



网络攻防技术与实践课程

2. 网络攻防实验环境构建

诸葛建伟

zhugejw@gmail.com



内容

- 1. 网络攻防实验环境**
- 2. 虚拟化技术与云计算热潮**
- 3. 蜜网(Honeynet)技术介绍**
- 4. 基于虚拟蜜网的网络攻防实验环境**
- 5. 网络攻防的活动与竞赛形式**



一些名言和典故

- “不闻不若见之，闻之不若见之，见之不若知之，知之不若行之，学至于行之而止矣，行之，明也。”——荀子《儒效篇》
- “实践出真知”，“实践是检验真理的唯一标准”——毛泽东《毛泽东选集》
- “纸上谈兵”（赵括）
- “知其然，而不知其所以然”——梁启超《论小说与群治之关系》
- “什么都略懂一点，生活更多彩一些”——？



为什么需要网络攻防实验环境？

- 网络攻防是基础知识和实践紧密结合的技术方向
 - 基础知识：计算机各个方面专业知识都要“略懂”
 - 操作系统、网络的基本结构与底层机制
 - 编程语言、汇编语言及软件编译执行机理
 - 密码学与信息安全专业基础
 - ...
 - 实践技能：各种网络和系统实践技能也要“略懂”
 - 系统底层机制进行深入探究的技术能力：网络、程序...
 - 掌握网络渗透测试的实践技能→支持更好的研究和防御
 - 掌握对攻击的分析实践技能→了解安全威胁,支持更好的防范
 - 掌握攻击防御和响应技能



专属的网络攻防实验环境

- 学习网络攻防技术需要一个实验环境
 - 学打篮球：你就需要篮球场

- 拿**Internet**直接作为攻防实验学习环境
 - 违背传统黑客道德与精神
 - 效率低下学习方式，“脚本小子”/低水平骇客

- 专属的网络攻防实验环境
 - 环境的可控性、可重复性
 - “我的地盘我作主”



网络攻防实验环境的基本组成

- 攻击机：发起网络攻击的主机
 - **Win32: Windows XP**
 - **Linux: more powerful**, 建议攻击平台
- 攻击目标主机（靶机）
 - **Win32桌面操作系统: Windows XP**
 - **Linux服务器操作系统: Ubuntu / ...**
 - **Win32服务器操作系统: Win 2K3 /Win 2K Server**
- 攻击检测、分析与防御平台
 - 攻击目标主机网关位置
 - 网关：网络流分析、检测、防御
 - 攻击目标主机：系统日志采集与分析
- 构建一个基本网络攻防环境，需要**4-5**台主机及相关联网设备



V-Net: 基于虚拟蜜网的攻防实验环境

□ 虚拟机技术 (Virtual Machine)

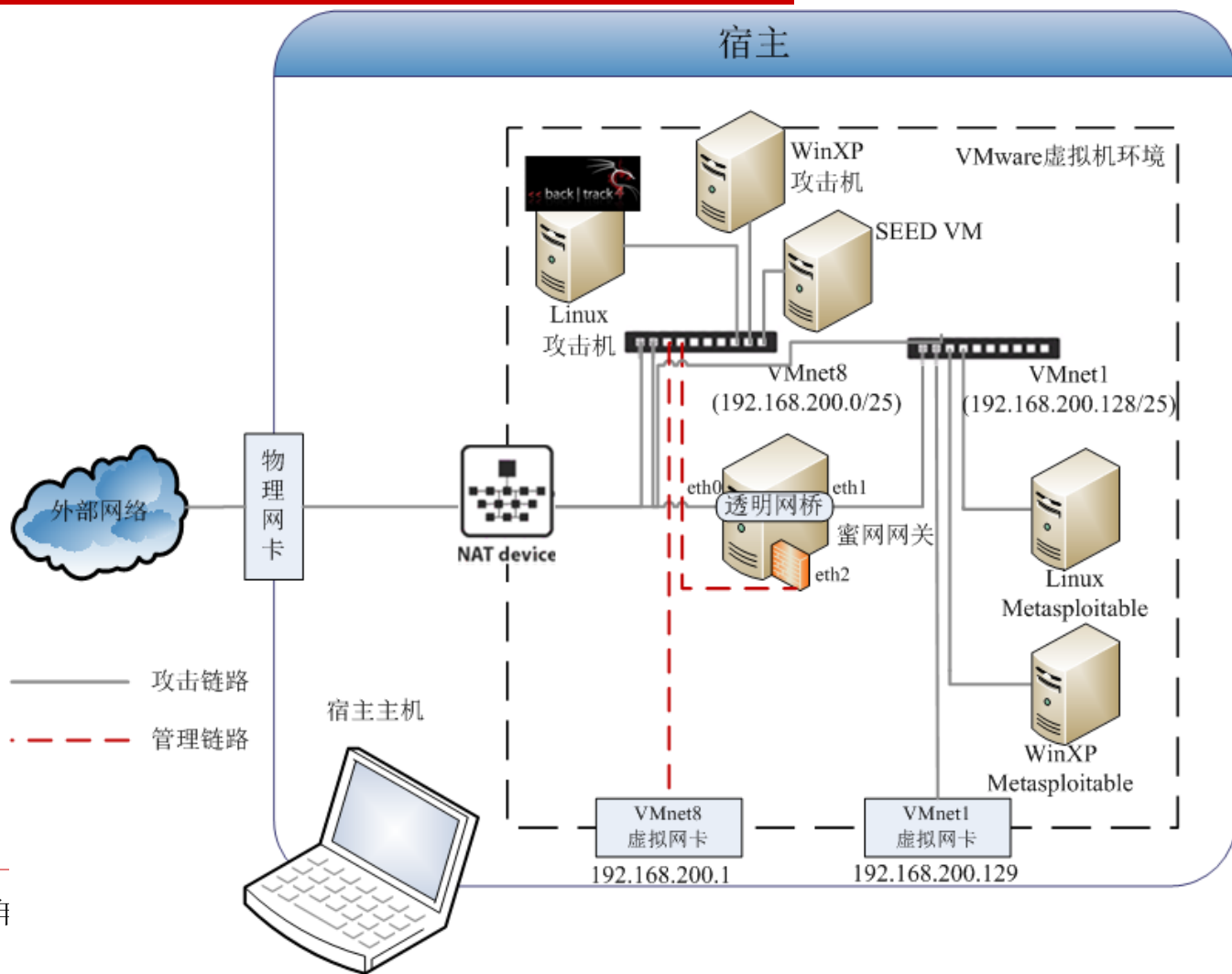
- 通过虚拟化技术在一台主机上构建攻防实验环境
- 降低部署成本同时提高易管理性
- 虚拟机软件: **VMware Workstation/vSphere**

□ 蜜网技术 (Honeynet)

- 陷阱网络: 诱骗和分析网络攻击
- 高交互式蜜罐: 提供攻击目标环境
- 蜜网网关/**Sebek**: 攻击网络/系统行为捕获与分析

□ 虚拟机+蜜网=虚拟蜜网 (Virtual Honeynet)

基于虚拟蜜网的攻防实验环境拓扑





内容

- 1. 网络攻防实验环境**
- 2. 虚拟化技术与云计算热潮**
- 3. 蜜网(Honeynet)技术介绍**
- 4. 基于虚拟蜜网的网络攻防实验环境**
- 5. 网络攻防的活动与竞赛形式**

虚拟化技术和云计算热潮

- ❑ **Google Trends:** 虚拟化和云计算查询热度趋势比较
- ❑ 虚拟化技术: **21**世纪以来的**IT**技术热点
- ❑ 云计算: 近年来**IT**领域最热门的词汇

virtualization 1.00 "cloud computing" 0.62





什么是虚拟化?

□ 虚拟化(**Virtualization**)

- 创建某种事物的虚拟(非真实)版本的方法和过程.

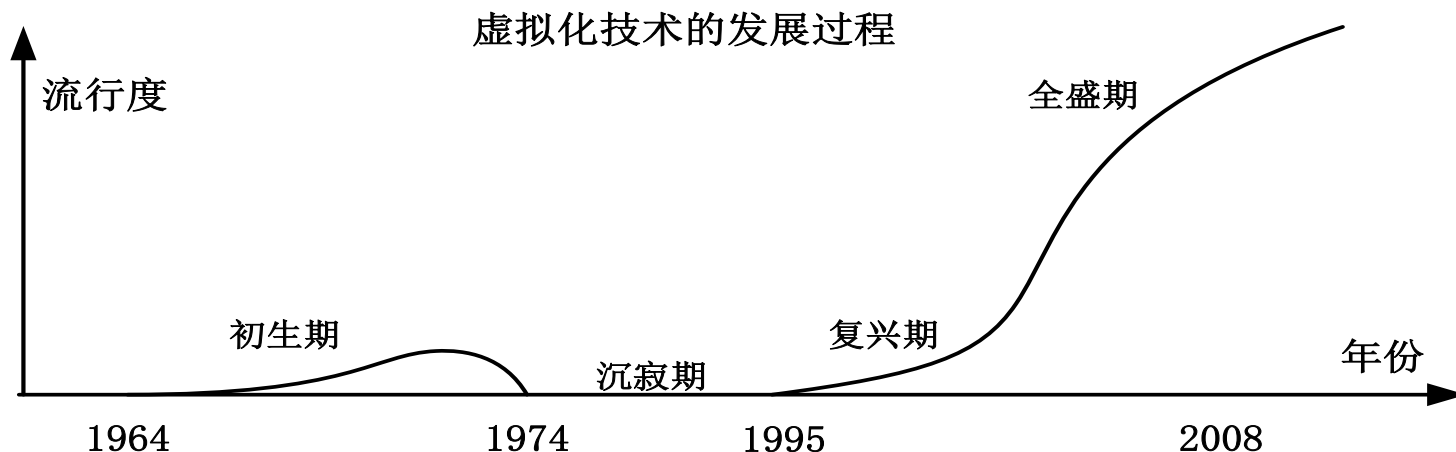
□ 虚拟(**Virtual**)

- 通常用于区分纯粹概念上的事物和拥有物理实体的事物.

□ 计算领域中的虚拟化[**whatis.com**] [**webopedia**]

- 创建某种计算资源的虚拟版本的方法和过程.
- 某种事物 → 某种计算资源
- 示例: 处理器, 内存, 磁盘, 完整的计算机, 网络等

虚拟化技术的提出与复兴



- 虚拟化技术Zero generation: 大型机虚拟化
 - 1964-1973: IBM mainframes (CP-40, M44/44X, S/360, CP-67, CP/CMS, S/370, VM/370) – 分时, 虚拟内存, run VM under VM, 对稀有的硬件资源进行多路复用, 支持运行多个作业程序.
 - 1974: IEEE Computer “Survey of Virtual Machine Research”
- 80s, 90s: 虚拟化技术消失, 由于现代多任务操作系统兴起和硬件价格飞速下降
- 1995-: 虚拟化技术的复兴 – Java VM (95), Virtual PC (Connectix, 97), VMware(98)



虚拟化技术的复兴：第一代虚拟化

- **第一代虚拟化技术：x86虚拟化 (1997-2005)**
 - 1997: Virtual PC for Macintosh by Connectix
 - 1998: Diane Greene和Mendel Rosenblum从Stanford创建VMware公司，申请专利技术
 - 1999: VMware Virtual Platform (Workstation) for x86
 - 2001: VMware GSX Server product (Server, 2006年免费发布)
 - 2003: MS并购Connectix (Virtual PC & Virtual Server), EMC并购VMware \$635 million
 - 第一代虚拟化技术：基于动态翻译技术的完全虚拟化



虚拟化技术的复兴：第二代虚拟化

- 第二代虚拟化技术：硬件/操作系统支持的虚拟化技术(05-)
- 硬件支持虚拟化技术-**native virtualization**
 - 2005: Intel在芯片中开始支持虚拟机 IVT (Vanderpool/Silverdale)
 - 2006: AMD在芯片中开始支持虚拟机 AMD-V (Pacifica)
- 操作系统支持虚拟化技术-**paravirtualization**
 - 2002: Denali by Washington U.
 - 2003: Xen by XenSource (from U. of Camb.)
 - 2005: Virtual Machine Interface by VMware
 - 2008: XenSource is also developing a compatibility layer for MS Windows Server 2008
- 虚拟基础设施
 - 2005-: Virtual Infrastructure by VMware

计算机系统最重要的三个接口

□ **ISA:** 指令集架构

- Interface 3: 系统ISA, OS可见, 用于管理硬件
- Interface 4: 用户ISA, 应用程序可见

□ **ABI:** 应用程序二进制接口

- Interface 2: 系统调用接口
- Interface 4: 用户ISA

□ **API:** 应用程序编程接口

- Interface 1: 高级编程语言库函数调用
- Interface 4: 用户ISA

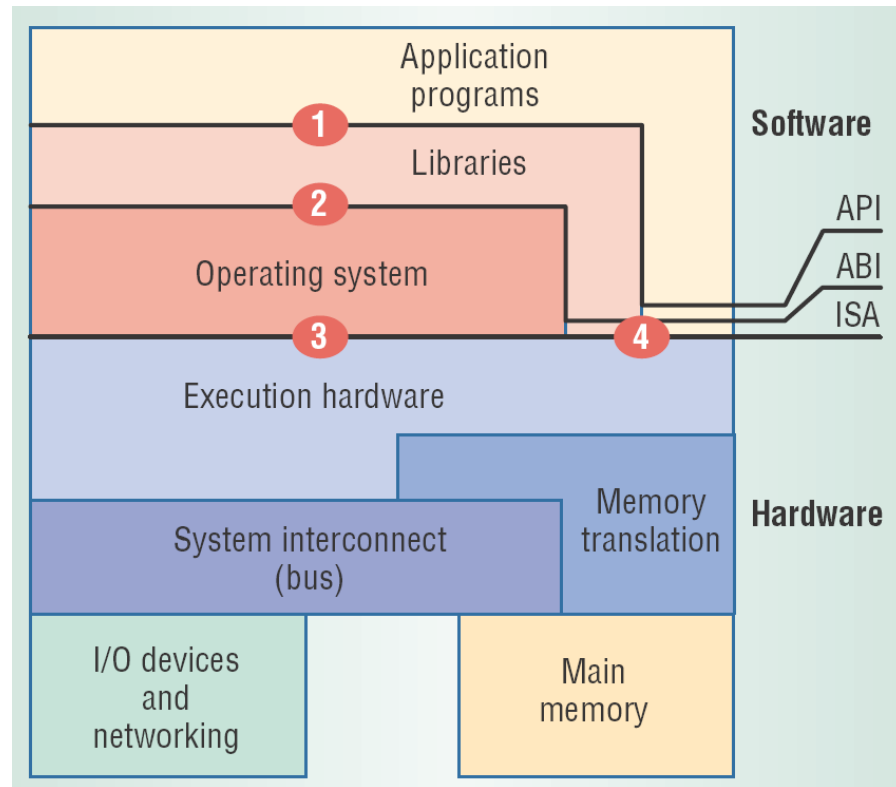


Figure: Computer System Architecture



什么是虚拟机？

□ 什么是虚拟机？

- 机器(“machine”)的虚拟版本

□ 那什么是机器“Machine”？

□ 从一个进程的角度定义机器

- 一个逻辑内存地址空间；用户级的指令和寄存器；I/O（仅通过操作系统系统调用可见）
- 实际上，ABI接口定义了进程角度所看到的机器；API接口定义了一个高级编程语言程序所看到的机器。

□ 从操作系统的角度定义机器

- 底层硬件特性定义了机器。
- ISA提供了操作系统和机器之间的接口。

进程级虚拟机和系统级虚拟机

□ 进程级虚拟机

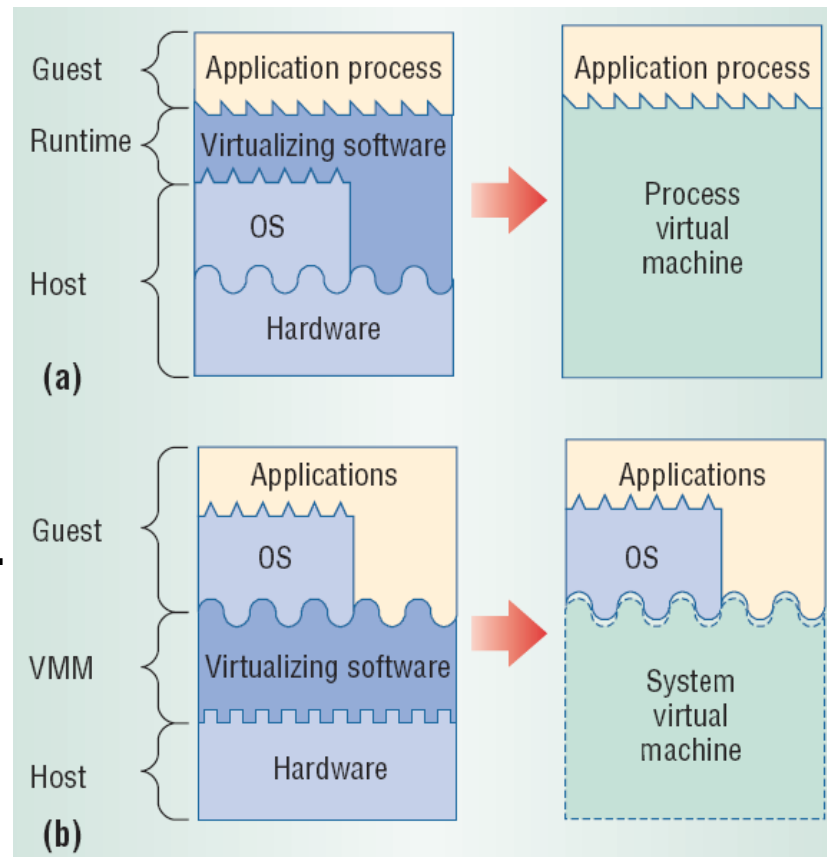
- 进程级虚拟机是执行单一进程的虚拟平台。
- Java VM, FVM Sandbox, etc.

□ 系统级虚拟机

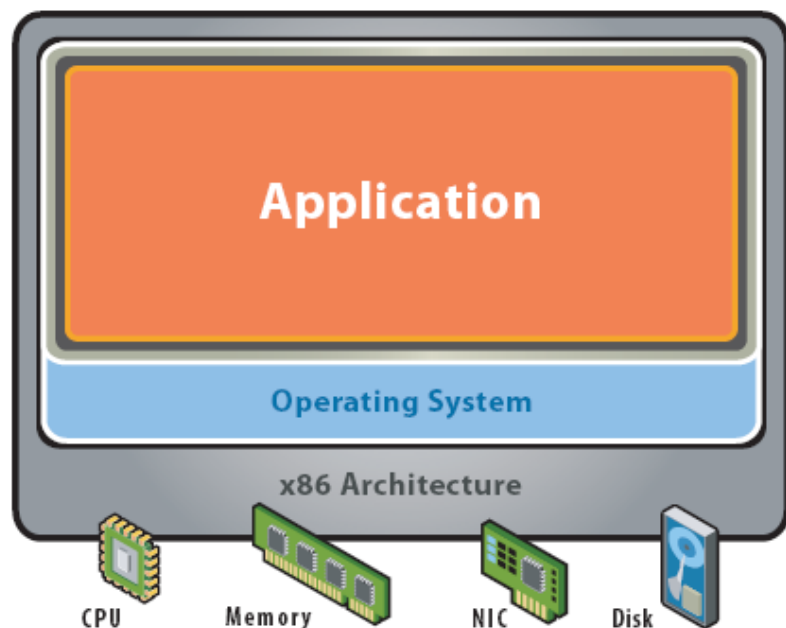
- 系统级虚拟机提供了支持操作系统和上层众多应用进程的一个完整、持久稳固的系统环境。
- VMware, Qemu, etc.

