

# 第二讲：蜜网技术

诸葛建伟

北京大学狩猎女神项目组

The Artemis Project

# 蜜网技术

- 蜜网技术的提出与发展历程
- 蜜网技术体系框架与核心机制
- 第三代蜜网技术
  - 数据控制机制
  - 数据捕获机制
  - 数据分析机制
  - 配置与管理机制
- 虚拟蜜网

# 蜜网技术

- 蜜网技术的提出与发展历程
- 蜜网技术体系框架与核心机制
- 第三代蜜网技术
  - 数据控制机制
  - 数据捕获机制
  - 数据分析机制
  - 配置与管理机制
- 虚拟蜜网

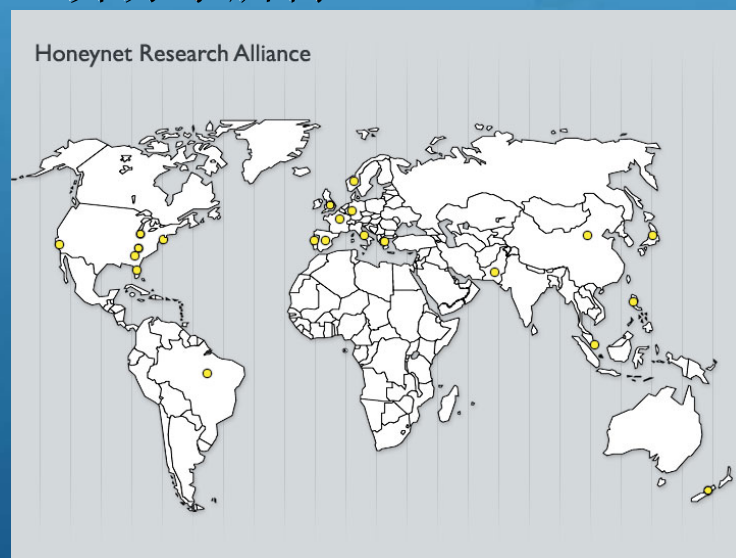


# 蜜网技术的提出—从蜜罐到蜜网

- 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

- 非赢利性研究机构
- 目标
  - To learn the tools, tactics, and motives of the blackhat community and share these lessons learned
  - 探寻黑客界的攻击工具、战术和动机，并分享所得
- 历史
  - 1999–非正式的邮件列表
  - June 2000–演变为蜜网项目组
  - Jan. 2002–发起蜜网研究联盟HRA
  - 目前，HRA会员20+（美/欧/亚太）
- 创始人及主席
  - Lance Spitzner





# 蜜网技术：过去, 现在 & 将来

## 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

## 过去



### 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

## 现在



### 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

## 将来



### 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
- 将在2007年发布

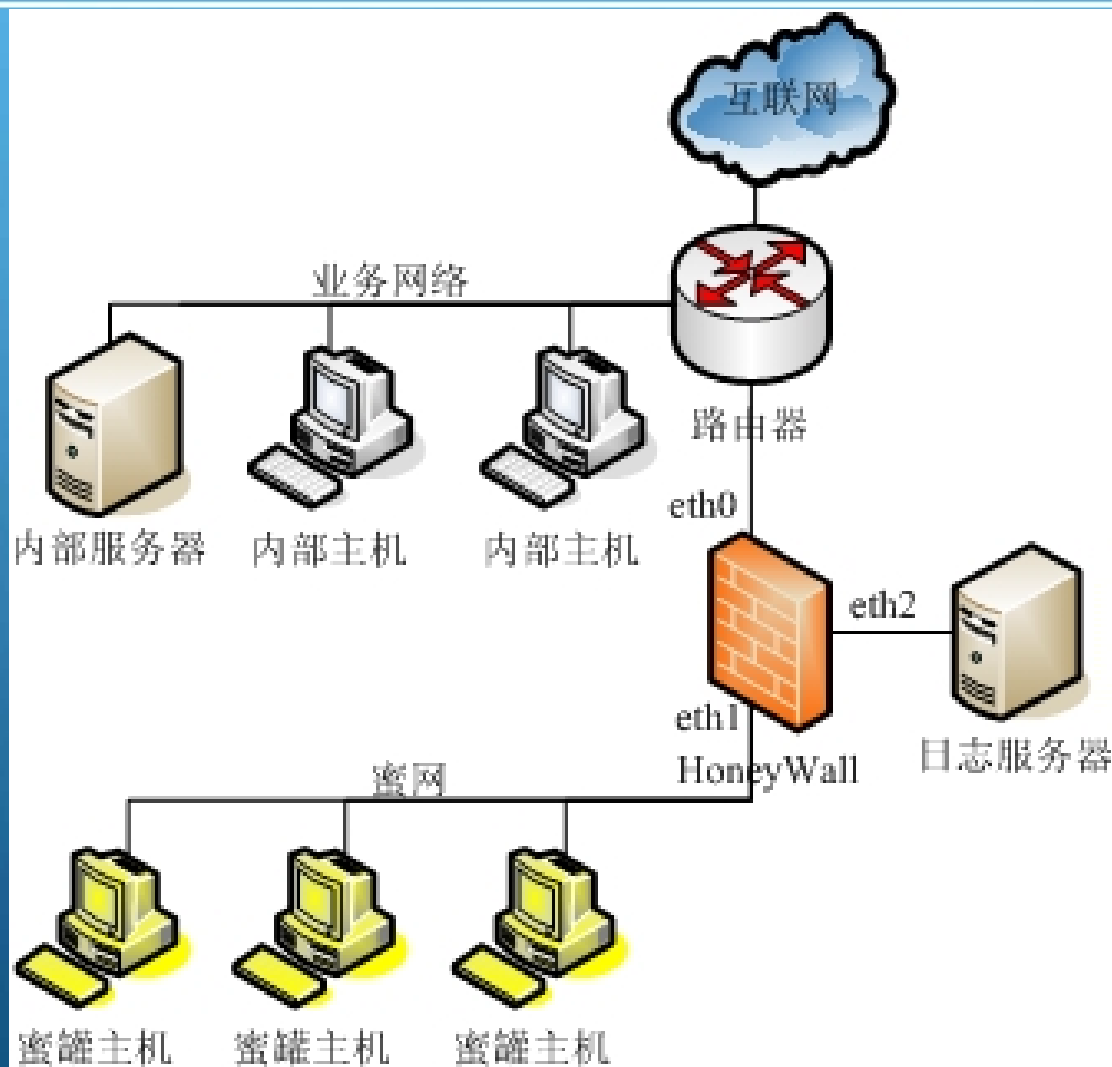
### 蜜网项目组 & 蜜网研究联盟

- 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://honeynet.org>

# 蜜网技术

- 蜜网技术的提出与发展历程
- 蜜网技术体系框架与核心机制
- 第三代蜜网技术
  - 数据控制机制
  - 数据捕获机制
  - 数据分析机制
  - 配置与管理机制
- 虚拟蜜网

