网络入侵分析与入侵响应

主 编 ⊙ 穆成坡 嵇春梅 于本成

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

网络入侵分析与入侵响应

主　编　穆成坡　嵇春梅　于本成
副主编　李　先　胡志强　彭奕平　张昌州

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

内 容 简 介

本书主要对入侵检测系统报警的各类分析处理技术、入侵在线风险评估技术和入侵响应决策技术进行介绍。内容包括：入侵检测系统报警处理所涉及的概念、标准、语言、分类和结构；报警聚合、报警统计、报警验证和报警关联等报警分析处理方法和模型；典型的报警处理工具；报警分级技术；定性和定量的在线入侵风险评估技术；自动入侵响应所涉及的关键技术、响应目的、响应策略、响应因素和响应措施等有关内容；各类入侵响应时机决策和入侵响应措施决策的方法和模型；各类网络安全设备的特点、使用和部署方法等。

本书可作为计算机、信息安全等相关专业高年级本科生、研究生的教学参考书，也可供网络安全领域的科研、设计和管理人员参考。

图书在版编目（CIP）数据

网络入侵分析与入侵响应 / 穆成坡，嵇春梅，于本成主编. —北京：北京理工大学出版社，2016.5

ISBN 978-7-5682-2145-0

Ⅰ. ①网…　Ⅱ. ①穆… ②嵇… ③于…　Ⅲ. ①计算机网络-安全技术　Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2016）第 071895 号

出版发行 / 北京理工大学出版社有限责任公司
社　　址 / 北京市海淀区中关村南大街 5 号
邮　　编 / 100081
电　　话 / (010)68914775(总编室)
(010)82562903(教材售后服务热线)
(010)68948351(其他图书服务热线)
网　　址 / http：//www.bitpress.com.cn
经　　销 / 全国各地新华书店
印　　刷 / 三河市天利华印刷装订有限公司
开　　本 / 787 毫米×1092 毫米　1/16
印　　张 / 10.25
字　　数 / 238 千字
版　　次 / 2016 年 5 月第 1 版　2016 年 5 月第 1 次印刷
定　　价 / 47.00 元

责任编辑 / 高　芳
文案编辑 / 高　芳
责任校对 / 周瑞红
责任印制 / 边心超

目　录

第 1 章

引　论

目前，计算机网络已经逐渐成为各行各业的基础性设施，网络安全涉及社会经济生活各个领域。信息与网络安全问题已上升为一个事关国家政治稳定、社会安定、经济有序运行的全局性问题。从 CERT 每年的安全事件报告可以看出，安全事件呈指数增长，威胁也越来越严重。据统计，目前在 Internet 上有超过 1/3 的防火墙曾被突破。另外，攻击技术也由简单攻击发展为复杂攻击，如组合式攻击、自动脚本攻击和协同攻击。同时，网络带宽的不断增加，新的网上应用业务的不断推出，都对网络安全系统和相关技术提出了新的挑战。本章将对网络安全技术的发展趋势以及主要网络安全技术相关知识进行简明扼要的介绍，最后阐述入侵检测报警分析、处理与入侵响应技术的重要性。

1.1　网络安全技术及其发展趋势

目前，网络安全技术可以划分为静态安全技术和动态安全技术。静态安全技术通过人工设定各种访问规则，来限定对目标的访问，以此达到保护系统、抵御入侵的目的。路由器访问控制列表（ACL）和防火墙（Firewall）都是这类技术的典型代表；动态安全技术通过对系统的主动检测、分析和响应等手段来保障系统的安全性。主要的动态安全技术包括入侵检测（Intrusion Detection）、在线风险分析（Online Risk Analysis）、安全漏洞扫描（Vulnerability Scan）和入侵响应（Intrusion Response）等。

以往人们大多采用的是静态安全技术，而在目前新的安全形式下，原来的网络访问控制、防火墙隔离等静态安全防御技术已经不能满足安全需求。网络安全的重要发展趋势是静态安全技术和动态安全技术相结合，集成不同功能、不同层次的安全系统，系统间功能相互补充、安全信息共享、协调互动，实现网络的动态、纵深防御。

目前，被网络安全领域所普遍接受的可适应信息安全防护体系（或称动态信息安全理论）的模型 P2DR 就是这一趋势的典型代表。如图 1-1 所示，此模型包含四个主要部分：Policy（安全策略）、Protection（防护）、Detection（检测）和 Response（响应）。在安全策略的指导下，防护、检测和响应组成了一个完整的、动态的安全循环，使系统从静态防

