第32卷 第18期 计 算 机 工 程 2006年9月
Vol.32 № 18 Computer Engineering September 2006
·安全技术· 文章编号：1000—3428(2006)18—0163—03 文献标识码：A 中图分类号：TP309

分布式虚拟陷阱网络系统的设计与实现

汪 洁[1]，王建新[1]，唐 勇[2]
(1. 中南大学信息科学与工程学院，长沙 410083；2. 国防科技大学计算机学院，长沙 410073)

摘 要：目前大部分安全技术被设计用来阻止未授权的可疑行为获取资源，同时安全工具是作为一种防御措施被布置，所以它们对网络的保护有限。在分析国内外研究现状的基础上，针对现有网络安全工具在入侵检测以及防护等方面的不足，设计和实现了分布式虚拟陷阱系统。该系统所分布的代理由混合 Honeynet 和低交互的 Honeypot 构成，降低了 Honeypot 固有的风险，增加了模拟的真实性，弥补了现存的各类 Honeypot 的不足。作为一种动态安全防御机制，可以有效地提高大规模网络的整体安全性，是传统安全机制的有力补充。
关键词：网络安全；入侵检测；蜜罐；陷阱网络

Design and Implementation of Distributed Virtual Honeynet System

WANG Jie[1], WANG Jianxin[1], TANG Yong[2]
(1. College of Information Science & Engineering, Central South University, Changsha 410083;
2. College of Computer, National University of Defense Technology, Changsha 410073)

【Abstract】 Most security technologies are designed to prevent unauthorized activity to resources, and security tools are put into place as a defensive measure. Therefore there is some shortcoming in protecting network. After analyzing the research situation and the shortcoming of security tools in intrusion detection and in protecting system, distributed virtual honeynet system is studied and implemented. The system is composed of hybrid virtual honeynet and low-interaction honeypot, which reduces the inherent risk of honeypot, adds the simulation's trueness, and it makes up the shortcoming of exiting different type honeypots. As a dynamic security defensive mechanism, it can improve effectively integrate safety of large scale of network, and is completely supplement of traditional security mechanism.
【Key words】 Network security; Intrusion detection; Honeypots; Honeynets

1 概述

目前，安全工具是作为一种防御措施被布置，对网络的保护有限，而且IDS和防火墙等安全工具的使用有许多公认的不足[1]，它们提供了太多的信息，使得管理员每天需要从几千兆字节里去挖掘真正有用的攻击信息[2]。所以需要新的技术和手段来保护脆弱的网络，而欺骗和诱骗可以作为一种新的策略来对网络进行保护[3]。

陷阱网络Honeypot技术是一种诱骗技术，是指“一种安全资源，它的价值就在于被探测、被攻击或被攻陷”[4]，它是一种主动的保护网络的手段。作为一种资源，它的目的是监视、记录那些探测、攻击和威胁其安全的活动[5]。

目前，Honeypot 有许多分类标准，按照 Honeypot 所允许黑客活动的级别，可以将其分为两种类型：

(1)低交互型 Honeypot

与外部主机有比较有限的交互作用，一般通过模拟服务和操作系统来实现。低交互 Honeypot 的例子有 Honeyd、Specter 和 KFSensor。

(2)高交互型 Honeypot——Honeynet

Honeynet 也称为陷阱网络或密网，它具有多个系统和应用程序供黑客探测和攻击，从而获得黑客的信息。与低交互 Honeypot 相比，它能捕获更多的信息，不需要预先设想黑客将会有什么样的行为。

从另外的角度来看，Honeynet 网络有真实的和虚拟的两种。真实的 Honeynet 指网络中的每一个系统都是一台真实的主机。虚拟的 Honeynet 是指在一台简单的系统上实现 Honeynet 的技术。虚拟的 Honeynet 网又可以分为两种：自包含虚拟 Honeynet(Self-contained Virtual Honeynet)和混合虚拟 Honeynet(Hybrid Virtual Honeynet)。

