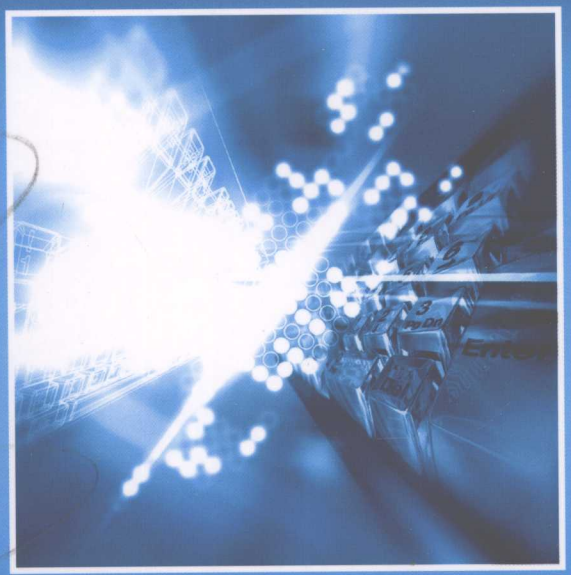
网络安全检测与协同控制技术

蒋卫华 主编



机械工业出版社
CHINA MACHINE PRESS

网络安全检测与协同控制技术

蒋卫华 主编
史兴键 张克旺 李伟华 盖玲兴 杜 君 参编

机 械 工 业 出 版 社

本书深入论述了网络安全检测的理论、策略、方法与面临的挑战，从描述、分析与提取入侵特征出发，通过对检测模型、检测框架和高速检测的分析，对网络安全协同控制技术和网络安全防护体系等方面做了重点阐述。在阐述关键技术的同时，引用了部分开发实例进行说明。最后，对安全评估和仿真诱骗技术进行了分析讨论。为便于读者准确掌握本书的主要内容，在每章的后面设计了思考题。

本书可作为高等院校计算机技术、信息安全、通信工程领域本科生和硕士研究生的教材，也可作为信息领域专业技术人员、研究人员、管理人员和教师的参考书。

图书在版编目（CIP）数据

网络安全检测与协同控制技术/蒋卫华主编．—北京：机械工业出版社，2008.1
ISBN 978－7－111－23078－6

Ⅰ．网…　Ⅱ．蒋…　Ⅲ．计算机网络－安全技术　Ⅳ．TP393.08

中国版本图书馆 CIP 数据核字（2007）第 194964 号

机械工业出版社（北京市百万庄大街 22 号　邮政编码 100037）
策划编辑：朱　林　责任编辑：朱　林　版式设计：霍永明
责任校对：姜　婷　封面设计：王奕文　责任印制：洪汉军
北京振兴源印务有限公司印刷厂印刷
2008 年 3 月第 1 版第 1 次印刷
184mm × 260mm·22 印张·546千字
0001—4000 册
标准书号：ISBN 978－7－111－23078－6
定价：40.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
销售服务热线电话：（010）68326294
购书热线电话：（010）88379639　88379641　88379643
编辑热线电话：（010）88379768
封面无防伪标均为盗版

前　言

在我们的生活和工作方式共享高科技成果的同时，网络与信息安全的重要性和紧迫性日益显现，金融、电信、证券、保险、民航、铁路、税收、海关等国家重要基础设施对网络的依赖程度越来越大，网络与信息安全对社会和经济的影响越来越明显，但网络和信息安全的形势不容乐观，安全意识还比较薄弱，重要的网络和信息系统还存在安全隐患，影响较大的网络与信息安全事故时有发生，可管理、可控制和可信任的网络系统建设刻不容缓。网络和信息安全整体上缺少全面、客观和严格的信任体系和信息安全管理系统（Information Securitry Management System，ISMS），对计算机终端、服务器、网络和使用者缺乏更加具有针对性的信息管理。

网络已经融入到我们生活的方方面面，网络与信息安全领域的研究将是目前和今后一个时期的研究热点和技术难点，需要有更多的网络安全技术人员的研究和成果。为了使广大信息行业从业人员及相关研究人员在入侵检测分析、安全协同防护体系与安全协同控制方面有一个全面、深入、系统的了解，作者认真总结和归纳了多年来课题组的研究成果并参考现有的资料，从网络安全检测及分析技术、网络安全协同控制技术和网络安全防护体系等方面进行重点阐述，在阐述关键技术的同时，引用了部分开发实例进行说明。为了便于读者准确掌握本书的主要内容，在每章的后面设计了思考题。希望能为国内网络安全领域的研究提供一本有价值的参考书。