# 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

# 蜜网技术

- 蜜网技术的提出与发展历程
- 蜜网技术体系框架与核心机制
- 第三代蜜网技术
  - 数据控制机制
  - 数据捕获机制
  - 数据分析机制
  - 配置与管理机制
- 虚拟蜜网

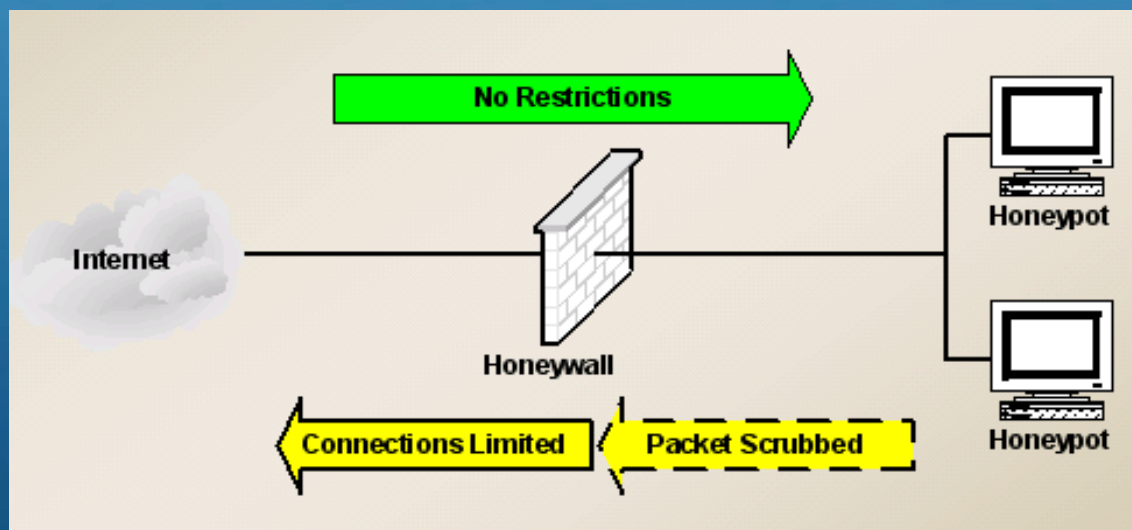
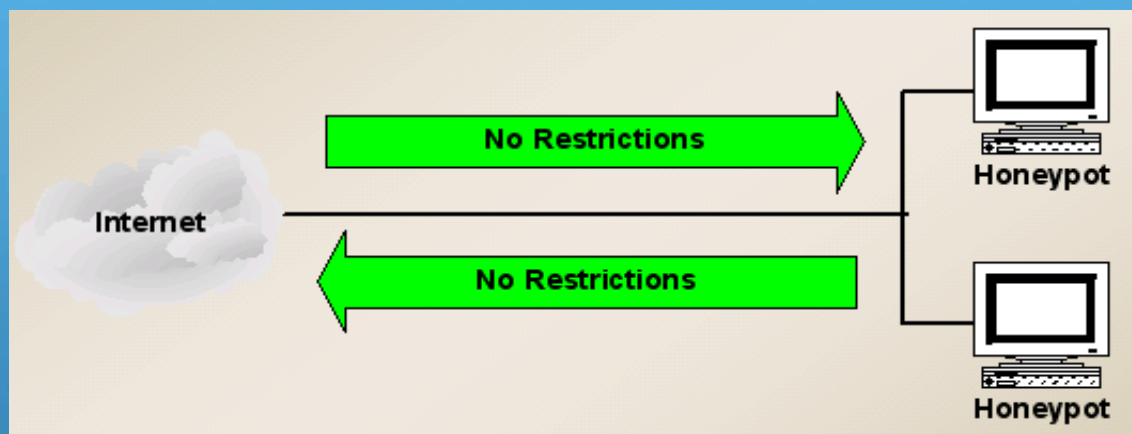
# 第三代蜜网

- 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
- 进一步研发中—Roo v2，预期发布时间2007年初

# 蜜网技术

- 蜜网技术的提出与发展历程
- 蜜网技术体系框架与核心机制
- 第三代蜜网技术
  - 数据控制机制
  - 数据捕获机制
  - 数据分析机制
  - 配置与管理机制
- 虚拟蜜网

