



南开大学

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月异



恶意代码分析与防治技术

第4章 虚拟机技术

王志

zwang@nankai.edu.cn

南开大学 网络空间安全学院

2023-2024学年



允公允能 日新月异

知识点

- 虚拟机的结构
- 创建虚拟机
- 使用虚拟机
- 虚拟机的风险
 - 重点：使用虚拟机进行病毒分析的优缺点



南开大学
Nankai University



南开大学

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月异



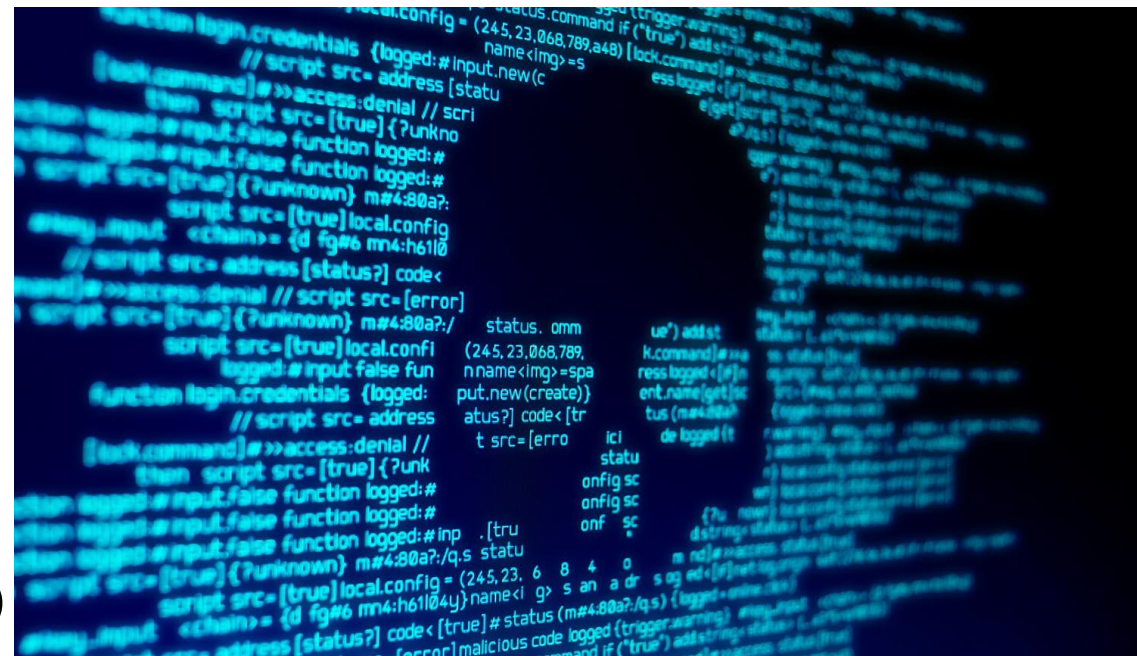
虚拟机的结构

计算机病毒动态分析为什么要使用虚拟机？

作答

Fresh malware can be full of surprises.

- 伪装 (Disguise)
- 恶意软件载荷 (Payloads)
- 技术进化 (Evolving Technique)
- 社会工程学 (Social Engineering)





允公允能 日新月异

动态分析

- 主动地运行恶意代码，监控并分析恶意代码的运行结果
- **需要安全、可控的运行环境**
 - 恶意代码可能会快速传播到网络中的其它计算机上
 - 隔离：阻止动态分析计算机与互联网和其他计算机的网络连接
 - 清理：分析结束后，要清除计算机中的病毒



物理机和虚拟机谁更适合构建计算机病毒的动态分析环境？

- ☐ A 物理机 (physical machine)
- ☐ B 虚拟机 (virtual machine)

提交



允公允能 日新月异

物理机

- 隔离
 - 断开网络的物理连接
 - 部分恶意代码的功能无法执行
- 清理
 - 难以彻底清除物理机上的计算机病毒
 - 需要重装系统
 - 分析的时间开销大