现在所布置的陷阱网络有低交互的 Honeypot(如 Honeyd)、高交互的 Honeypot(如 Honeynet)、虚拟的 Honeynet。低交互的 Honeyd 虽然所需的资源少，能模拟很多的网络服务，但是它所模拟的服务的程度有限。可能仅仅能与黑客进行一二次交互，而且它的日志都是记录在本地，这就提高了被黑客发现和篡改日志的风险。同样，真实的 Honeynet 陷阱网络也有很多不足的地方，例如开销很大，它的高欺骗性是以高的资源开销换来的。目前，Honeynet 陷阱网络都是放在一个网段内，它受到黑客的探测和攻击的几率远低于它分布于多个网段内所受到的黑客攻击和探测的几率，这样它所学习到的黑客攻击方法和攻击工具相对而言是有限的，而且无法检测其他网段内所发生的黑客攻击。

针对目前 Honeynet 中存在的问题，本文提出了分布式的虚拟陷阱网络系统。它是将高交互的虚拟 Honeynet 和低交互的 Honeypot 作为代理分布在各个网段内。虚拟的 Honeynet 布置在多个局域网内，它不仅能够弥补单一 Honeynet 的不足，而且它的实际开销也比真实的 Honeynet 要低，并且因为陷阱网络里面有真实的网络服务和黑客进行交互，所以降低

基金项目：国家自然科学基金资助项目(60403032)
作者简介：汪 洁(1980—)，女，硕士，主研方向：网络信息安全；王建新，博导；唐 勇，博士生
收稿日期：2005-12-02 **E-mail：**lovelywangjie@163.com

了整个陷阱网络被发现的风险。而网段内布置的低交互Honeypot能够模拟大量的主机，使得真实主机被攻击的概率大大降低。

2 分布式虚拟陷阱网络系统的设计

本文采用典型的Honeynet网和虚拟软件相结合的自包含虚拟Honeynet网，设计了分布式虚拟陷阱网络系统(Dis-VHoneypot)。它由3个层次构成，它们之间是树型关系，可适用于大规模的网络环境。第1层节点是总控制中心；第2层节点是控制中心；第3层是代理节点，代理节点由位于同一台主机上的一级和二级代理构成。一个网段内设有控制中心和代理，总控制中心部署在不同的网段内。总控制中心是一台装有Windows XP操作系统的主机，代理是虚拟Honeynet，控制中心是一台主机，它对网段内的代理进行配置和管理。基于虚拟Honeynet的分布式陷阱网络系统(Dis-VHoneypot)的结构如图1所示。

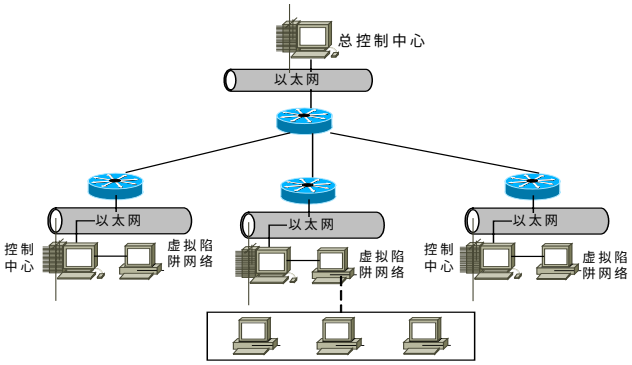

图1 Dis-honeypot结构

2.1 控制中心

控制中心包括总控制中心和代理控制中心，其中代理控制中心是一台普通的主机，上面安装了防火墙，用来控制代理往外的连接；总控制中心负责接收代理发送的信息并对其进行分析。

如图2所示，总控制中心(MCCenter-Master Control Center)主要包括通信部件、报警处理和显示部件，其主要功能是完成报警接收和显示以及报警分析和结果显示等。MCCenter主要组成部件有通信部件、报警接收部件、报警分析部件、报警显示界面、报警分析显示界面、用户界面。