□ 基本概念

- guest, host, runtime, VMM

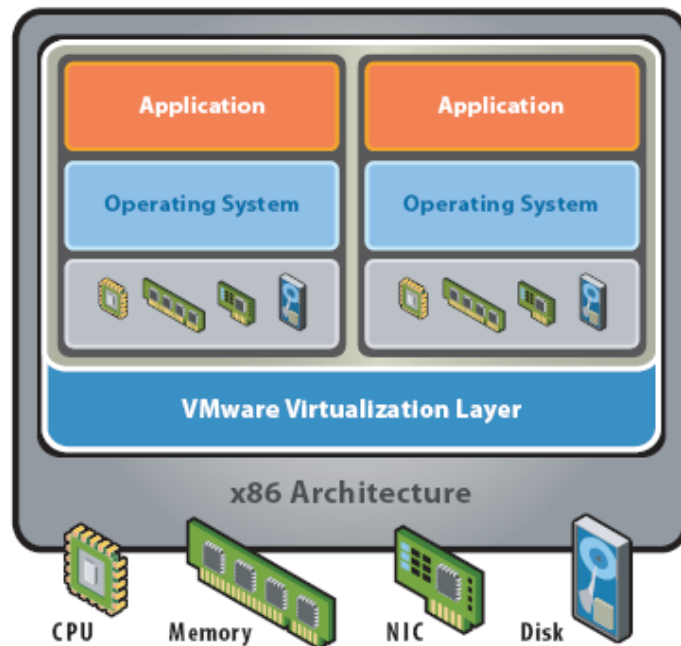


系统级虚拟机



Before Virtualization:

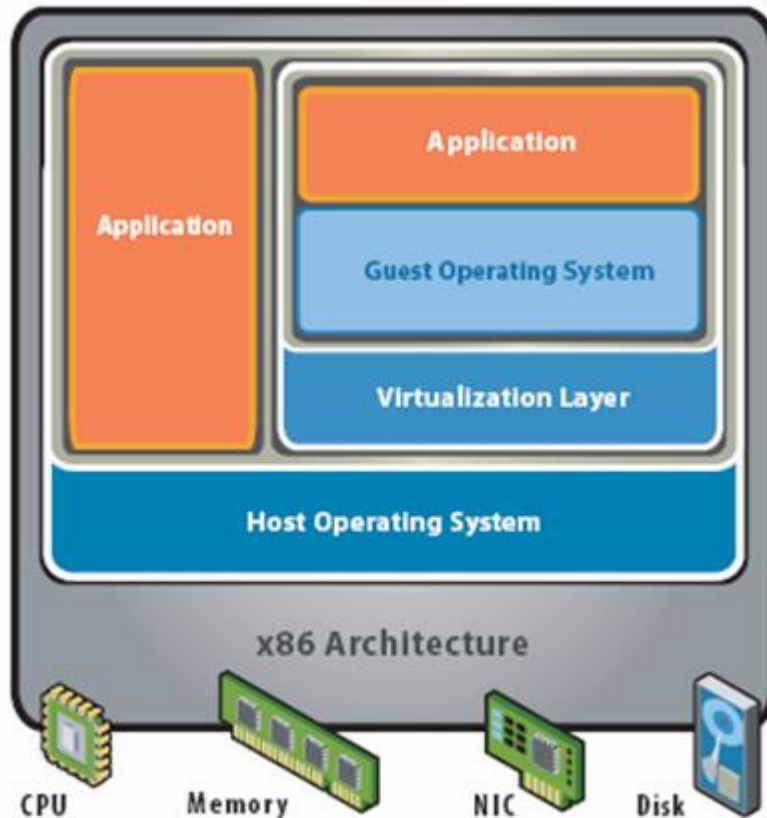
- Single OS image per machine
- Software and hardware tightly coupled
- Running multiple applications on same machine often creates conflict
- Underutilized resources
- Inflexible and costly infrastructure



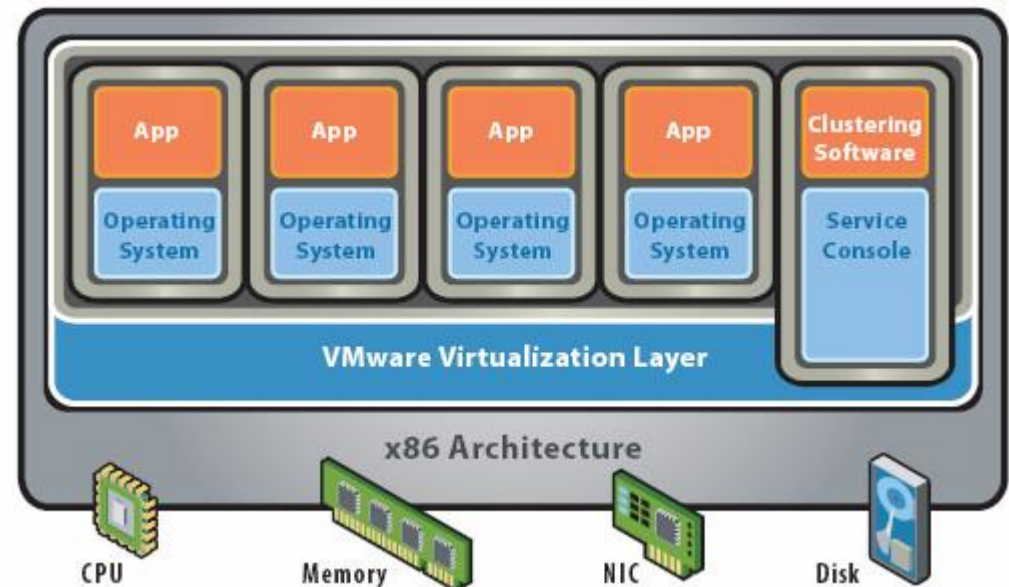
After Virtualization:

- Hardware-independence of operating system and applications
- Virtual machines can be provisioned to any system
- Can manage OS and application as a single unit by encapsulating them into virtual machines

Hosted VS. Hypervisor



Hosted VM



Hypervisor VM



系统级虚拟机实现需求和目标

□ 系统级虚拟机实现需求

- 向Guest OS提供与真实硬件相类似的硬件接口
- 硬件接口: CPU, Memory, I/O (Disk, Network, 外设)

□ 系统级虚拟机实现目标

- 兼容性: 具备运行历史遗留软件的能力
- 性能: 较低的虚拟化性能开销
- 简单性: 支持安全隔离 (没有/很少安全缺陷), 可靠性 (不失效)
- 多种不同技术, 分别提供不同的设计平衡



CPU虚拟化技术

□ CPU 架构可虚拟化:

- 如果支持基础的虚拟化技术——直接执行(direct execution)

□ 直接执行

- 在VMM保持对CPU的最终控制权前提下，能够让虚拟机中的指令直接在真实主机上运行
- 实现直接执行需要：
 - 虚拟机特权级和非特权级代码：CPU的非特权模式执行
 - VMM：CPU特权模式执行
 - 虚拟机执行特权操作时：CPU traps到VMM，在模拟的虚拟机状态上仿真执行特权操作

□ 提供可虚拟化的CPU体系框架的关键

- 提供trap semantics,使得VMM可以安全的、透明地、直接的使用CPU执行虚拟机.

CPU虚拟化的挑战

- ❑ 大部分modern CPU 并不支持可虚拟化, 如x86
- ❑ 需直接访问内存和硬件的操作系统特权代码必须在Ring 0执行
- ❑ CPU虚拟化必须在Guest OS下面添加VMM(Ring 0)
- ❑ 一些关键指令在非Ring 0权限级执行具有不同语义: 不能有效虚拟化, 如POPF指令
- ❑ 非特权级指令可以查询CPU的当前特权级, x86并不trap这些指令

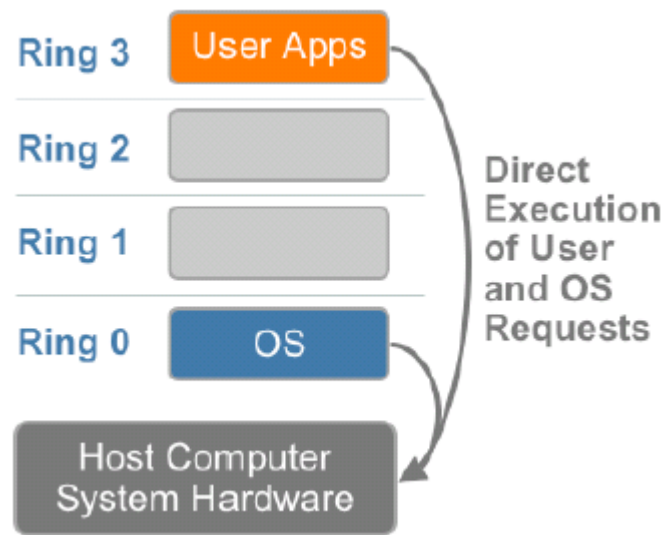


Figure: x86 privilege level architecture without virtualization

CPU虚拟化技术：动态代码翻译

- 结合直接执行和动态代码翻译
 - 运行普通程序代码的CPU模式可虚拟化：直接运行
 - 保证高性能
 - 不可虚拟化的特权级CPU模式：代码翻译器
 - 快速：相同ISA架构时，较低延迟
 - 动态：paravirtualization(静态)
 - 兼容：对Guest OS全透明，可以运行无需修改的历史遗留软件
- 动态代码翻译技术是无需硬件和OS支持实现对特权指令虚拟化唯一选择。

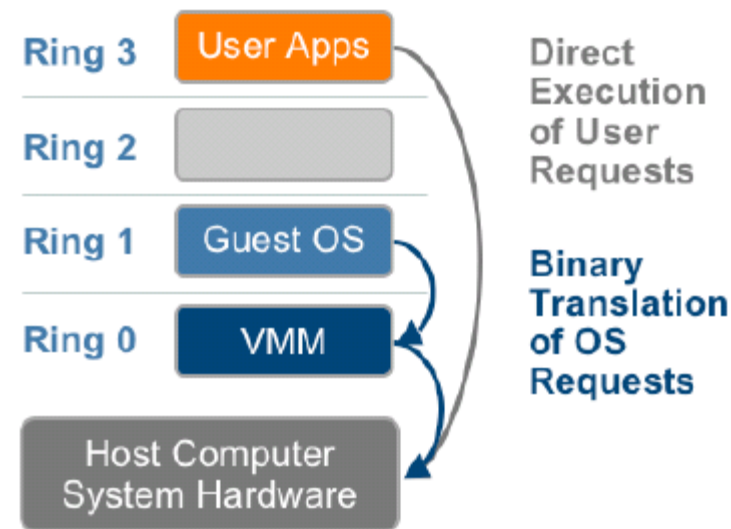


Figure: the binary translation approach to x86 virtualization

CPU虚拟化技术: Paravirtualization

□ Paravirtualization

- alongside virtualization
- OS支持的虚拟化
- VMM设计者需要定义虚拟机接口, 将不可虚拟化的指令替换为可虚拟化/可高效直接执行的等价指令
- 优势: 消除trap等虚拟化overhead, 高效
- 弱势: 不兼容, 需要修改操作系统, 对商业OS第三方无法移植

□ Xen, Windows Svr 2008, VMware Virtual Machine Interface

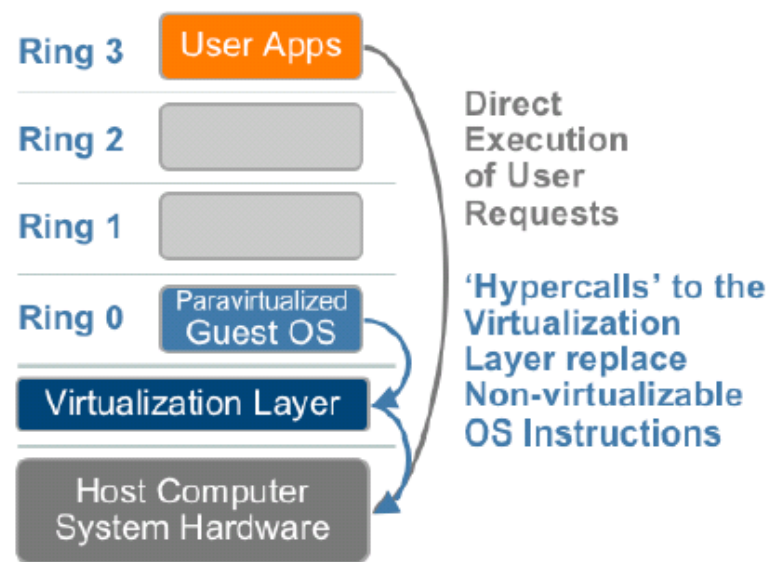


Figure: the paravirtualization approach to x86 virtualization

CPU虚拟化技术: Native Virtualization

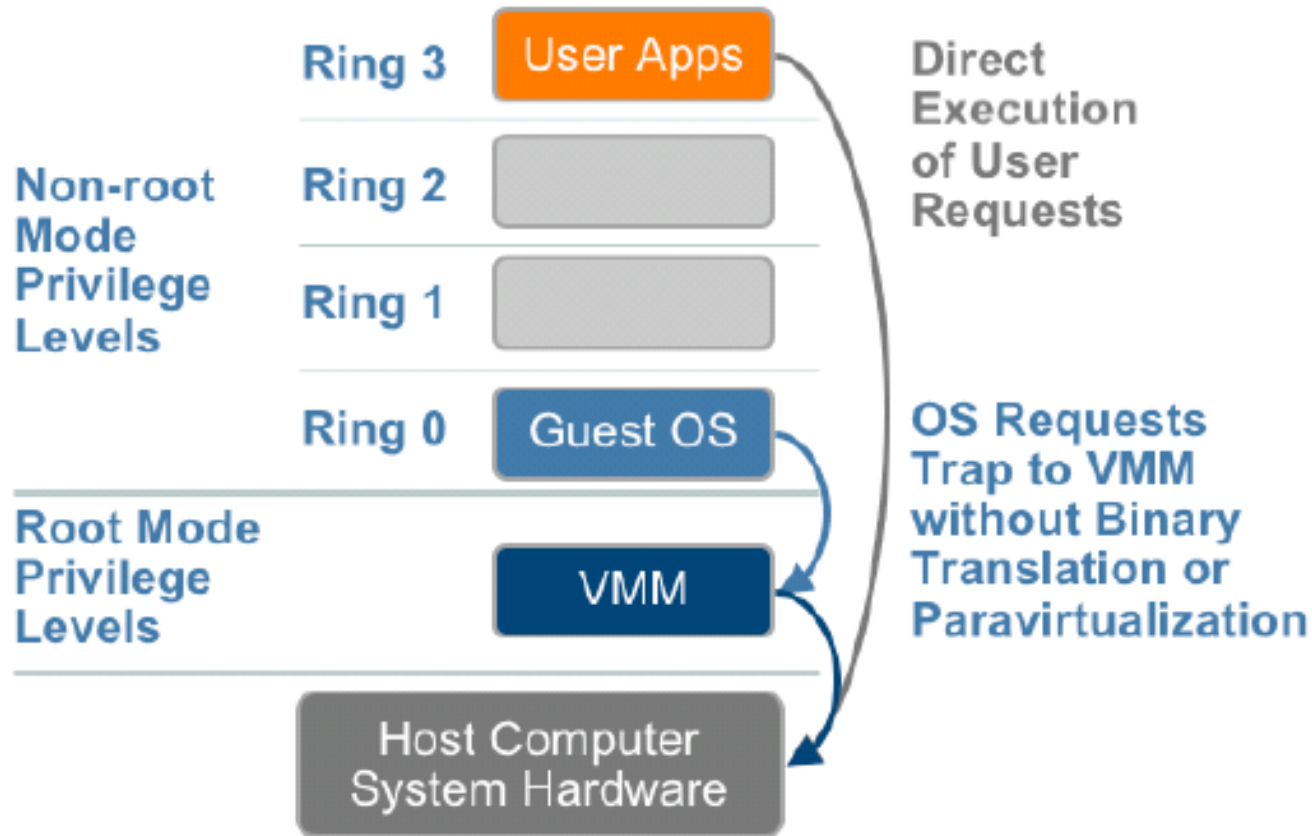


Figure: the native virtualization approach to x86 virtualization



CPU虚拟化技术: Native Virtualization

- 可虚拟化CPU架构
 - 随着虚拟化技术复兴, 硬件厂商快速跟进并推出简化虚拟化技术的CPU新特性
 - Intel Virtualization Technology (VT-x)
 - AMD's AMD-V
- 针对特权代码的虚拟化
 - 在Ring 0之下增加一个新的root mode (VMM)
 - 特权代码会自动trap至hypervisor, 无需paravirtualization或动态代码翻译
 - guest state存储于Virtual Machine Control Structures (VT-x) / Virtual Machine Control Blocks (AMD-v)
 - 弱势: 较高的hypervisor到guest的转换延迟
 - VMware使用场景受限 (64-bit guest support), Xen 3.0

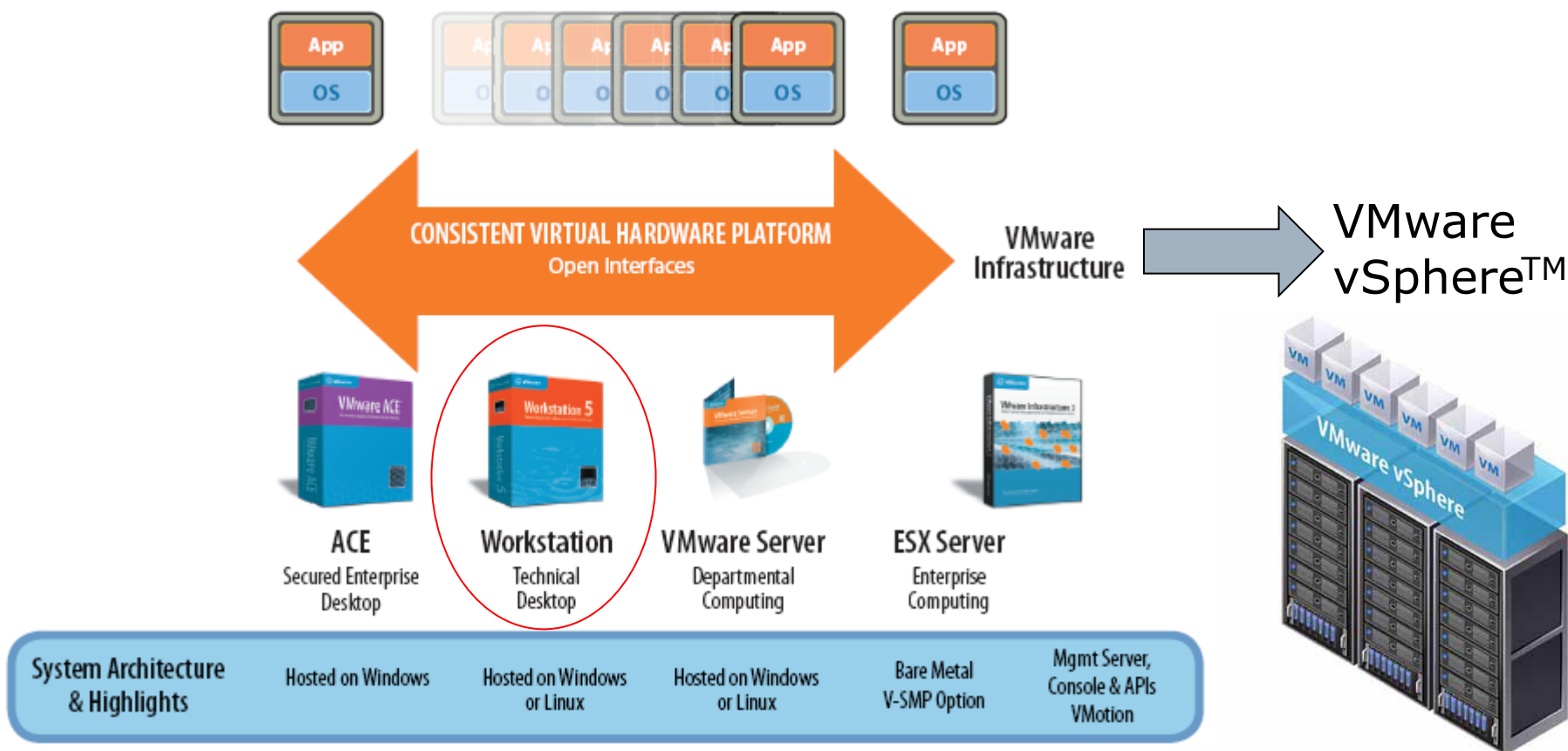
CPU虚拟化技术：小结

| | 动态代码翻译 | Paravirtualization | Native Virtualization |
|-----|--------|--------------------|-----------------------|
| 兼容性 | 优秀 | 差 | 优秀 |
| 性能 | 好 | 优秀 | 一般 |
| 简单性 | 差 | 一般 | 好 |

