第 5 章

防火墙与入侵检测

学习目标：

- 掌握防火墙和入侵检测的定义、设置。
- 掌握分组过滤防火墙的定义和入侵检测系统检测的步骤。
- 了解防火墙的分类、系统模型，了解入侵检测系统检测的方法。

5.1 防 火 墙

5.1.1 防火墙的概念

防火墙(firewall)是一项协助确保信息安全的设备，会依照特定的规则，允许或是限制传输的数据通过。防火墙可以是一台专属的硬件也可以是架设在一般硬件上的一套软件。所谓防火墙指的是一个由软件和硬件设备组合而成的，在内部网和外部网之间、专用网与公共网之间的界面上构造的保护屏障，是一种获取安全方法的形象说法，它是一种计算机硬件和软件的结合，使 Internet 与 Intranet 之间建立起一个安全网关(security gateway)，从而保护内部网免受非法用户的侵入，防火墙主要由服务访问规则、验证工具、包过滤和应用网关四部分组成，防火墙就是一个位于计算机和它所连接的网络之间的软件或硬件。该计算机流入流出的所有网络通信和数据包均要经过此防火墙。

在网络中，所谓“防火墙”，是指一种将内部网和公众访问网(如 Internet)分开的方法，它实际上是一种隔离技术。防火墙是在两个网络通信时执行的一种访问控制尺度，它能允许你同意的人和数据进入你的网络，同时将你不同意的人和数据拒之门外，最大限度地阻止网络中的黑客来访问你的网络。换句话说，如果不通过防火墙，公司内部的人就无法访问 Internet，Internet 上的人也无法和公司内部的人进行通信。

Windows 系统可以很方便地定义过滤掉数据包，例如 Internet 连接防火墙(ICF)，它就是用一段“代码墙”把计算机和 Internet 分隔开，时刻检查出入防火墙的所有数据包，决定拦截或是放行哪些数据包。防火墙可以是一种硬件、固件或者软件，例如专用防火墙设备就是硬件形式的防火墙，包过滤路由器是嵌有防火墙固件的路由器，而代理服务器等软件就是软件形式的防火墙。

5.1.2 防火墙的分类

常见的防火墙有三种类型：分组过滤防火墙、应用代理防火墙、状态检测防火墙。

1. 分组过滤防火墙

分组过滤防火墙作用在协议组的网络层和传输层,可视为一种 IP 封包过滤器,运作在底层的 TCP/IP 协议堆栈上。我们可以以枚举的方式,只允许符合特定规则的封包通过,其余的一概禁止穿越防火墙。这些规则通常可以由管理员定义或修改,根据分组报头源地址、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,只有满足过滤逻辑的数据包才被转发到相应的目的地的出口端,其余的数据包则从数据流中丢弃。

建立防火墙规则集的基本方法有两种:明示允许(inclusive)型或明示禁止(exclusive)型。明示禁止的防火墙规则,默认允许所有数据通过防火墙,而这种规则集中定义的则是不允许通过防火墙的流量,换言之,与这些规则不匹配的数据,全部是允许通过防火墙的。明示允许的防火墙正好相反,它只允许符合规则集中定义的流量通过,而其他所有的流量都被阻止。

明示允许型防火墙能够提供对于传出流量更好的控制,这使其更适合那些直接对 Internet 公网提供服务的系统的需要。它也能够控制来自 Internet 公网到私有网络的访问类型。所有和规则不匹配的流量都会被阻止并记录在案。一般来说,明示允许防火墙要比明示禁止防火墙更安全,因为它们显著地减少了允许不希望的流量通过可能造成的风险。例如,定义的防火墙规则集如表 5-1 所示。

表 5-1 定义的防火墙规则集

组序号	动作	源 IP	目的 IP	源端口	目的端口	协议类型
1	允许	10.1.1.1	*	*	*	TCP
2	允许	*	10.1.1.1	20	*	TCP
3	禁止	*	10.1.1.1	20	<1024	TCP