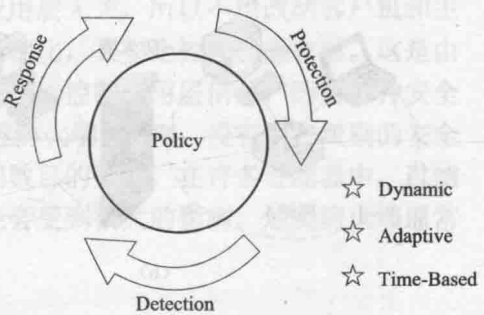

图 1-1　P2DR 模型

护转化为动态防护，从而保证信息系统的安全。其主要思想是强调在安全策略的指导下，将各个相对独立的安全环节协调起来，进行全过程的整体防御，而不是单一的安全系统发挥作用。

网络安全企业界最近所推出入侵防御系统 IPS（Intrusion Prevention System）和入侵管理系统 IMS（Intrusion Management System）是上述网络安全技术发展趋势的具体体现，显示了各项动态安全技术的重要性和必要性。IPS 在入侵检测系统 IDS（Intrusion Detection System）中使用了多重入侵检测机制和粒度更细的规则，增强了入侵响应机制。特别是 IMS，它以 IDS 为核心，联合防火墙、漏洞扫描，主机保护、安全审计、网管等安全与网络产品进行全局协调检测、响应，实现对系统的防御和保护。

1.2 防火墙技术

1.2.1 防火墙及其作用

当构筑和使用木质结构房屋时，为防止火灾的发生和蔓延，人们将坚固的石块堆砌在房屋周围作为屏障，这种防护构筑物被称为防火墙。在计算机网络中，人们借助了这个概念，使用防火墙来实现不同网络之间（或主机与网络之间）访问控制和安全边界的逻辑隔离。

在逻辑上，防火墙是一个分离器，一个限制器，也是一个分析器。具体来说，防火墙是指设置在不同网络（如可信任的内部网和不可信的公共网，如图 1-2（a）所示）或网络安全域之间（如图 1-2（b）所示）或主机与网络之间（如图 1-2（c）所示）的一系列软、硬件的组合，是不同网络、网络安全域或主机与网络之间信息的唯一出入口，能根据安全策略控制（允许、拒绝、监测）出入网络或主机的信息流，保证内网或主机的安全，且本身具有较强的抗攻击能力。它是提供信息安全服务，实现网络和信息安全的基础设施。其主要作用如下：

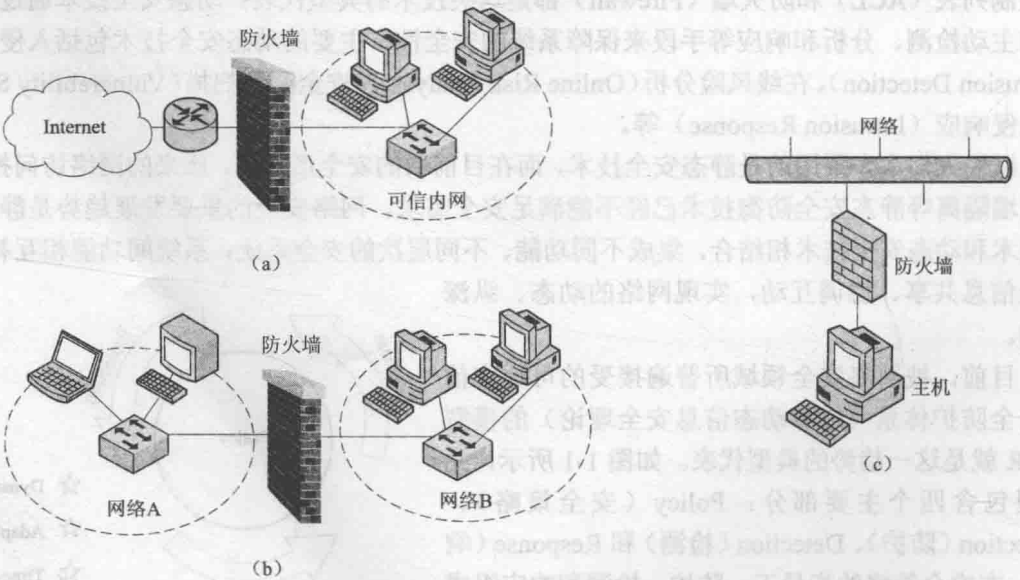

图 1-2 防火墙部署

1. 实现了网络安全边界的划分与隔离

目前，众多类型的防火墙可以根据用户的安全需要，实现不同范围或粒度安全区域的划分和隔离。所划分的安全区域可以是一个大型网络，也可以是一个小型网络，甚至为一台主机。一个防火墙（作为阻塞点、控制点）能极大地提高一个内部网络的安全性，并通过过滤不安全的服务而降低风险。由于只有经过精心选择的应用协议才能通过防火墙，所以网络环境变得更安全。