□ 三种现有的CPU虚拟化技术

- 动态代码翻译, Paravirtualization, Native Virtualization
- 各种技术具有独特的优势和弱势
- CPU虚拟化技术发展趋势
 - 更多, 更好的硬件支持: 达到更好的性能
 - 更多, 更好的操作系统支持: 提供标准化的虚拟机接口, 提升paravirtualization技术的兼容性
 - 多种技术模式的灵活选择架构, 根据环境选择合适的技术

VMware的产品线和技术解决方案



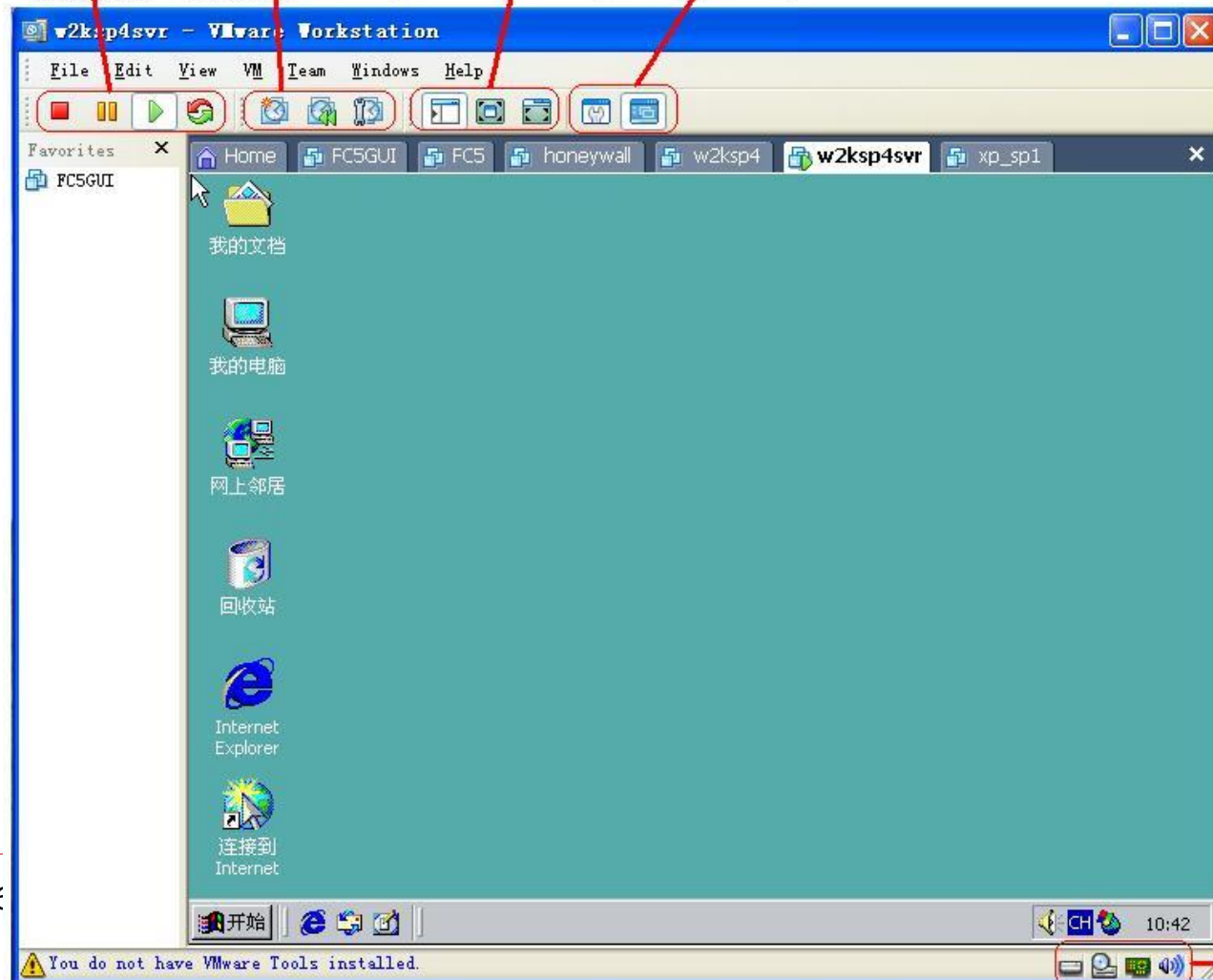
VMware Workstation

控制虚拟机的
停机、暂停、
启动、重启等行为

新建 snapshot、恢复到
最新的 snapshot、管理
snapshot

VMware窗口布局调整

在虚拟机内部系统与
虚拟机设置之间界面
切换



硬件工作状态及控制

VMware虚拟机的虚拟硬件设置

□ CPU

- 虚拟CPU(单核/双核)

□ 内存

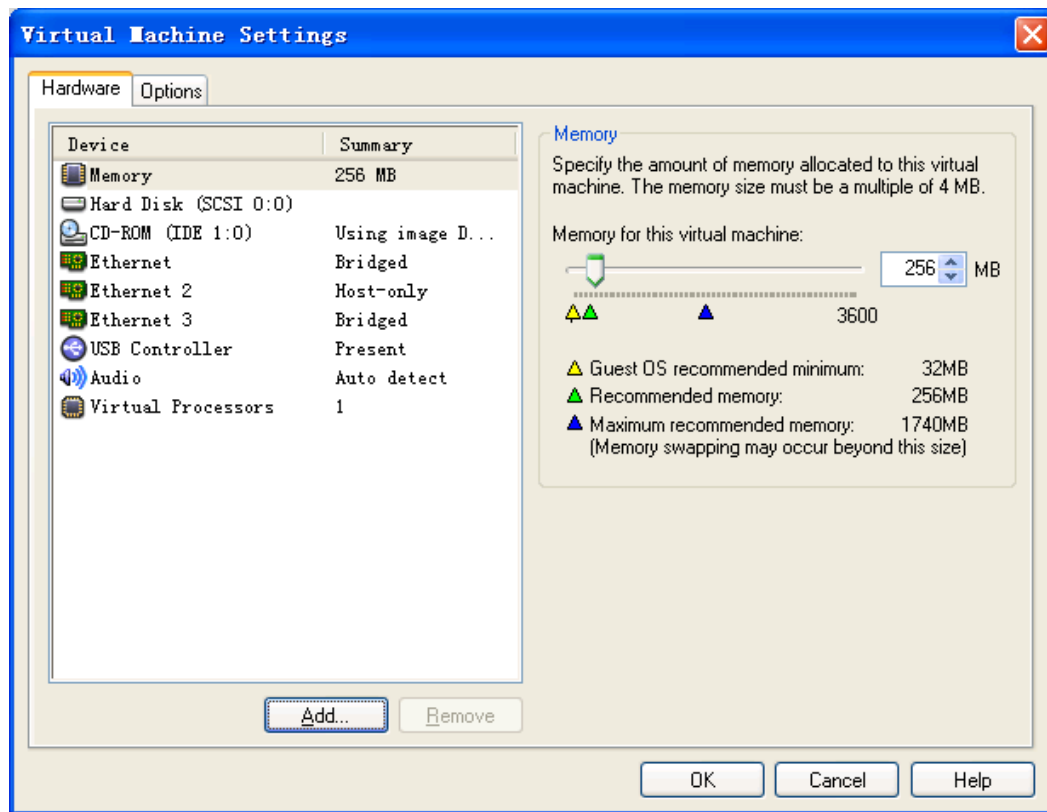
- 从宿主物理内存分配

□ 硬盘

- 宿主文件系统中文件

□ 外设

- 网卡
- 光驱
- **USB**
- 声卡
- ...



VMware支持的虚拟网络拓扑模式

□ VMware虚拟网卡支持三种基本拓扑连接

■ 桥接模式(bridged)

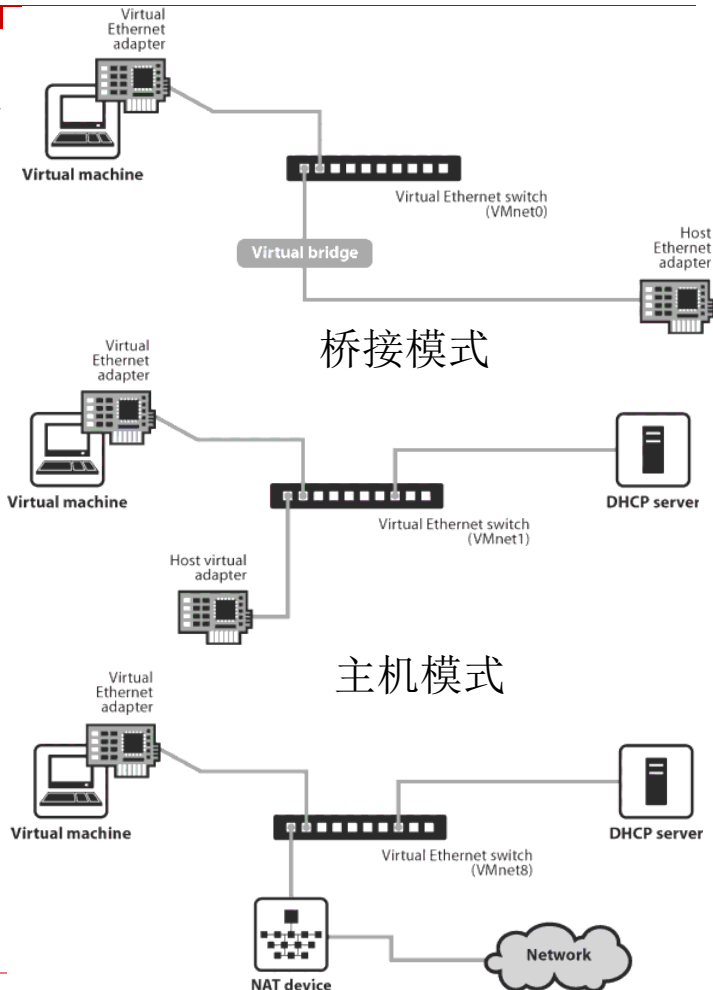
- 虚拟的透明网桥
- 虚拟机网卡对外可见，可直接绑定外网IP

■ 主机模式(host-only)

- 虚拟交换机

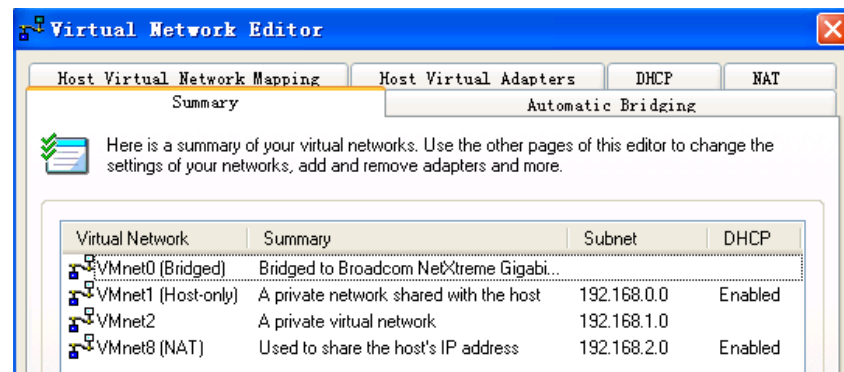
■ 网络地址转换模式(NAT)

- 虚拟机不能直接连接外网
- 由宿主进行网络地址转换后访问外网



VMware的虚拟网络管理

- VMware for Windows版本
 - Edit | Virtual Network Settings
 - ...



- VMware for Linux版本
 - vmware-config.pl

Configuring a bridged network for vmnet0.

Your computer has multiple ethernet network interfaces available: eth0, eth1, eth2. Which one do you want to bridge to vmnet0? [eth0] eth1

The following bridged networks have been defined:

. vmnet0 is bridged to eth1

Do you wish to configure another bridged network? (yes/no) [no] yes

Configuring a bridged network for vmnet2.

Your computer has multiple ethernet network interfaces available: eth0, eth2. Which one do you want to bridge to vmnet2? [eth0] eth2



上手实践 – Play with VMware

□ 安装VMware Workstation

- 1) 下载VMware Workstation软件
- 2) 安装VMware Workstation软件
- 3) 查看VMware的虚拟网卡和虚拟网络设置

□ 新建虚拟机，安装蜜网网关虚拟机镜像

- 1) 下载蜜网网关ROO的安装镜像
- 2) 新建虚拟机，分配资源
- 3) 安装蜜网网关ROO镜像
- 4) 做好虚拟机snapshot，挂起系统



云计算热潮

- 云计算(**Cloud Computing**)热潮的起源
 - 20世纪60年代
 - **John McCarthy**:计算将以一种公用事业方式提供
 - **Douglas Parkhill**: 《计算机公用事业的挑战》
 - 20世纪90年代
 - 电信公司:服务提供商和客户之间的分界点
- **Amazon 2006年推出 Amazon Web Service (AWS)**对公众提供效能计算服务
- **2007年开始, Google、IBM和其他机构大规模投入**到云计算研究与开发中, 形成云计算热潮



什么是云计算？

□ 流传已久的解释

- 用一朵云来表示互联网，“云计算”：基于互联网的新型计算方式
- 铺天盖地的解释和说法，让人无所适从

□ **NIST**对云计算的定义

- 云计算是一种能够通过网络以便利的、按需的方式获取计算资源的模式，这些资源来自一个共享的、可配置的资源池，并能够以最小化管理代价及与服务提供商的交互进行快速地获取与释放。

□ 五大关键要素

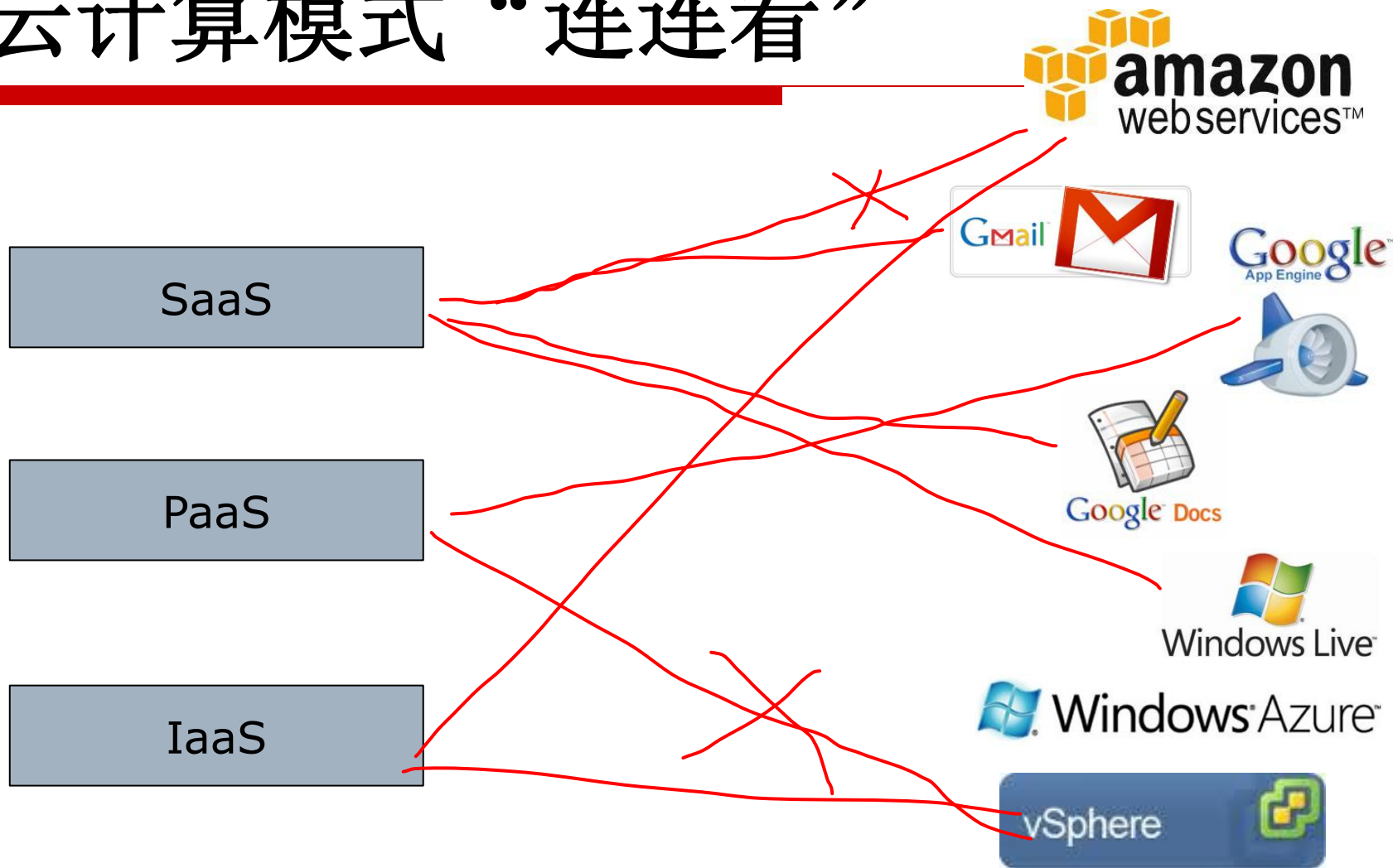
- 按需自助服务
- 通过宽带网络访问
- 资源池，多租户模式
- 快速伸缩性
- 可量化的服务



云计算模式的分类

- “云”计算的三大交付模式，称为**S-P-I**模式
- 软件即服务(**SaaS: Software as a Service**)
 - 在云基础架构中运行的商业应用
 - 交付给客户的是定制化软件
- 平台即服务(**PaaS: Platform as a Service**)
 - 在云基础架构中的可编程的运行平台
 - 交付给客户的是“云中间件”资源
- 基础设施即服务(**IaaS: Infrastructure as a Service**)
 - 在云基础架构中的处理、存储、网络和其他基础计算资源
 - 交付给客户的是基础计算资源

云计算模式“连连看”





云计算的四大部署模式

□ 私有云(**Private Cloud**)

- 单独地为一个组织所运营的
- 可以由组织自己管理或委托第三方管理

□ 公有云(**Public Cloud**)

- 提供给公众或一个大型工业企业
- 归一个出售云服务的组织所有

□ 社区云(**Community Cloud**)

- 由多个组织所共享的
- 支撑一个具有共享需求的社区

□ 混合云(**Hybrid Cloud**)

- 两个或多个云的混合，由标准化或私有技术联合绑定

私有云

- 为一个客户单独使用而构建的云基础设施
- 提供对数据、安全性和服务质量的最有效控制
- **2009年VMware推出了业界首款云操作系统VMware vSphere 4**