第一条规则:主机 10.1.1.1 任何端口访问任何主机的任何端口,基于 TCP 的数据包都允许通过。

第二条规则:任何主机的 20 端口访问主机 10.1.1.1 的任何端口,基于 TCP 的数据包允许通过。

第三条规则:任何主机的 20 端口访问主机 10.1.1.1 小于 1024 的端口,如果基于 TCP 的数据包都禁止通过。

2. 应用代理防火墙

应用代理防火墙也叫应用网关(application gateway),它作用在应用层,其特点是完全"阻隔"网络通信流,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。实际中的应用网关通常由专用工作站实现。

应用代理服务器是运行在防火墙上的一种服务器程序,防火墙主机可以是一个具有两个网络接口的双重宿主主机,也可以是一个堡垒主机。

应用代理服务器被放置在内部服务器和外部服务器之间,用于转接内外主机之间的通信,它可以根据安全策略来决定是否为用户进行代理服务。应用代理服务器运行在应用层,因此又被称为"应用网关"。例如,一个应用代理服务器可以限制 FTP 用户只能够从 Internet 上获取文件,而不能将文件上传到 Internet 上。

3. 状态检测防火墙

状态检测(status detection)防火墙直接对分组里的数据进行处理,并且结合前后分组的数据进行综合判断,然后决定是否允许该数据包通过。

5.1.3　常见防火墙系统模型

常见防火墙系统一般按照四种模型构建:筛选路由器模型、单宿主堡垒主机(屏蔽主机防火墙)模型、双宿主堡垒主机(屏蔽防火墙系统)模型和屏蔽子网模型。

(1) 筛选路由器模型是网络的第一道防线,功能是实施包过滤。创建相应的过滤策略时对工作人员的 TCP/IP 的知识有相当的要求,如果筛选路由器被黑客攻破,那么内部网络将变得十分危险。该防火墙不能够隐藏内部网络的信息,不具备监视和日志记录功能。典型的筛选路由器模型如图 5-1 所示。

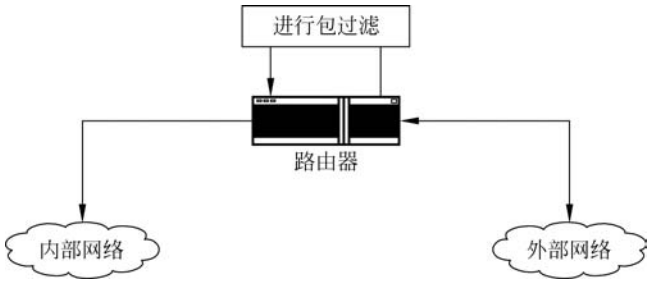

图 5-1　典型的筛选路由器模型

(2) 单宿主堡垒主机(屏蔽主机防火墙)模型由防火墙和堡垒主机组成。该防火墙系统提供的安全等级比筛选路由器防火墙系统要高,因为它实现了网络层安全(包过滤)和应用层安全(代理服务)。所以入侵者在破坏内部网络的安全性之前,必须首先渗透两种不同的安全系统。单宿主堡垒主机模型如图 5-2 所示。