2. 可对网络存取和访问进行监控审计

防火墙所隔离的内外网之间的访问通信都要经过防火墙，防火墙可以记录下这些访问，并可以根据管理员的安全需求做出日志记录，从而可以对这些访问实施监控、审计。同时，也能提供网络使用情况的统计数据。当发生可疑动作时，防火墙能进行适当的报警，并提供网络是否受到攻击的详细信息。

3. 可以防止内部信息的外泄

通过防火墙可实现内部网重点网段的隔离，可以掩盖内部网络结构和被保护主机的详细情况，防止外网用户对内网或主机的恶意侦测，从而限制了局部重点或敏感网络安全问题对全局网络造成的影响。

除了安全作用，通过防火墙的地址转换 NAT 功能，可以缓和现有 IP 地址空间不足的问题。有的防火墙还支持 VPN（Virtual Private Network）功能，可将企事业单位在地域上分布在全世界各地的 LAN 或专用子网有机地联成一个整体。不仅省去了专用通信线路，而且为信息共享提供了技术保障。

1.2.2 防火墙的分类

1. 根据实现层次分类

防火墙大体可以分为：包过滤防火墙、代理防火墙和复合防火墙。其详细情况如下。

（1）包过滤防火墙

包过滤或分组过滤防火墙（Packet Filteing）作用在网络层和传输层，它根据分组包头源地址、目的地址和端口号、协议类型等标志确定是否允许数据包通过。只有满足过滤逻辑条件的数据包才被转发到相应的目的地出口端，其余数据包则被从数据流中丢弃。过滤的逻辑条件是管理员根据安全策略制定的。

由于此类防火墙过滤规则不十分复杂，不做内容过滤，容易通过硬件方式实现，所以过滤速度快。另外，因为它工作在网络层和传输层，与应用层无关，所以不用改动客户机和主机上的应用程序，对用户是完全透明的。和代理防火墙相比，其安全控制性能有限。这是由于其过滤判别的依据只有网络层和传输层的有限信息，不能控制应用层信息，因而各种安全要求不可能充分满足。黑客通过盗用合法 IP 很容易穿透防火墙。同时，没有用户级别的安全日志很难发现黑客攻击记录。此外，其过滤性能受规则数目的影响。在许多过滤器中，过滤规则的数目是有限制的，且随着规则数目的增加，性能会受到很大的影响。这类防火墙通常和应用网关配合使用，共同组成防火墙系统。

（2）代理防火墙

应用代理（Application Proxy）防火墙也叫应用网关（Application Gateway），作用在应用

层，通过对每种应用服务编制专门的代理程序，实现监视和控制应用层通信流的作用。

此类防火墙能够理解应用层上的协议，可以做一些复杂的访问控制，具有较强的访问控制能力，能够支持用户认证，并可以提供用户级别的日志信息，便于对黑客的追踪。但应用层网关对用户是不透明的，需要用户改变自己的行为，每种服务都需要有相应的代理服务器，实现起来比较复杂和困难。

（3）复合防火墙

由于对更高安全性的要求，常把基于包过滤的方法与基于应用代理的方法结合起来，形成复合型防火墙产品，实现两类防火墙各方面性能的互补。

2. 根据体系结构分类

（1）双宿主机结构防火墙

其结构如图 1-3 所示，防火墙由堡垒主机上配置双网卡来实现，两块网卡分别与内网和外网相连，堡垒主机运行防火墙软件，使内外网用户不能直接通信，但内网用户可以与堡垒主机通信，外网用户也可以同堡垒主机通信，中间通过防火墙安全控制检查，最终实现内外网用户间的通信。其缺点是，当黑客攻破堡垒主机后就可以自由对内网资源进行访问。

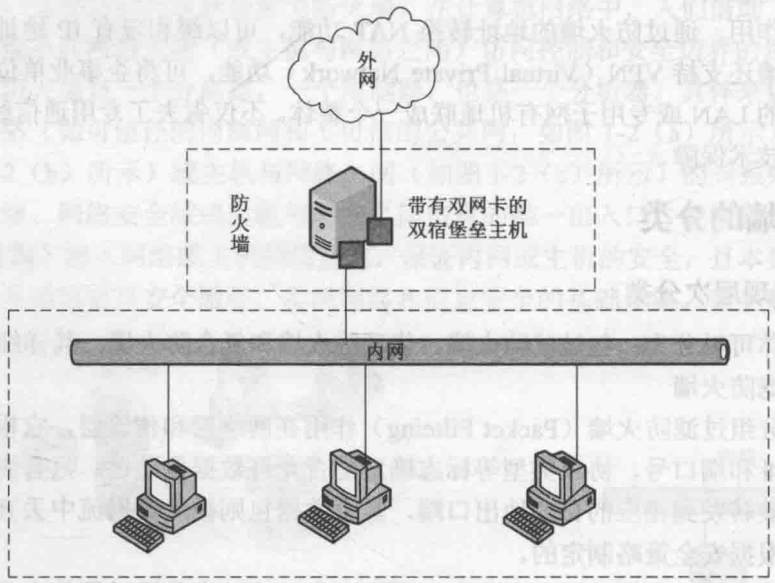

图 1-3　双宿主机结构防火墙

（2）屏蔽主机结构防火墙

屏蔽主机防火墙由过滤路由器和堡垒主机组成，如图 1-4 所示。根据被保护网络的安全需求，在过滤路由器上设立过滤规则，并使堡垒主机成为从外网唯一可直接访问的主机，从而保证内网主机不被外网非法用户攻击。与双宿主机结构防火墙类似，当堡垒主机被外网用户攻破后，其内网就会受到很大威胁。