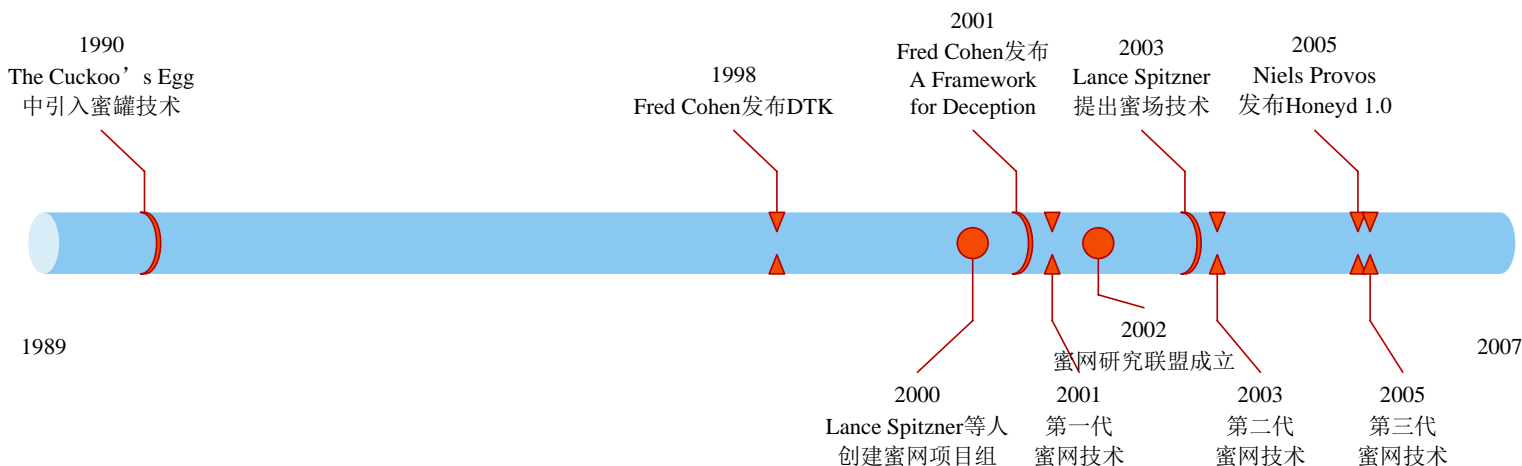


内容

- 1. 网络攻防实验环境**
- 2. 虚拟化技术与云计算热潮**
- 3. 蜜网(Honeynet)技术介绍**
- 4. 基于虚拟蜜网的网络攻防实验环境**
- 5. 网络攻防的活动与竞赛形式**

蜜罐(Honeypot)技术的提出

- 防御方尝试改变攻防博弈不对称性提出的一种主动防护技术
 - 蜜罐：一类安全资源，其价值就在于被探测、被攻击及被攻陷
 - “蜜罐公理”：无任何业务用途→任何蜜罐捕获行为都是恶意
 - 绕过攻击检测“NP难”问题
- 蜜罐技术的提出和发展



蜜罐技术—如何实施诱骗？

□ 欺骗环境(Pot)的构建：黑洞 VS. 模拟 VS. 真实

- 零交互式蜜罐：黑洞，没有任何响应
- 低交互式蜜罐—虚拟蜜罐：模拟网络拓扑、协议栈、服务 (Honeyd/Nepenthes)；模拟OS (Sandbox)
- 高交互式蜜罐
 - 物理蜜罐：完全真实的硬件、OS、应用、服务
 - 虚拟机蜜罐：模拟的硬件(VMWare)/真实的OS、应用、服务

□ 部署陷阱，诱骗攻击者(Honey)

- 守株待兔：安全漏洞—针对扫描式攻击
- 酒香也怕巷子深：散播陷阱信息，引诱攻击者 (Google Hacking HoneyPot, HoneyEmail)
- 重定向技术 (Honeyfarm)
- 主动出击：利用爬虫技术—客户端蜜罐(HoneyClawer 恶意网站监测)

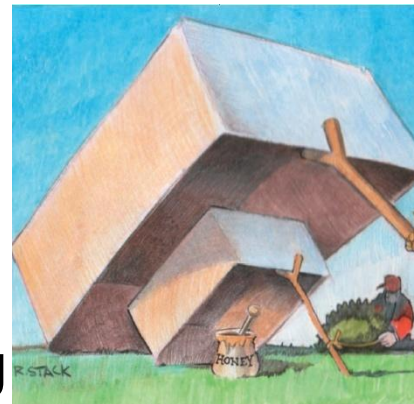
蜜罐技术—诱骗之后

❑ 欺骗环境的核心功能需求

- 数据控制
- 数据捕获
- 数据分析
- 欺骗环境的配置管理

❑ 欺骗与反欺骗的较量

- 欺骗环境伪装: 环境伪装/业务伪装
- 对欺骗环境的识别: **fingerprinting**
- **Anti-Honeypot, Anti-Anti-Honeypot, ...** — 更深一层的博弈问题





低交互式蜜罐技术

□ 低交互式蜜罐技术

- 具有与攻击源主动交互的能力
- 模拟网络服务响应，模拟漏洞
- 容易部署，容易控制攻击
- 低交互式—交互级别由于模拟能力而受限，数据获取能力和伪装性较弱，一般仅能捕获已知攻击

□ 低交互式蜜罐工具

- **iSink** – 威斯康星州立大学
- **Internet Motion Sensor** – 密歇根大学, **Arbor Networks**
- **Honeyd** – Google公司软件工程师**Niels Provos**
- **Nepenthes** – **Nepenthes**开发团队
- 商业产品: **KFSensor, Specter, HoneyPoint...**

高交互式蜜罐技术

□ 高交互式蜜罐技术

- 使用真实的操作系统、网络服务与攻击源进行交互
- 高度的交互等级—对未知漏洞、安全威胁具有天然的可适性，数据获取能力、伪装性均较强
- 弱势—资源需求较大，可扩展性较弱，部署安全风险较高

□ 虚拟机蜜罐 **VS.** 物理蜜罐

- 虚拟机(**Virtual Machine**)/仿真器(**Emulator**)技术
- 节省硬件资源、容易部署和控制、容易恢复、安全风险降低

□ 高交互式蜜罐工具

- **Honeynet** – 蜜网项目组 (**The Honeynet Project**)
- **HoneyBow** (基于高交互式蜜罐的恶意代码捕获器) – 北京大学狩猎女神项目组
- **Argos** – 荷兰阿姆斯特丹大学 (**Vrije Universiteit Amsterdam**) 欧盟分布式蜜罐项目(**NoAH**)参与方



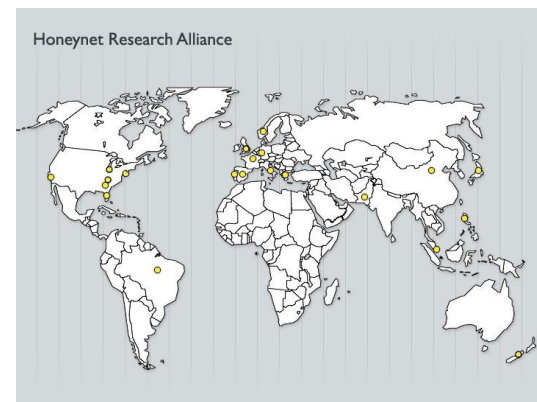
蜜网技术的提出—从蜜罐到蜜网

- 低交互式(虚拟)蜜罐→高交互式(虚拟机/物理)蜜罐
 - 使用真实的网络拓扑，操作系统和应用服务
 - 为攻击者提供足够的活动空间
 - 能够捕获更为全面深入的攻击信息
- 单点蜜罐工具→蜜网体系框架
 - 体系框架中可包含多个蜜罐
 - 同时提供核心的数据控制、数据捕获和数据分析机制
 - 构建一个高度可控的攻击诱骗和分析网络

蜜网项目组(The Honeynet Project)

□ 全球非赢利性研究机构

- 1999年起源于邮件组WarGames
- 2000-今: 19 Chapters, 50+ FMs
- 狩猎女神项目组—China Chapter



□ 目标

- 探寻黑客界的攻击工具、战术和动机，并分享所得

□ 著名成员

- 创始人/CEO: Lance Spitzner
- Fyodor, Dave Dittrich, Niels Provos, Anton Chuvakin, Ron Dodge ...

蜜网技术的发展

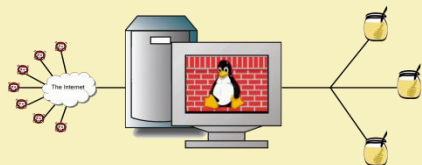
原理

- 蜜罐系统没有任何业务用户和用途
- 所有在蜜网中的网络行为都是可疑的
- 黑客认为蜜罐系统是业务网络中的一部分
- 蜜罐系统被黑客扫描、攻击及攻陷
- 网络流监听工具记录蜜网中所有的网络流
- 对从被攻陷蜜罐发起的向外攻击进行阻断

1999-2005

2005-2007

2007-

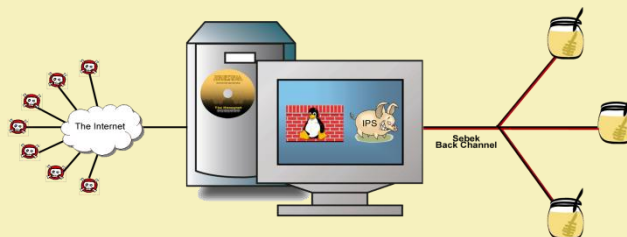


配置

- Lance Spitzner在1999年提出并实现
- 在Linux操作系统上构建
- 蜜罐主机位于一个3层路由器后面
- 防火墙限制往外连接
- 网络流抓捕工具记录所有的数据包

困难

- 攻击可以绕过防火墙
- 只能抓取和监听明文通讯
- 需要多个不同类型工具一起工作
- 难以构建、配置和部署
- 运营和维护需要花费大量的时间
- 没有内嵌的数据分析功能



蜜网网关光盘

- 可启动的Linux光盘可在5分钟内完成蜜网网关的安装
- 集成了数据捕获、数据控制和分析的所有工具
- 提供蜜网部署的标准化工具

数据捕获

- 每个进出蜜网的数据包都被记录
- IDS提供对攻击的高层摘要视图
- Sebek将记录在蜜罐系统中的攻击行为，上传到蜜网网关

数据控制

- 由2层防火墙进行网络连接数限制
- 网络入侵防御系统阻断向外发起的攻击

数据分析

- 所有捕获的数据均可通过一个Web接口进行查看
- 通过Email报警通知管理员蜜网中的可疑行为



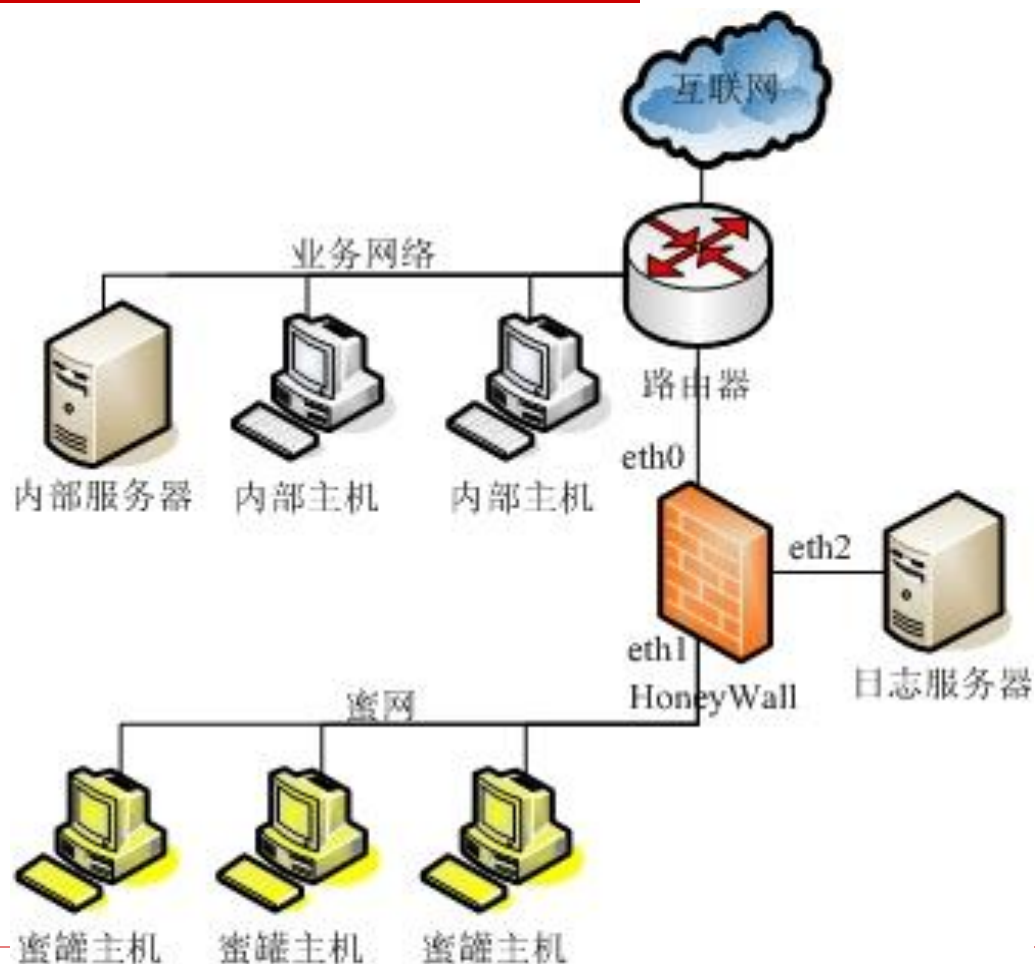
分布式蜜网

- 由世界各国组织机构部署多个蜜网
- 通过集中点对分布式蜜网进行管理
- 收集到的攻击数据汇总到集中数据库
- 通过蜜网网关光盘进行实现和部署
- 目前正在进行积极研发

蜜网项目组

- 来自世界各国的信息安全专家
- 研发开源蜜网技术和工具
- 发布多本著作及大量学术论文
- 更多信息: <http://www.honeynet.org>

蜜网体系框架





蜜网技术核心机制

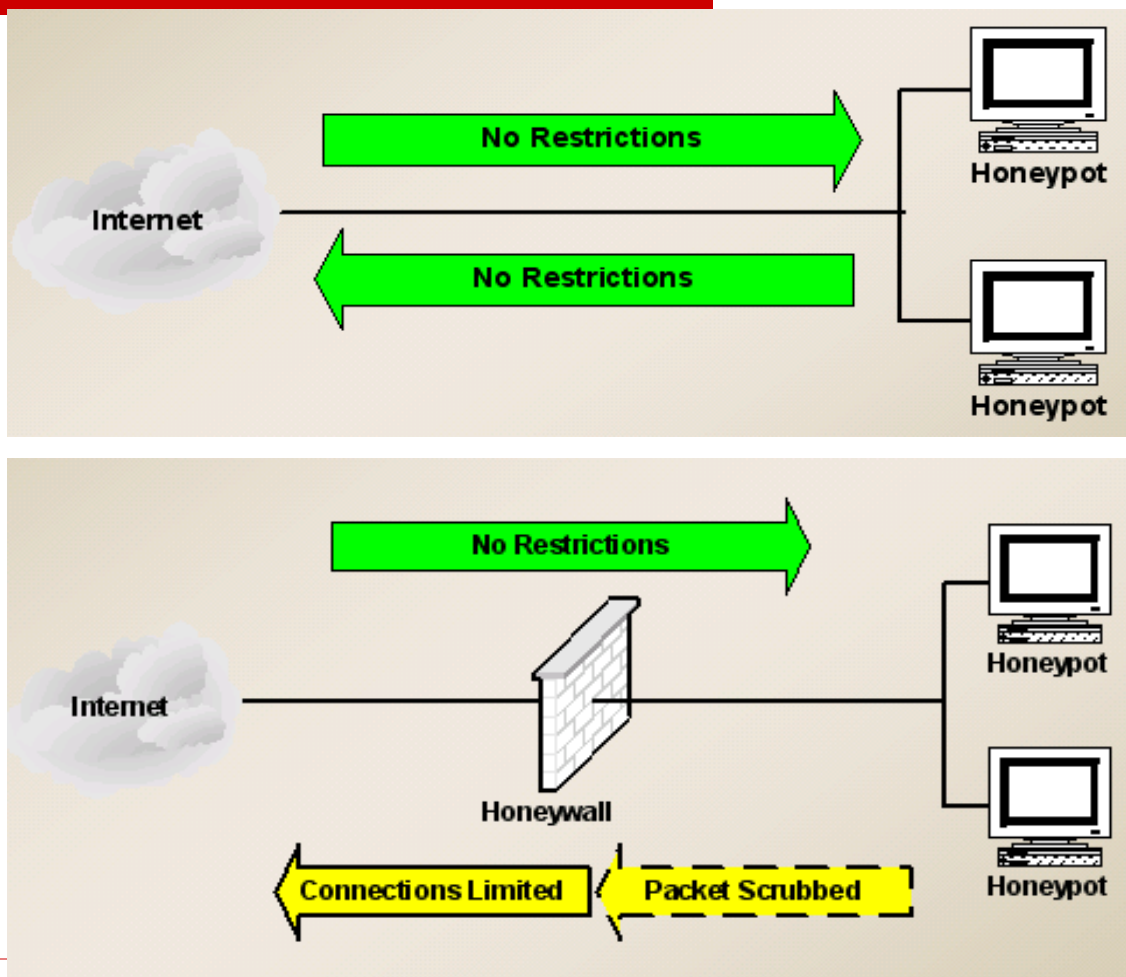
- 数据控制机制
 - 防止蜜网被黑客/恶意软件利用攻击第三方
- 数据捕获机制
 - 获取黑客攻击/恶意软件活动的行为数据
 - 网络行为数据—网络连接、网络流
 - 系统行为数据—进程、命令、打开文件、发起连接
- 数据分析机制
 - 理解捕获的黑客攻击/恶意软件活动的行为
- 配置和管理机制
 - 有效的配置和管理蜜网环境



第三代蜜网

- 第二代蜜网技术—**2003年Eeyore**光盘概念验证性实现
- 第三代蜜网技术—**2005年5月发布ROO**蜜网网关光盘
 - 从**LiveCD**到安装光盘—更易部署和定制
 - 基于最小化版本的**Fedora Core 3**—更安全，**yum**自动化升级
 - 多种配置机制(**hwctl, menu, walleye**)—更容易配置
 - 提供数据分析工具**Walleye**—更加易用

数据控制





IPTables实现连接数限制

□ 网络连接数限制

- 对内部发起到外部的网络连接进行数量限制
- **TCP/UDP/ICMP/other IP**
- **/etc/init.d/rc.firewall**通过**IPTables**进行配置实现

□ **Roach Motel Mode** — “黑店模式”

- “反接”防火墙，只进不出
- 允许外部发起到内部的网络连接
- 阻断内部发起到外部的网络连接

攻击数据包过滤

□ Snort_inline: NIPS

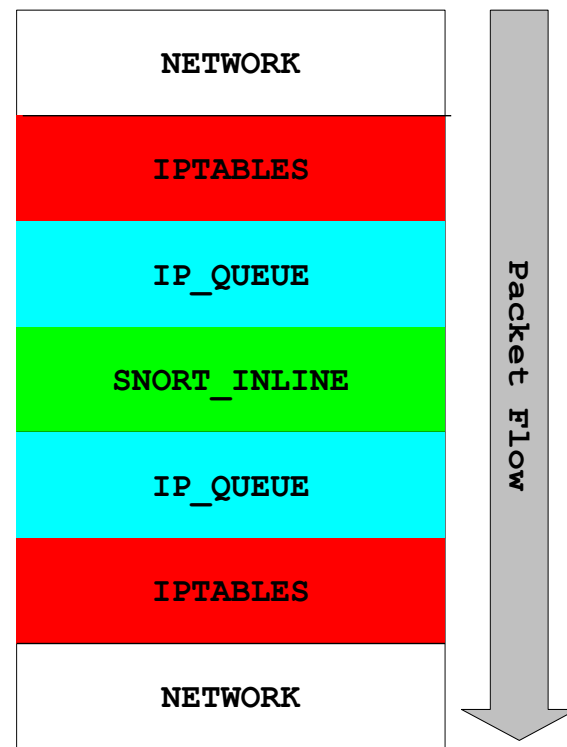
- iptables -A FORWARD -i \$LAN_IFACE -m state --state RELATED,ESTABLISHED -j QUEUE