南开大学
Nankai University



允公允能日新月异

虚拟机

- 隔离

- 虚拟机与物理机之间不能直接访问
- 虚拟网卡和网络服务

- 清除

- 建立快照（snapshot），快速恢复之前的状态
- 计算机病毒动态分析
 - 虚拟机

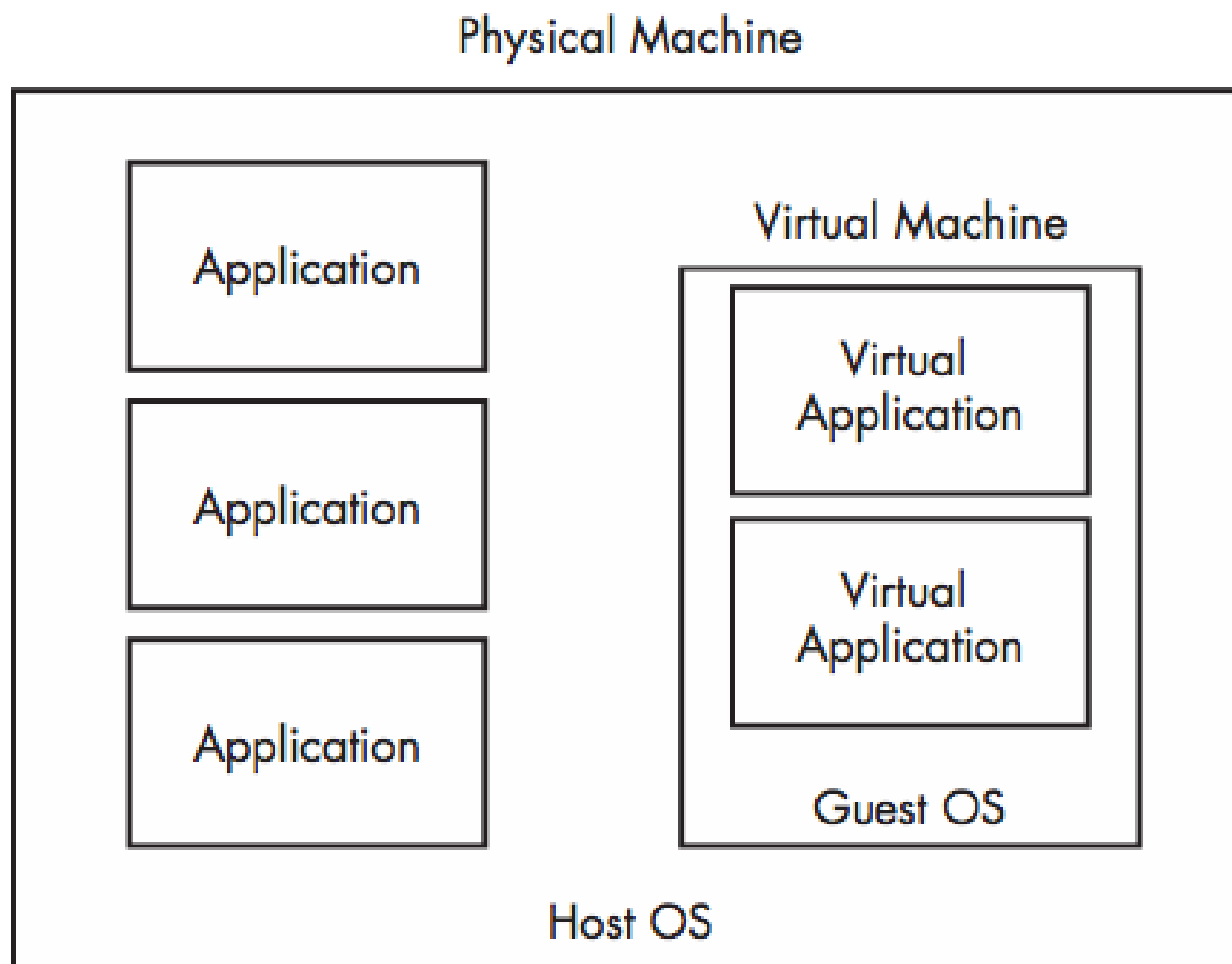


南开大学
Nankai University



允公允能 日新月异

虚拟机的结构



在物理机上动态分析计算机病毒有哪些缺点？

- ☒ A 难以清除计算机病毒
- ☒ B 对计算机造成破坏
- ☐ C 可控性好
- ☒ D 无法连接网络

提交



在虚拟机上进行计算机病毒动态分析有哪些优点

- ☒ A 与主机隔离
- ☒ B 可控性好
- ☒ C 可以快速恢复计算机的状态
- ☐ D 虚拟机逃逸