（3）屏蔽子网结构防火墙

屏蔽子网防火墙由内部路由器、外部路由器和堡垒主机构成，如图 1-5 所示。外部路由器连接外网，内部路由器连接内网，中间的堡垒主机可作为外网用户的访问点。内、外路由

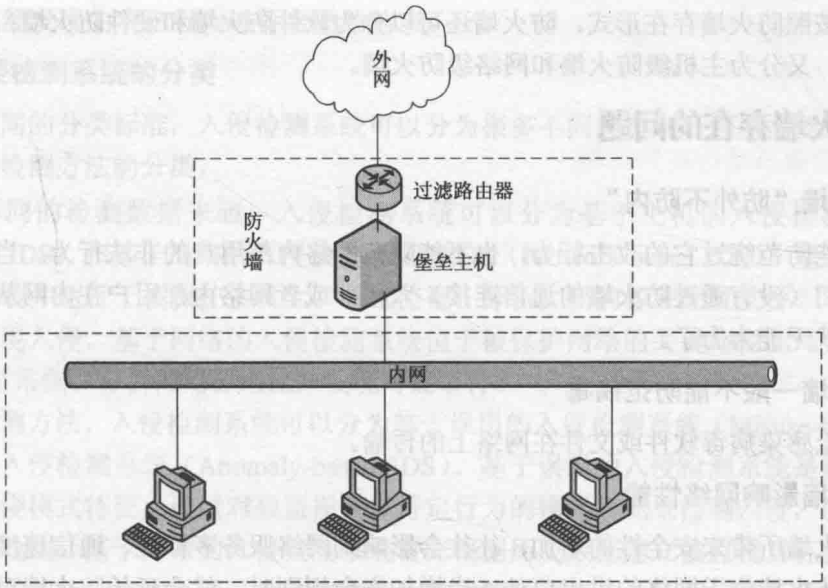

图 1-4 屏蔽主机结构防火墙

器中间部分的网络被称为非军事区（Demilitarized Zone，DMZ）或隔离区。这样一种结构比前两种结构复杂，外部路由器管理所有外网用户对 DMZ 内资源的访问，并隔离外网非法用户的攻击，内部路由管理 DMZ 内资源实体（如堡垒主机）对内部网络上资源的访问。这样，外网的黑客必须通过三个不同区域（外部路由器、堡垒主机和内网路由器）才能到达内网，所以可以提供多层次和更安全的防护。

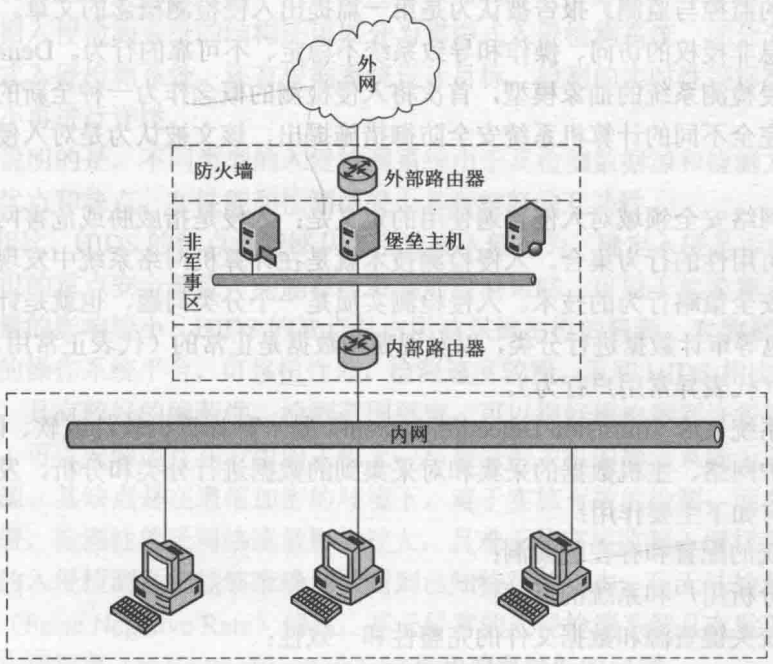

图 1-5 屏蔽子网结构防火墙

此外，按照防火墙存在形式，防火墙还可以分为软件防火墙和硬件防火墙；按照受保护对象和规模，又分为主机级防火墙和网络级防火墙。

1.2.3 防火墙存在的问题

1. 防火墙“防外不防内”