- 过滤模式:

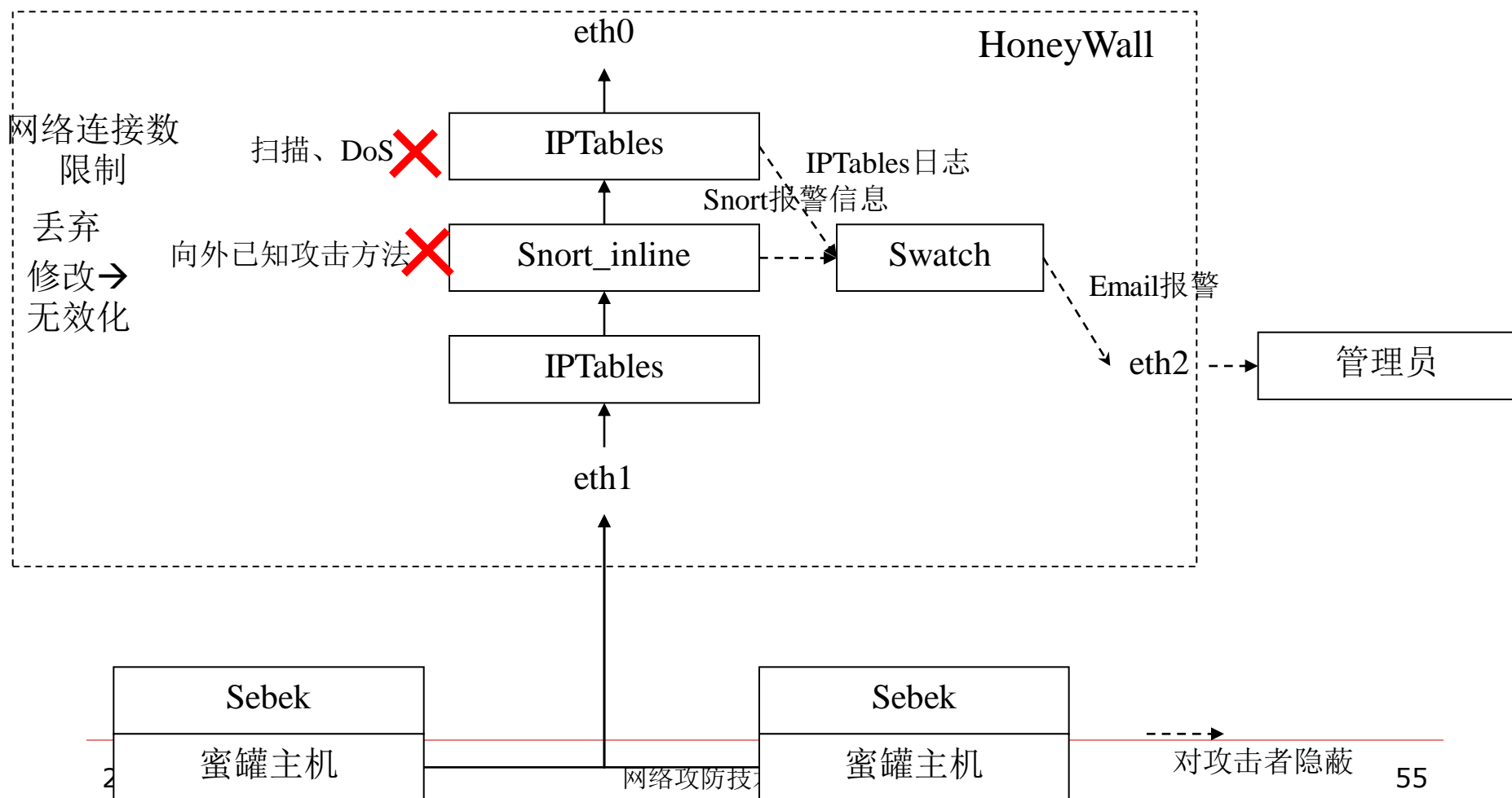
- 丢弃(**Drop**): 简单丢弃攻击数据包
- 拒绝(**Reject**): 丢弃并发RST
- 替换(**Replace**): 替换攻击数据内容

- **Replace**规则示例

```
alert ip $HONEYNET any -> $EXTERNAL_NET any
(msg:"SHELLCODE x86 stealth NOOP"; sid:651;
 content:"|EB 02 EB 02 EB 02|";
 replace:"|24 00 99 DE 6C 3E|";)
```



数据控制机制图示





数据捕获机制

□ 快数据通道

■ 网络行为数据 – **HoneyWall**

- 网络流数据: **Argus**

- 入侵检测报警: **Snort**

- 操作系统信息: **p0f**

■ 系统行为数据 – **Sebek@Honeypot**

- 进程、文件、命令、键击记录

- 以**rootkit**方式监控**sys_socket, sys_open, sys_read**系统调用

■ 网络行为与系统行为数据之间的关联 – **sys_socket**

□ 慢数据通道

■ 网络原始数据包 – **tcpdump@HoneyWall**



网络行为数据

□ Argus网络流捕获工具

- 网络连接5元组<**sip, sport, dip, dport, proto**>+连接统计信息
- Thu 12/29 06:40:32 S tcp 132.3.31.15.6439 -> 12.23.14.77.23 CLO
- <http://qosient.com/argus/>

□ Snort网络入侵检测工具

- 给出网络流中已知攻击的报警信息
- www.snort.org

□ P0f被动操作系统识别工具

- 被动监听网络流，通过不同操作系统协议栈的不同实现（指纹）识别网络连接双方的操作系统
- <http://lcamtuf.coredump.cx/p0f.shtml>

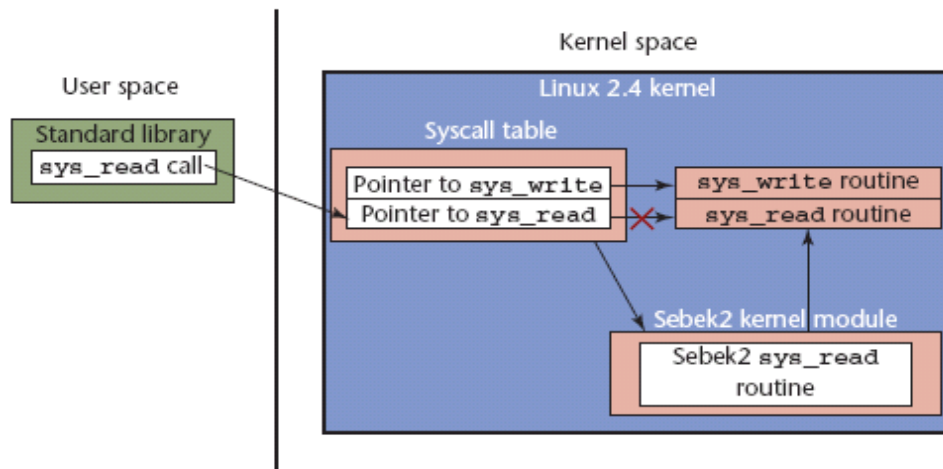
系统行为数据-Sebek

□ Sebek工作原理

- 劫持Linux系统调用-**sys_read, sys_open, sys_socket, ...**
- 劫持Win32核心API-**ZwOpenFile, ZwReadFile, ZwEnumerateKey, ZwSecureConnectPort**等**13个**核心API

□ Sebek版本

- **3.2.0 for Linux**
- **3.0.0 for *BSD**
- **3.0.4 for Win32**
- ...





Sebek的隐藏机制

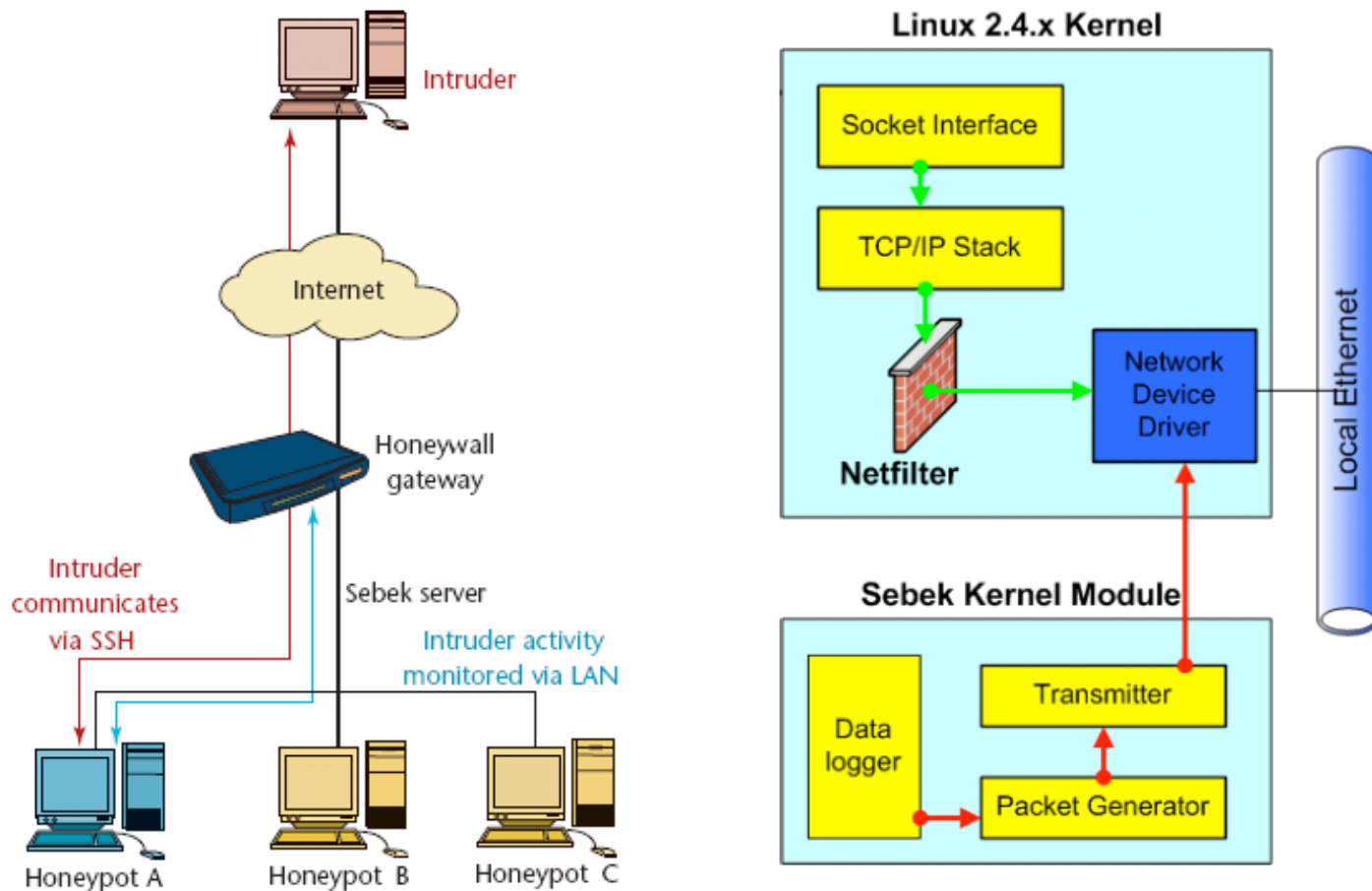
□ Sebek Linux Client

- 采用一种**Rookit**隐藏机制
- **Sebek**: 可装载内核模块(**LKM: loadable kernel module**)
- **Cleaner**: 另一内核模块, 从内核模块列表中清除**Sebek**内核模块