提交





南开大学

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月异

创建虚拟机

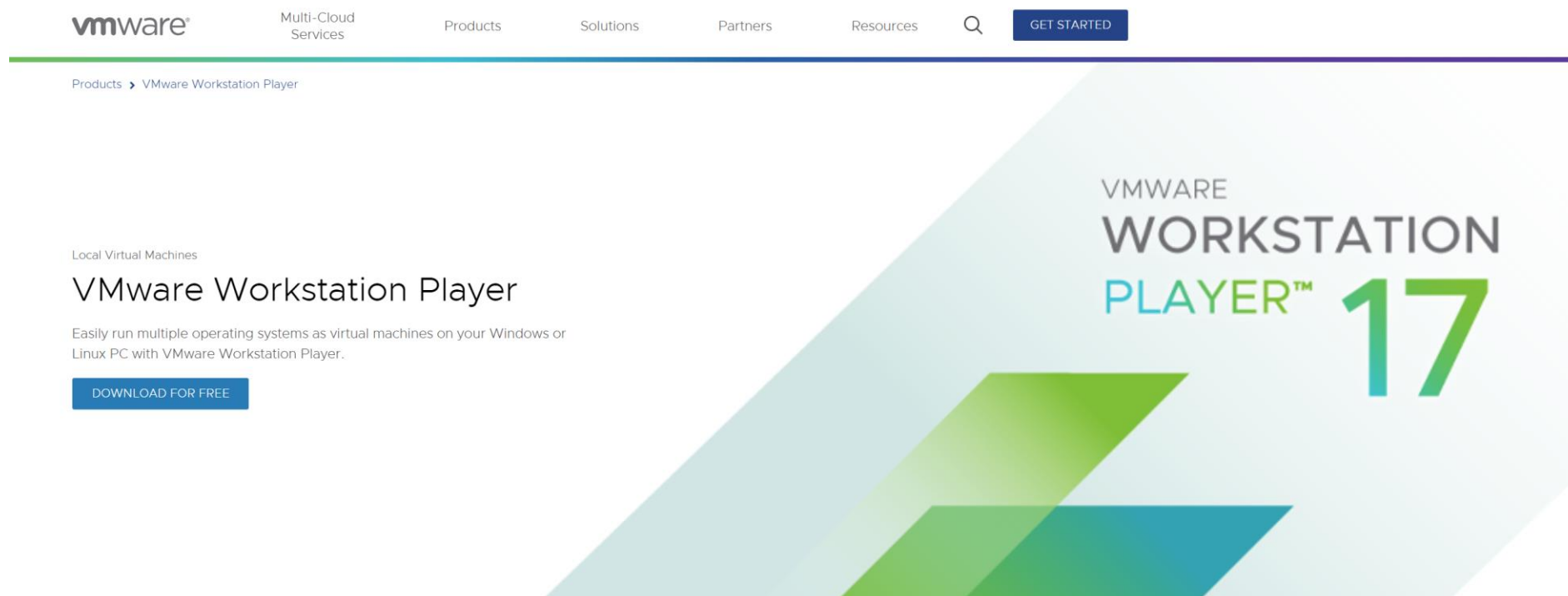
大家用过哪些创建虚拟机的软件？

作答

允公允能 日新月异

VMware Workstation Player

- 个人用户免费、不支持快照



南开大学
Nankai University



虚拟机配置

- 硬盘
 - 虚拟机操作系统、动态监控工具
 - 20 GB 硬盘





允公允能 日新月异

虚拟机配置

- 操作系统
 - Windows XP 操作系统
 - 大部分恶意代码可以在Windows XP操作系统上执行
 - 应用程序向下兼容
 - 正在编写新的教材，将使用Windows 10操作系统