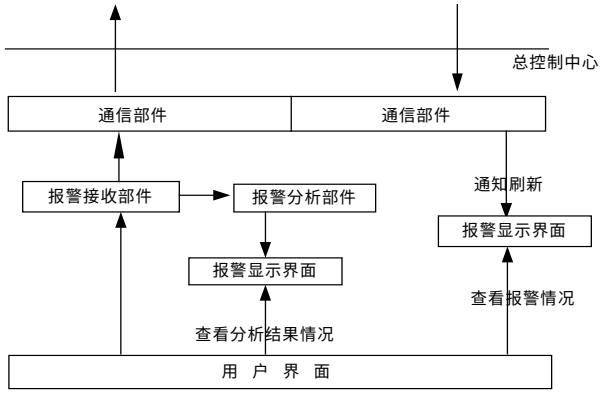

图2 总控制中心结构

2.2 代理节点的基本结构

本系统的代理是安装在代理控制中心上的3台虚拟主机，在其中一台虚拟主机上配置了监测代理(MAgent)。系统代理的结构如图3所示，图的左边是MAgent的组成部件，右边是配置了不同操作系统的3台虚拟主机。

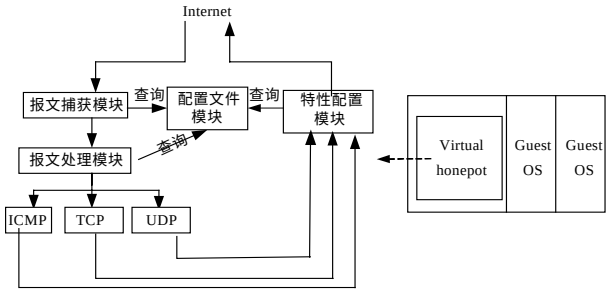

图3 代理结构

MAgent是属于低交互的Honeypot，可以使某台主机在网络上伪装成多个地址，同时监视所有未使用的IP地址。MAgent由以下5部分组成：

(1)报文捕获模块：MAgent将目的IP地址属于虚拟Honeypot配置范围内的报文捕获。

(2)报文处理模块：首先将收到的报文作适当的处理，然后对报文进行分类，并使用预先配置好的网络服务来对所接收到的报文进行处理。

(3)个性配置模块：将准备发送的报文根据不同的操作系统配置不同的特性，使得黑客对代理进行扫描时，能够得到相应操作系统的信息。

(4)配置文件模块：对配置文件进行管理，管理员可以根据具体的需要去配置虚拟Honeypot，例如可以配置不同的网络拓扑和操作系统以及相应的网络服务。

(5)报警引擎：将MAgent捕获的关于黑客的信息进行整理并转换成XML格式，发送到总控制中心。

3 Dis-VHoneypot关键模块的实现

3.1 总控制中心的关键模块实现

总控制中心MCCenter的主要功能是完成报警接收和显示以及报警分析和结果显示等功能，是在Windows XP平台下进行的设计和实现。

报警接收部件的功能主要是接收传感器的XML信息，调用XML解释器对其进行解释，判断其是报警信息，还是代理的生存性信息。接收部件还要维护与代理的连接，当连接因为网络问题或者其它问题而中断时，接收模块会在设定的超时时间内检测到这一事实，从而关闭连接和与连接相关联的资源(如线程、网络资源等)，同时将远程代理的工作状态存入数据库。

