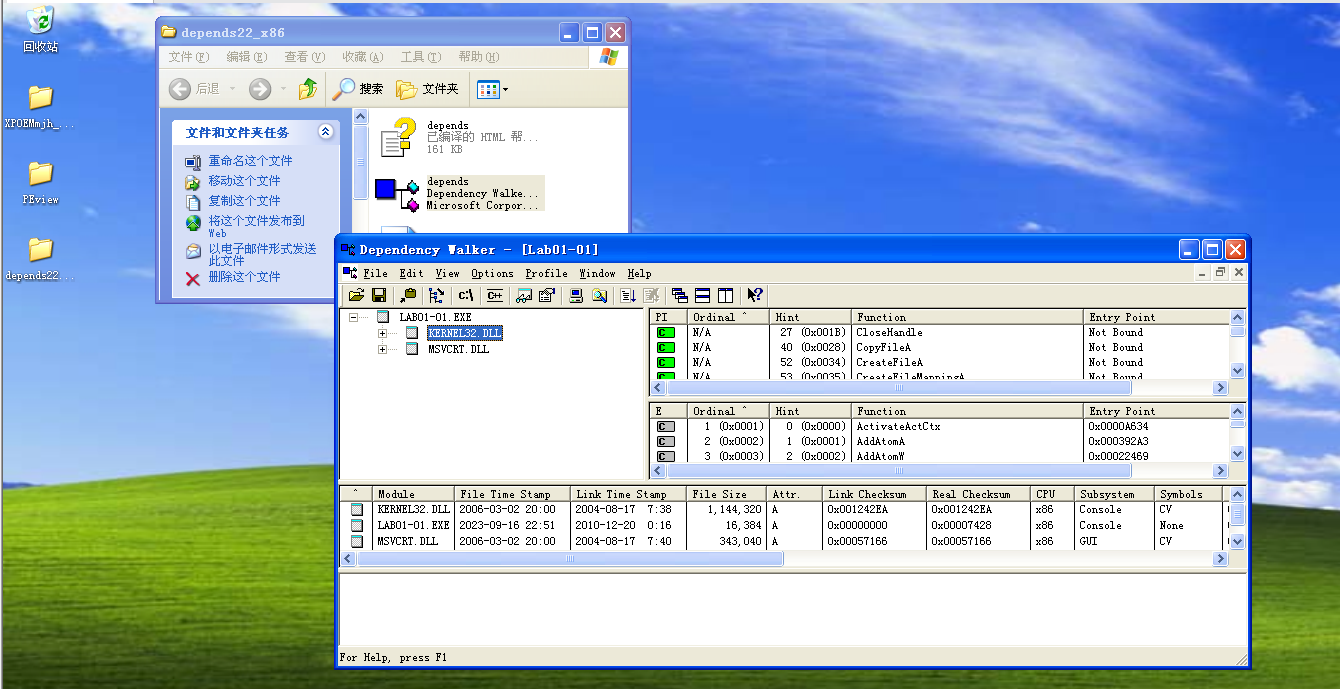
无论是在主机下载压缩包后送到虚拟机，还是直接在虚拟机联网下载均可，然后解压压缩包：



使用PEview分析Lab01-01.exe:



Dependency同理：

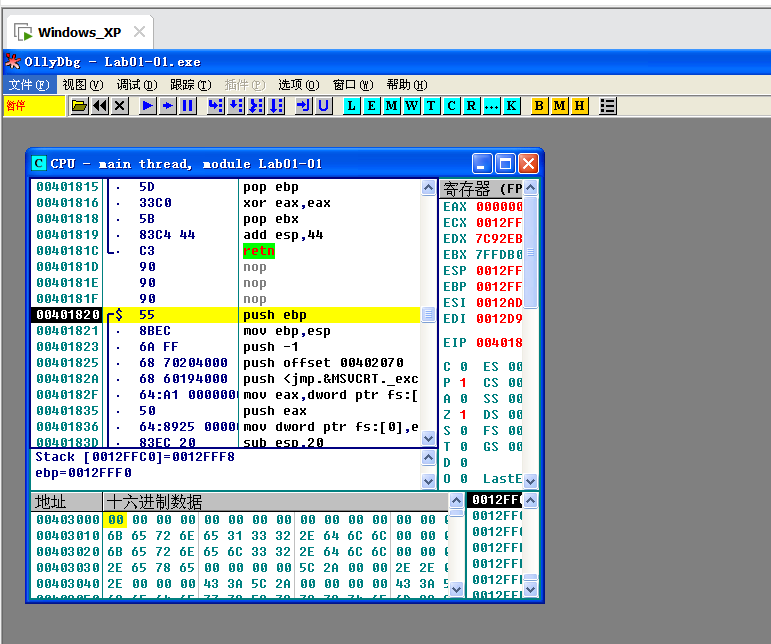


1. 动态分析工具安装：

同样先获得压缩包，解压即可：



使用OllyDBG分析Lab01-01.exe:



其余动静态分析工具的安装和使用均同理，不再赘述。

1. **实验结论及心得体会**

## 各分析工具的功能：

**静态：**

1. string.exe：一个命令行工具，用于在二进制文件中查找和提取ASCII和Unicode字符串。

2. PEView：一个用于查看和分析可执行文件（PE文件）的工具。它可以显示文件的结构、导入和导出函数、节表、资源等信息。

3. PEID：一个用于识别PE文件的工具。它可以通过分析文件的头部信息和导入函数来确定文件的类型和特征。

4. resource\_hacker：一个用于修改和查看Windows可执行文件中资源的工具。它可以编辑和替换文件中的图标、位图、字符串等资源。

5. dependency walker：一个用于查看可执行文件的依赖关系的工具。它可以显示文件所依赖的DLL文件和函数，帮助分析和解决文件加载和运行时的问题。

1. IDA：一个用于反汇编和分析二进制文件的工具。它可以将机器码转换为汇编代码，并提供反汇编、调试和分析功能。

**动态：**

7. OllyDBG：一个用于动态分析可执行文件的调试器。它可以在运行时跟踪程序的执行，查看和修改内存、寄存器和变量的值，帮助理解程序的行为和逻辑。

8. Process Monitor：一个用于监视和记录Windows系统上进程活动的工具。它可以显示进程的文件操作、注册表操作、网络活动等信息，帮助分析程序的运行和行为。

9. Process Explorer：一个用于查看和管理正在运行的进程的工具。它可以显示进程的详细信息、线程、模块、打开的句柄等，帮助分析和解决进程相关的问题。

10. RegShot：一个用于监视和比较Windows系统注册表的工具。它可以记录注册表的变化，并生成两个时间点之间的注册表差异报告，帮助分析和调试注册表相关的问题。

1. WireShark：一个用于网络分析和数据包捕获的工具。它可以捕获和分析网络流量，显示协议的详细信息，帮助分析和故障排除网络通信问题。

## 实验心得：

虚拟机安装技术的熟练，主要的进步在于对虚拟机桥接模式和NAT模式的理解。