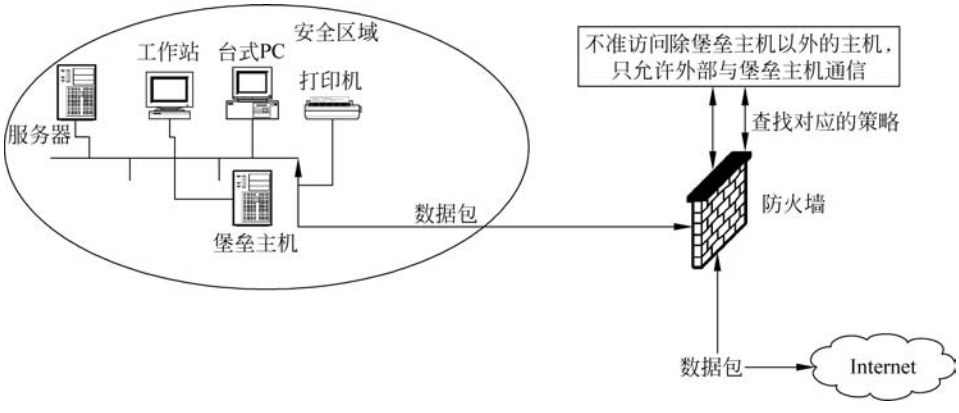

图 5-2　单宿主堡垒主机模型

(3) 双宿主堡垒主机(屏蔽防火墙系统)模型可以构造更加安全的防火墙系统。双宿主堡垒主机有两种网络接口,但是主机在两个端口之间直接转发信息的功能被关掉了。

在物理结构上强行将所有去往内部网络的信息经过堡垒主机。双宿主堡垒主机模型如图5-3所示。

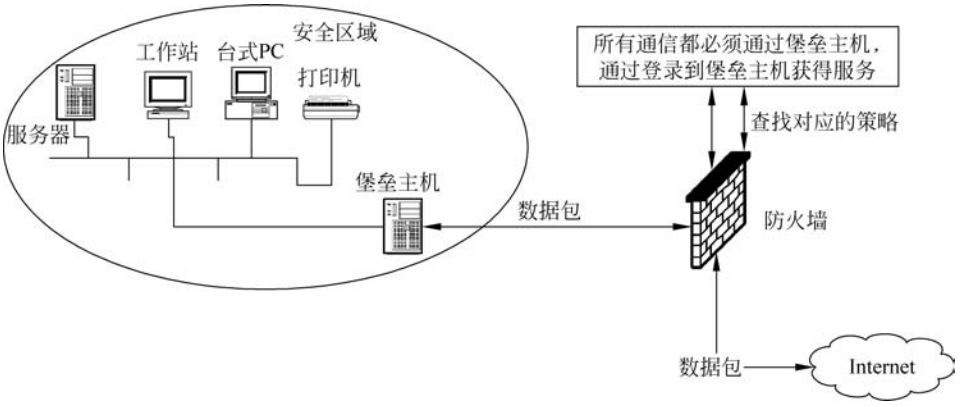

图5-3 双宿主堡垒主机模型

(4) 屏蔽子网模型用了三个防火墙和一个堡垒主机。它是最安全的防火墙系统之一,因为在定义了"中立区"(demilitarized zone,DMZ)网络后,它支持网络层和应用层的安全功能。网络管理员将堡垒主机、信息服务器、Modem组,以及其他公用服务器放在DMZ网络中。如果黑客想突破该防火墙,那么必须攻破以上三个单独的设备,模型如图5-4所示。

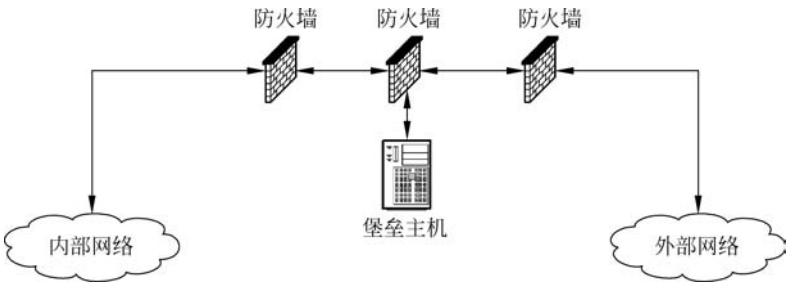

图5-4 屏蔽子网模型

难点说明:堡垒主机是一种被强化的可以防御进攻的计算机,作为进入内部网络的一个检查点,以达到把整个网络的安全问题集中在某个主机上解决,从而省时省力,不用考虑其他主机的安全的目的。

堡垒主机是网络中最容易受到侵害的主机,所以堡垒主机也必须是自身保护最完善的主机。一个堡垒主机使用两个网卡,每个网卡连接不同的网络。一个网卡连接公司的内部网络用来管理、控制和保护,而另一个连接另一个网络,通常是公网也就是Internet。