本书可作为高等院校计算机技术、信息安全、通信工程领域本科生和硕士研究生的教材，也可作为信息领域专业技术人员、研究人员、管理人员和教师的参考书。

全书分为15章，下面概括介绍每章的内容。

第1章主要介绍了网络安全的基本概念、现状、相关标准以及网络安全的体系及评价标准等。

第2章主要介绍了网络攻击威胁的基本概念、目前网络安全遭受的主要攻击方法及当前网络攻击的特征与发展趋势。

第3章主要介绍了网络安全的基本理论，从密码学的数学基础入手，结合当前主流的网络安全防护技术，着重阐述了入侵检测技术和网络安全协同控制技术。

第4章首先介绍了攻击与漏洞、攻击模式和攻击技术的发展趋势，接着介绍了网络入侵检测技术、检测策略、检测方法及网络入侵检测系统面临的挑战。

第5章主要介绍了入侵特征的描述与提取及网络入侵行为的分析方法。

第6章主要介绍了入侵检测模型及其应用实例。其中，着重阐述了系统调用序列审

计模型及确定的并发变迁面向对象的 Petri 网模型，并基于这些模型介绍了几个当前入侵检测实例及其入侵检测的评估方法等。

第 7 章主要介绍了高速入侵检测相关技术，提出了基于网桥的动态分流体系结构分析和最佳完整性动态均衡分流算法设计，并进行了实验测试。

第 8 章主要介绍了“安全协同”这一重要的概念，首先介绍了协同的两个主要应用方向即“攻击”和“防御”，然后由现在常用的协同方式入手对现有各种安全技术之间的协同方式进行了介绍。

第 9 章主要介绍了安全协同控制框架与协同防御体系的相关概念及技术，首先分别对协同控制相关技术和协同控制框架的组成进行了介绍，最后围绕协同防御体系进行了详细分析。

第 10 章对安全协同机制的一些细节问题进行了讨论，首先对安全协同的相关概念及研究目的进行了简要介绍，然后对安全协同机制中的一些必须元素进行了分析，最后提出了“代理群落”这一概念，并对其一些简单的协同行为进行了分析。

第 11 章对基于多代理体系的协同框架设计进行了详细讨论，首先对协同控制框架进行了简要介绍，对框架设计中需要涉及的重要元素进行了详细的讨论，最后以一个简单的框架为例简要分析了基于代理协同框架设计的实现。

第 12 章主要介绍了网络安全防护体系设计的相关概念、技术及实现，首先对网络安全防护体系的整体结构进行了介绍，然后对网络安全防护体系涉及到的模型进行了讨论。

第 13 章主要对安全评估这一网络安全中非常重要的部分进行了讨论，首先对现有安全评估技术进行了对比及分析，然后对安全评估的主要技术基础进行了讨论，最后对安全评估模型进行了研究，并使用一个例子对其运行进行了分析。

第 14 章主要从网络安全中常见问题入手，具体分析其应对策略等内容。网络安全防护体系及策略是网络安全领域中非常重要的一个组成部分。本章主要对常见的网络安全防护策略进行了介绍，对自防御、层次化防御以及动态防御等 3 种策略进行了分析，最后对无线网络安全策略问题进行了讨论。

第 15 章对网络安全中一个较新的概念“仿真和诱骗”进行了详细的讨论，首先对网络仿真的相关技术进行了介绍和分析，然后对黑客诱骗技术进行了简要的介绍，最后对网络仿真与黑客诱骗技术的融合实现进行了描述和分析。