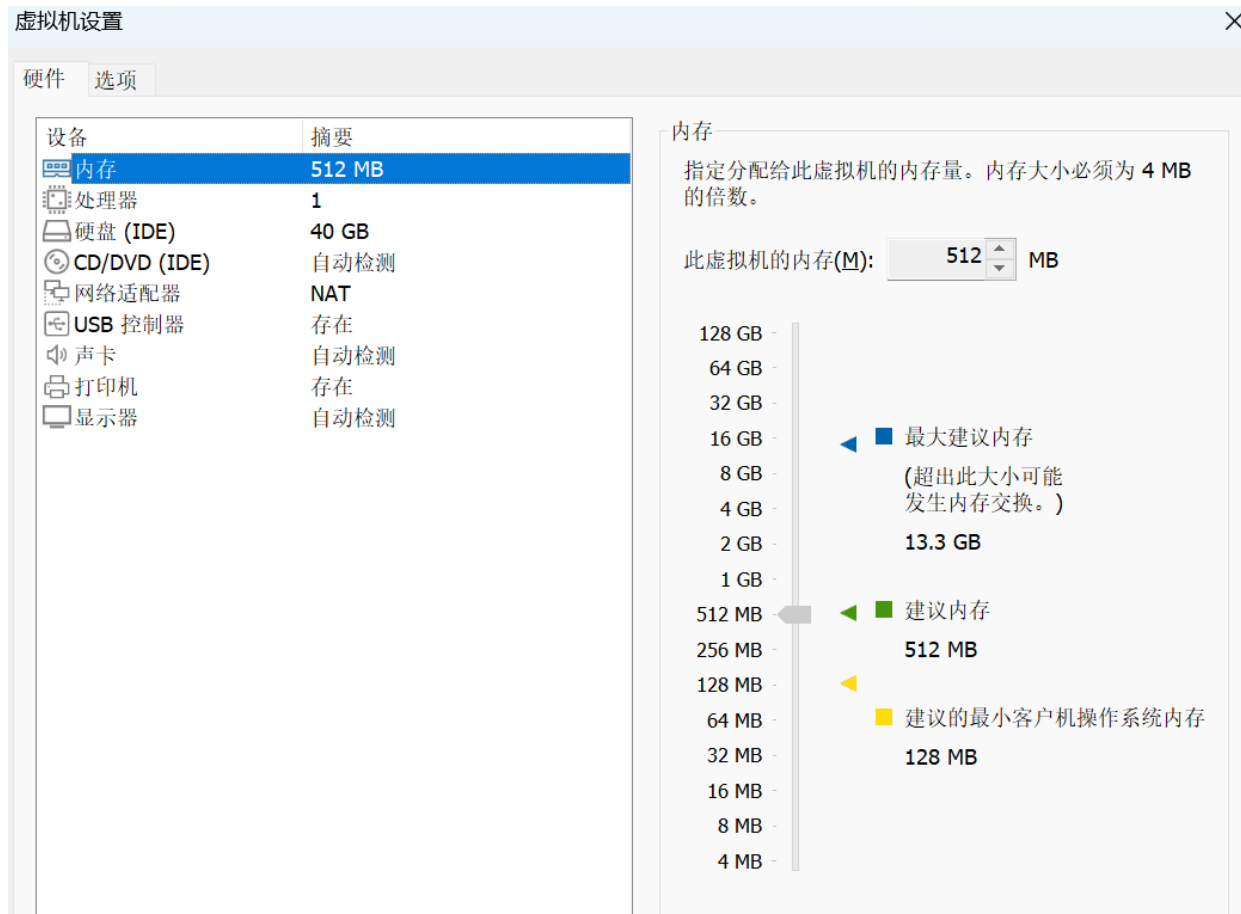


虚拟机配置

- 应用程序
 - VMware虚拟机
 - IDA Pro
 - OllyDBG
 - WinDBG
 - Appendix B
 - tools.pediy.com



虚拟机配置



虚拟机配置

虚拟机设置

硬件 选项

设备	摘要
内存	512 MB
处理器	1
硬盘 (IDE)	40 GB
CD/DVD (IDE)	自动检测
网络适配器	NAT
USB 控制器	存在
声卡	自动检测
打印机	存在
显示器	自动检测

处理器

处理器数量(P): 1

每个处理器的内核数量(C): 1

处理器内核总数: 1

虚拟化引擎

☐ 虚拟化 Intel VT-x/EPT 或 AMD-V/RVI(V)

☐ 虚拟化 CPU 性能计数器(U)

☐ 虚拟化 IOMMU (IO 内存管理单元)(I)





虚拟机配置

虚拟机设置

硬件

选项

设备	摘要
内存	512 MB
处理器	1
硬盘 (IDE)	40 GB
CD/DVD (IDE)	自动检测
网络适配器	NAT
USB 控制器	存在
声卡	自动检测
打印机	存在
显示器	自动检测

磁盘文件

D:\vmware\winxp\Windows XP Professional-000001.vr

容量

当前大小: 1.8 GB
系统可用空间: 852.5 GB
最大大小: 40 GB

磁盘信息

没有为此硬盘预分配磁盘空间。
硬盘内容存储在多个文件中。

磁盘实用工具

☐

只有关闭虚拟机电源时, 才能使用磁盘实用工具。

将该虚拟机磁盘映射到本地卷。

映射(M)...

整理文件碎片并整合可用空间。

碎片整理(D)

扩展磁盘容量。

扩展(E)...