3.2 MAgent的报文处理流程

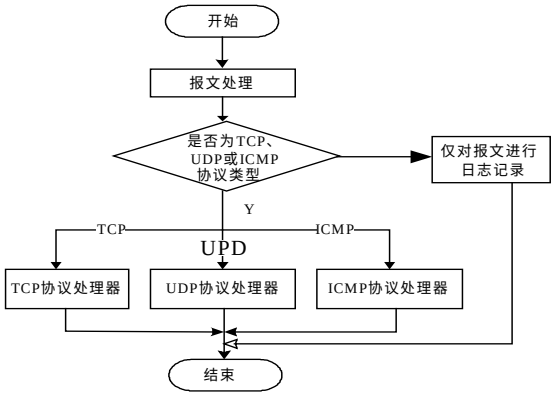

图4 报文处理流程

MAgent能够对外部主机发过来的TCP等协议的报文进行处理，报文处理的流程如图4所示。在处理报文之前，会先进行一些准备工作。

3.3 MAgent 的协议处理器

根据前面介绍的报文处理流程，MAgent 包含 ICMP 协议处理器、UDP 协议处理器和 TCP 协议处理器。

(1)ICMP 协议处理器

ICMP 协议处理器支持大部分的 ICMP 请求。默认情况下，所有的蜜罐配置都响应 echo 请求并处理那些目的不可达的信息。对其他请求的处理取决于配置的特性，处理完之后会进行日志记录和报警发送。

(2)UDP 协议处理器

MAgent 能为 UDP 建立与任何服务的连接。这里所谓的服务是指在标准输入流接收数据并将其发送到标准输出流的外部应用程序。当接收到端口已关闭的 UDP 包时，只要预先配置的特性允许，MAgent 就发出一个端口不可到达的 ICMP 信息。

(3)TCP 协议处理器

MAgent 包含一个简单的 TCP 状态机。它能充分支持通过 FIN 或 RST 建立和撤销 3 次握手的连接。TCP 报文的处理流程如图 5 所示。

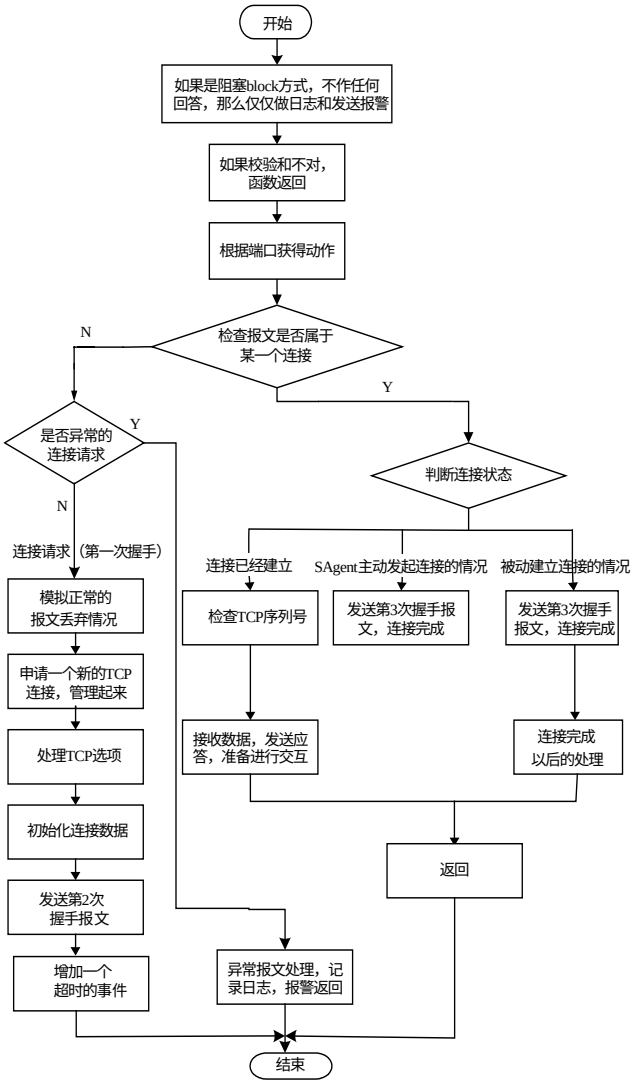

图 5 TCP 协议连接处理流程

在连接建立之后，MAgent 会与连接主机进行进一步的交互。配置文件里面会给蜜罐的许多相应的端口设置许多的活动，即当外部主机与这个端口进行交互时，MAgent 应该作出什么样的响应。有些端口没有设置具体的响应行为，那么就采用通用的响应方式。整个处理流程见图 6 所示。