在本书写作的过程中，李昀博士和王文奇博士的研究成果促进了本书的诞生，在此表示诚挚的感谢。同时也衷心感谢恩师李伟华和李俊山教授的教诲和言传身教。

希望本书的出版能够得到读者的认可，由于作者水平有限，书中难免有错误和疏漏，请广大同行赐教和指正。

编 者

2007 年 10 月

目　录

第1篇 基础知识

本篇主要介绍了网络安全的基础知识。从网络安全的基本概念、涵盖范围及相关标准入手，通过对目前网络安全面临的各种威胁现状及发展趋势的介绍，有针对性而又不失全面地阐述了目前网络安全的基本理论、主流的网络安全防护技术，其中着重介绍了入侵检测技术和协同控制技术。通过对基础知识的介绍，使读者能够对网络安全技术的整体概况有一个全面的把握和了解。

第1章 网络安全的基本概念

本章主要介绍了网络安全的概念、现状、标准以及网络安全的涵盖范围、安全框架等。

1.1 网络安全概述

1.1.1 网络安全问题的产生

随着以互联网为代表的全球信息化浪潮日益推进，信息网络技术的应用正日益普及和广泛，应用层次正在深入，应用领域从传统的小型业务系统逐渐向大型关键业务系统扩展，典型的如党政部门信息系统、金融业务系统、企业商务系统等。伴随网络的普及，网络安全也日益成为了影响网络效能的重要问题，而互联网所具有的开放性、国际性和自由性在增加应用自由度的同时，对安全提出了更高的要求，这主要表现在：

1）网络的开放性导致网络技术的全开放性，任何一个人、团体都可能获得，因而网络所面临的破坏和攻击可能是多方面的，例如：可能来自物理传输线路的攻击，也可能是对网络通信协议和实现进行攻击；可以对软件实施攻击，也可以对硬件实施攻击。

2）一个国际性的网络还意味着网络的攻击不仅仅来自本地网络的用户，它还可以来自互联网上的任何一台机器，也就是说，网络安全所面临的是一个国际化的挑战。

3）网络自由意味着最初对用户的使用并没有提供任何的技术约束，用户可以自由访问网络，自由地使用和发布各种类型的信息。用户只对自己的行为负责，而没有任何的法律限制。

尽管开放的、自由的、国际化的互联网的发展给政府机构、企事业单位带来了革命性的改革和开放，使得他们能够利用互联网提高办事效率和市场反应能力，以便更具竞争力，但是通过互联网，他们在从异地获取重要数据的同时，又要面对互联网开放性带来的数据安全的新挑战和新危险。如何保护企业的机密信息不受黑客和工业间谍的入侵，已成为政府机构、企事业单位信息化健康发展所要考虑的重要问题之一。

简单地说，网络安全是指使信息系统中硬件、软件和系统中的数据受到保护，不因偶然因素或者恶意攻击而遭到破坏、更改、泄露，系统连续可靠地运行，网络服务不中断。从广义上讲，凡是涉及到网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、应用数学、信息论等多种领域的综合性学科。

计算机网络安全的因素很多，有人为因素，也有自然因素，其中人为因素的危害性最大。归结起来，针对网络安全的威胁主要有以下几个方面：

1. 人为的无意失误

如操作员安全配置不当造成的安全漏洞；不合理地设定资源访问控制，一些资源就有可能被偶然或故意地破坏；用户安全意识不强，用户对口令的设定和使用不慎，将自己的账号随意转借他人或与别人共享等都会对网络安全带来威胁。

2. 人为的恶意攻击

这是计算机网络所面临的最大威胁，敌手的攻击和计算机犯罪就属于这一类。此类攻击又可以分为以下两种：一种是主动攻击，它以各种方式有选择地破坏信息的有效性和完整性，如截取网上的信息包，并对其进行更改而使它失效；故意添加一些有利于自己的信息，起到信息误导的作用；登录进入系统，使用并占用大量网络资源，造成资源的消耗，损害合法用户的利益。这种侵犯者的破坏作用最大，另一类是被动攻击，它是在不破坏网络正常工作的情况下，使用截获、窃取、破译等手段获得重要机密信息。这两种攻击均可对计算机网络造成极大的危害，并导致机密数据的泄漏。

另外，还有拒绝服务攻击，它不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪，影响正常用户的使用，甚至使合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务。

3. 非授权访问

没有预先经过同意，就使用网络或计算机资源被看作非授权访问，如有意避开系统访问控制机制，对网络设备及资源进行非正常使用，或擅自扩大权限，越权访问信息。表现有假冒身份攻击、非法用户进入网络系统进行违法操作、合法用户以未授权方式进行操作等。