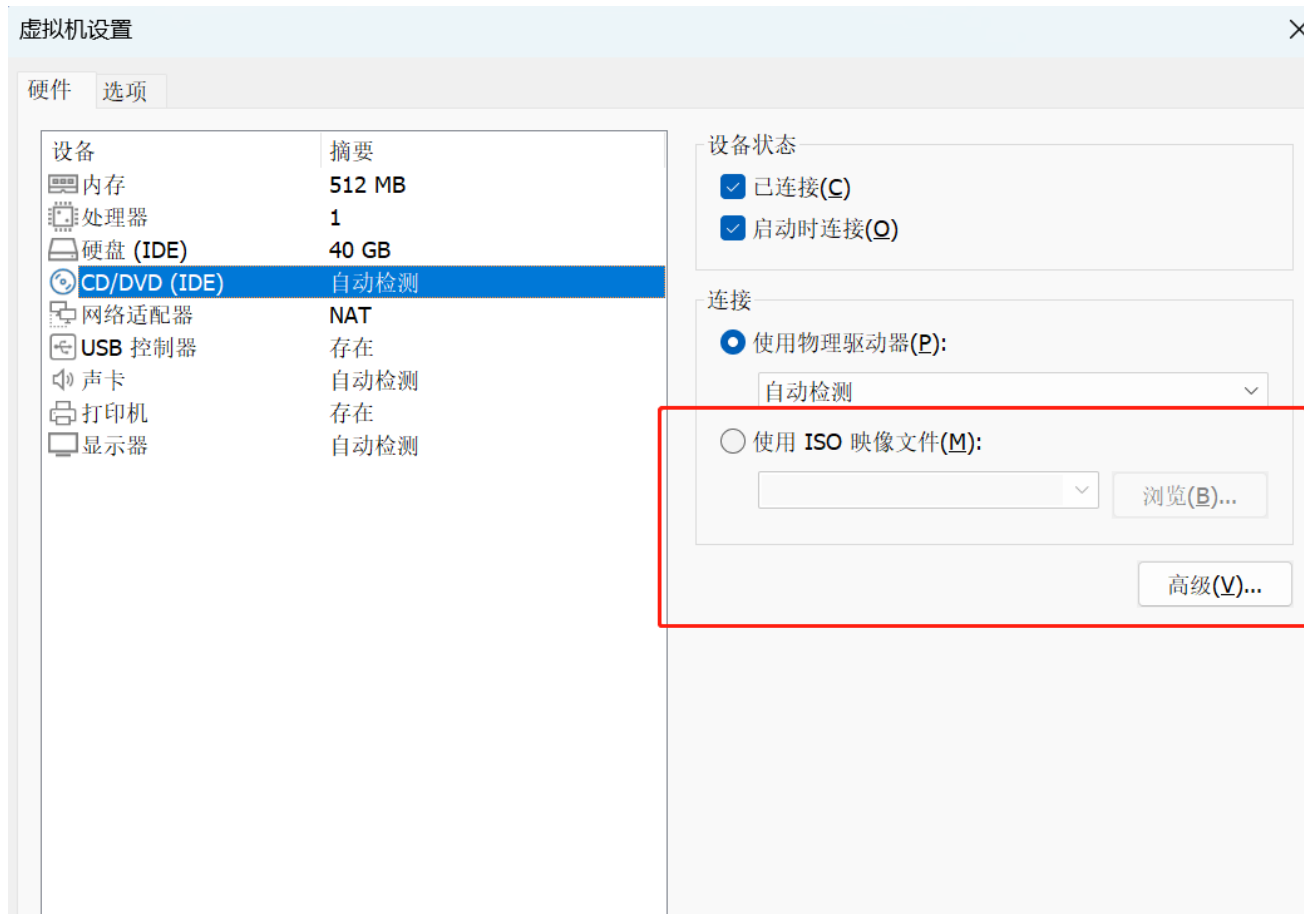
压缩磁盘以回收未使用的空间。

压缩(C)

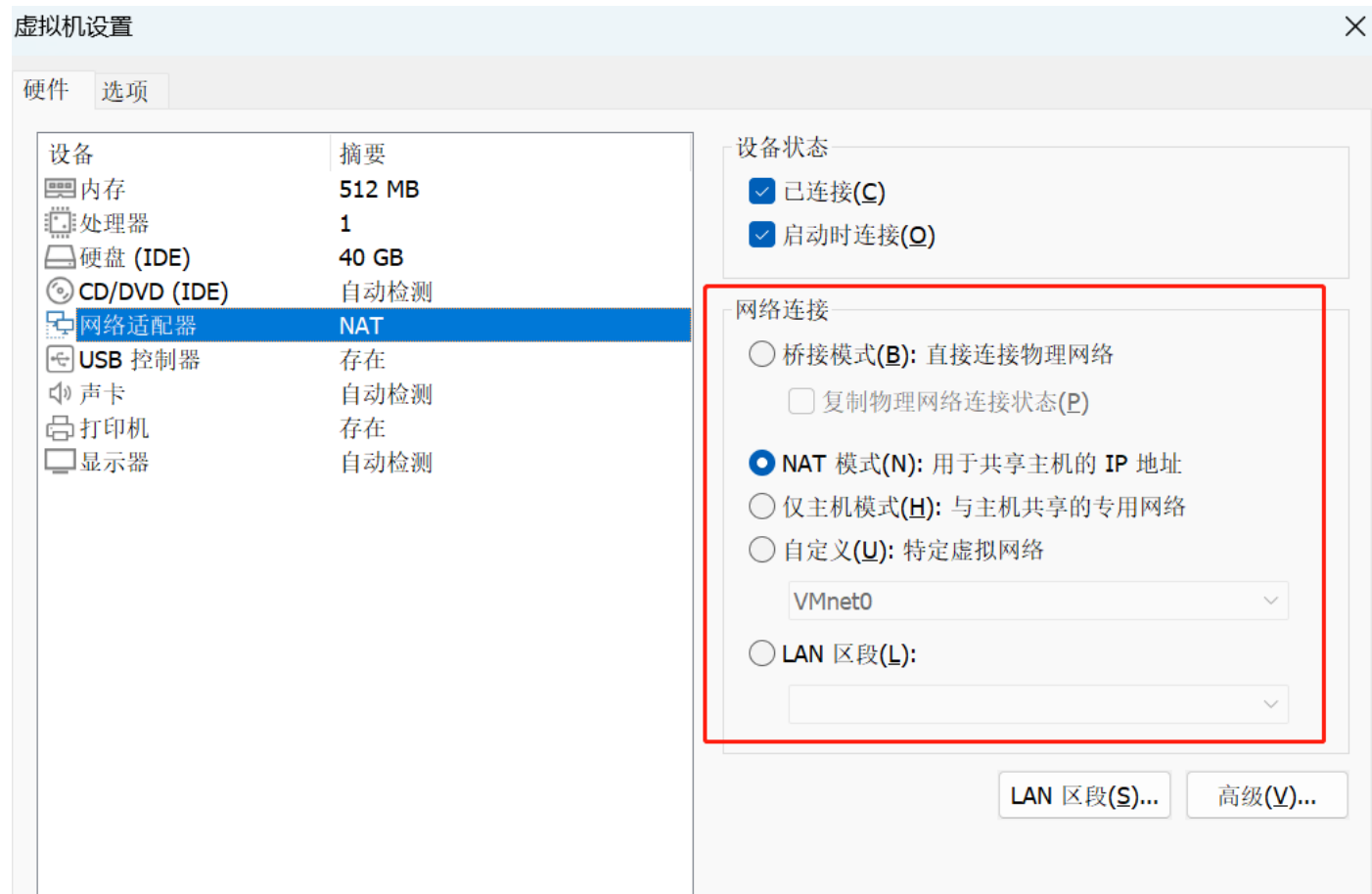
高级(V)...