# 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

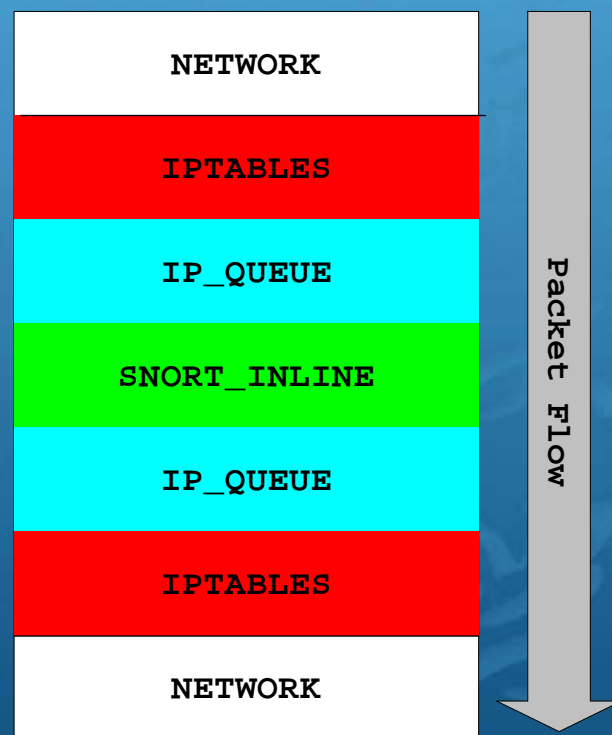


# 攻击数据包过滤

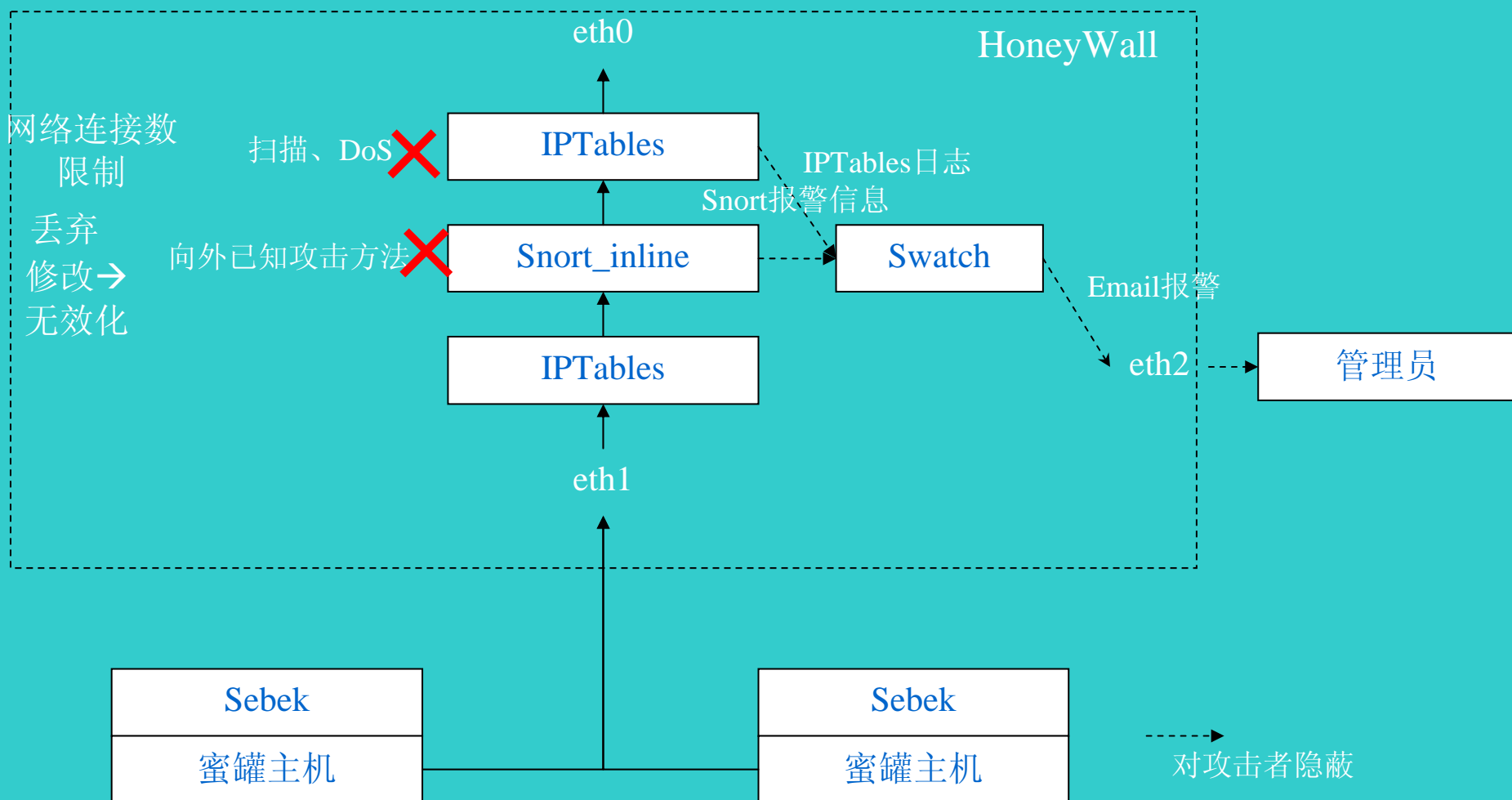
## ■ Snort\_inline: NIPS

- `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



# 蜜网技术

- 蜜网技术的提出与发展历程
- 蜜网技术体系框架与核心机制
- 第三代蜜网技术
  - 数据控制机制
  - 数据捕获机制
  - 数据分析机制
  - 配置与管理机制
- 虚拟蜜网

# 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<src, sport, dst, 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](http://www.snort.org)
- POf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>

