|  |  |
| --- | --- |
| 论文作者姓名 | ：胡逢彬 |
| 作者学号 | ：2225060716 |
| 所在学院 | ：软件学院 |
| 所学专业 | ：网络工程 |
| 导师姓名职称 | ：赵辉（讲师） |
| 论文完成时间 | ：2022年11月15日 |

2022年11月15日

基于蜜网的入侵监控平台

**河南大学2013届本科毕业论文**

Intrusion Monitoring Platform Based On Honeynet

学号：2225060803

**目录**

[摘要 I](file:///D:\\zm桌面\\2225060716-张英涛-实验3-003班.docx" \l "_Toc119443236)

[ABSTRACT II](#_Toc119443237)

[第1章绪论 1](#_Toc119443238)

[1.1课题来源 1](#_Toc119443239)

[1.2课题背景 1](#_Toc119443240)

[1.3国内外在该方向的研究现状及分析 1](#_Toc119443241)

[1.3.1蜜罐（Honeypot）技术 1](#_Toc119443242)

[1.3.2蜜网（Honeynet）工程 2](#_Toc119443243)

[1.4使用的开发平台 2](#_Toc119443244)

[第2章系统总体分析和设计 3](#_Toc119443245)

[2.1整体网络拓扑 3](#_Toc119443246)

[2.2组网 3](#_Toc119443247)

[第3章蜜网搭建 4](#_Toc119443248)

[3.1Honeyd介绍 4](#_Toc119443249)

[3.2具体搭建过程 4](#_Toc119443250)

[3.2.1定义配置文件 4](#_Toc119443251)

[3.2.2运行honeyd 5](#_Toc119443252)

[3.2.3搭建后测试 5](#_Toc119443253)

[第4章详细设计 6](#_Toc119443254)

[4.1系统采用的技术原理 6](#_Toc119443255)

[4.5数据分析模块 6](#_Toc119443256)

[4.5.1攻击规则库的定义 6](#_Toc119443257)

[4.5.2（小节题目） 7](#_Toc119443258)

[结论 8](#_Toc119443259)

[参考文献 9](#_Toc119443260)

# 摘要

近年来，随着互联网在全球范围内的发展和普及，人们可以方便地共享各种各样网络资源，与此同时，网络攻击问题也越来越引起人们的关注。因此，网络安全已经成为网络技术发展中最重要的一环。

本文首先分析了网络安全现状和存在的问题，然后介绍了一种新的主动式安全机制——蜜网技术。在此基础上，设计了基于蜜网的入侵监控平台。设计过程主要包括蜜网搭建和入侵平台设计两大部分。其中蜜网搭建部分利用Honeyd工具进行，具有灵活、方便、易于维护的特点。入侵平台设计部分基于.NET平台，采用C#语言和Oracle数据库，主要实现数据控制、数据捕获和数据分析蜜网技术的三大核心需求。

本论文主要解决以下问题：

1. 在虚拟机上利用Honeyd工具实现虚拟蜜网的搭建。

2. 入侵监控平台利用SSH协议远程登陆蜜网的入口主机，通过设置入口主机的Iptables实现数据控制功能。

3. 在入口主机处监听数据包，捕获入侵者的活动信息，实现数据捕获功能。

4. 将捕获到的数据包与入侵规则库进行匹配，分析入侵行为，并通过可视化界面将分析后的信息友好地展示给用户。

关键词：蜜网；入侵监控；数据控制；数据捕获；数据分析

# ABSTRACT

Recently, with the development and widespread use of the internet globally, people can share comprehensive resources conveniently. But at the same time, the problems of network intrusion are given more and more attention by people gradually. Therefore, network security had become one of the most important fields in computer technology.

Thesis analyzes firstly present status of the network security and existent problems, then introduce a new active security mechanism, honeynet technology. On the basis of the introduction, intrusion monitoring platform based on honeynet is to be designed. The design process includes two main parts, the set-up of honeynet and the design of inrusion monitoring flatform. Honeyd, a software tool, is made use of during the set-up of honeynet, which has the characteristics of flexibility, convenience and maintainability. The design of intrusion monitoring platform is based on .NET platform, and employs C# programming language and Oracle 9i DataBase. This parts mainly implements data control, data capture,and data analysis, which are three central reqiurements of honeynet technology.

The problems settled in this thesis are as follows:

1. virtual honeynet is set up with the tool honeyd, which runs on the VMWare.

2. telnet from instrusion monitoring platform to the entry host of honeynet via the protocol SSH, and make rules for Iptables on the entry host to implement data control.