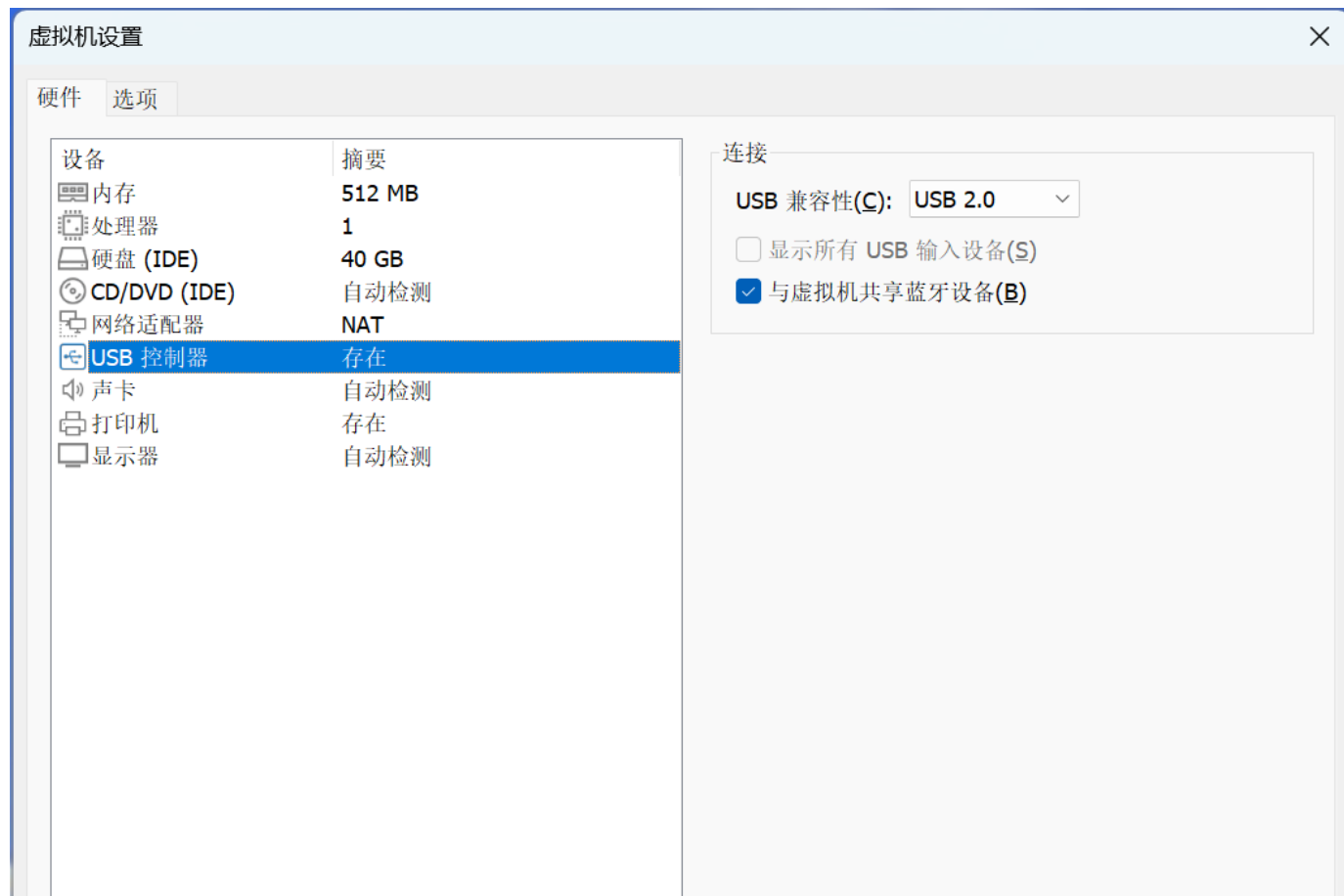
虚拟机配置



虚拟机配置



虚拟机配置



计算机病毒动态分析为什么选择Windows XP作为虚拟机的操作系统?

- ☐ A 没有病毒运行在Windows XP上
- ☒ B 恶意代码的攻击目标
- ☒ C 兼容性更好
- ☒ D 体积小、安装快

提交





南开大学

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月异

使用虚拟机



允公允能 日新月异

连接互联网

- 更加真实的执行计算机病毒
- **Risks:**
 - 病毒的扩散、DDoS攻击, Spam垃圾邮件等等
- **Pre-analysis:**
 - 判断病毒是否连接互联网
 - 如果不连接互联网对其行为有什么影响