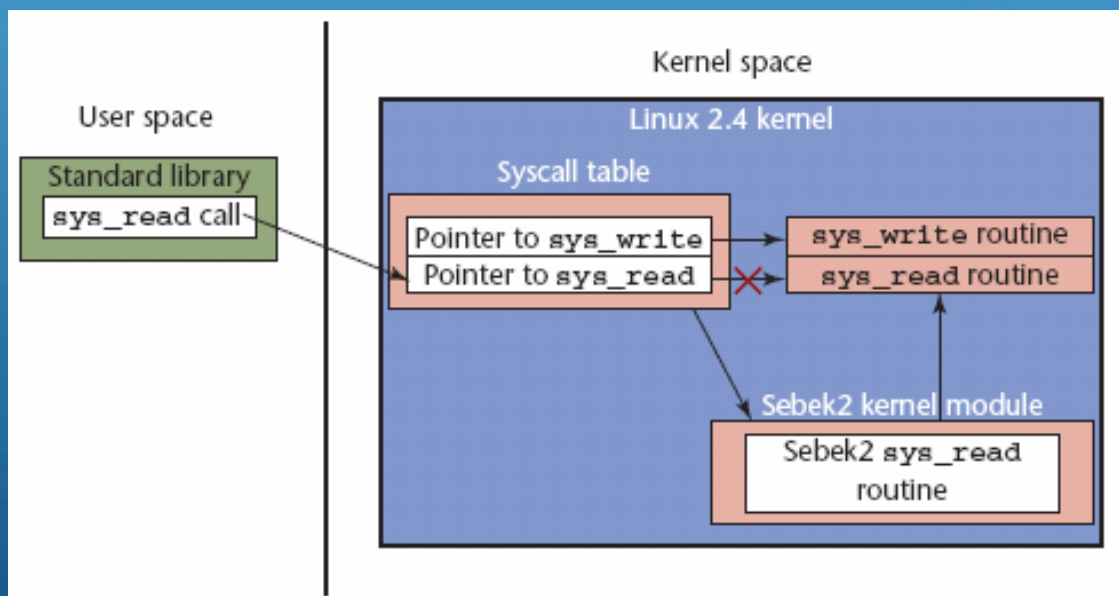
# 系统行为数据-Sebek

## ■ 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

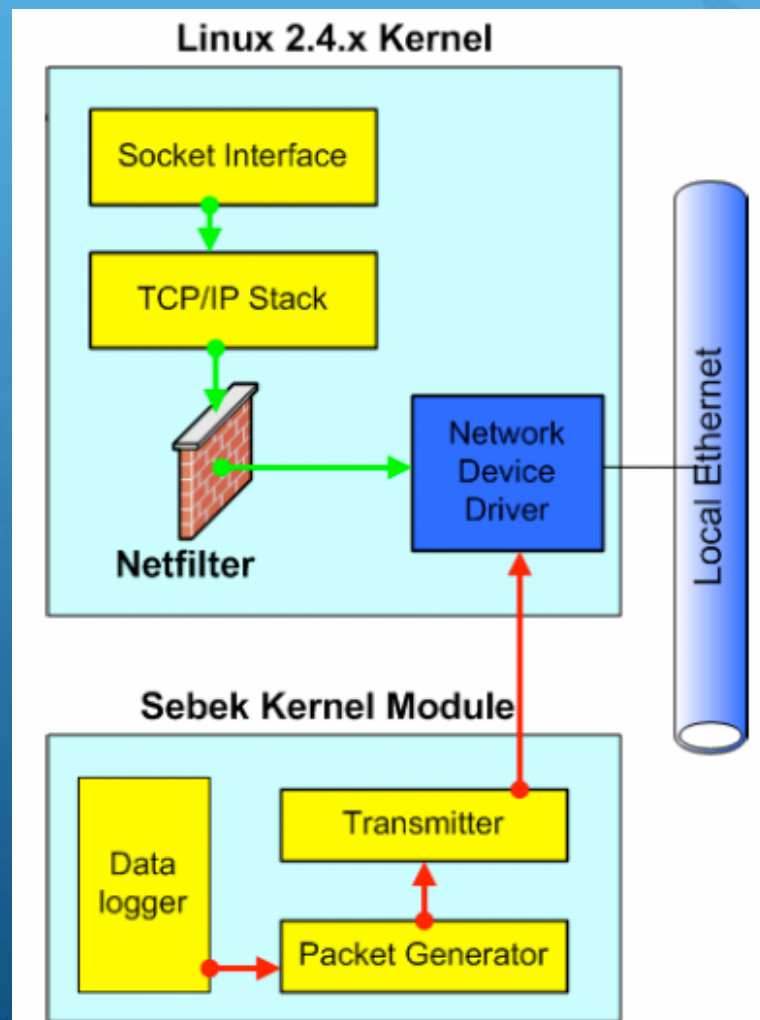
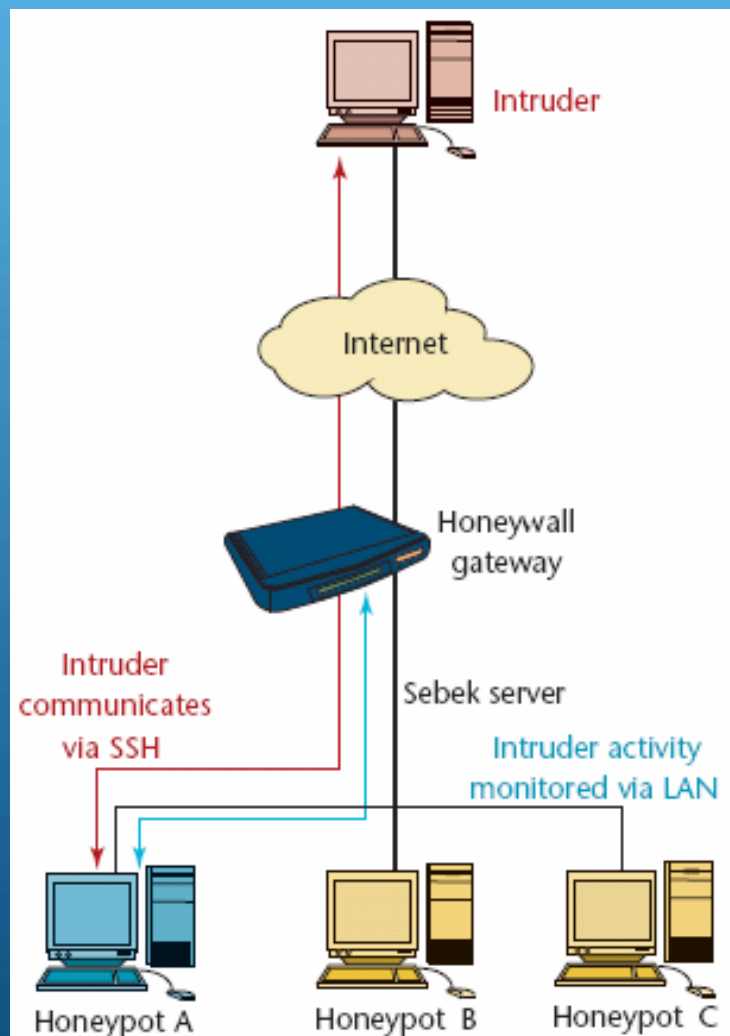
## ■ Sebek Linux Client