它既不能防范绕过它的攻击行为，也不能防范网络内部用户的非法行为。当入侵者通过网络中的后门（没有通过防火墙的通信连接）入侵，或者网络内部用户在内网从事非法操作时，防火墙就无能为力了。

2. 防火墙一般不能防范病毒

不能防止感染病毒软件或文件在网络上的传输。

3. 防火墙影响网络性能

随着防火墙所带来安全性的增加，往往会影响到网络服务多样性、通信速度和开放性。例如，由于防火墙位于网络的进出口处，当增加安全规则时，就会延长防火墙对信息的处理时间，过多的安全规则就可能产生通信“瓶颈”，影响到内外网之间的通信速度。

1.3 入侵检测技术

1. 入侵检测系统及其作用

人们对入侵检测技术的研究开始于 20 世纪 80 年代初，由 James Anderson 所提交的《计算机安全威胁的监控与监测》报告被认为是第一篇提出入侵检测概念的文章。Anderson 将入侵定义为对信息非授权的访问、操作和导致系统不稳定、不可靠的行为。Denning 在 1987 年提出了一个入侵检测系统的抽象模型，首次将入侵检测的概念作为一种全新的与传统加密认证和访问控制完全不同的计算机系统安全防御措施提出，该文被认为是对入侵检测研究的推动性工作。

目前，在网络安全领域对入侵普遍使用的定义是：入侵是指威胁或危害网络资源的完整性、机密性和可用性的行为集合。入侵检测技术就是在计算机网络系统中发现并报告包括入侵等各种违反安全策略行为的技术。入侵检测实质是一个分类问题，也就是针对各种主机日志、网络数据包等审计数据进行分类，以发现哪些数据是正常的（代表正常用户行为），哪些数据是异常的（代表异常用户行为）。

入侵检测系统 IDS（Intrusion Detection System）是一种计算机软件或软、硬件组合系统。它通过对被保护网络、主机数据的采集和对采集到的数据进行分类和分析，发现入侵行为。入侵检测系统有如下主要作用：

- 审计系统的配置和存在的漏洞；
- 监测、分析用户和系统的活动；
- 评估系统关键资源和数据文件的完整性和一致性；
- 识别已知的攻击行为，统计分析异常行为；
- 发现正在进行的或已经实现的违反系统安全策略的活动；

- 对已经发现的攻击行为进行合适的响应。

2. 入侵检测系统的分类

根据不同的分类标准，入侵检测系统可以分为很多不同的类别，这里主要介绍基于数据来源和基于检测方法的分类。

根据不同的检测数据来源，入侵检测系统可以分为基于主机的入侵检测系统 HIDS（Host-based IDS）和基于网络的入侵检测系统 NIDS（Network-based IDS）。基于主机的入侵检测系统安装并运行于被保护主机上，通过监视、分析主机的各种配置文件、审计记录和日志文件来发现入侵。基于网络的入侵检测系统位于被保护网络的关键路径上（如网络的进出口处），通过采集、分析网络分组流来发现可疑事件。

根据检测方法，入侵检测系统可以分为基于误用的入侵检测系统（Misuse-based IDS）和基于异常的入侵检测系统（Anomaly-based IDS）。基于误用的入侵检测系统是根据已知的系统漏洞和入侵模式特征，通过对被监视目标特定行为的模式匹配来检测入侵，所以误用检测又称为特征检测。基于异常的入侵检测系统首先根据历史数据建立被监视目标在正常情况下的行为和状态的统计描述，通过检测这些统计描述的当前值是否显著偏离了其相应的正常情况下的统计描述来进行入侵的检测。

用于误用检测的方法有表达式匹配（Expression Matching）、状态转移（State Transition Analysis）、专用语言分析（Dedicated Languages Analysis）、基因算法（Genetic Algorithms）和 Petri 网等；用于异常检测的方法有统计模型分析（Statistical Model Analysis）、免疫系统方法（Immune System Approach）、神经网络（Neural Nets）、基于贝叶斯推理检测（Bayes-based Analysis）和支持向量机（Support Vector Machine）等。目前，几乎所有机器学习和数据挖掘的方法都被人们尝试用于入侵检测。关于这些方法的细节，请参阅参考文献中的内容。

此外，根据入侵检测系统的结构还可以分为集中式入侵检测系统、部分分布式入侵检测系统和全分布式入侵检测系统。还有根据系统设计目标、检测的实时性等标准进行入侵检测分类的，这里不再进行详述。