3. monitor data packages on the entry host, and capture intruders’ information. The purpose is to achieve data capture.

4. match data packages captured with intrusion rules base, and then analyze intrusion actions. At last, information analyzed is to be showed by means of visional interface to users friendly.

Keywords: Honeynet; intrusion monitoring; data control; data capture; data analysis

# 第1章绪论

随着互联网的扩张和基于互联网应用的发展，网络安全越来越受到人们的关注。网络入侵的检测和防范也越来越受到人们的重视。该文提出了一个基于蜜网的入侵监控平台，通过搭 建蜜网系统，诱骗入侵者进入受控环境，利用各种技术监控入侵者的入侵行为，分析其采用的攻击工具和攻击方法，从而有针对性采取对策降低入侵者取得成功的可能性，提高系统安全性。可见，开发基于蜜网的入侵监控平台对网络安全具有重要的现实意义。

## 1.1课题来源

该课题为自选课题。（或者：该课题为导师指定的题目。）

## 1.2课题背景

众所周知，互联网技术的发展十分迅猛，已经在各行各业得到了广泛的应用。与此同时，针对网络的攻击手段层出不穷，使得网络安全问题日益严重。随着网络攻击技术的发展，特别是分布式拒绝服务（DDoS）攻击，僵尸网络（Bot net）、网络钓鱼（Phishing）和网络蠕虫（Internet Worms）的泛滥，互联网上的每一台主机都已经成为攻击的目标。互联网俨然成了攻击者的天堂。

……

## 1.3国内外在该方向的研究现状及分析

目前国外在网络信息欺骗技术方面的研究成果主要有两大类：蜜罐技术和蜜网工程。但国内在这方面的研究成果不多。

## 1.3.1蜜罐（Honeypot）技术

“蜜罐”是一种信息系统资源，其价值在于被非授权者或非法者所使用（A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource.）。这个定义表明蜜罐并无其他实际作用，因此所有流入/流出蜜罐的网络流量都可能预示了扫描、攻击和攻陷。而蜜罐的核心价值就在于对这

些攻击活动进行监视、检测和分析。

蜜罐技术的发展历程可以分为以下三个阶段。

……

## 1.3.2蜜网（Honeynet）工程

“蜜网”，又可称为诱捕网络。它是在传统蜜罐技术的基础上，由“蜜网项目组”提出并倡导的由真实主机、操作系统、网络服务和应用程序构成的网络体系框架，结合了一系列数据控制、捕获和分析工具，使得安全研究人员能够更好地在一个高度可控的环境中了解互联网的安全威胁。

……

## 1.4使用的开发平台

蜜网环境搭建：VMWare +Red Hat Linux 内核版本：2.64.20-8 smp + Honeyd 1.5c，入侵监控平台：Windows XP，开发工具VS 2008、语言C#、数据库Oracle 10g。如表1-1所示。

|  |  |  |  |
| --- | --- | --- | --- |
| 表头 |  |  |  |
| 表文 |  |  |  |
|  |  |  |  |

表1-1表标题

# 第2章系统总体分析和设计

本章从平台的整体网络拓扑、系统结构和软件架构三个方面对该平台进行了总体分析说明。蜜网环境搭建之后，主要通过数据控制模块、数据捕获模块、数据分析模块、行为统计回放模块、拓扑探测和系统管理模块实现蜜网的数据捕获、数据分析和数据控制三大核心需求。