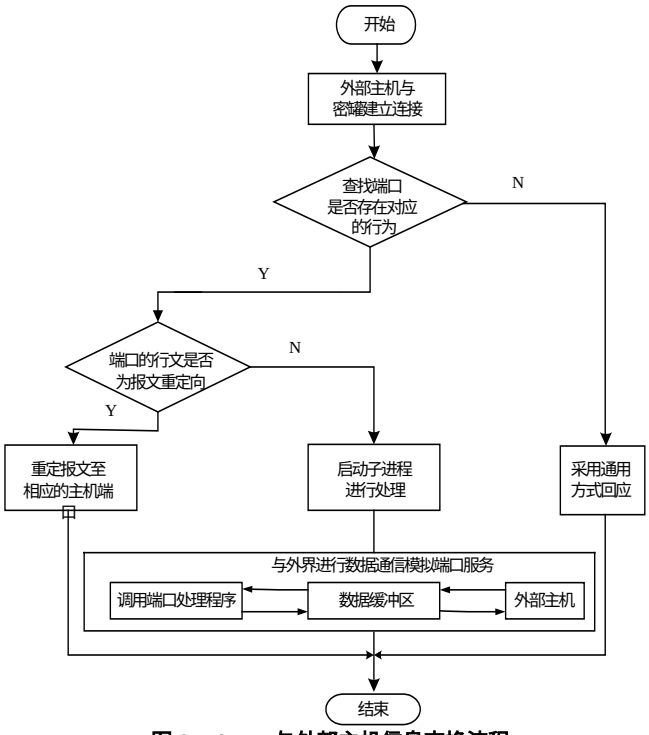

图 6 MAgent 与外部主机信息交换流程

4 Dis-VHoneypot 系统的测试

测试是用来检验提出的 Dis-VHoneypot 系统模型是否正确，系统的各部分设计是否合理，功能是否达到了设计的要求。

测试的具体环境由一台控制中心主机、攻击主机、交换机以及网络内配置的 100 台虚拟主机构成，如图 7 所示。

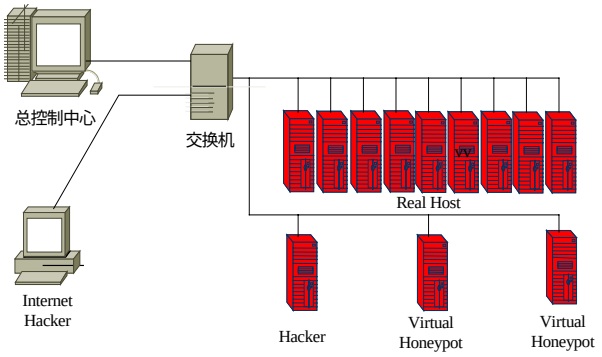

图 7 测试环境

本系统采用的测试工具如表 1 所示。

表 1 测试工具

工具类型	工具名称
扫描类攻击工具	Nmap 扫描器、SuperScan 扫描器、X-Scan 扫描器
远程溢出类攻击工具	Snake IIS、Webdavx3、0x333samba
口令猜测类攻击工具	BrutusAET2
后门类攻击工具	Back office2000、nodoom、netbus
拒绝服务类攻击工具	ms04007dos

本文以 Nmap 和 X-Scan 工具为例，使用 Nmap 对某一虚拟主机 192.168.0.173 进行端口扫描，扫描结果如表 2 所示。使用 X-Scan 对网络进行主机扫描，扫描到的虚拟主机信息如表 3 所示。

(下转第 177 页)