需要着重说明的是，不同类型的入侵检测系统由于其检测数据源和检测方法的不同，各自具有不同的优点和缺点，在性能和检测结果上具有很好的互补性。

和 NIDS 相比，HIDS 的优点是能够从高层监视入侵行为，确定入侵是否成功，可以有针对性地监视主机的重点安全部位，实施粒度更细的检测策略，可用于加密和交换环境，检测性能受网络流量的影响较小。HIDS 的缺点是占用被保护主机的资源，对数据源的选择敏感，都是基于特定的操作系统平台，可移植性差，检测速度较慢。而和 HIDS 相比，NIDS 的优点是检测速度快，具有较好的隐蔽性，检测范围更宽，可以很好地检测到许多基于网络通信协议漏洞的攻击，可以安装运行在专用的主机上，与被保护主机的操作系统无关，且不占用被保护主机的资源。其缺点是在通信加密的环境下，难于实施有效的检测，而在交换网络的环境下，难于部署，检测性能受网络流量影响较大，且难于从高层监测入侵行为等。

基于误用的入侵检测系统能够准确地检测到已知特征的攻击，但无法检测未知的攻击行为，其漏报率（False Negative Rate）偏高；基于异常的入侵检测系统具有发现未知攻击行为的能力，但存在误报率（False Positive Rate）过高和效率较低的问题。

根据数据融合理论，不同传感器之间的差异性越大，将这些传感器检测数据进行融合后

对检测性能的改善就越明显。不同类型入侵检测系统之间的这种检测方法、检测数据源和结构的差异性，以及性能和检测结果的互补性，为通过报警融合降低误报率和漏报率打下了很好的基础。

3. 入侵检测系统存在的问题

入侵检测系统作为重要网络安全工具，虽然经过了 20 多年的发展，但仍然处于发展阶段，还存在很多需要完善的地方。目前，存在的问题有如下几个方面：

（1）误报和漏报严重

误报（False Positive）就是入侵检测系统误将网络或主机上所发生的正常事件识别为入侵事件，并产生报警；漏报（False Negative）是被保护系统上已经发生了入侵，而入侵检测系统没有检测到这样的事件。

（2）海量信息难以分析

入侵检测系统会在短时间内产生成千上万条报警信息，数据量非常大，同时这些报警信息里面又掺杂着大量误报信息以及漏报导致的不完整信息，使得网络安全管理人员很难对这些信息进行分析，进而进行正确的响应决策。

（3）难以同其他设备联动

当发生入侵时，目前绝大多数的入侵检测系统只限于发出报警信息，不能和其他安全系统（如防火墙等）进行联动，对报警的分析以及对入侵的响应都由管理员手工完成。

（4）难以部署

一般来说，基于主机的入侵检测系统都安装在被保护的主机上，这会加重保护主机的负担，造成系统性能下降；基于网络的入侵检测系统要从网络中采集数据包进行检测分析。在交换环境下，NIDS 的部署位置既要保证检测到来自内网的入侵活动，同时也能检测到来自外网的攻击是一件较困难的事情。另外，如何在高带宽环境下保证不丢失数据包也是目前 IDS 部署中面临的问题。

（5）本身存在安全隐患

入侵检测系统所运行的平台和系统都会存在安全漏洞。即使没有漏洞，入侵检测系统的检测和报警机制也可能被入侵者利用，这些都是入侵检测系统的安全隐患。

1.4 入侵响应技术

1. 入侵响应系统及其作用

入侵检测与入侵响应是紧密相关的问题，入侵检测报警是入侵响应决策的依据，同时入侵检测系统只有通过入侵响应才能有效地实现其安全目标。以前，人们往往将入侵响应系统作为入侵检测系统的一部分，实际上，两者既紧密相关，又相对独立。两者在目标、功能上有明显的区分，在模型和实现方法也有很大不同。前者通过对原始数据的分类发现异常活动和入侵，后者通过对入侵报警的融合等处理回归真实入侵过程，然后对入侵过程进行合适的响应，达到保护目标系统的目的。

入侵响应（Intrusion Response）就是在发现或检测到入侵后，针对入侵所采取的措施和行动，这些行动和措施是为了在发生入侵的情况下，确保被保护目标的机密性、完整性和可

用性。入侵响应系统 IRS（Intrusion Response System）就是实现入侵响应的软件或软、硬件组合系统。入侵响应的主要作用如下：

- 对入侵的告警。也就是通知相关安全管理人员有入侵发生。告警的方式包括控制台报警显示、发送电子邮件和手机短信等。
- 对事件的记录。将报警安全事件及其相关数据进行记录，便于管理员对事件的分析与追查。
- 对入侵的隔离与阻断。对正在发生的入侵进行隔离与阻断，以阻止入侵进展，防止入侵对被保护系统造成更大的损失。隔离与阻断措施有基于主机的方法（如隔离被入侵主机、隔离被入侵服务、中断用户进程、锁定用户账户等），也有基于网络的方法（如 VLAN 隔离、路由阻断、防火墙阻断和交换机端口阻断等）。
- 对入侵者的主动反击。就是对被发现的攻击者实施警告、跟踪和攻击。警告攻击者可以使其放弃攻击行为，达到保护系统的目的；而跟踪攻击者可以发现入侵者在网络中的位置；反攻击方法通常包括所有黑客攻击手段（如 DoS 攻击）。反攻击措施受到法律与制度的约束，是必须慎重使用的。