- 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

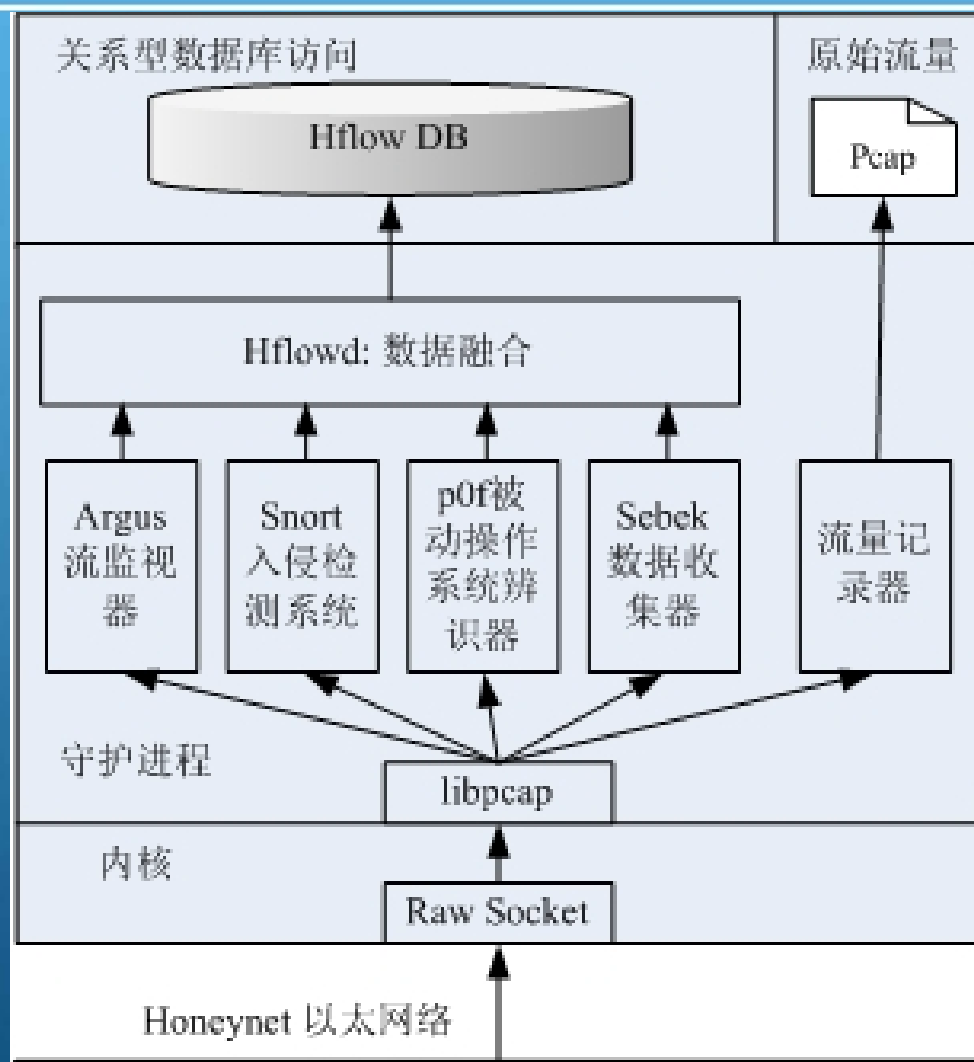
## ■ Sebek Win32 Client

- 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系统行为数据的上传



# 数据捕获机制体系结构图



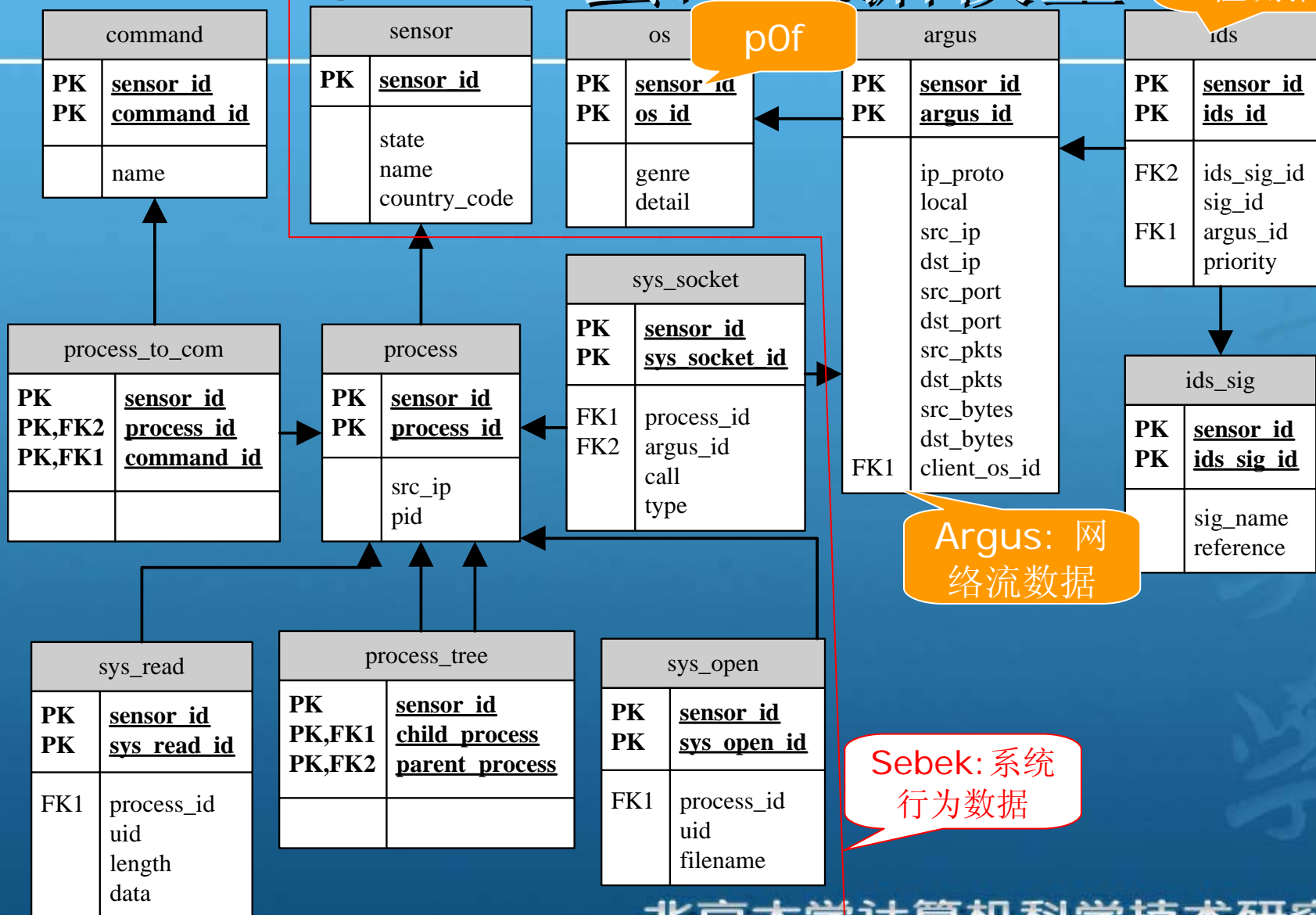
# Gen 3 蜜网数据模型

Snort: 入侵  
检测报警

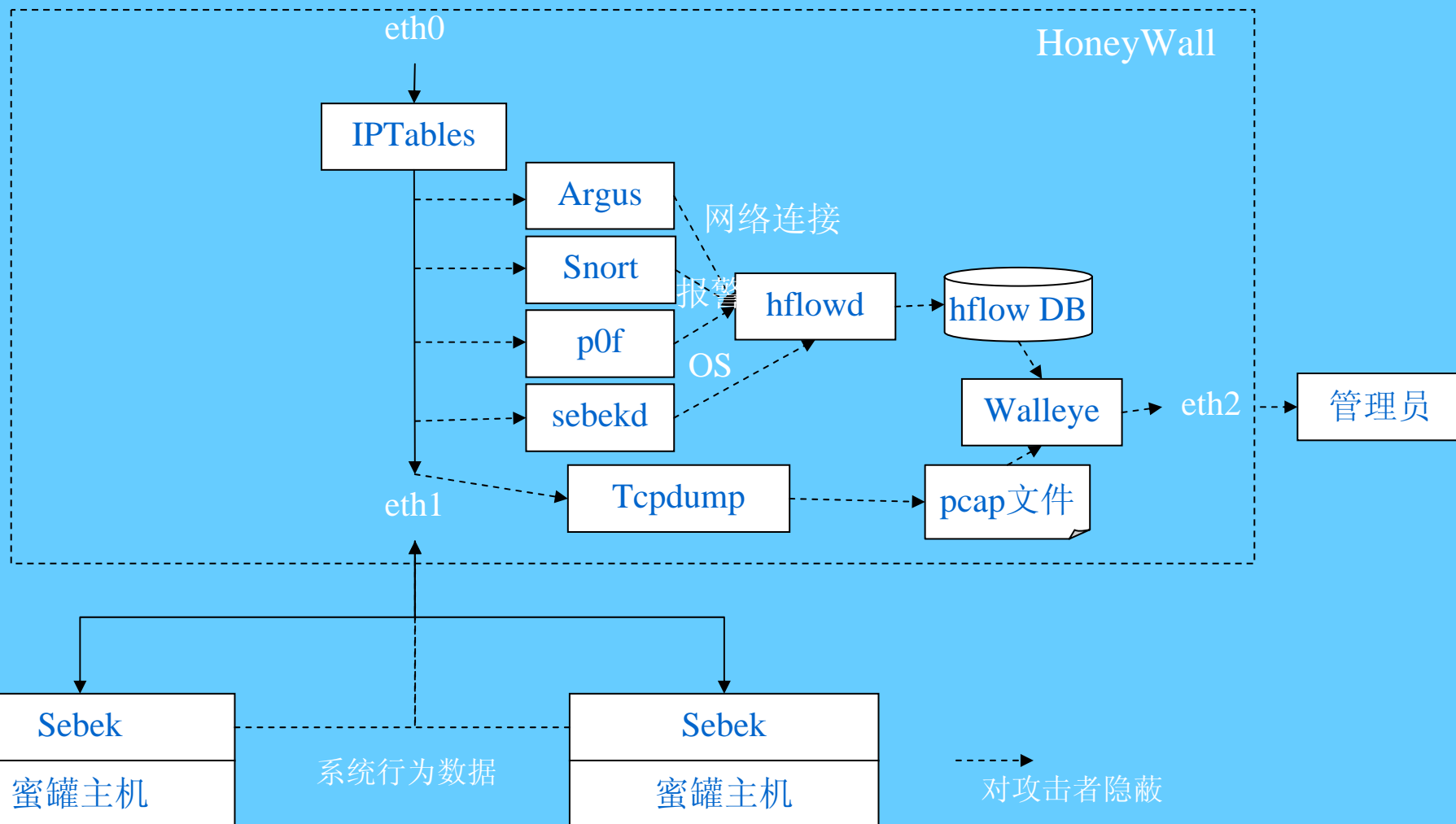
p0f

Argus: 网  
络流数据

Sebek: 系统  
行为数据



# 数据捕获机制图示



# 蜜网技术

- 蜜网技术的提出与发展历程
- 蜜网技术体系框架与核心机制
- 第三代蜜网技术
  - 数据控制机制
  - 数据捕获机制
  - 数据分析机制
  - 配置与管理机制
- 虚拟蜜网