4. 网络软件的漏洞和“后门”

网络软件一般总会存在某些缺陷和漏洞，这些漏洞和缺陷恰恰是黑客进行攻击的首选目标。曾经出现过的黑客攻入网络内部的事件大部分就是因为网络软件有漏洞，导致安全措施不完善所招致的苦果。另外，软件的“后门”都是软件公司的编程人员为了自便而设置的，一般不为外人所知，但一旦“后门”洞开，造成的后果将不堪设想。

5. 信息泄漏或丢失

指敏感数据被有意或无意泄漏出去或丢失。它通常包括：信息在传输中丢失或泄漏（如“黑客”利用电磁泄漏或搭线窃听等方式截获机密信息；通过对信息流向、流量、通信频度和长度等参数的分析，推出有用信息，如用户口令、账号等重要信息）；信息在存储介质中丢失或泄漏；通过建立隐蔽隧道窃取敏感信息等。

6. 破坏数据完整性

以非法手段窃取对数据的使用权，删除、修改、插入或重发某些重要信息，以取得有益于攻击者的响应；恶意添加、修改数据，以干扰用户的正常使用。

7. 利用网络传播病毒

通过网络传播计算机病毒，其破坏性大大高于单机系统，而且用户很难防范。

1.1.2　网络安全的现状

计算机资源及网络系统安全无疑是当今最为引人瞩目的研究领域之一，其原因就在于计算机的大规模普及、互联网的高速发展及整个计算机以及网络系统内在的脆弱性。根据犯罪现场调查（Crime Scene Investigation，CSI）机构的第七次计算机犯罪及安全问题年度调查表明：

90%的被调查机构（主要是大型公司和政府部门）在过去的 12 个月中都检测到大量的入侵行为。

80%的被调查机构由于出现计算机安全问题而造成了巨大经济损失。

44%的机构（223 个）对其经济损失进行了计算，损失总额高达 455 848 000 美元。

2002 年上半年发生的黑客攻击事件上升了 32%，平均每个公司每个星期被攻击 32 次，更糟糕的是，竟有大量公司根本没有意识到自己曾被攻击过。

据统计，全球约每 20s 就有一次计算机入侵事件发生，互联网上的网络约有 1/4 的防火墙被突破，约 70%以上的网络信息主管人员报告因机密信息泄露而受到了损失。

从另一个网络安全的权威机构——计算机应急响应小组（Computer Emergency Response Team，CERT）的最新统计数字及年度报告也可以看出网络安全问题的严重程度。CERT 的最新统计数据见表 1－1。

表 1－1　CERT 的最新统计数据

年度报告的网络安全事件数量

年份	1988	1990	1992	1994	1996	1998	1999	2000	2001	2002
事件数	6	252	773	2 340	2 573	3 734	9 859	21 756	52 658	82 094

年度报告的漏洞数量

年份	1995	1996	1997	1998	1999	2000	2001	2002
漏洞数量	171	345	311	262	417	1 090	2 437	4 129

计算机信息技术和其他科学技术一样是一把双刃剑。当人们利用信息技术提高工作效率，为社会创造更多财富的同时，却有少数人利用信息技术做着相反的事情。他们非法侵入他人的计算机系统窃取机密信息或篡改和破坏数据，给社会造成难以估量的巨大损失。网络安全是一个关系国家安全和主权、社会的稳定、民族文化的继承和发扬的重要问题。

当前，在全球范围内，随着互联网的迅猛发展，对计算机及网络安全基础设施的入侵已经成为一个越来越严重的问题。对于网络入侵的检测和防护已日益成为迫切的要求。网络入侵相对于传统的破坏手段而言，具有以下特征：