堡垒主机是一台完全暴露给外网攻击的主机。它没有任何防火墙或者包过虑路由器设备保护。堡垒主机执行的任务对于整个网络安全系统至关重要。事实上,防火墙和包过滤路由器也可以被看作堡垒主机。由于堡垒主机完全暴露在外网安全威胁之下,需要做许多工作来设计和配置堡垒主机,使它遭到外网攻击的风险性减至最低。其他类型的

堡垒主机包括 Web、Mail、DNS、FTP 服务器。

一些网络管理员会用堡垒主机做牺牲品来换取网络的安全。这些主机吸引入侵者的注意力，耗费攻击真正网络主机的时间并且使追踪入侵企图变得更加容易。

5.1.4　建立防火墙的步骤

建立一个可靠的规则集对于实现一个成功的、安全的防火墙来说是非常关键的一步。因为如果防火墙规则集配置错误，再好的防火墙也只是摆设。在安全审计中，经常能看到花巨资购入的防火墙由于某个规则配置的错误而将机构暴露于巨大的危险之中。

成功的创建一个防火墙系统一般需要六步：①制定安全策略；②搭建安全体系结构；③制定规则次序；④落实规则集；⑤注意更换控制；⑥做好审计工作。

1. 制定安全策略

防火墙和防火墙规则集只是安全策略的技术实现。管理层规定实施什么样的安全策略，防火墙是策略得以实施的技术工具。所以，在建立规则集之前，我们必须首先理解安全策略，假设它包含以下三方面内容。

(1) 内部雇员访问 Internet 不受限制。

(2) 规定 Internet 用户有权使用公司的 Webserver 和 Internet E-mail。

(3) 任何进入公用内部网络的通话必须经过安全认证和加密。

显然，大多数机构的安全策略要远远比这复杂，需要根据单位的实际情况制定安全策略。

2. 搭建安全体系结构

作为一名网络管理员，要将安全策略转化为安全体系结构。根据安全策略规定 Internet 用户有权使用公司的 Webserver 和 Internet E-mail。这就要求为公司建立 Web 和 E-mail 服务器。由于任何人都能访问 Web 和 E-mail 服务器，所以它们不安全。我们通过把它们放入 DMZ 来实现该项策略。DMZ 是一个孤立的网络，通常把不信任的系统放在那里，DMZ 中的系统不能启动连接内部网络。DMZ 有两种类型，有保护的和无保护的。有保护的 DMZ 是与防火墙脱离的孤立的部分，无保护的 DMZ 是介于路由器和防火墙之间的网络部分。这里建议使用有保护的 DMZ，我们把 Web 和 E-mail 服务器放在那里。

3. 制定规则次序

在建立规则集之前，有一件事必须提及，即规则次序。哪条规则放在哪条规则之前是非常关键的。同样的规则，以不同的次序放置，可能会完全改变防火墙的运转情况。很多防火墙(例如 SunScreen EFS、Cisco IOS、FW-1)以顺序方式检查信息包，当防火墙接收到一个信息包时，它先与第一条规则相比较，然后是第二条、第三条……当它发现一条匹配规则时，就停止检查并应用那条规则。如果信息包与每一条规则比较而没有发现匹配的，这个信息包便会被拒绝。一般来说，通常的顺序是较特殊的规则在前，较普通的规则在后，防止在找到一个特殊规则之前一个普通规则便被匹配，这可以避免防火墙配置错误。

4. 落实规则集

选好素材就可以建立规则集了，下面简要概述每条规则。

(1) 切断默认。在默认情况下需要切断默认性能。

(2) 允许内部出网。规则是允许内部网络的任何人出网,与安全策略中所规定的一样,所有的服务都被许可。

(3) 添加锁定。现在添加锁定规则,阻塞对防火墙的任何访问,这是所有规则集都应有的一条标准规则,除了防火墙管理员,任何人都不能访问防火墙。

(4) 丢弃不匹配的信息包。在默认情况下,丢弃所有不能与任何规则匹配的信息包。但这些信息包并没有被记录。把它添加到规则集末尾来改变这种情况,这是每个规则集都应有的标准规则。