# 数据分析—Walleye



北  
京  
大  
学

- 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数据一慢通道

# Walleye摘要视图

Applications Actions Mon Oct 10, 10:41 PM

Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://192.168.1.3/walleye.pl

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

## The Honeynet PROJECT®

### Walleye: Honeywall Web Interface

Mon Oct 10 21:42:33 2005 GMT  
Logged in as admin

Data Analysis System Admin Logout

#### Online Sensors

Honeywall: 3232235779 Created: Mon Oct 10 21:40:22 2005 Last Update: Mon Oct 10 21:42:27 2005

	Bidirectional		Total	
	In	Out	In	Out
1 hour	0	0	66	64
48 hour	0	0	66	64

2000  
1000  
0

21:00 5:00 13:00 21:00

KBytes Transferred N/10 Alerts

#### Search (short term soln)

Oct 9 2005 21:42:33 End Oct 10 2005 21:42:33

ANY

Prefix Port 0

Source Prefix Port 0

Destination Prefix Port 0

Result Format Pcap File

Submit Query

Done 192.168.1.3

File Browser: root@zhugejw root@zhugejw root@zhugejw root@zhugejw VMWare Work Mozilla Firefox Mozilla Firefox

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=3232235522;page=2>

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

All Time Periods  
Sebek Tracked  
Submit Query

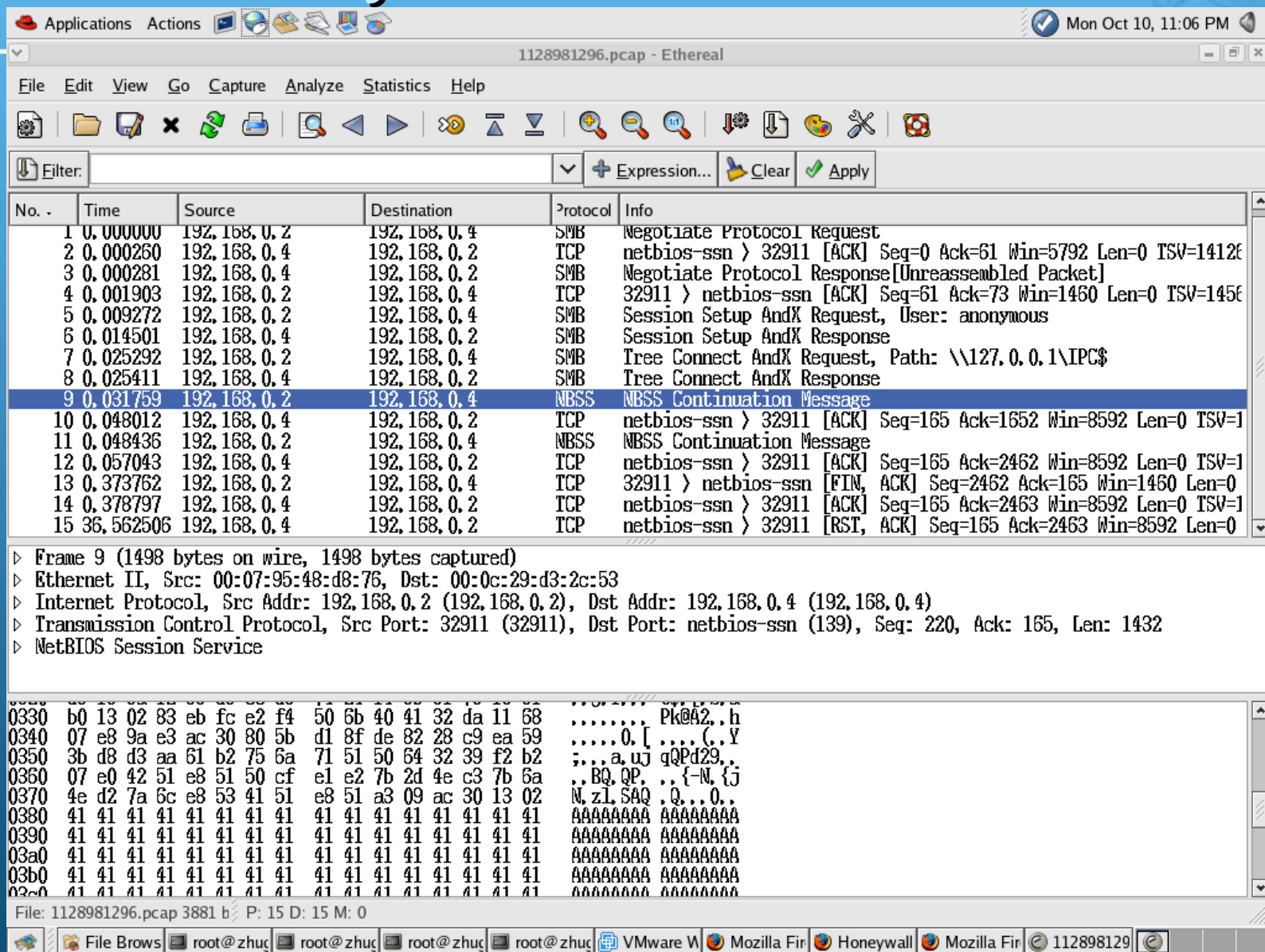
Protocol	Source IP	Source Port	Destination IP	Destination Port	OS	Bytes	Packets	Direction	Notes
TCP	192.168.0.2	32909	192.168.0.4	netbios-ssn	os unkn	3 kB	10 pkts	->	<-2-NETBIOS SMB trans2open buffer overflow attempt
RST	192.168.0.2	32909	192.168.0.4	netbios-ssn	os unkn	<-0 kB	8 pkts	->	
TCP	192.168.0.2	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	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	->	
FIN	192.168.0.4	1032	192.168.0.2	rwhois	Linux	<-0 kB	10 pkts	->	

Snort 报警

pOf操作系统辨识

File Browse root@zhuge root@zhuge root@zhuge root@zhuge VMware Workstation Mozilla Firefox Honeywall A Mozilla Firefox