1）没有地域和时间的限制；

2）网络攻击往往混杂在大量正常的网络活动之中，隐蔽性强；

3）入侵手段和方法更加复杂多变；

4）入侵行为的技术含量越来越高，造成的后果和危害更加严重；

5）入侵攻击工具日益完善，攻击者不需要专业知识就能够完成复杂的攻击过程。

1.1.3 网络安全工作的目的

网络安全工作的目的，就是为了在相关法律、法规、政策的支持与指导下，通过采用合适的安全技术与安全管理措施，完成以下任务：

1）使用访问控制机制，阻止非授权用户进入网络，即“进不来”，从而保证网络系统的可用性。

2）使用授权机制，实现对用户的权限控制，即不该拿走的“拿不走”，同时结合内容审计机制，实现对网络资源及信息的可控性。

3）使用加密机制，确保信息不暴露给未授权的实体或进程，即“看不懂”，从而实现信息的保密性。

4）使用数据完整性鉴别机制，保证只有得到允许的人才能修改数据，而其他人“改不了”，从而确保信息的完整性。

5）使用审计、监控、防抵赖等安全机制，使得攻击者、破坏者、抵赖者“走不脱”，并进一步对网络出现的安全问题提供调查依据和手段，实现信息安全的可审查性。

1.1.4 网络安全的原则与策略

一般而言，对信息系统安全的认知与评判标准，包含五项原则：机密性（Confidentiality）、完整性（Integrity）、可用性（Availability）、可控性（Controllability）与抗否认性（Non-Repudiation）。这五项原则虽各自独立，在实际维护系统安全时，却又环环相扣，缺一不可。

1. 机密性

确保信息不暴露给未授权的实体或进程。当信息被其提供人、收受人之外的第三者得知时，就丧失了私密性。某些形式的信息特别强调隐私性，诸如个人身份资料、信用交易记录、医疗保险记录、公司研发资料及产品规格等。

2. 完整性

只有得到允许的人才能修改数据，并且能够判别出数据是否已被篡改。当信息被非预期方式改动时，就丧失了完整性。如飞行航空交通、金融交易等应用场合，在资料遭受非法变动后，可能会造成严重后果，因此须特别重视资料的完整性。

3. 可用性

得到授权的实体在需要时可访问数据，即攻击者不能占用所有的资源而阻碍授权者的工作。身份鉴别确保使用者能够提出与相称身份相符的证明。对于信息系统，这项证明可能是电子形式（如使用者账号密码、IC卡等），或其他独一无二的方式（如指纹、虹膜、声纹等生物辨识）。

4. 可控性

可以控制授权范围内的信息流向及行为方式。系统必须能够判定用户是否具备充分的权限，进行特定的活动，如开启档案、执行程序等。因为系统授权给特定用户后，用户有权运行于系统之上，因此用户事先必须经由系统进行身份鉴别，才能取得对应的权限。

5. 抗否认性

对出现的网络安全问题提供调查的依据和手段。用户在系统进行某项运作后，若事后能提出证明，且无法加以否认，便具备抗否认性。因为在系统运作时必须拥有权限，抗否认性

通常架构在授权机制之上。

安全策略是指在一个特定的环境里，为保证提供一定级别的安全保障所必须遵守的规则。一个安全策略模型应包括建立安全环境的严明的法律、先进的技术和严格的管理 3 个重要组成部分，即：

1. 严明的法律

安全的基石是社会法律、法规与手段，这部分用于建立一套安全管理标准和方法。即通过建立与信息安全相关的法律、法规，使非法分子慑于法律，不敢轻举妄动。

2. 先进的技术

先进的安全技术是信息安全的根本保障，用户对自身面临的威胁进行风险评估，决定其需要的安全服务种类，选择相应的安全机制，然后集成先进的安全技术。

3. 严格的管理

各网络使用机构、企业和单位应建立相应的信息安全管理办法，加强内部管理，建立审计和跟踪体系，提高整体信息安全意识。

针对猖獗的入侵行为，以前的一些网络安全方案主要是从防范网络入侵的角度来制定的。无论是防火墙还是入侵检测系统，都只是一种被动的、始终落后于攻击手段的方法。事实上，大多数网络安全方案都处于一种被入侵者牵着鼻子走的尴尬处境。应对入侵的办法就是不停地更新自己现有的检测库，但始终落后于攻击者。

古语道：知己知彼，百战不殆。事实上，每一位入侵者都是一位网络安全方面的专家，因为他们熟知攻击的原理和技巧，能够巧妙地绕过现有的安全防范体系，并侵入系统。如果我们能够对这一过程进行分析和总结，那么找到的就不仅是漏洞，还包含入侵者如何发现漏洞的过程和方法等。这一点对于建立一个高效的、智能化的网络安全防护体系来说是至关重要的。