(5) 丢弃并不记录。通常网络上大量被防火墙丢弃并记录的通信通话会很快将日志填满。创立一条规则丢弃或拒绝这种通话但不记录它。这是一条很有必要的标准规则。

(6) 允许 DNS 访问。允许 Internet 用户访问 DNS 服务器。

(7) 允许邮件访问。允许 Internet 和内部用户通过 SMTP(简单邮件传递协议)访问邮件服务器。

(8) 允许 Web 访问。允许 Internet 和内部用户通过 HTTP(服务程序所用的协议)访问 Web 服务器。

(9) 阻塞 DMZ。内部用户公开访问 DMZ,这是必须阻止的。

(10) 允许内部的 POP 访问。让内部用户通过 POP(邮件协议)访问邮件服务器。

(11) 强化 DMZ 的规则。DMZ 应该从不启动与内部网络的连接。如果你的 DMZ 能这样做,就说明它是不安全的。这里希望加上这样一条规则,只要有从 DMZ 到内部用户的通话,它就会拒绝、做记录并发出警告。

(12) 允许管理员访问。允许管理员(受限于特殊的资源 IP)以加密方式访问内部网络。

(13) 提高性能。只要有可能,就把最常用的规则移到规则集的顶端。因为防火墙只分析较少数的规则,这样能提高防火墙性能。

(14) 增加 IDS。对那些喜欢基础扫描检测的人来说,这会有帮助。

(15) 附加规则。可以添加一些附加规则,例如阻塞与 AOL ICQ 的连接,不要阻塞入口,只阻塞目的文件 AOL 服务器。

5. 注意更换控制

在恰当地组织好规则之后,还建议写上注释并经常更新。注释可以帮助你明白哪条规则做什么,对规则理解得越好,错误配置的可能性就越小。对那些有多重防火墙管理员的大机构来说,建议当规则被修改时,把下列信息加入注释中,这可以帮助跟踪谁修改了哪条规则以及修改的原因。

(1) 规则更改者的名字。

(2) 规则变更的日期/时间。

(3) 规则变更的原因。

6. 做好审计工作

建立好规则集后,检测很关键。防火墙实际上是一种隔离内外网的工具。在如今 Internet 访问的动态世界里,在实现过程中很容易犯错误。通过建立一个可靠的、简单的

规则集，可以创建一个更安全的被防火墙所隔离的网络环境。

需要注意的是规则越简单越好，一个简单的规则集是建立一个安全的防火墙的关键所在。尽量保持规则集简洁和简短，因为规则越多，就越可能犯错误，规则越少，理解和维护就越容易。一个好的准则是最好不要超过30条。一旦规则超过50条，就会以失败而告终。当要从很多规则入手时，就要认真检查一下整个安全体系结构，而不仅仅是防火墙。规则越少，规则集就越简洁，错误配置的可能性就越小，系统就越安全。因为规则少意味着只分析少数的规则，防火墙的CPU周期就短，防火墙效率就可以提高。

用Windows自带防火墙实现访问控制参见第9章实验11，用路由器ACL实现包过滤参见第9章实验12。

5.1.5　iptables防火墙的设置

iptables是Linux中对网络数据包进行处理的一个功能组件，相当于防火墙，可以对经过的数据包进行处理，如数据包过滤、数据包转发等，是Ubuntu Linux系统自带启动的防火墙。

1. iptables结构

iptables其实是一堆规则，防火墙根据iptables里的规则，对收到的网络数据包进行处理。iptables里的数据组织结构分为表、链、规则链。

1）表

表(tables)提供特定的功能，iptables里面有四个表：filter表、nat表、mangle表和raw表，分别用于实现包过滤、网络地址转换、包重构和数据追踪处理。每个表里包含多个链。

2）链

链(chains)是数据包传播的路径，每一条链其实就是众多规则中的一个检查清单，每一条链中可以有一条或数条规则。当一个数据包到达一个链时，iptables就会从链中第一条规则开始检查，看该数据包是否满足规则所定义的条件。如果满足，系统就会根据该条规则所定义的方法处理该数据包；否则iptables将继续检查下一条规则。如果该数据包不符合链中任一条规则，iptables就会根据该链预先定义的默认策略进行转发。