南开大学
Nankai University

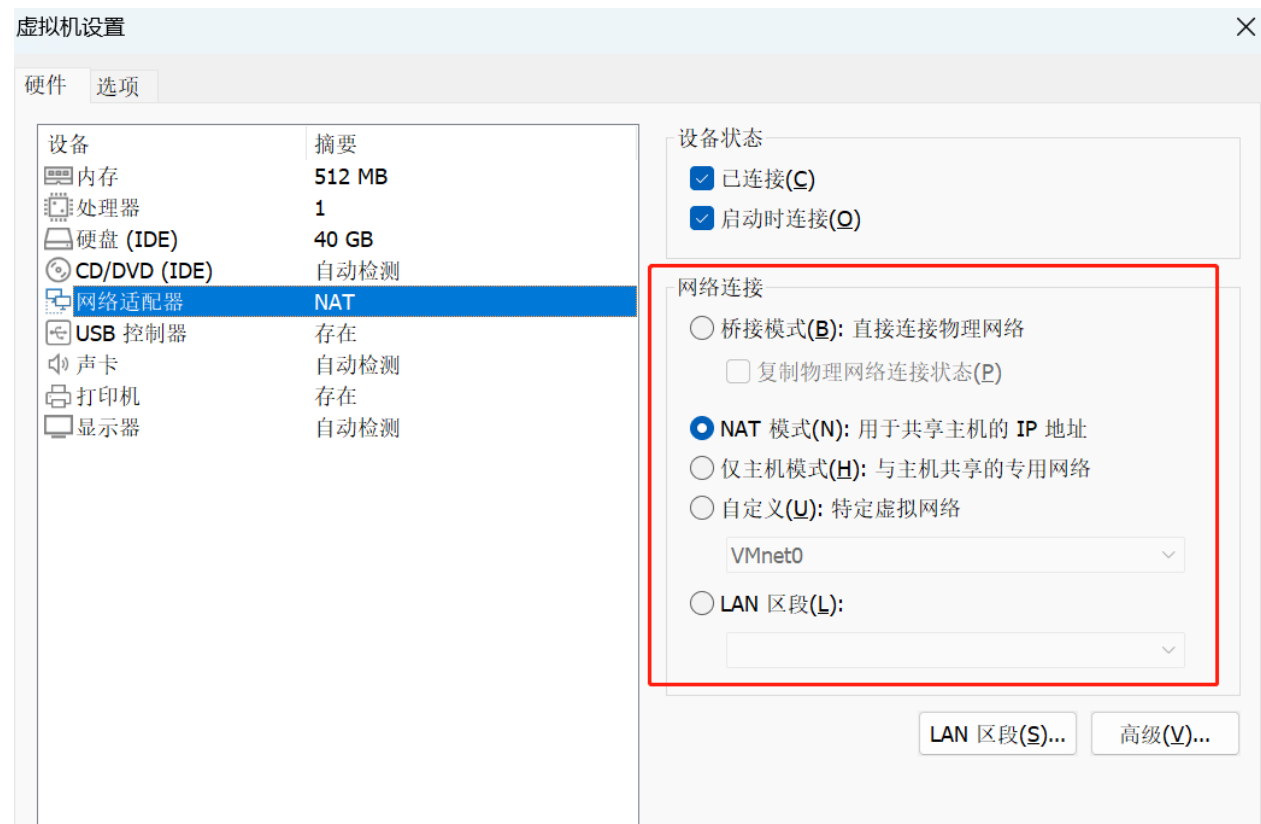
连接方式

• NAT 模式

- 共享IP地址，端口映射
- 建立了一个虚拟的路由器
- 虚拟机之间可以通信、可以连接互联网

• Bridged桥接模式

- 直接连接到主机所在的局域网中
- 影响局域网中的其它主机
- 例如病毒扩散、DDoS攻击等



快照Snapshots

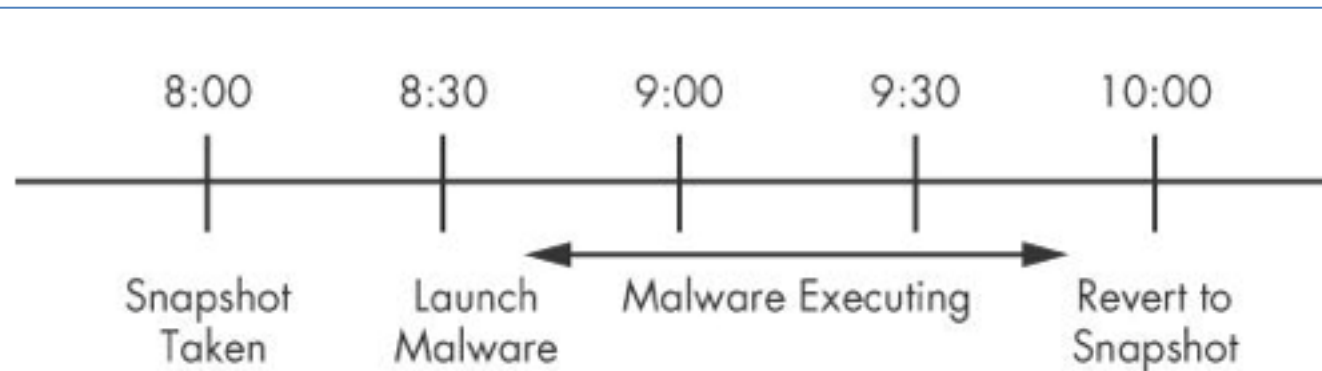


Figure 3-5. Snapshot timeline



允公允能 日新月异

文件传输

- VMware的drag-and-drop 文件传输
 - from host OS to guest OS
 - from guest OS to host OS
- 共享文件夹Shared folder
 - 主机和虚拟机可以共同访问一个文件夹



VMware虚拟机的网络连接方式有哪些?