软件正进入智能化时代，对于防火墙和入侵检测系统等网络安全系统来说，智能化的重要性显得尤为突出。这是因为网络安全防护体系不仅应熟知大量现有的入侵手段和安全漏洞，而且应能判断出入侵者是否正在尝试一种全新的攻击手段。智能化软件的最大特点就在于：它拥有的绝不再仅仅是大量的知识，而且还具有操纵普通知识的高阶知识——智慧，从而能做到主动地防护网络信息安全。

1.2　网络安全的基础知识

1.2.1　网络安全的概念

本质上讲，网络安全就是网络上的信息安全，而信息安全可以定义为：在既定安全密级条件下，信息系统抵御意外事件和恶意行为的能力，这些事件和行为将危及所存储、处理和传输的数据以及经由这些系统所提供的服务的可用性、机密性、完整性、抗否认性和可控性。

可用性是指在突发事件下，被授权实体依然可得到或使用相关数据和服务；机密性是指数据不受非法截获和未经授权的浏览；完整性是指能够保障被传输、接收或存储的数据是完整的和未被篡改的；抗否认性是指能够保证信息行为人不能否认其信息行为；可控性是指保

证信息和信息系统的授权认证和监控管理。

然而，信息安全与网络安全还是有一定的区别：信息安全指对信息的机密性、完整性和可用性的保护，即面向数据的安全；而网络安全的内涵又扩展到面向使用者的安全，即鉴别、授权、访问控制、抗否认性、可服务以及个人隐私、知识产权保护等，网络安全不仅包括计算机上信息存储的安全性，还要考虑信息传输过程的安全性。

1.2.2 网络安全的特征

无国家属性，即互联网无国界，无管制空间，无信息关防。

无军事特征，即军民系统难以分开，导致出现信息战时战争目标的不确定性。

无管制手段，即作为一种高技术，难以像控制武器那样控制人们对该技术的掌握与使用。

越先进往往越脆弱，即随着经济、生活对信息系统依赖的加深，安全问题使得所涉及的系统变得十分脆弱。

信息攻击具有不确定性，即发生时机的不确定性，攻击者的不确定性，攻击目标的不确定性，攻击发起地点的不确定性。

攻击面广，即核武器的威慑范围是一个城镇，但信息武器的威慑范围可以是一个国家。

相对性，即只有相对的安全，没有绝对的安全系统。

时效性，即新的漏洞与攻击方法不断发现，日常管理中的不同配置会引入新的问题（安全测评只证明特定环境与特定配置下的安全），新的系统部件会引入新的问题。

1.2.3 国内外网络安全等级保护

计算机系统安全评价标准是一种技术性法规。由于信息安全产品和系统的安全评价事关国家的安全利益，因此许多国家都在充分借鉴国际标准的前提下，积极制定本国的计算机安全评价认证标准。

较著名的有1985年美国国防部计算机安全中心首先提出的计算机安全标准：可信任计算机标准评估规则（Trusted Computer Standards Evaluation Criteria，TCSEC）桔皮书。该标准描述了不同类型的物理安全和操作系统软件的可信度。后来美国国防部计算机安全中心更名为国家计算机安全中心，并将计算机安全方面的有关文件汇集成册，其中桔皮书将安全分为4个方面：安全政策、可说明性、安全保障和文档，并依此划分为A、B、C、D共4类7个安全级别，其中D类安全级别最低，A级别最高（D < C1 < C2 < B1 < B2 < B3 < A），各个级别分别描述如下：

D级：说明整个系统是不可信的，指评估的产品基本上没有采用任何的安全措施。

C1级：又称为自选安全保护系统，对硬件进行某种程度的保护，用户必须通过用户名和口令才能登录系统，不同的用户有不同的权限，根用户（超级用户）拥有全部的权限。

C2级：除了拥有C1级的特性，还强化了审计跟踪，可以创建受控访问环境，要求对事件加以审核，每个事件都有审计记录。

B1级：称为标志安全保护（Labeled Security Protection），可以设置强制访问控制之下的对象，所有目标均为秘密水平，并采用正规或非正规的安全模型规范。

B2级：称为结构保护（Structure Protection），要求系统中所有对象都加注标签，并给设