## 2.1整体网络拓扑

入侵监控平台：是源程序的运行主机，采用Windows XP操作系统。

入口控制主机：通过虚拟机实现，虚拟机上安装Red Hat Linux（内核版本2.64.20-8 smp）

虚拟蜜网：利用在虚拟机上安装的Honeyd工具进行搭建。

本演示系统采用的拓扑结构如图2-1所示。

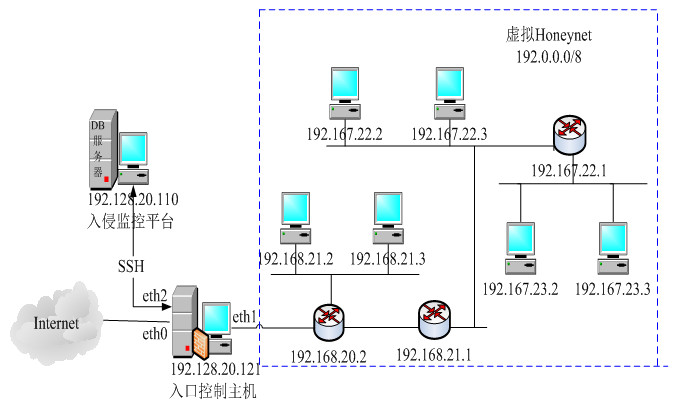


图2-1 平台拓扑结构

入口控制主机包括三个网络接口，eth0接入外网，eth1连接蜜网，而eth2作为一个秘密通道，连接到一个监控平台。……

## 2.2组网

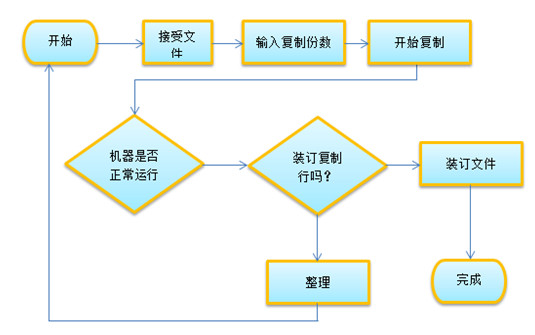


图2-2 流程图

# 第3章蜜网搭建

由于受到资金、实验环境、技术等因素的制约，本系统采用了易于部署的虚拟蜜网作为演示平台。虚拟蜜网的具体搭建过程是先在虚拟机（VMWare）上安装Red Hat Linux 2.4.20-8smp操作系统，然后在其上安装Honeyd软件。其中，Red Hat Linux作为入口控制主机，蜜网的部署由Honeyd实现。

## 3.1Honeyd介绍

Honeyd是一个很小巧的用于创建虚拟的网络上的主机的后台程序，这些虚拟主机可以配置使得它们提供任意的服务，利用个性处理可以使得这些主机显示为在某个特定版本的操作系统上运行[1]。……

## 3.2具体搭建过程

Honeyd提供了易于掌握的虚拟蜜网配置方法。通过自定义配置文件可以定义整个蜜网系统的拓扑构架，虚拟蜜网中受控主机所运行的操作系统，受控主机如何应答关闭的端口，什么样的端口提供怎么样的服务等。服务的伪装实现是通过将服务脚本绑定到一个网络端口，脚本可以是标准的模拟某种服务的shell脚本，而且我们可以本方便地从网上下载常用的，如SMTP、HTTP和Telnet等服务的脚本。

## 3.2.1定义配置文件

Honeyd支持创建任意的网络拓扑结构，对路由树的模拟需要首先配置一个路由进入点，然后将路由器绑定到与它直接相连的网络，并指明通过该网络可以到达的其他路由器。在绑定过程可配置链路时延和丢包率[4]。

……

举例：以下配置文件配合图2-1的网络拓扑结构。程序代码如下：

＃定义蜜网中主机的操作系统类型以及提供的服务＃

create aix

set aix personality "Microsoft Windows NT 4.0 SP3"

add aix tcp port 80 "sh /home/honeyd/honeyd-1.5c/scripts/web.sh"

add aix tcp port 22 "sh /home/honeyd/honeyd-1.5c/scripts/test.sh &ipsrc &dport"

set aix default tcp action reset

#默认情况下的操作系统类型以及提供的服务#

……

将上述的配置文件命名为Honeyd.conf，然后运行如下的命令来运行honeyd。

## 3.2.2运行honeyd

在运行honeyd之前，需要保证honeyd主机对配置的虚拟蜜网中的受控主机的IP作出arp请求的应答，即将MAC地址与伪装IP进行映射。可以通过运行arpd软件来做出arp应答，arpd将对指定的IP地址范围内使用的IP用honeyd主机的MAC地址作出arp应答。

……

## 3.2.3搭建后测试

Honeyd提供仿真服务脚本来对应用层的协议进行模拟，安装honneyd后，可以在源代码包中的scripts目录下找到honeyd提供的脚本。Honeyd提供的脚本的语法并不复杂，基本的规则就是当入侵者登陆后，输入命令，脚本会做出相应的输出回应，使入侵者无法辨别出真实服务和虚拟服务。

……

# 第4章详细设计

本章主要对各个功能模块的详细设计做具体说明。首先对系统中所采用的技术原理做一概述，然后对各模块间的架构进行阐述，最后分别对各个模块的设计特别是一些关键技术进行详细论述。其中，最重要的是数据控制模块、数据捕获模块和数据分析模块。

## 4.1系统采用的技术原理

……

## 4.5数据分析模块

数据分析就是将数据捕获模块获得的信息，与定义好的攻击规则库进行模式匹配和行为提取，最终形成报警信息。并将报警信息存入数据库，供行为回放和统计模块查询。其中最关键的技术就是攻击规则库的定义和模式匹配算法的效率，它们直接关系到数据分析的准确性。