3）规则链

INPUT——进来的数据包应用此规则链中的策略。

OUTPUT——外出的数据包应用此规则链中的策略。

FORWARD——转发数据包时应用此规则链中的策略。

PREROUTING——对数据包作路由选择前应用此链中的规则。

POSTROUTING——对数据包作路由选择后应用此链中的规则。

表链结构如下。

filter表——三个链：INPUT、FORWARD、OUTPUT。

作用：过滤数据包。

内核模块：iptables_filter。

Nat表——三个链：PREROUTING、POSTROUTING、OUTPUT。

作用：用于网络地址转换(IP、端口)。

内核模块：iptable_nat。

Mangle 表——五个链：PREROUTING、POSTROUTING、INPUT、OUTPUT、FORWARD。

作用：修改数据包的服务类型、TTL、并且可以配置路由实现 QoS 内核模块。

Raw 表——两个链：OUTPUT、PREROUTING。

作用：决定数据包是否被状态跟踪机制处理。

2. iptables 操作

1) iptables 的格式

```
iptables [ -t 表名] 命令选项 [链名] [条件匹配] [ -j 目标动作或跳转]
```

说明：表名、链名用于指定 iptables 命令所操作的表和链，命令选项用于指定管理 iptables 规则的方式(如插入、增加、删除、查看等)；条件匹配用于指定对符合什么样条件的数据包进行处理；目标动作或跳转用于指定数据包的处理方式，如允许通过、拒绝、丢弃、跳转(Jump)给其他链处理。

2) iptables 命令的管理控制选项

-A 在指定链的末尾添加(append)一条新的规则。

-D 删除(delete)指定链中的某一条规则，可以按规则序号和内容删除。

-I 在指定链中插入(insert)一条新的规则，默认在第一行添加。

-R 修改、替换(replace)指定链中的某一条规则，可以按规则序号和内容替换。

-L 列出(list)指定链中所有的规则进行查看。

-E 重命名用户定义的链，不改变链本身。

-F 清空(flush)。

-N 新建(new-chain)一条用户自己定义的规则链。

-X 删除指定表中用户自定义的规则链。

-P 设置指定链的默认策略(policy)。

-Z 将所有表的所有链的字节和数据包计数器清零。

-n 使用数字形式(numeric)显示输出结果。

-v 查看规则表详细信息(verbose)。

-V 查看版本(version)。

-h 获取帮助(help)。

3) 防火墙处理数据包的四种方式

ACCEPT 允许数据包通过。

DROP 直接丢弃数据包，不给任何回应信息。

REJECT 拒绝数据包通过，必要时会给数据发送端一个响应的信息。

LOG 用于针对特定的数据包打 log，在/var/log/messages 文件中记录日志信息，然后将数据包传递给下一条规则。

5.2　入侵检测

入侵检测系统(intrusion detection system,IDS)是一种对网络传输进行即时监视,在发现可疑传输时发出警报或者采取主动反应措施的网络安全系统。它与其他网络安全系统的不同之处在于,IDS是一种积极主动的安全防护技术。IDS最早出现于1980年4月,后来IDS逐渐发展成为入侵检测专家系统(IDES)。1990年,IDS分化为基于网络的IDS和基于主机的IDS,后又出现分布式IDS。

由于入侵检测系统的市场在近几年飞速发展,许多公司投入到这一领域中。Venustech(启明星辰)、Internet Security System(ISS)、思科、赛门铁克等公司都推出了自己的产品。