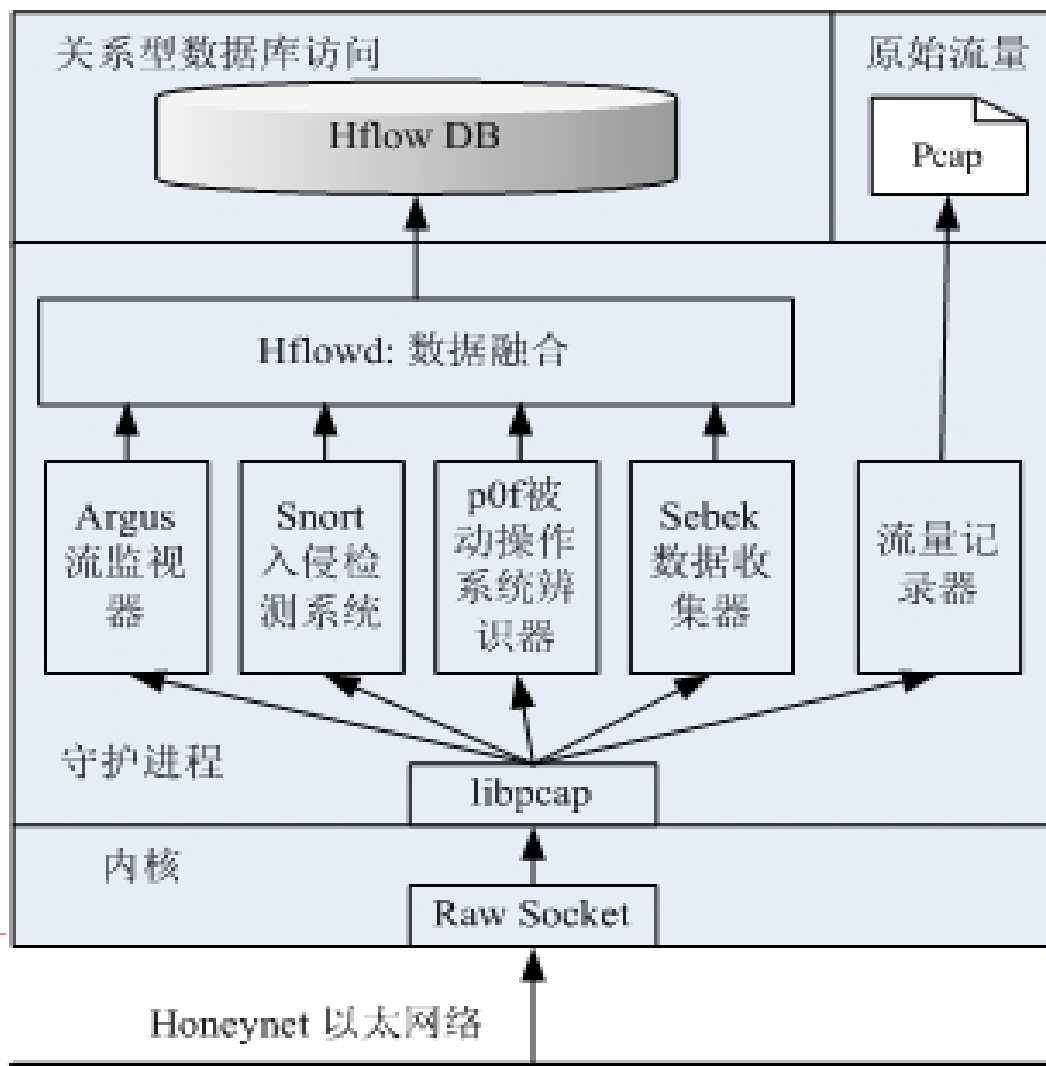
□ Sebek Win32 Client

- 实现为一个系统内核驱动, 进行隐藏
- 但通过遍历**PsLoadedModuleList**可发现

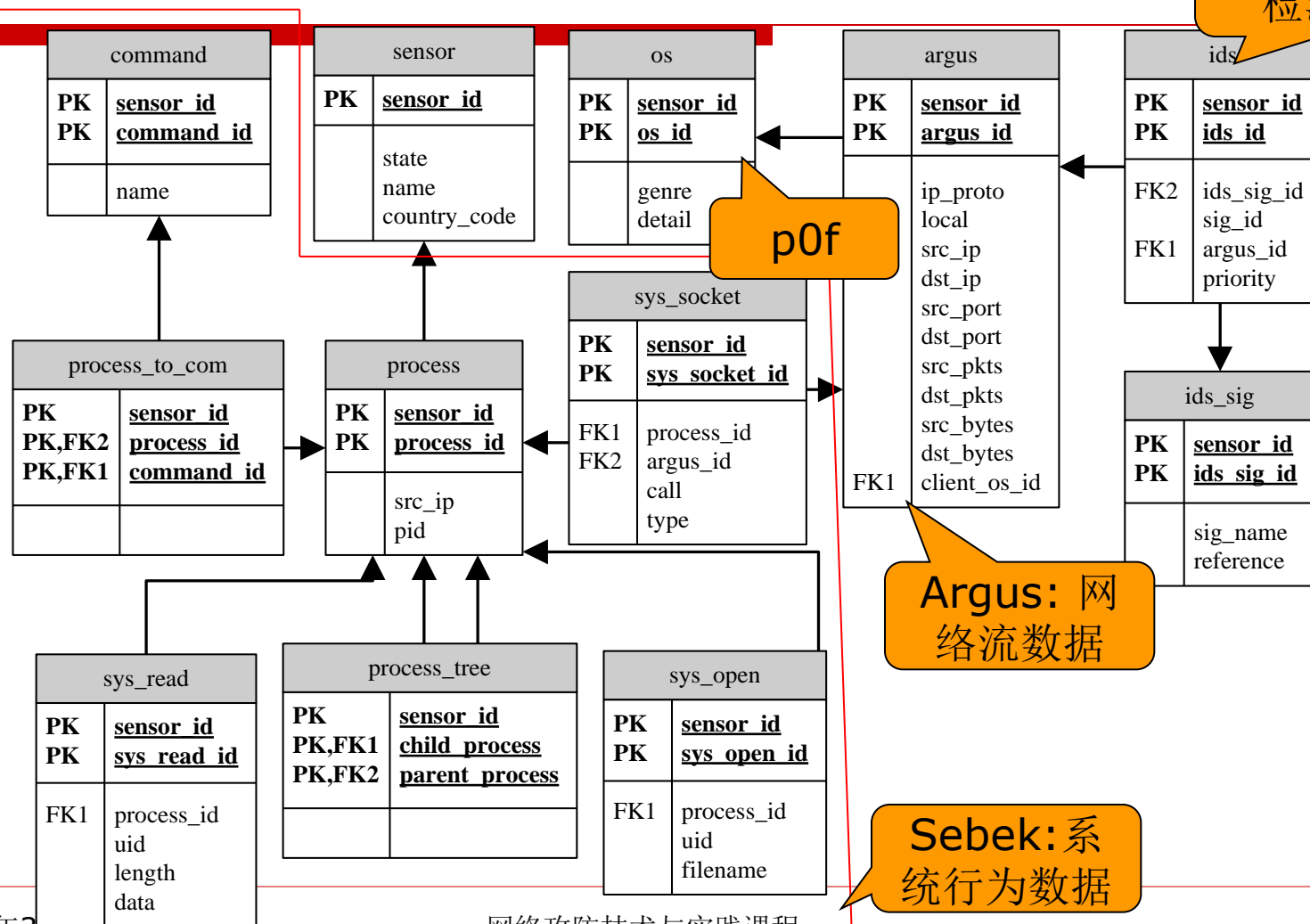
Sebek系统行为数据隐蔽上传



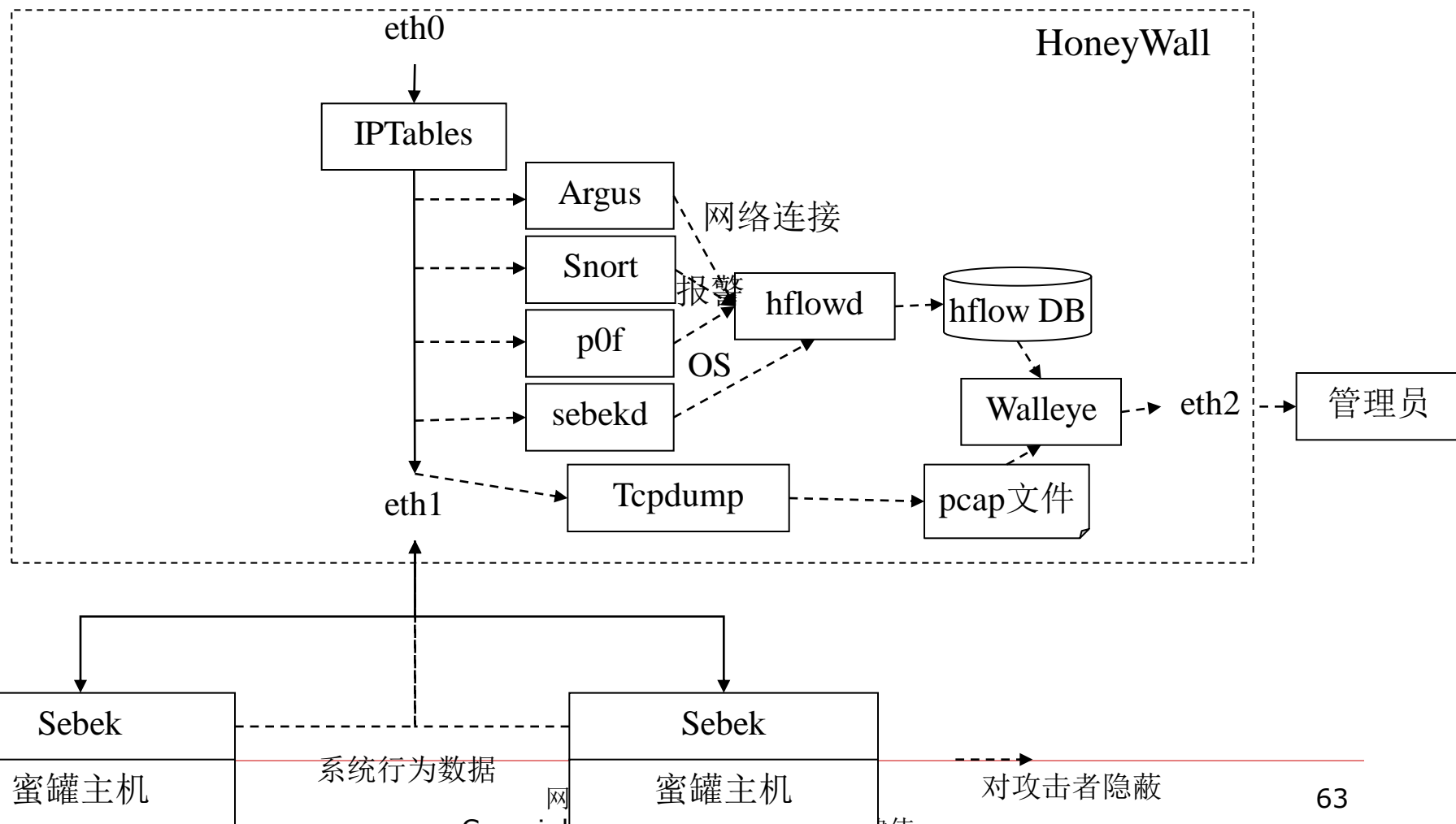
数据捕获机制体系结构图



Gen 3 蜜网数据模型



数据捕获机制图示





数据分析—Walleye

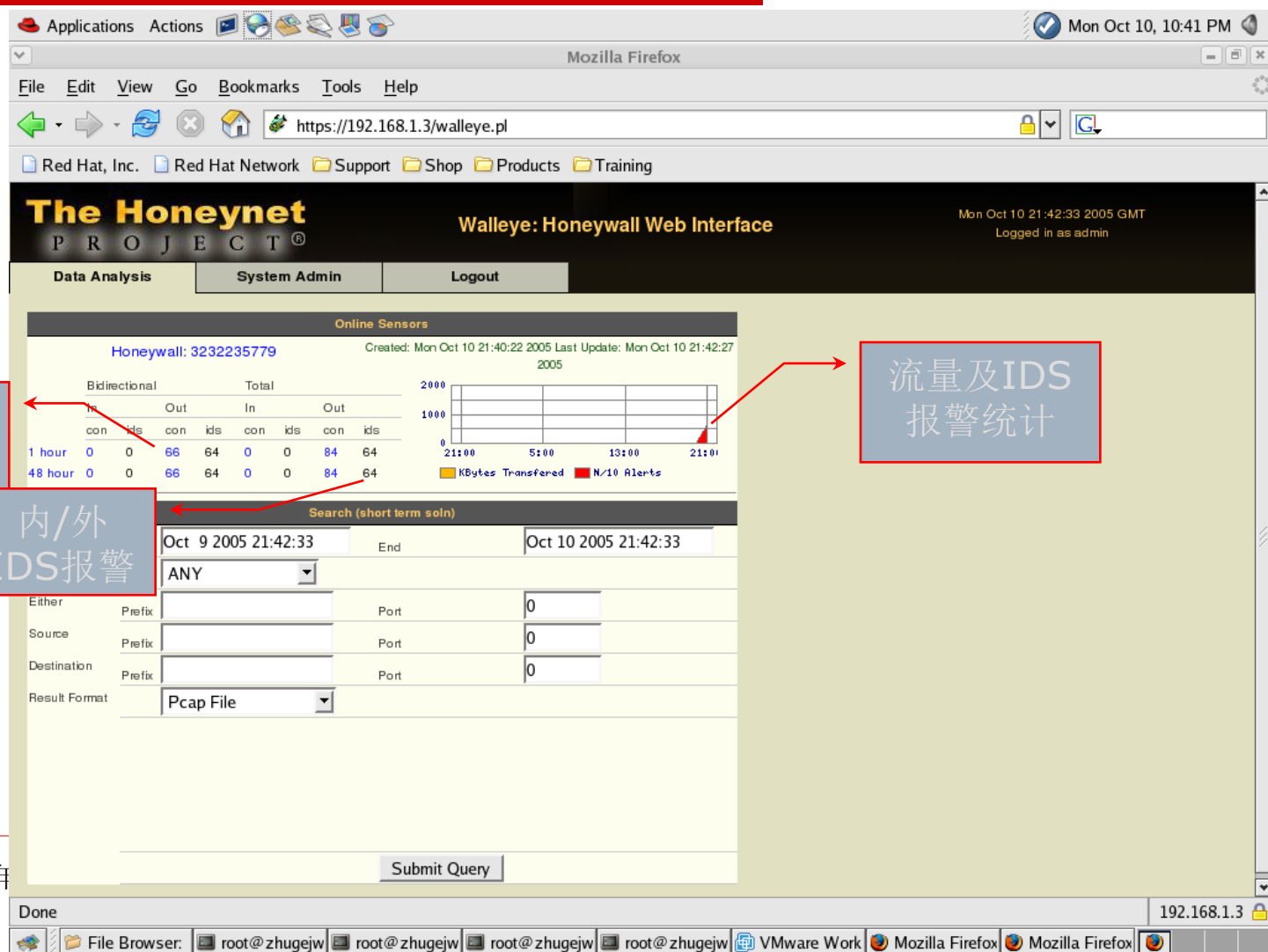
□ Perl语言编写的Web GUI

- 通过DBI连接mysql数据库
- mysql数据库中的信息由hflowd.pl提交

□ 数据分析视图

- 摘要视图
- 网络流视图
- 进程树视图
- 进程细节信息（**open_file, read_data, command...**）
- 网络流信息：网络流数据包解码，**snort**检测结果
- **Pcap**数据—慢通道

Walleye摘要视图



内/外
连接数

内/外
IDS报警

流量及IDS
报警统计



Walleye—网络连接视图

Applications Actions

Mon Oct 10, 10:49 PM

Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://192.168.1.3/?act=ct;ip=323235522;page=2

Red Hat, Inc. Red Hat Network Support Shop Products Training

All Time Periods
Sesbek Tracked
Submit Query

| Protocol | Source IP | Source Port | Destination IP | Destination Port | OS | Packet Count | Direction | Notes |
|----------|-------------|-------------|----------------|------------------|---------|----------------|-----------|--|
| TCP | 192.168.0.2 | 32909 | 192.168.0.4 | netbios-ssn | os unkn | 3 kB 10 pkts | --> | <-2-NETBIOS SMB trans2open buffer overflow attempt |
| RST | 192.168.0.2 | 32909 | 192.168.0.4 | netbios-ssn | os unkn | <-0 kB 8 pkts | --> | |
| TCP | 192.168.0.2 | 32908 | 192.168.0.4 | netbios-ssn | os unkn | 0 kB 0 pkts | --> | |
| TCP | 192.168.0.2 | 32909 | 192.168.0.4 | netbios-ssn | os unkn | 0 kB 0 pkts | --> | |
| TCP | 192.168.0.2 | 32910 | 192.168.0.4 | netbios-ssn | os unkn | 2 kB 8 pkts | --> | <-2-NETBIOS SMB IPC\$ share access |
| RST | 192.168.0.2 | 32910 | 192.168.0.4 | netbios-ssn | os unkn | <-0 kB 7 pkts | --> | <-2-NETBIOS SMB trans2open buffer overflow attempt |
| TCP | 192.168.0.2 | 32910 | 192.168.0.4 | netbios-ssn | os unkn | 0 kB 0 pkts | --> | |
| TCP | 192.168.0.2 | 32911 | 192.168.0.4 | netbios-ssn | os unkn | 3 kB 9 pkts | --> | <-2-NETBIOS SMB IPC\$ share access |
| RST | 192.168.0.2 | 32911 | 192.168.0.4 | netbios-ssn | os unkn | <-0 kB 9 pkts | --> | <-2-NETBIOS SMB trans2open buffer overflow attempt |
| TCP | 192.168.0.2 | 32911 | 192.168.0.4 | netbios-ssn | os unkn | 0 kB 0 pkts | --> | |
| TCP | 192.168.0.4 | 1032 | 192.168.0.2 | rwhois | Linux | 1 kB 10 pkts | --> | p0f操作系统辨识 |
| FIN | 192.168.0.4 | 1032 | 192.168.0.2 | rwhois | Linux | <-0 kB 10 pkts | --> | |

Snort 报警

p0f操作系统辨识

2011年3

6



Walleye—网络原始流视图

Applications Actions 1128981296.pcap - Ethereal Mon Oct 10, 11:06 PM

File Edit View Go Capture Analyze Statistics Help

Filter: + Expression... Clear Apply

| No. | Time | Source | Destination | Protocol | Info |
|-----|-----------|-------------|-------------|----------|---|
| 1 | 0.000000 | 192.168.0.2 | 192.168.0.4 | SMB | Negotiate Protocol Request |
| 2 | 0.000260 | 192.168.0.4 | 192.168.0.2 | TCP | netbios-ssn > 32911 [ACK] Seq=0 Ack=61 Win=5792 Len=0 TSV=1412f |
| 3 | 0.000281 | 192.168.0.4 | 192.168.0.2 | SMB | Negotiate Protocol Response[Unreassembled Packet] |
| 4 | 0.001903 | 192.168.0.2 | 192.168.0.4 | TCP | 32911 > netbios-ssn [ACK] Seq=61 Ack=73 Win=1460 Len=0 TSV=145f |
| 5 | 0.009272 | 192.168.0.2 | 192.168.0.4 | SMB | Session Setup AndX Request, User: anonymous |
| 6 | 0.014501 | 192.168.0.4 | 192.168.0.2 | SMB | Session Setup AndX Response |
| 7 | 0.025292 | 192.168.0.2 | 192.168.0.4 | SMB | Tree Connect AndX Request, Path: \\127.0.0.1\IPC\$ |
| 8 | 0.025411 | 192.168.0.4 | 192.168.0.2 | SMB | Tree Connect AndX Response |
| 9 | 0.031759 | 192.168.0.2 | 192.168.0.4 | NBSS | NBSS Continuation Message |
| 10 | 0.048012 | 192.168.0.4 | 192.168.0.2 | TCP | netbios-ssn > 32911 [ACK] Seq=165 Ack=1652 Win=8592 Len=0 TSV=1 |
| 11 | 0.048436 | 192.168.0.2 | 192.168.0.4 | NBSS | NBSS Continuation Message |
| 12 | 0.057043 | 192.168.0.4 | 192.168.0.2 | TCP | netbios-ssn > 32911 [ACK] Seq=165 Ack=2462 Win=8592 Len=0 TSV=1 |
| 13 | 0.373762 | 192.168.0.2 | 192.168.0.4 | TCP | 32911 > netbios-ssn [FIN, ACK] Seq=2462 Ack=165 Win=1460 Len=0 |
| 14 | 0.378797 | 192.168.0.4 | 192.168.0.2 | TCP | netbios-ssn > 32911 [ACK] Seq=165 Ack=2463 Win=8592 Len=0 TSV=1 |
| 15 | 36.562506 | 192.168.0.4 | 192.168.0.2 | TCP | netbios-ssn > 32911 [RST, ACK] Seq=165 Ack=2463 Win=8592 Len=0 |

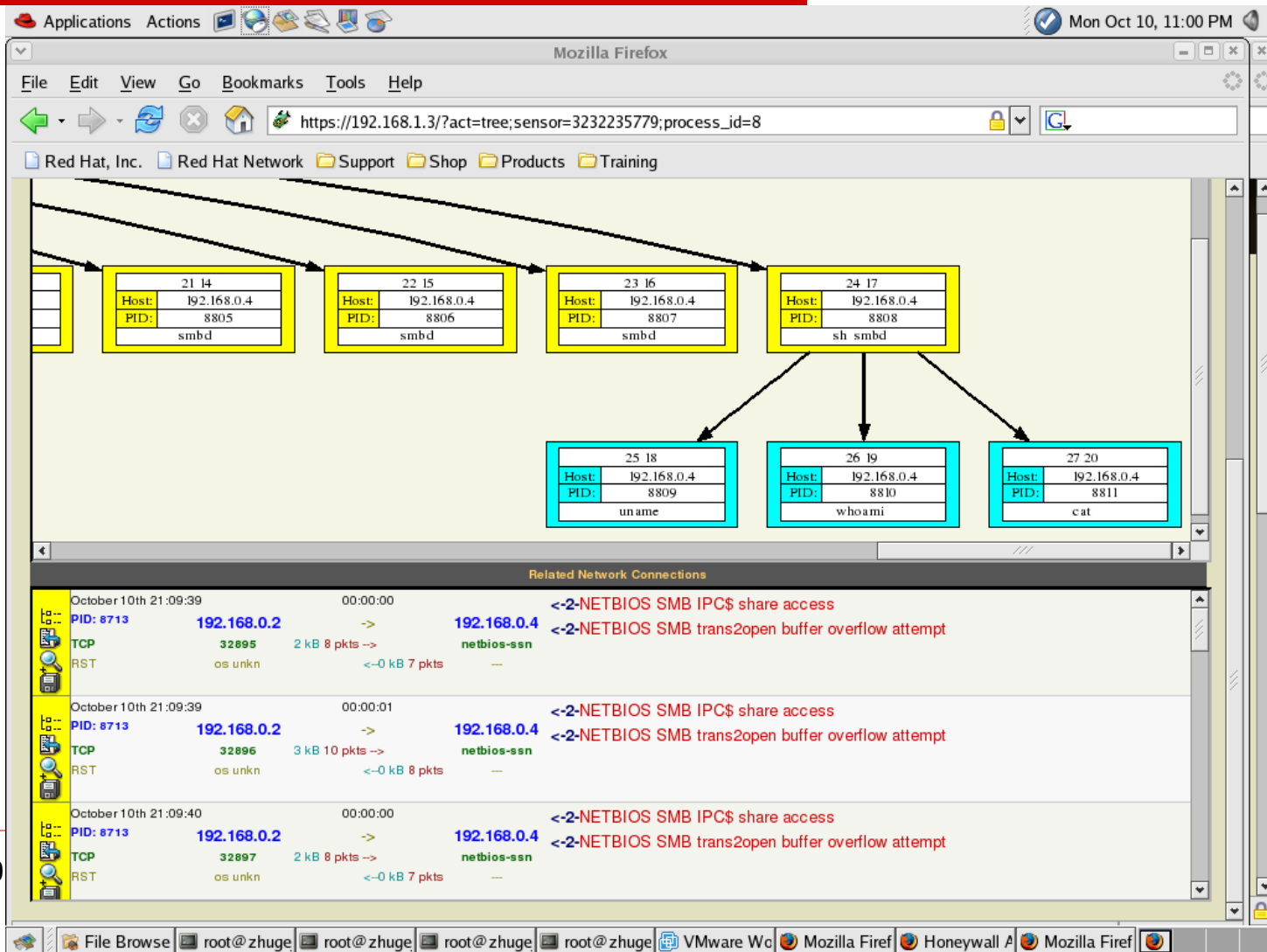
Frame 9 (1498 bytes on wire, 1498 bytes captured)
Ethernet II, Src: 00:07:95:48:d8:76, Dst: 00:0c:29:d3:2c:53
Internet Protocol, Src Addr: 192.168.0.2 (192.168.0.2), Dst Addr: 192.168.0.4 (192.168.0.4)
Transmission Control Protocol, Src Port: 32911 (32911), Dst Port: netbios-ssn (139), Seq: 220, Ack: 165, Len: 1432
NetBIOS Session Service

0330 b0 13 02 83 eb fc e2 f4 50 6b 40 41 32 da 11 68 Pk@A2..h
0340 07 e8 9a e3 ac 30 80 5b d1 8f de 82 28 c9 ea 59 0. [.... C.Y
0350 3b d8 d3 aa 61 b2 75 6a 71 51 50 64 32 39 f2 b2 ... a.uj qQpD29..
0360 07 e0 42 51 e8 51 50 cf e1 e2 7b 2d 4e c3 7b 6a ..BQ.QP..{-N.{j
0370 4e d2 7a 6c e8 53 41 51 e8 51 a3 09 ac 30 13 02 N.zL.SAQ.Q...0..
0380 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 ..AAAAAAAAAAAAAAAA
0390 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 ..AAAAAAAAAAAAAAAA
03a0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 ..AAAAAAAAAAAAAAAA
03b0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 ..AAAAAAAAAAAAAAAA
03c0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 ..AAAAAAAAAAAAAAAA