此外，响应的作用还包括对入侵所造成损失的评估与恢复、对入侵的取证等工作。

根据实施响应措施的自动化程度，入侵响应系统可以分为通知响应系统、手动响应系统和自动响应系统。通知响应系统除了发出入侵的报警，不采取其他响应措施；在手动响应系统中，管理员根据报警等情况进行响应决策，从事先编制好的响应程序集中选择合适的响应程序执行；自动响应系统可以自己根据报警等情况进行响应决策，选择合适的响应措施执行。自动入侵响应系统响应速度最快，是目前入侵响应系统的主要发展方向。所以，自动入侵响应技术是本书阐述的重点。

2. 入侵响应系统存在的问题

Curtis A. Carver Jr.曾经对 56 个入侵检测系统进行了调研，有 18 个系统有自动入侵响应机制。在这 18 个自动入侵响应系统中，14 个系统使用了简单的静态响应决策方法，只有 4 个系统根据多种相关因素进行决策推理，来决定合适的响应措施。目前，人们往往都将入侵响应系统作为入侵检测系统的一部分，或将两者结合起来使用，这些响应系统通常只发出报警，响应分析和响应措施实施由管理员手动完成，响应延迟时间较长，不能做到及时发现入侵和及时响应。自动入侵响应系统是响应速度最快、最及时的响应系统，但目前自动入侵响应系统也存在误响应、漏响应问题，其响应决策模型多采用简单静态映射方法，缺乏推理，自适应能力差，不能均衡考虑响应的有效性与响应的负面效应之间的关系，不能运用响应策略来实现多种响应目的。本书将在第 4 章详细讨论自动入侵响应的问题和解决方法。

1.5 漏洞扫描技术

漏洞是在计算机系统的硬件、操作系统、应用软件和各种协议的设计、安装、配置以及使用过程中所产生的安全缺陷。借助于漏洞，入侵者可以违反计算机系统的安全策略，非法访问、破坏各种目标资源。漏洞扫描系统就是用于检测和发现这些漏洞的软件、硬件

系统。不同的漏洞扫描系统采取了其中一种或多种漏洞扫描技术，漏洞扫描技术的分类如图 1-6 所示。

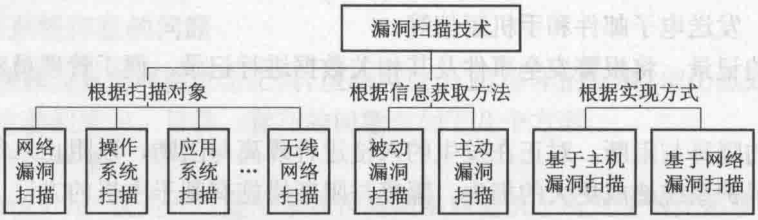

图 1-6 漏洞扫描技术的分类

首先根据扫描对象的不同，漏洞扫描技术可以划分为：

- 网络漏洞扫描技术。网络扫描技术是针对网络设备（包括防火墙、交换机、路由器等）漏洞的扫描技术。
- 操作系统扫描技术。扫描对象为主机的操作系统上的漏洞（包括 Windows 系列操作系统、Unix 系列操作系统等）。
- 应用系统扫描技术。其扫描对象为各种网络应用系统（包括 Web 服务、Ftp 服务和 Database 服务等网络应用系统）上的漏洞。
- 无线网络扫描技术。所针对的扫描对象为各种无线网络上的漏洞。

漏洞扫描针对不同的扫描对象所采取的扫描技术特点是不同的。同时，针对不同的扫描对象，扫描系统具有相对应的漏洞库。根据在扫描过程中信息的获取方法，漏洞扫描技术可以划分为：

- 被动漏洞扫描技术。被动漏洞扫描不主动向扫描目标发送信息，而是通过被动接收相关信息（如网络数据包）来检测目标漏洞。
- 主动漏洞扫描技术。主动漏洞扫描主动向被扫描目标发送相关信息，然后通过目标的反馈信息来检测目标漏洞。

被动扫描技术的优点在于其扫描活动不易被发现，容易掩盖其扫描踪迹，而且也不易受到防火墙等访问控制系统的影响。其缺点是扫描速度慢，准确性较差；主动扫描技术的优点是扫描速度快，准确性较高。其缺点是容易暴露其扫描踪迹，从而被对方发现，并且扫描效果容易受到防火墙等安全系统的影响。根据扫描技术的实现方式，漏洞扫描技术可以划分为：