5.2.1　入侵检测系统的概念

入侵检测系统指的是一种硬件或者软件系统,其通过实时监视系统对系统资源的非授权使用能够做出及时的判断和记录,一旦发现异常情况就发出报警。

入侵检测(intrusion detection)是对入侵行为的检测,它通过收集和分析网络行为、安全日志、审计数据、其他网络上可以获得的信息以及计算机系统中若干关键点的信息,检查网络或系统中是否存在违反安全策略的行为和被攻击的迹象。入侵检测作为一种积极主动的安全防护技术,提供了对内部攻击、外部攻击和误操作的实时保护,在网络系统受到危害之前拦截和响应入侵。因此被认为是防火墙之后的第二道安全门,在不影响网络性能的情况下能对网络进行监测。入侵检测通过执行以下任务来实现监视、分析用户及系统活动:系统构造和弱点的审计;识别已知进攻的活动模式并向相关人士报警;异常行为模式的统计分析;评估重要系统和数据文件的完整性;操作系统的审计跟踪管理,并识别用户违反安全策略的行为。

入侵检测是防火墙的合理补充,帮助系统对付网络攻击,扩展了系统管理员的安全管理能力(包括安全审计、监视、进攻识别和响应),提高了信息安全基础结构的完整性。它从计算机网络系统中的若干关键点收集信息,并分析这些信息,看看网络中是否有违反安全策略的行为和遭到袭击的迹象。入侵检测提供对内部攻击、外部攻击和误操作的实时保护。

5.2.2　入侵检测系统的功能

入侵检测系统的功能主要有以下几种。

1. 识别黑客常用入侵与攻击手段

入侵检测技术通过分析各种攻击的特征,可以全面快速地识别探测攻击、拒绝服务攻击、缓冲区溢出攻击、电子邮件攻击、浏览器攻击等各种常用攻击手段,并做相应的防范。一般来说,黑客在进行入侵的第一步探测、收集网络及系统信息时,就会被IDS捕获,向管理员发出警告。

2. 监控网络异常通信

IDS会对网络中不正常的通信连接做出反应,保证网络通信的合法性;任何不符合网络安全策略的网络数据都会被IDS侦测到并警告。

3. 鉴别对系统漏洞及后门的利用

IDS一般带有系统漏洞及后门的详细信息,通过对网络数据包连接的方式、连接端口以及连接中特定的内容等特征分析,可以有效地发现网络通信中针对系统漏洞进行的非法行为。

4. 完善网络安全管理

IDS通过对攻击或入侵的检测及反应,可以有效地发现和防止大部分的网络犯罪行为,给网络安全管理提供了一个集中、方便、有效的工具。使用IDS的监测、统计分析、报表功能,可以进一步完善网络管理。

5.2.3 入侵检测系统的分类

1. 基于主机

一般主要使用操作系统的审计、跟踪日志作为数据源,某些也会主动与主机系统进行交互,以获得不存在于系统日志中的信息来检测入侵。这种类型的检测系统不需要额外的硬件,对网络流量不敏感,效率高,能准确定位入侵并实时反应,但是占用主机资源,依赖于主机的可靠住,所能检测的攻击类型受限,不能检测网络攻击。

2. 基于网络

通过被动地监听网络上传输的原始流量,对获取的网络数据进行处理,从中提取有用的信息,再通过与已知攻击特征相匹配或与正常网络行为原型相比较来识别攻击事件。此类检测系统不依赖操作系统作为检测资源,可应用于不同的操作系统平台;配置简单,不需要任何特殊的审计和登录机制;可检测协议攻击、特定环境的攻击等多种攻击。但它只能监视经过本网段的活动,无法得到主机系统的实时状态,精确度较差。大部分入侵检测工具都是基于网络的入侵检测系统。

3. 分布式

入侵检测系统一般为分布式结构,由多个部件组成,在关键主机上采用主机入侵检测,在网络关键节点上采用网络入侵检测,同时分析来自主机系统的审计日志和来自网络的数据流,判断被保护系统是否受到攻击。

5.2.4 入侵检测的方法

入侵检测的方法归纳起来有两类:异常检测方法和误用检测方法。

1. 异常检测方法

异常检测(anomaly detection)的假设是入侵者活动异常于正常主体的活动。根据这一理念建立主体正常活动的"活动简档",将当前主体的活动状况与"活动简档"相比较,当违反其统计规律时,认为该活动可能是入侵行为。异常检测的难题在于如何建立"活动简档"以及如何设计统计算法,从而不把正常的操作作为"入侵"或忽略真正的"入侵"行为。在异常入侵检测系统中常常采用以下几种检测方法。