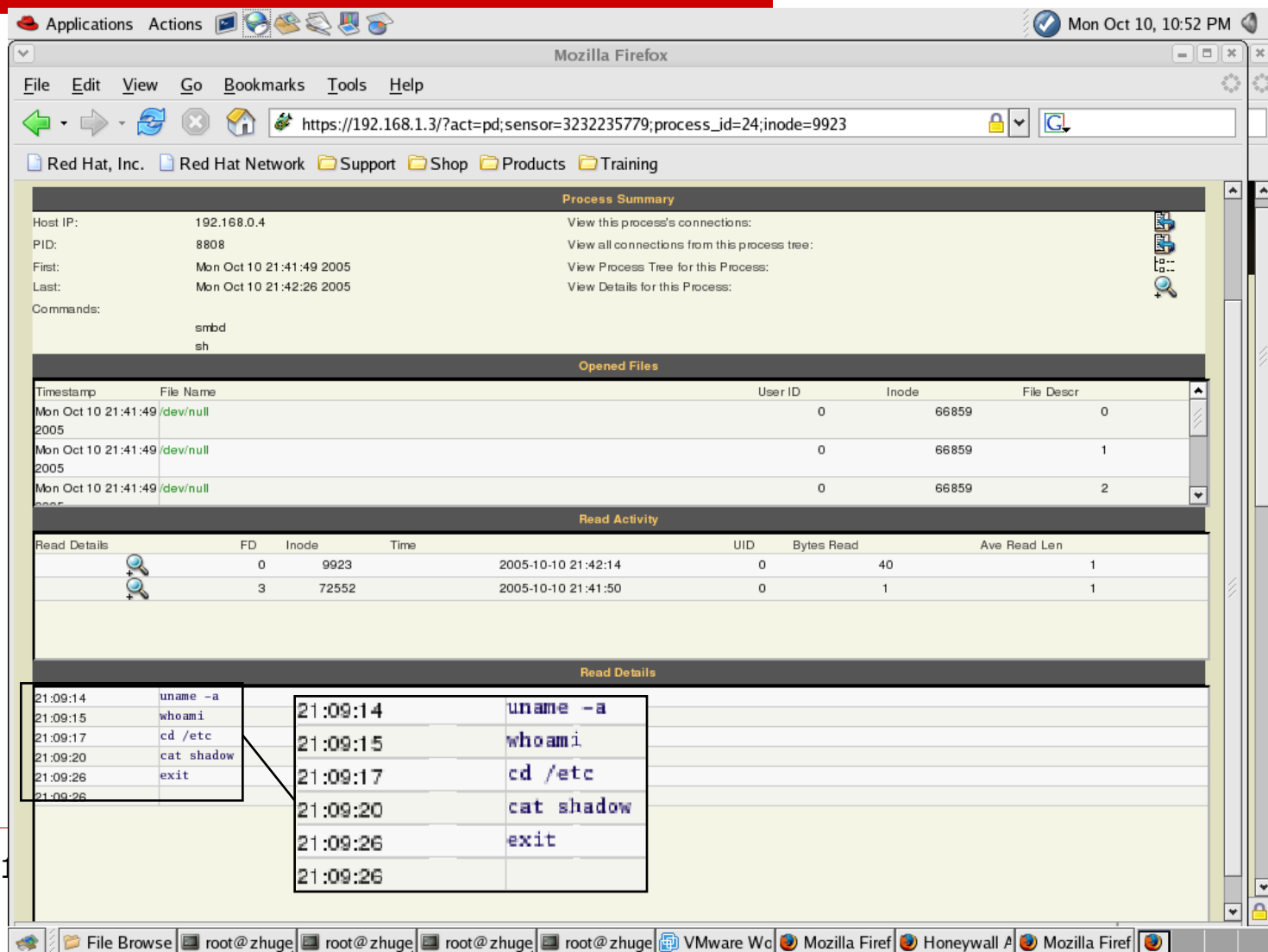
File: 1128981296.pcap 3881 b P: 15 D: 15 M: 0

File Brows root@zhuc root@zhuc root@zhuc root@zhuc VMware W Mozilla Fir Honeywall Mozilla Fir 112898129

Walleye—进程树视图



Walleye—键击记录视图



Applications Actions Mon Oct 10, 10:52 PM

Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://192.168.1.3/?act=pd;sensor=323235779;process_id=24;inode=9923

Red Hat, Inc. Red Hat Network Support Shop Products Training

Process Summary

Host IP: 192.168.0.4 View this process's connections:
 PID: 8808 View all connections from this process tree:
 First: Mon Oct 10 21:41:49 2005 View Process Tree for this Process:
 Last: Mon Oct 10 21:42:26 2005 View Details for this Process:
 Commands: smbd
 sh

Opened Files

| Timestamp | File Name | User ID | Inode | File Descr |
|--------------------------|-----------|---------|-------|------------|
| Mon Oct 10 21:41:49 2005 | /dev/null | 0 | 66859 | 0 |
| Mon Oct 10 21:41:49 2005 | /dev/null | 0 | 66859 | 1 |
| Mon Oct 10 21:41:49 2005 | /dev/null | 0 | 66859 | 2 |

Read Activity

| Read Details | FD | Inode | Time | UID | Bytes Read | Ave Read Len |
|--------------|----|-------|---------------------|-----|------------|--------------|
| | 0 | 9923 | 2005-10-10 21:42:14 | 0 | 40 | 1 |
| | 3 | 72552 | 2005-10-10 21:41:50 | 0 | 1 | 1 |

Read Details

| | | | |
|----------|------------|----------|------------|
| 21:09:14 | uname -a | 21:09:14 | uname -a |
| 21:09:15 | whoami | 21:09:15 | whoami |
| 21:09:17 | cd /etc | 21:09:17 | cd /etc |
| 21:09:20 | cat shadow | 21:09:20 | cat shadow |
| 21:09:26 | exit | 21:09:26 | exit |
| 21:09:26 | | 21:09:26 | |

2011

69



内容

- 1. 网络攻防实验环境**
- 2. 虚拟化技术与云计算热潮**
- 3. 蜜网(Honeynet)技术介绍**
- 4. 基于虚拟蜜网的网络攻防实验环境**
- 5. 网络攻防的活动与竞赛形式**

网络攻防虚拟机镜像

| 虚拟机镜像名称 | 虚拟机镜像类型 | 基础操作系统 | 发布者 |
|----------------------|-------------|--------------|----------------------|
| Linux Metasploitable | Linux靶机 | Ubuntu 8.04 | Metasploit Project |
| WinXP Metasploitable | Windows靶机 | WinXP SP0 En | Self-built |
| SEED VM | Linux攻击机/靶机 | Ubuntu 9.04 | SEED Project |
| Back Track 4 | Linux攻击机 | Ubuntu 8.10 | Remote Exploit Team |
| WinXP Attacker | Windows攻击机 | WinXP SP3 CN | Self-built |
| HoneyWall | 蜜网网关 | ROO v1.4 | The Honeynet Project |



Linux Metasploitable

- 发布时间
 - 2010.5, Metasploit Project
- Linux Metasploitable
 - 基础操作系统: **Ubuntu 8.04 Server**
 - 构建虚拟机软件: **VMware 6.5**
 - 开放服务: **proftpd/openssh/telnet/bind/apache/samba/mysql/distccd/postgres**
 - Web服务: **tomcat/tikiwiki/twiki**
 - Metasploit Exploit: **distcc/tomcat/tikiwiki/twiki**
 - 弱口令:
smb/ssh/telnet/apache/mysql/postgres/tomcat
- 有待进一步丰富漏洞环境



Windows Metasploitable

□ Win2ks_Metasploitable

- 基础操作系统版本: **Windows 2000 Server SP4 EN**
- 网络服务: **IIS, MSSQL, SMB, ServU, ...**
- **Metasploit**适用的攻击模块: **~150(未测试)**

□ WinXP_Metasploitable

- 基础操作系统版本: **WinXP SP2 EN**
- 客户端软件: **IE, Adobe, Office, Realplayer, baofeng, winamp, ...**
- **Metasploit**适用的攻击模块: **200-300(未测试)**

□ To Be Added

- **Win2k3_Metasploitable**



SEED VM

□ SEED (SEcurity EDucation)

- 信息安全教育实验环境
- 美国纽约雪城大学(Syracuse University)的Wenliang Du教授

□ SEED VM

- TCP/IP协议栈攻击；SQL注入/XSS攻击

| SEED虚拟机镜像配置项 | 具体配置情况 |
|--------------|--|
| 操作系统版本 | Ubuntu 9.04 with the Linux kernel v2.6.28 |
| 系统用户帐号/口令 | root/seedubuntu(不允许直接登录) seed/dees |
| 网络设置 | NAT模式，即使用宿主网卡作为路由器进行地址转换和报文转发 |
| 已安装软件包 | tcl, tk, libnet1, libnet1-dev, libpcap0.8-dev, libattr1-dev, vim, apache2, php5, libapache2-mod-php5, mysql-server, wireshark, bind9, nmap, sun-java6-jdk, xpdf, vsftpd, telnetd, zsh, libpcap 2.16, netlib/netwox/netwag 5.35.0 |
| 已安装服务器 | MySQL(用户名/口令: root/seedubuntu, apache/apache) Apache2(/var/www目录) bind9 DNS Server vsftpd FTP Server telnetd Server |

Back Track 4

□ Back Track

- 非常流行的渗透测试和信息安全审计的**Linux**发行版本
- 基于**Ubuntu 8.10**
- 集成了二十多类几百款安全软件
- 攻击破解之利器，蹭网卡附带**DVD**光盘

| BT4软件包集合 | 软件包用途 | BT4软件包集合 | 软件包用途 |
|-----------------------|------------|-----------------------|------------|
| BackTrack-Enumeration | 查点工具软件 | BackTrack-Bluetooth | 蓝牙攻击破解软件 |
| BackTrack-Tunneling | 隧道工具软件 | BackTrack-Sniffers | 网络嗅探工具软件 |
| BackTrack-Bruteforce | 暴力破解软件 | BackTrack-VOIP | 网络电话攻击软件 |
| BackTrack-Spoofing | 欺骗攻击软件 | BackTrack-Debuggers | 调试工具软件 |
| BackTrack-Passwords | 口令破解软件 | BackTrack-Penetration | 渗透测试攻击软件 |
| BackTrack-Wireless | 无线攻击破解软件 | BackTrack-Database | 数据库软件 |
| BackTrack-Discovery | 扫描发现软件 | BackTrack-RFID | RFID攻击破解软件 |
| BackTrack-Cisco | Cisco攻击软件 | BackTrack-Python | Python |
| BackTrack-Web | Web渗透测试软件 | BackTrack-Drivers | 驱动 |
| Applicaitons | 应用程序 | BackTrack-GPU | GPU计算 |
| BackTrack-Forensics | 取证分析软件 | BackTrack-Misc | 其他 |
| BackTrack-Fuzzers | Fuzz注入测试软件 | | |



WinXP Attacker虚拟机镜像

□ 自制WinXP攻击机镜像

| 软件工具包类别 | 包含软件列表 |
|---------|---|
| 基础环境配置 | JAVA SDK 1.6.21、CC/G++编译器 (MinGW) 4.5.0、Python解释器2.7、Adobe Flash Player 10.1、cygwin 1.7.7-1、Adobe Reader 9.3、Perl Strawberry 5.12.0 |
| 浏览器软件 | Firefox 3.6.9 中国版、Chrome 6.0.472.53、Opera 10.61、IE 6.0 |
| 网络传输软件 | Filezilla Server 0.9.36、Filezilla Client 3.3.4.1 |
| 编程工具 | Eclipse Classic 3.6、DEV-CPP 4.9.9.2 |
| 文本编辑器 | Source Navigator 4.2、MadEdit 0.1.2 beta、WinHex 15.7 SR-3 试用版 |
| 反汇编工具 | OllyDbg 2、IDA Pro 5.7 demo、IDA Pro 4.9 Free、C32asm 0.8.8、W32Dasm 8.93 |
| 反编译工具 | JD-GUI 0.3.3、dcc、boomerang alpha 0.3.1 |
| 静态分析工具 | Peid 0.95、LordPE、超级巡警脱壳器 v1.3、ASpack unpacker v1.1、upx 3.06、fs |
| 渗透攻击工具 | Metasploit 3.4.2-dev、Metasploit 2.7 |
| 网络扫描与嗅探 | Nmap /Zenmap 5.30 beta1、Wireshark 1.4.0、Nessus 4.2.2、Xscan 3.3、Snort 2.8.6.1 |
| 密码学工具 | CryptoCal 1.2、PrimeGenerator 1.1、RSAtools 2、DSAtools 1.3、Ultra Cracking Machine、MD5Crack 4.1 |
| 监视工具 | WinDump 3.9.5、Process Explorer 12.04、Process Monitor 2.92 |



HoneyWall虚拟机镜像

- **HoneyWall** - 虚拟蜜网中最核心的功能部件
 - **The Honeynet Project**开源发布
 - **ROO v1.4**
- **数据捕获**
 - **IPTables/Snort/tcpdump/Sebekd**
- **数据控制**
 - **IPTables/Snort_inline**
- **数据分析**
 - **Hflowd/walleye**



个人版网络攻防实验环境宿主要求

□ 硬件

- **CPU: P4 1.5G**以上
- *内存: **1G**以上, 建议**2G**以上
- 硬盘: **3-4**个虚拟机需**20G**左右空间
- 联网 (或激活) 的百兆网卡以上

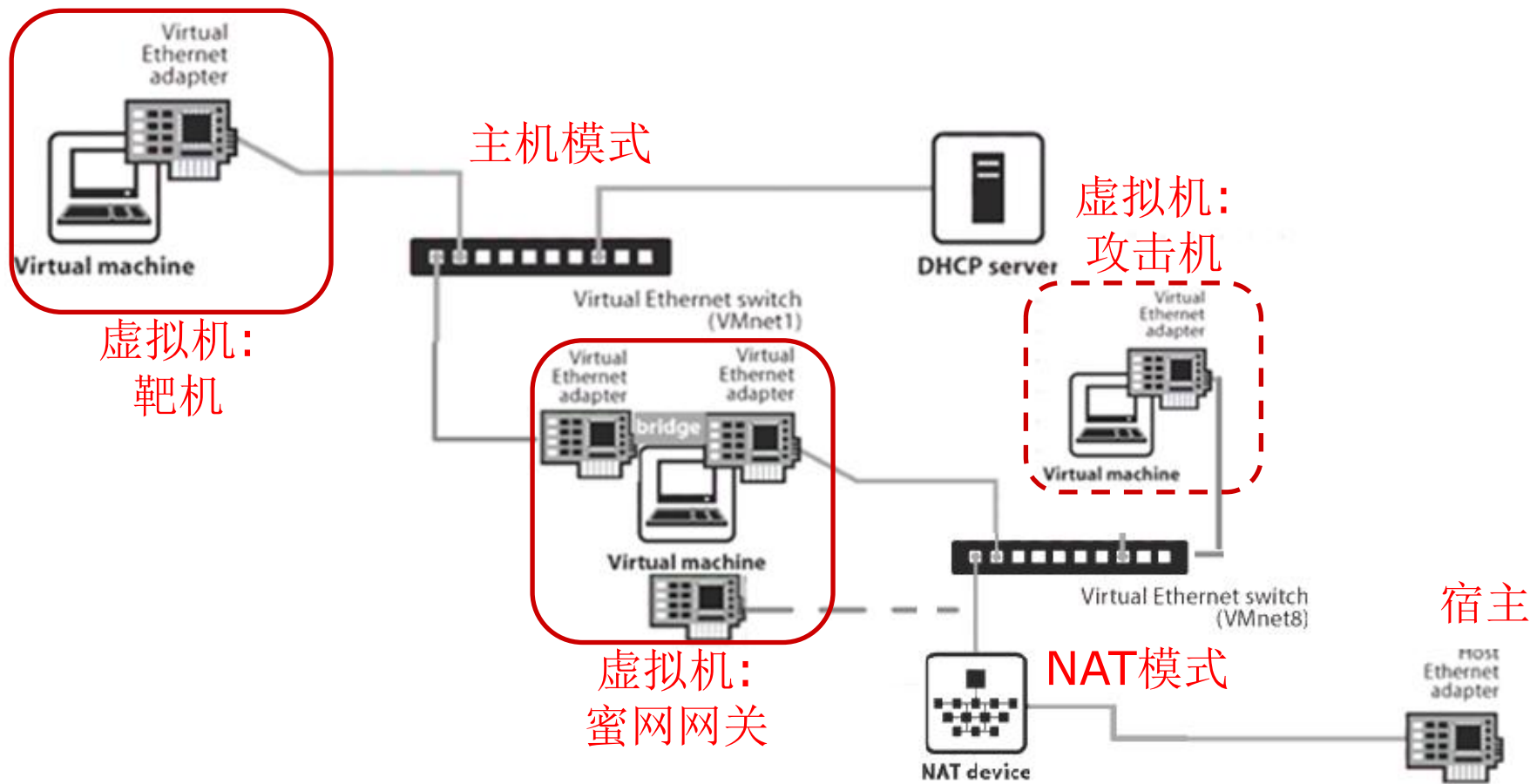
□ 软件

- **Windows**平台/**Linux**平台均可, 个人兴趣
- **VMware Workstation**或**Server**版本

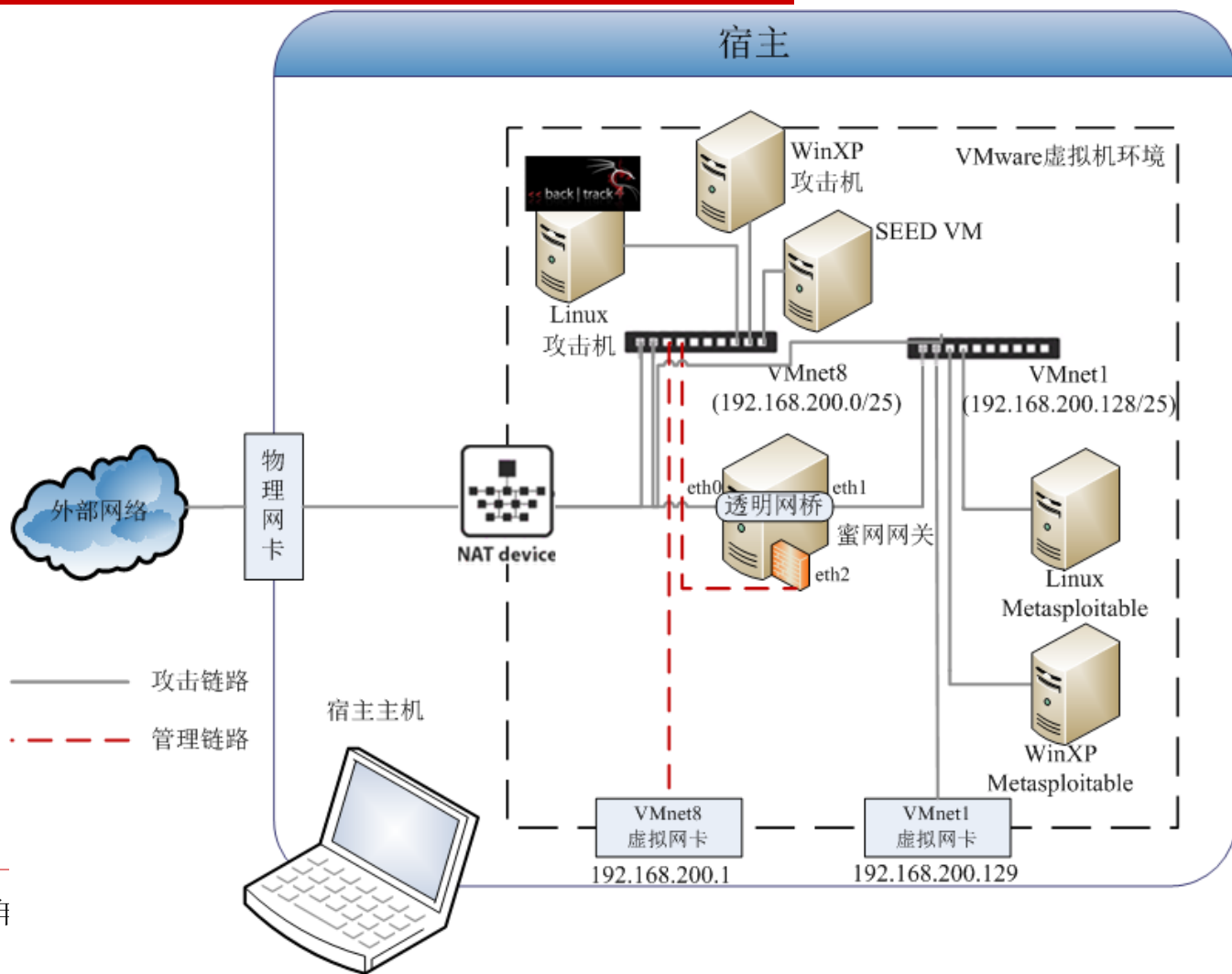
□ 虚拟机

- 蜜网网关: 虚拟**CPU/256M+/8G/3**虚拟网卡; **ROO v1.4**
- 靶机: 虚拟**CPU/128M+/4G+/1**虚拟网卡; **Windows/Linux**
- 攻击机: 虚拟**CPU/128M+/4G+/1**虚拟网卡;
Windows/Linux