- 基于主机的扫描技术。基于主机的扫描是一个从被扫描主机用户的角度来检测目标主机上的漏洞的扫描。其实现需要在主机上安装 Agent，通过此 Agent 访问主机上的资源（包括主机上的文件、注册表、用户配置以及进程等），获取相关信息，然后发送到中央扫描服务器，扫描服务器通过对这些信息的分析来发现其中的漏洞。
- 基于网络的漏洞扫描技术。此类技术是基于各种网络技术来远程检测目标漏洞的技术，它是以一个外部攻击者的角度来实现漏洞扫描的。通常通过执行一些脚本文件来模拟对系统的攻击，通过记录目标的反应，来检测目标漏洞。

基于主机的扫描技术的优点是扫描的漏洞多，易于集中化管理，网络流量负载小。其缺点是基于此类技术的扫描器价格较高，技术复杂，在主机上安装 Agent 容易带来新的安全问

题，扫描响应速度受到扫描范围的影响；基于网络的扫描技术的优点是技术上容易实现，维护简单，价格便宜，扫描速度较快。其不足是其扫描效果容易受到各种访问控制机制（如防火墙）的影响。

目前，大多数的漏洞扫描系统是基于网络漏洞扫描技术的。基于网络扫描系统的技术核心包括端口扫描技术和漏洞扫描技术等。端口扫描技术是一项自动检测本地和远程目标系统端口开放情况的技术，它通过向目标主机服务端口发送探测数据包，并通过反馈信息来判断端口的开放情况，以此获取端口提供服务的情况。通过端口扫描所获得的信息可以帮助分析目标的漏洞情况。漏洞扫描技术是建立在端口扫描技术的基础上的，它通过两种方法来检测目标主机上的漏洞：

① 漏洞库方法。将端口扫描所获取的相关信息和漏洞扫描系统的漏洞数据进行比较，以发现是否存在相匹配的漏洞。

② 通过对目标进行模拟攻击，并根据攻击的反馈信息来发现漏洞。例如对 Ftp 进行模拟弱口令攻击，如果攻击成功，则此 Ftp 服务器存在弱口令漏洞。

漏洞扫描技术是一种主动防御技术，它可以在入侵发生之前实施，发现漏洞后通过各种安全手段进行弥补（例如，对漏洞程序打补丁）。但由于操作系统、应用软件系统类型和版本繁多，软件更新速度也较快，及时更新漏洞扫描系统的漏洞库和模拟攻击脚本就面临很大的挑战，所以漏洞扫描系统也很容易产生漏洞的漏扫和误扫等问题。

上述几项网络安全技术都是与本书重点阐述的报警分析、处理技术以及入侵响应技术密切相关的。此外，网络安全技术还有网络防病毒技术、数据加密技术和认证技术等。由于本书重点是入侵分析和入侵响应的相关技术，这里就不对这些技术进行详细叙述了。

1.6 入侵检测报警分析与自动入侵响应技术的重要性

要集成不同系统，实现网络的动态、纵深防御，入侵检测报警分析、处理和入侵响应等相关技术是其中的技术核心。图 1-7 为《网络世界》杂志所进行的一次用户调查的结果。从调查结果来看，用户所希望增加的“主动阻断”“与安全设备的联动”功能都属于自动入侵响应的范畴，而“分析攻击事件”和“按紧急程度不同发出报警”功能属于报警分析的内容，也是在入侵响应决策之前所必须进行的工作。这两项内容之和占了用户希望增加 IDS 功能总和的 73%，这说明了入侵检测报警分析与入侵响应所涉及的有关研究问题都是网络安全研究领域所亟待解决的问题，也是本书阐述的主要内容。

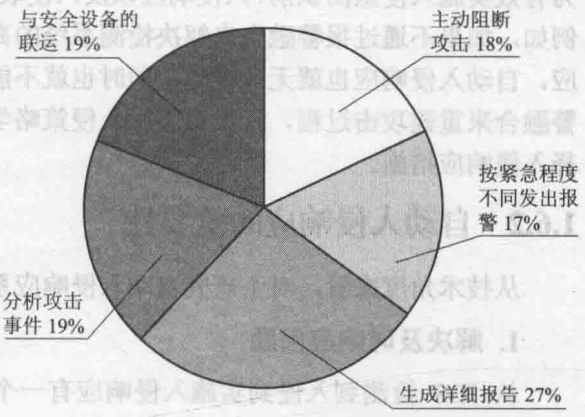

图 1-7 用户希望增加的 IDS 功能

1.6.1 入侵检测报警分析、处理的重要性

入侵报警分析、处理技术的重要性主要体现在如下两个方面。