# 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=14126
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=1456
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 AAAAAAAAAA AAAAAAAAAA  
 0390 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAA AAAAAAAAAA  
 03a0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAA AAAAAAAAAA  
 03b0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAA AAAAAAAAAA  
 03c0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAA AAAAAAAAAA

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

Applications Actions

Mon Oct 10, 11:00 PM

Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://192.168.1.3/?act=tree;sensor=3232235779;process\_id=8

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

Process Tree:


- 21 14: Host: 192.168.0.4, PID: 8805, smbd
- 22 15: Host: 192.168.0.4, PID: 8806, smbd
- 23 16: Host: 192.168.0.4, PID: 8807, smbd
- 24 17: Host: 192.168.0.4, PID: 8808, sh smbd
  - 25 18: Host: 192.168.0.4, PID: 8809, un ame
  - 26 19: Host: 192.168.0.4, PID: 8810, whoami
  - 27 20: Host: 192.168.0.4, PID: 8811, cat

Related Network Connections

Time	PID	Source IP	Destination IP	Protocol	Size	Direction	OS	Details
October 10th 21:09:39	8713	192.168.0.2	192.168.0.4	TCP	32895	2 kB 8 pkts ->	os unkn	<-2-NETBIOS SMB IPC\$ share access
				RST		<-0 kB 7 pkts		<-2-NETBIOS SMB trans2open buffer overflow attempt
October 10th 21:09:39	8713	192.168.0.2	192.168.0.4	TCP	32896	3 kB 10 pkts ->	os unkn	<-2-NETBIOS SMB IPC\$ share access
				RST		<-0 kB 8 pkts		<-2-NETBIOS SMB trans2open buffer overflow attempt
October 10th 21:09:40	8713	192.168.0.2	192.168.0.4	TCP	32897	2 kB 8 pkts ->	os unkn	<-2-NETBIOS SMB IPC\$ share access
				RST		<-0 kB 7 pkts		<-2-NETBIOS SMB trans2open buffer overflow attempt




File Browse root@zhuge root@zhuge root@zhuge root@zhuge VMware Workstation Mozilla Firefox Honeywall A Mozilla Firefox

# 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=3232235779;process\\_id=24;inode=9923](https://192.168.1.3/?act=pd;sensor=3232235779;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
21:09:15	whoami
21:09:17	cd /etc
21:09:20	cat shadow
21:09:26	exit
21:09:26	

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

File Browse root@zhuge root@zhuge root@zhuge root@zhuge VMware Wc Mozilla Firef Honeywall A Mozilla Firef



# 数据分析技术的进一步研究

- HoneySnap—攻击数据摘要工具
  - 英国蜜网项目组→The Honeynet Project
  - 输入：Tcpdump捕获的原始网络包pcap文件
  - 输出：统计信息、HTTP/FTP/IRC应用层摘要信息、Sebek键击记录等
- Athena—攻击关联分析工具
  - 狩猎女神项目组，7th IEEE IAW发表
  - 在AI领域中经典规划图和目标规划图模型基础上，提出扩展目标规划图模型，实现攻击规划识别算法
  - 输入：IDS报警信息、Argus网络连接数据等多源数据
  - 输出：高层攻击场景图
- UDAF—统一数据分析框架
  - The Honeynet Project
  - 具有良好逻辑性设计、自完备的、跨平台的数据分析中间件
  - 提供：不同格式的数据获取、数据过滤、数据融合、数据输出以及数据可视化

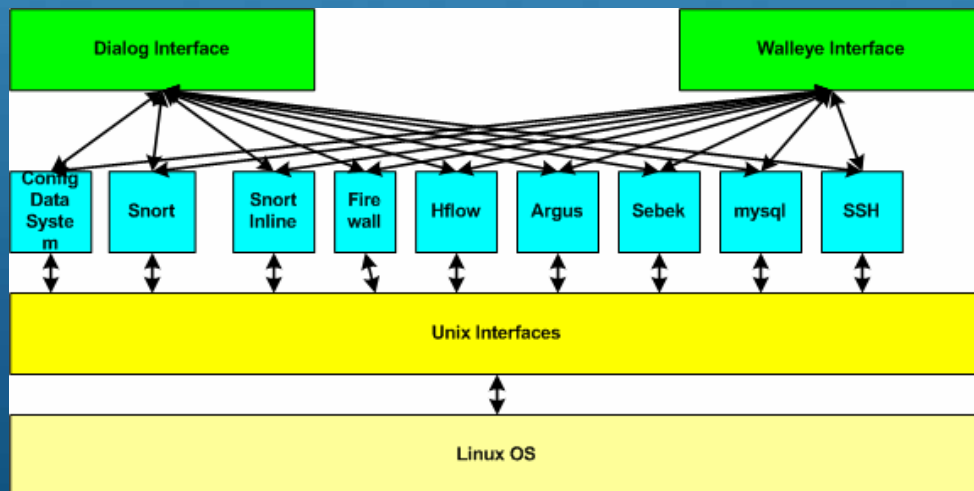
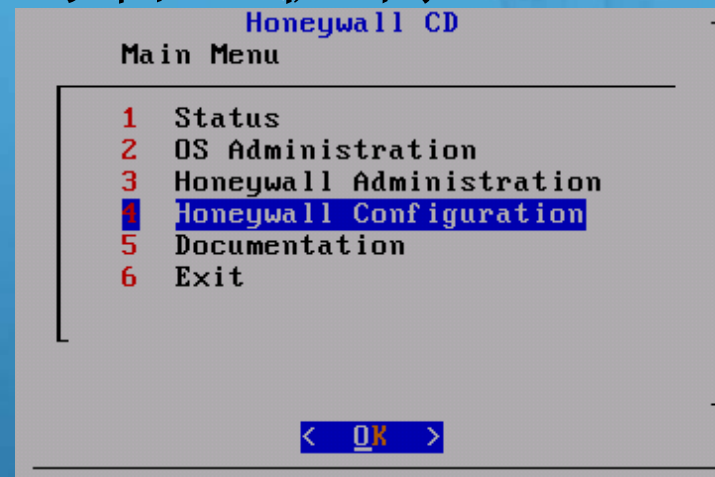
# 蜜网技术

- 蜜网技术的提出与发展历程
- 蜜网技术体系框架与核心机制
- 第三代蜜网技术
  - 数据控制机制
  - 数据捕获机制
  - 数据分析机制
  - 配置与管理机制
- 虚拟蜜网