☒ A Host-Only

☒ B Bridge

☒ C NAT

☐ D WiFi

提交





南开大学

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月异



虚拟机的安全风险



允公允能 日新月异

虚拟机的安全风险

- 计算机病毒会检测到自己运行在一个虚拟机中
 - Chapter 17: anti-VMware techniques
- VMware 的安全漏洞
 - 计算机病毒会利用VMware的漏洞进行攻击
 - drag-and-drop漏洞
 - 需要及时打补丁
- 计算机病毒有可能感染和破坏主机
 - 不要使用存储重要数据的计算机进行病毒分析



南开大学
Nankai University



VMware安全漏洞

343 Results

Sort By Recently Added >

Advisory ID	Severity	CVE(s)	Updated On
> VMSA-2023-0019.1	Important	VMware Tools updates address a SAML Token Signature Bypass Vulnerability (CVE-2023-20900)	2023-09-05
> VMSA-2023-0018.1	Critical	VMware Aria Operations for Networks updates address multiple vulnerabilities. (CVE-2023-34039, CVE-2023-20890)	2023-08-31
> VMSA-2023-0017	Moderate	VMware Horizon Server updates address multiple security vulnerabilities (CVE-2023-34037, CVE-2023-34038)	2023-08-03
> VMSA-2023-0016	Moderate	VMware Tanzu Application Service for VMs and Isolation Segment updates address information disclosure vulnerability (CVE-2023-20891)	2023-07-25
> VMSA-2023-0015	Moderate	VMware SD-WAN update addresses a bypass authentication vulnerability (CVE-2023-20899)	2023-07-12
> VMSA-2023-0014	Important	VMware vCenter Server updates address multiple memory corruption vulnerabilities (CVE-2023-20892, CVE-2023-20893, CVE-2023-20894, CVE-2023-20895, CVE-2023-20896)	2023-06-22
> VMSA-2023-0013	Low	VMware Tools update addresses Authentication Bypass vulnerability (CVE-2023-20867)	2023-06-13
> VMSA-2023-0012.2	Critical	VMware Aria Operations for Networks updates address multiple vulnerabilities. (CVE-2023-20887, CVE-2023-20888, CVE-2023-20889)	2023-06-20
> VMSA-2023-0011	Moderate	VMware Workspace ONE Access and Identity Manager update addresses an Insecure Redirect Vulnerability. (CVE-2023-20884)	2023-05-30
> VMSA-2023-0010	Moderate	NSX-T update addresses cross-site scripting vulnerability (CVE-2023-20868)	2023-05-23
> VMSA-2023-0009	Important	VMware Aria Operations update addresses multiple Local Privilege Escalations and a Deserialization issue (CVE-2023-20877, CVE-2023-20878, CVE-2023-20879, CVE-2023-20880)	2023-05-11
> VMSA-2023-0008	Critical	VMware Workstation and Fusion updates address multiple security vulnerabilities (CVE-2023-20869, CVE-2023-20870, CVE-2023-20871, CVE-2023-20872)	2023-04-25
> VMSA-2023-0007.1	Critical	VMware Aria Operations for Logs (Operations for Logs) update addresses multiple vulnerabilities. (CVE-2023-20864, CVE-2023-20865)	2023-07-10
> VMSA-2023-0006	Moderate	VMware Workspace ONE Content update addresses a passcode bypass vulnerability (CVE-2023-20857)	2023-02-28
> VMSA-2023-0004	Critical	VMware Carbon Black App Control updates address an injection vulnerability (CVE-2023-20858)	2023-02-21
> VMSA-2023-0005	Important	VMware vRealize Orchestrator update addresses an XML External Entity (XXE) vulnerability (CVE-2023-20855)	2023-02-21



虚拟机进行计算机病毒动态分析的安全风险？

- ☒ A 计算机病毒检测虚拟机，改变其动态行为
- ☒ B 虚拟机软件的漏洞
- ☒ C 虚拟机逃逸
- ☐ D 可控性好

提交





总结

Analyzing malware using VMware

1. Start with a **clean snapshot** with no malware running on it.
2. **Transfer** the malware to the virtual machine.
3. Conduct your **analysis** on the virtual machine.
4. Take your **notes, screenshots, and data** from the virtual machine and transfer it to the physical machine.
5. **Revert** the virtual machine to the clean snapshot.



讨论

- Malware authors thought **only analysts** would be running the malware in a virtual machine.
 - VM is becoming more and more common
 - **valuable victim** ?
- Will anti-VM techniques probably become even **less common** ?

讨论：计算机病毒的反虚拟机技术

是不是只有计算机病毒分析员在使用虚拟机？ 计算机病毒会不会遇到虚拟机就不在做恶意行为了？

作答



实验课

- 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
- 虚拟机中安装静态分析工具
 - string.exe、PEView、dependency walker、IDA等工具
- 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
- **实验报告内容**: 1. 虚拟机的安装和配置过程; 2. 静态分析工具的功能和安装过程; 3. 动态分析工具的功能和安装过程。





南开大学

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月异



恶意代码分析与防治技术

第4章 虚拟机技术

王志

zwang@nankai.edu.cn

南开大学 网络空间安全学院

2023-2024学年