## 4.5.1攻击规则库的定义

攻击规则库按照入侵行为的种类划分为相应的表，用户可以根据需要选取对应的表进行匹配，每一类表中包括数十条的规则，分别代表同一种类型的不同入侵行为。

进行数据分析时，应该遵循先匹配所有入侵行为的共同特征后才是个体特征的原则。例如：如果首先匹配IP地址，一旦发现并不属于匹配范围之内，就立即匹配下一个数据包而非继续匹配该包的其他字段。这样就保证了分析的快速性。

……

(1) 规则头

规则头包括：协议、源/目的IP地址、子网掩码以及源/目的端口。

1) 协议

现在可以分析可意包的协议有：TCP、UDP、ICMP、和IP。

2) IP地址

地址由数字型的IP地址和一个cidr块组成。Cidr块指示作用在规则地址和需要检查的进入任何包的网络掩码。/24表示C类网络，/16表示B类网络，/32

表示一个特定及其的IP地址。否定运算符”!”可以应用到Ip地址上，表示匹配除了列出的IP地址之外的所有IP地址。

3) 端口号

端口号可以用几种方法表示，包括”any”端口、静态端口定义、范围、以及通过否定操作符。”any”端口是一个通配府，表示任何端口。静态端口定义表示一个单个端口号，例如23表示telnet。端口范围用范围操作符“：”表示。范围操作符可以有数种使用方法。

【例1】描述udp any any -> 192.168.1.0/24 1:500 记录来自目标端口范围在1到500的udp流。

tcp any any -> 192.168.1.0/24 :1024 记录来自目标端口小于等于1024的tcp流

tcp any :1024-> 192.168.1.0/24 1024: 记录来自任何小于等于1024的特权端口，目标端口大于等于1024的tcp流

tcp any any -> 192.168.1.0/24 !1024: 端口否定操作符用“！”表示

示例，描述：

udp any any -> 192.168.1.0/24 1:500 记录来自目标端口范围在1到500的udp流

tcp any any -> 192.168.1.0/24 :1024 记录来自目标端口小于等于1024的tcp流

……

(2) 操作步骤

## 4.5.2（小节题目）

# 结论

本论文分析了当前网络安全的现状和网络安全重要性，以及传统安全技术的被动防御局限性。为了突破这一不足，引入了蜜网这一主动防御安全技术，设计了基于蜜网的入侵监控平台。蜜网搭建利用安装在VMWare上Honeyd工具进行虚拟搭建，入侵监控平台采用VS 2008开发工具，C#开发语言，基于.NET Framework上的三层C/S模式。

本平台具有以下优点：

1．部署方便成本低：利用Honeyd进行虚拟部署，可以灵活地根据需要模拟蜜网的拓扑结构，蜜网中受控主机的服务和开放端口，配置文件语法简单、易于修改。另外，用虚拟蜜网代替实际蜜网是部署成本大大降低。

2．低漏报率和误报率：由于虚拟蜜网不提供任何实际的作用，因此其收集到的数据很少，同时收集到的数据很大可能就是由于黑客攻击造成的，收集的数据保真度高。

3．易用性强，C#界面友好，操作简便。

存在以下局限性：

1．采用虚拟蜜网会带来更大的风险，黑客有可能识别出虚拟操作系统软件的指纹，也可能攻破虚拟操作系统软件从而获得对整个虚拟蜜网的控制权。

2．数据分析部分需要进一步完善和改进，特别是入侵规则库定义需要优化，模式匹配过程需要进一步提高实时性和准确性。

# 参考文献

[1] 崔继强，乔佩利．虚拟蜜罐Honeyd的分析和研究．机电信息，2004年第13期，p27-29．

[2] The Honeynet Project / Know Your Enemy: Honeynets-What a honeynet is, its value, overview of how it works, and risk/issues involved, The Honeynet Whitepapers, http://www.honeynet.org/papers/honeynet/, March 2006．

[3] 诸葛建伟，吴智发，张芳芳．利用蜜网技术深入剖析互联网安全威胁．中国计算机大会，2005．

[4] Niels Provos,Honeyd: A Virtual Honeypot Framwork, in 13th USENIX Security Symposium, San Diego, CA, 2004．

[5] 马骏．C#网络应用编程（第2版），人民邮电出版社，2010年3月．

[6] 谢希仁．计算机网络（第4版）．电子工业出版社，2003年6月．