# 配置与管理机制

## ■ 目前Roo蜜网网关的配置与管理机制

- Honeywall.conf
- 命令行: hwctl
- 配置对话框: Menu
- Web配置界面: Walleye



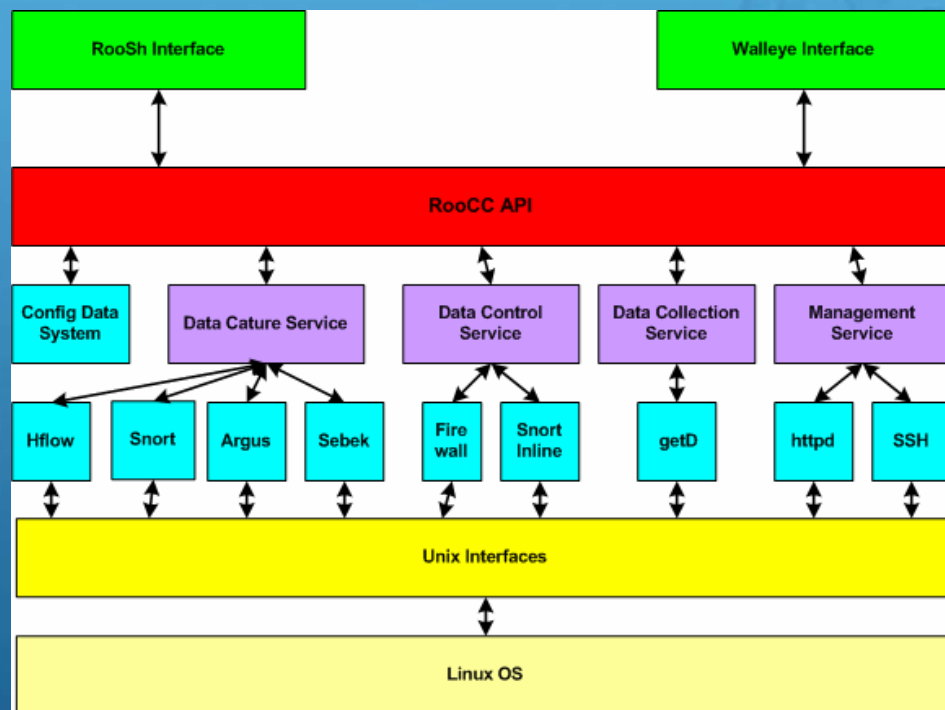
# 配置与管理机制—Future

## ■ Roo2.x最大改进

- RooCC API配置与管理中间层
- 实现RooSH接口
- 通过XML-RPC支持分布式配置与管理—构建分布式蜜网

## ■ 对蜜罐的配置与管理

- 狩猎女神项目组—PotManager



# 蜜网技术

- 蜜网技术的提出与发展历程
- 蜜网技术体系框架与核心机制
- 第三代蜜网技术
  - 数据控制机制
  - 数据捕获机制
  - 数据分析机制
  - 配置与管理机制
- 虚拟蜜网



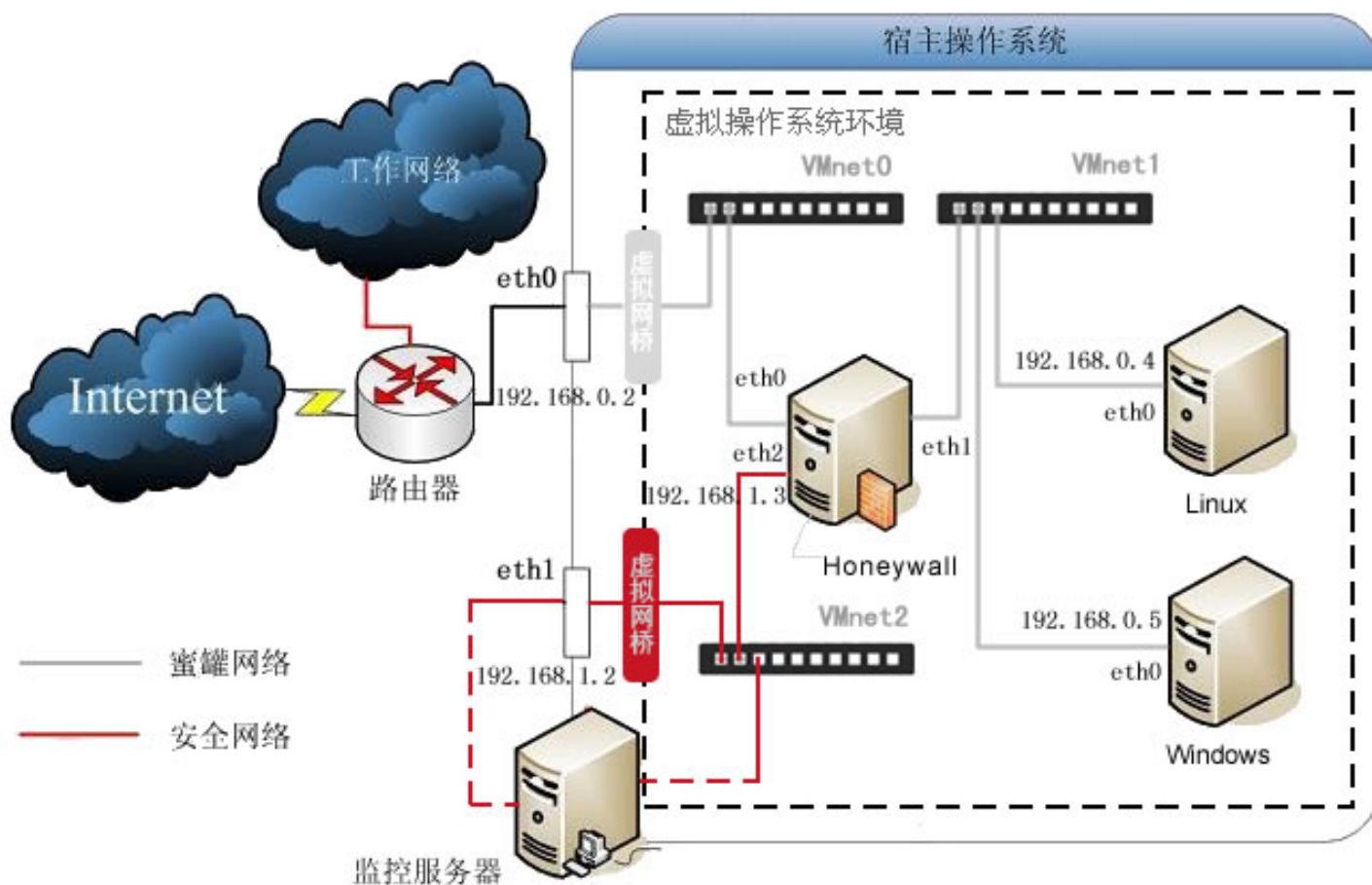
# 虚拟蜜网

- 虚拟蜜网(Virtual Honeynet)
  - 通过虚拟机技术，在一台计算机上部署整个蜜网体系的解决方案
  - 优势：低成本、易于管理
  - 弱势：性能问题、更高的安全风险、容易被 fingerprinting 识别
- 虚拟机(Virtual Machine)技术
  - Vmware: player, workstation, GSX server, ESX server
  - Virtual PC
  - User Mode Linux



# 虚拟蜜网部署拓扑图

## 第三代虚拟蜜网roo网络拓扑图



# 蜜网技术在进一步发展 —HRA workshop 2006



# 演示：Win32平台下构建 第三代虚拟蜜网