V-Net攻防环境使用的联网方式



个人版网络攻防实验环境拓扑结构

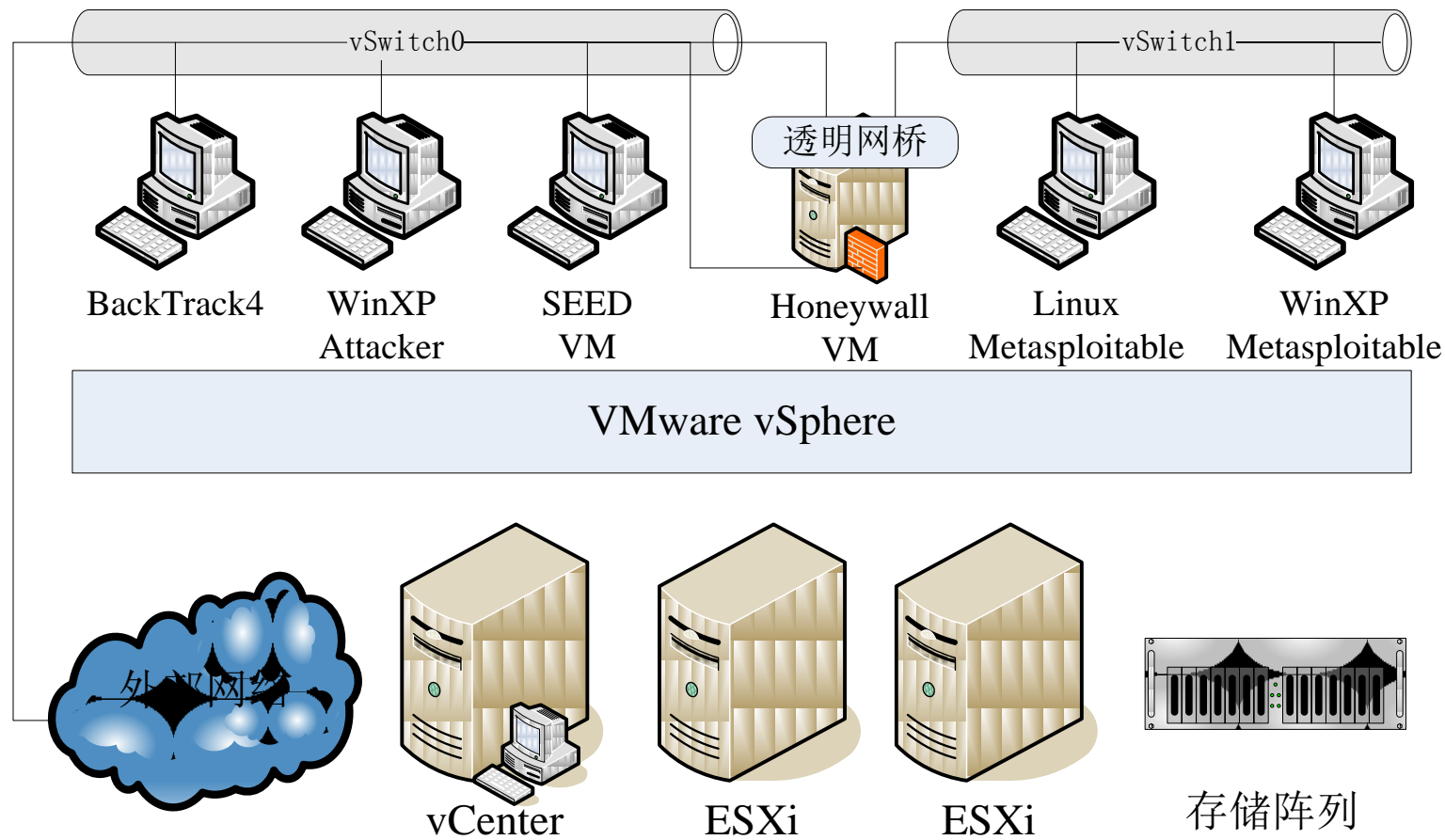




个人版网络攻防实验环境中的网络配置

- 宿主+VMware虚拟机软件
 - **vmnet1** – 主机模式
 - **vmnet8** – NAT模式，连接宿主物理网卡，通过NAT后连接外网
- 虚拟机-蜜网网关
 - **eth0**(外网口) – 连接**vmnet8: NAT模式**
 - **eth1**(内网口) – 连接**vmnet1: 主机模式**
 - **eth0**和**eth1**构成一个透明网桥
 - **eth2**(管理口) – 连接**vmnet8: NAT模式**
 - 宿主通过**vmnet8**的虚拟网卡对蜜网网关进行管理
- 虚拟机-靶机
 - **eth0** – 连接**vmeth1: 主机模式**
- 虚拟机-攻击机
 - **eth0** – 连接**vmeth8: NAT模式**

专业版网络攻防实验环境拓扑结构





内容

- 1. 网络攻防实验环境**
- 2. 虚拟化技术与云计算热潮**
- 3. 蜜网(Honeynet)技术介绍**
- 4. 基于虚拟蜜网的网络攻防实验环境**
- 5. 网络攻防的活动与竞赛形式**



黑客会议-网络攻防活动集中场所

- 国际上最著名的两大黑客会议
 - **Defcon (since 1992)**
 - **Blackhat (since 1997)**
 - 拉斯维加斯, **Jeff Moss**
- 中国最著名的黑客会议
 - **XCon (since 2002)**
 - 北京, **8月**, 安全焦点团队主办

2010 黑帽大会/Defcon大会专题

黑帽大会、Defcon大会：全球黑客云集

黑帽和Defcon是备受全球瞩目的年度安全大会。黑帽大会吸引的群众比Defcon更专业。而在Defcon会议上，常看到年轻的黑客在空档时间耍一些花招，像是破解ATM和饭店电梯，或是参与开锁比赛等活动。[全文]



黑客破解GSM网络



黑客远程偷读护照RFID芯片数据



现场报道



黑客轻松让ATM机狂吐现金

在周三的黑帽大会上，Barnaby Jack，IOActive的安全测试经理，拉了两台ATM机上了黑帽大会的讲台，并向现场观众演示了令人惊讶的一幕：只见他按动一个按钮，于是两台ATM机便吐出了一大堆的钞票，撒满了一地。[全文]

▪ 研究人员可轻松让ATM机狂吐现金

▪ 美黑客使自动提款机变自动吐钱机



伪装电话咨询 20分钟窃取企业机密

社交工程黑客能够欺骗员工做或者说他们不应该做或者不应该说的事情。社交工程黑客星期五(7月30日)在Defcon大会开展的比赛中对财富500强企业进行了试验攻击，展示了如何轻而易举地让人们讲话，只要你会说恰当的谎言。[全文]



Black Hat和Defcon黑客大会的五大看点

- 终结者2现实版，让ATM自动吐钞
- DNSSEC是否能保DNS万无一失?
- 移动bug，普通人也能玩窃听
- 除了IT可以Hack，工业领域也可以
- 或许会有意外，充满压力的黑客大会 [全文]



黑帽和Defcon安全大会回顾

- 黑帽安全大会流媒体视频被破解
- 假冒手机基站
- 谷歌充满恶意软件风险
- Android安全性不佳
- 更多安全漏洞
- 全美安全状况堪忧
- 银行安全 [全文]





“不可能被黑的” Android手机轻松被黑

在本周召开的黑帽大会上，安全研究人员的演示表明，一度曾被认为是“不可能被黑的”Android手机也被黑了。演示表明，隐藏在壁纸软件中的可疑代码能够从被感染的手机上收集各种个人信息，并将这些信息发送给一家据说在中国的网站。 [\[全文\]](#)

· 谷歌Android操作系统存漏洞 黑客可控制设备



多数浏览器都会泄露使用者个人信息

计划参加本周举办的黑帽大会的一位安全专家称，所有最流行的互联网浏览器，如IE、Firefox、Chrome和Safari都存在一个漏洞，可被人利用来盗取使用者的个人信息。白帽安全公司CTO Jeremiah Grossman称，“我在大会上要介绍的一些工具利用这些漏洞可以说毫无困难。” [\[全文\]](#)

· 电脑间谍声称1亿美元2年可建网军攻陷美国



更多黑客新闻

- HTTPS和SSL存在安全漏洞
- 思科迈克菲均“被漏洞”
- 美国众多黑客来北京开会 称中国也有好黑客
- 密码心理学 看黑客如何来破解密码
- 德国黑客遥控摄像头偷窥多名女生遭逮捕

相关专题



2009黑帽大会

相比“奇装异服”的江湖派Defcon，Black Hat 更像是一场温文尔雅的学院派交流。。



2008黑帽安全大会

黑帽安全大会及随后举办的姊妹会议DefCon 黑客大会是网络安全业界备受关注的事件。

现场图片



2011年3月6日

网络攻防活动与竞赛形式

-Demo

□ Demo - “耳听为虚、眼见为实”



Barnaby Jack 在2010年Black Hat会议上远程操纵ATM机疯狂吐现金演示

网络攻防活动与竞赛形式

-上手体验 (Hands-on)

□ “纸上得来终觉浅，绝知此事要躬行”



2011年3月6日

网络攻防技术与实践课程
Copyright (c) 2008–2009 诸葛建伟

88



网络攻防活动与竞赛形式 -实验 (Lab)

□ 计算机专业学习需要**Lab**

- 编程语言 – 编程实习, **ACM POJ**
- 操作系统 – 操作系统实习(**Minix**)
- 计算机网络 – 网络实习
- ...

□ 网络攻防技术 – 网络攻防实验**Lab**

- **SEED(SECURITY EDUCATION)**信息安全教育实验环境: **TCP/IP**协议攻击, **SQL/XSS**攻击
- 本课程定制**Lab**



网络攻防活动与竞赛形式-挑战(Challenge)

□ 取证分析挑战(Forensic Challenge)

- [The Honeynet Project](#)取证分析挑战中文版启航，欢迎华语世界安全人士参与
- [The Honeynet Project](#)取证分析挑战5：日志中的神秘现象, **deadline: 9月30日**
- [The Honeynet Project](#)取证分析挑战2010第四次-网络电话攻击

□ 程序破解(CrackMe)、逆向分析(ReverseMe)、生成注册机(Keygenme)

- 软件安全分析与破解技术
- 看雪学院论坛活动



取证分析挑战5：日志中的神秘现象

- 您的任务是分析从一台可能被攻陷服务器获取到的所有日志文件，以确定这台虚拟服务器上出了什么事情。
 - 系统被攻陷了吗？你是如何确认的？
 - 如果服务器被攻陷了，请描述攻击的方法？
 - 你能找出有多少攻击者攻击失败吗？有多少攻击成功？多少攻击在第一次成功后被阻断了？
 - 日志文件中是否显示出存在一个被其他人用于访问这台机器的后门工具？
 - 请指出认证日志的位置，其中是否包含了暴力破解攻击的记录？如有，进行了多少次？
 - 请给出重要事件的时间线，你对这些时间点的把握性多大？
 - 在日志中还有其他看起来很可疑的地方吗？是误配置吗？还是其他问题？
 - 是否是通过一个自动化的工具发起攻击？如果是，是哪个工具？
 - 你认为攻击者的目标和方法是什么？



网络攻防活动与竞赛形式

-竞赛 (Contest)

- **Defcon**每年都会有多达几十个不同的竞赛
 - 经典的撬锁(也被纳入物理安全范畴)
 - 系统破解
 - **Wi-Fi**天线**DIY**
 - **CTF**夺旗竞赛...
- **CanSecWest**会议从**2007**年开始的**Pwn2Own**
- **CTF(Capture the Flag)**

黑客会议上的夺旗赛

Defcon 2008 CTF赛现场



2011年3月6日

网络攻防技术与实践课程
Copyright (c) 2008–2009 诸葛建伟

93

CTF现场-没有硝烟的战场



2011年3月6日

网络攻防技术与实践课程
Copyright (c) 2008-2009 诸葛建伟

94

网络攻防活动与竞赛形式

-绵羊墙(The Wall of Sheep)

- 起源于2002年defcon
- “F**ked sheep”
- 引起人们对网络安全的关注，用来教育人们





网络攻防活动与竞赛形式

-开源软件开发

- 最传统也可能是最重要的一项活动是开源软件开发
 - **RMS**为精神领袖、自由软件基金会与**GNU**为核心力量开源社区
- 安全社区中的一些著名开源与非盈利性团队
 - **Nmap**
 - **The HoneyNet Project**
 - **SANS**
 - **ShadowServer**
 - **OWASP, ...**
- 一些支持开源的公司
 - **Google: Google Summer of Code**
 - **...**



作业2-网络攻防实验环境搭建和测试(个人, 10分)

- 作业内容: 利用虚拟蜜网技术进行网络攻防实验环境构建, 并进行网络连通性测试与验证
 - 至少包括一台攻击机、一台靶机、**SEED**虚拟机和蜜网网关
- 作业提交: 实验报告, 根据自己的理解和实验经过, 详细说明网络攻防实验环境的结构和组成模块; 搭建和测试过程及遇到的问题; 解决问题的过程、方法和收获等
- 参考: **ftp/materials/HackingExposed_2_VNet**虚拟蜜网构建.pdf
- 提交时间: **10月12日**
- 提交方式: 电子邮件给助教**zhanghuilin@icst.pku.edu.cn**
- 注意: 开源的蜜网技术可能存在不稳定的问题
 - 发现问题和解决问题是提升实践技能最重要的途径
 - 答疑: **BBS**版面(推荐)/助教**Email**

Thanks

诸葛建伟
zhugejw@gmail.com



下堂课预告

- **9月29日10-12节, 10月13日10节,网络信息收集技术**
- **建议课前阅读:**
 - **第3章《网络信息收集技术》讲义**
 - **《黑客大曝光》第一部分: 第1章(踩点)、第2章(扫描)、第3章(查点)**
- **建议课前使用和了解的工具**
 - **Google, whois, ip地址查询, ping, traceroute**
 - **nmap, nessus或xscan**
- **可从课程共享FTP获取相关资源**



黑客游戏

- ❑ **Monyer**系列（黑客游戏）
 - ❑ 1. <http://monyer.com/game/game1/>（中文）
 - ❑ 2. <http://monyer.com/game/game2/>（英文）

- ❑ **Sunnyspeed**系列（英文）- 解谜类
 - ❑ 1. <http://sunnyspeed.com/puzzle/>（英文）
 - ❑ 2. <http://sunnyspeed.com/secret/>（英文）
 - ❑ 3. <http://sunnyspeed.com/crazy/>（英文）

- ❑ **Hack Forever**（英文）- 实战攻防类
 - ❑ <http://www.hackerforever.com>

- ❑ **Hacker Funny Game**（英文）- 模拟实战攻防类（**FLASH GAME**）
 - ❑ <http://www.funnygames.co.nz/play/hacker>

- ❑ **Hacker Skills**（英文）- 网页过关类
 - ❑ <http://www.hackerskills.com/>



- ❑ **Uplink**（英文）- 模拟 **Linux** 攻防（需下载游戏）
- ❑ **<http://www.introversion.co.uk/uplink/>**

- ❑ **UPLINK** 是一款基于**Linux**平台的黑客模拟游戏。玩家在其中扮演一位神通广大的黑客为U
- ❑ **P L I N K**公司工作，窃取各大公司的数据库机密资料。深受广大游戏玩家的喜爱。游
- ❑ 戏里不需要你懂得太多的专业知识,反而会教你许多东西,只要你英语过得去.你是作为
- ❑ **UPLINK**的一个黑客,注册了以后你会得到一笔初始的资金和初始的软 硬件.如果你熟悉黑
- ❑ 客的知识,你可以自己去做,如果不会的话,会有一个教学模式一步一步的教你,我这个菜鸟
- ❑ 也看得懂要做什么.然后你的等级会上升,你就可以正式在**UPLINK**的**SERVER**上联系客户,接
- ❑ 取工作,完成工作就会获得回报(当然是钱啦)等级越高,任务的难度就会越高.在**SERVER**里
- ❑ ,你还可以买到更厉害的软件和硬件,让你容易完成任务。

- ❑ **51CTO** - 黑客游戏系列（中文）- 实战攻防类
- ❑ 第一季【原创：黑客游戏 I】危险的telnet（**[http://bbs.51cto.com/thread-659015-1.h](http://bbs.51cto.com/thread-659015-1.html)**
- ❑ **tml**）
- ❑ 第二季【原创：黑客游戏 II】致命的SA权限（**[http://bbs.51cto.com/thread-659512-1.h](http://bbs.51cto.com/thread-659512-1.html)**
- ❑ **tml**）
- ❑ 第三季【原创：黑客游戏 III】神秘的远程桌面端口（**[http://bbs.51cto.com/thread-6598](http://bbs.51cto.com/thread-659854-1.html)**
- ❑ **54-1.html**）



-
- ❑ **MOX-X**（英文）- 综合类
 - ❑ **<http://www.mod-x.co.uk/main.php>**

 - ❑ **Hacker Evolution**（英文）- 模拟攻防类（需下载游戏）
 - ❑ **<http://www.hackerevolution.org/>**

 - ❑ 路路解密破解游戏（中文）- 综合类
 - ❑ **<http://www.666666666666.com/Index.Asp>**

 - ❑ **Arthur's Online Riddle**（中文）- 网页过关类
 - ❑ **<http://riddle.arthurluk.net/>**

 - ❑ **Level Game**（英文）趣味过关游戏（**FLASHGAME**）
 - ❑ **<http://www.levelgame.net/>**



- **sqybi** 的解谜游戏（中文）- 网页过关类
- **<http://sqybi.com/game/>**

- **NotPron**（中英文）- 解密类游戏（这个游戏是我的最爱）
- 中文版: **<http://deathball.net/notpron/china/notpron.htm>** 目前只有**8**关而已
- 英文版: **<http://deathball.net/notpron/levelone.htm>** 有**132**关,全球只有**82**人通关咯

- 有道谜题（中文）- 推理游戏 - **FLASHGAME**
- **<http://www.youdao.com/nanti/mi2010/>**

- **【中安网培】黑客游戏**（中文）- 网页过关类（貌似最后几关坏掉了）
- **<http://game.enet.org.cn/>**

- **Hack The Game**（英文）- 模拟攻防类（需下载游戏）
- **<http://chaozz.deepunder.dk/index.php?dir=released/hackthegame/>**

- 游戏中玩家扮演黑客，完成各种入系统入侵任务，之后会有酬金和提升名气。目前网络上
- 各种真伪日益盛行，有兴趣的朋友可以亲身体验一下，过一回当黑客的瘾哟



-
- ❑ 黑客榜中榜（中文） - 网页过关类
 - ❑ <http://www.cn-hack.cn/qs/5.htm>

 - ❑ PCSEC'Game（中文） - 网页过关类
 - ❑ <http://www.pcsec.org/game/>

 - ❑ 黑客游戏（英文）
 - ❑ <http://www.chaozz.nl/?downloadid=20&type=ziponly>

 - ❑ 国外黑客游戏集锦
 - ❑ <http://hackergames.net/>
 - ❑ 以后会写一些游戏破关的思路，另外如果有其他黑客游戏地址的朋友，麻烦请通知我，我会加到列表里的。

 - ❑ <http://ingeration.blogspot.com/2007/12/challenge-sites.html>（被GFW了）