

**恶意代码课程实验报告**

**实验二**

****

学 院 网络空间安全学院

专 业 信息安全、法学

学 号 2111454

姓 名 李潇逸

班 级 信息安全、法学

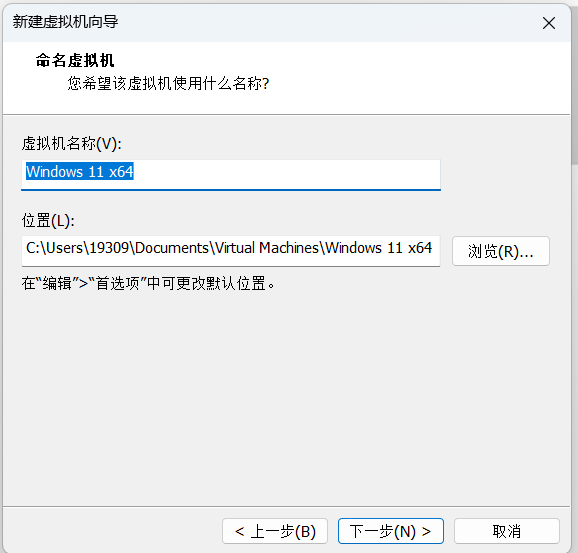
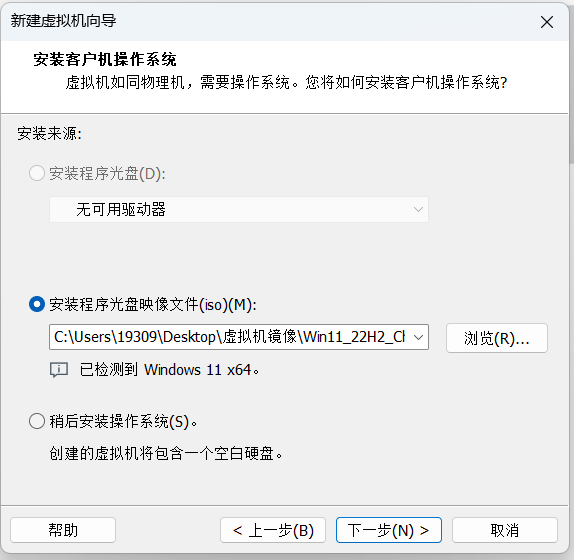
1. **实验环境**

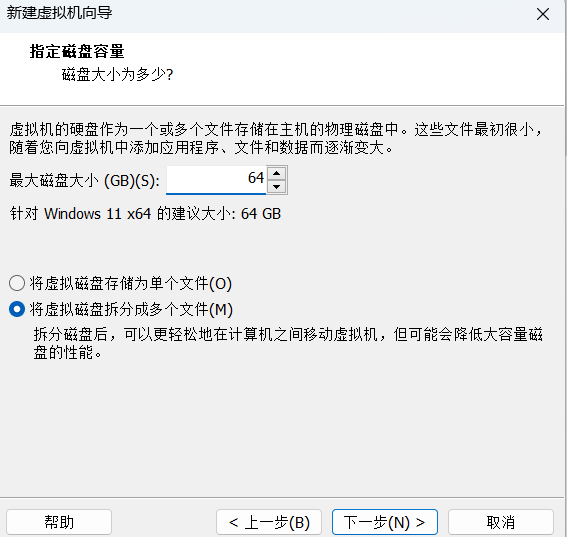
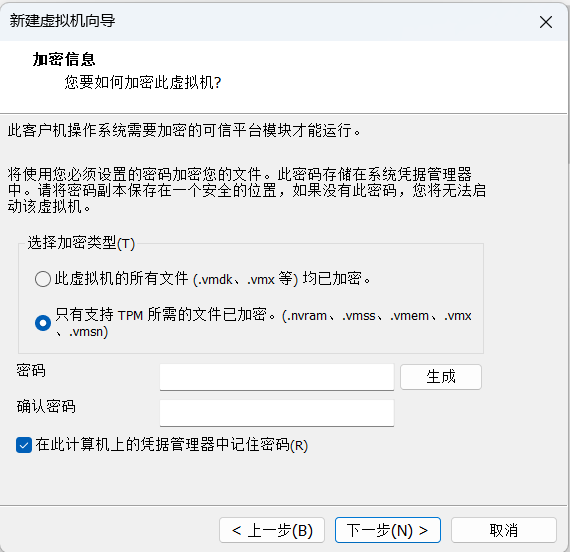
VMWARE，Windows11

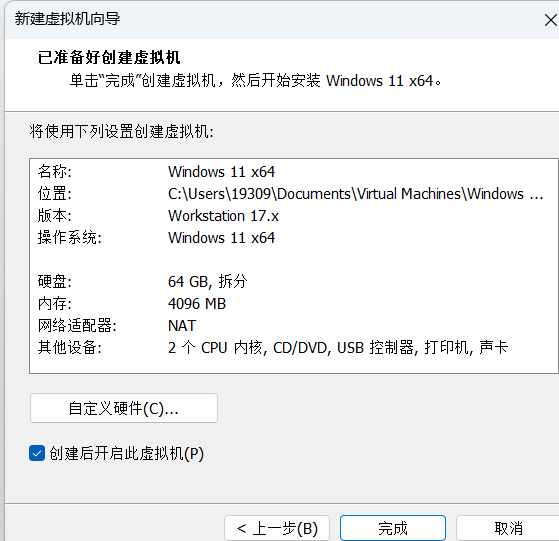
1. **实验工具**

string.exe、PEView、dependency walker、IDA、OllyDBG、Process Monitor、Process Explorer、RegShot、WireShark

1. **实验过程**
2. **Windows11安装**

****

****

****

1. **工具安装**



1. **工具功能**
2. **String：查找二进制文件中的字符串**
3. **PEview：查看PE文件二进制内容**
4. **dependency walker：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**
5. **IDA：静态反汇编**
6. **Ollydbg：动态反汇编，可调试**
7. **Process Monitor：系统进程监视软件**
8. **RegShot：注册表比较器，通过扫描并保存注册表的“快照”，并对两次快照进行自动的对比，找出快照间存在的不同之处，结果保存成txt或者html文档**
9. **WireShark：网络封包分析软件，可以截取各种网络封包，显示网络封包的详细信息**
10. **实验心得**

**安装配置了环境工具，对恶意代码和恶意代码分析工具有了更深的理解。**