（1）基于贝叶斯推理检测法：该方法通过在任何给定的时刻，测量变量值，推理判断系统是否发生入侵事件。

（2）基于特征选择检测法：指从一组度量中挑选出能检测入侵的度量，用它来对入侵行为进行预测或分类。

（3）基于贝叶斯网络检测法：用图形方式表示随机变量之间的关系。通过指定的与邻接节点相关的一个小的概率集来计算随机变量的连接概率分布。按给定全部节点组合，所有根节点的先验概率和非根节点概率构成这个集。贝叶斯网络是一个有向图，弧表示父节点、子节点之间的依赖关系。当随机变量的值变为已知时，就允许将它吸收为证据，为其他的剩余随机变量条件值判断提供计算框架。

（4）基于模式预测的检测法：事件序列不是随机发生的而是遵循某种可辨别的模式，是基于模式预测的异常检测法的假设条件，其特点是事件序列及相互联系被考虑到了，只关心少数相关安全事件是该检测法的最大优点。

（5）基于统计的异常检测法：该方法是根据用户对象的活动为每个用户都建立一个特征轮廓表，通过对当前特征与以前已经建立的特征进行比较，来判断当前行为的异常性。用户特征轮廓表要根据审计记录情况不断更新，其包括许多衡量指标，这些指标要根据经验值或一段时间内的统计而得到。

（6）基于机器学习检测法：该方法是根据离散数据临时序列学习获得网络、系统和个体的行为特征，并提出了一个实例学习法 IBL，IBL 是基于相似度的，该方法通过新的序列相似度计算将原始数据（如离散事件流和无序的记录）转化成可度量的空间。然后，应用 IBL 学习技术和一种新的基于序列的分类方法，发现异常类型事件，从而检测入侵行为。其中，成员分类的概率由阈值的选取来决定。

（7）数据挖掘检测法：数据挖掘的目的是要从海量的数据中提取出有用的数据信息。网络中会有大量的审计记录存在，审计记录大多都是以文件形式存放的。如果靠手工方法来发现记录中的异常现象是远远不够的，所以将数据挖掘技术应用于入侵检测中，可以从审计数据中提取有用的知识，然后用这些知识区检测异常入侵和已知的入侵。采用的方法有 KDD 算法，其优点是具有处理大量数据的能力与数据关联分析的能力，但是实时性较差。

（8）基于应用模式的异常检测法：该方法是根据服务请求类型、服务请求长度、服务请求包大小分布计算网络服务的异常值。通过实时计算的异常值和所建立的阈值比较，从而发现异常行为。

（9）基于文本分类的异常检测法：该方法是将系统产生的进程调用集合转换为“文档”。利用 K 邻聚类文本分类算法计算文档的相似性。

2. 误用检测方法

误用入侵检测系统中常用的检测方法有以下三种。

（1）模式匹配法：该方法常常被用于入侵检测技术中。它是通过把收集到的信息与网络入侵和系统误用模式数据库中的已知信息进行比较，从而对违背安全策略的行为进行发现。模式匹配法可以显著地减少系统负担，有较高的检测率和准确率。

（2）专家系统法：这个方法的思想是把安全专家的知识表示成规则知识库，再用推

理算法检测入侵。主要是针对有特征的入侵行为。

(3) 基于状态转移分析的检测法：该方法的基本思想是将攻击看成一个连续的、分步骤的并且各个步骤之间有一定的关联的过程。在网络中发生入侵时及时阻断入侵行为,防止可能还会进一步发生的类似攻击行为。在状态转移分析方法中,一个渗透过程可以看作是由攻击者做出的一系列的行为而导致系统从某个初始状态变为最终某个被危害的状态。

5.2.5 入侵检测的步骤

入侵检测一般分为三个步骤,依次为信息收集、数据分析、响应(被动响应和主动响应)。

1. 信息收集

信息收集包括系统、网络、数据及用户活动的状态和行为。入侵检测利用的信息一般来自系统日志、目录以及文件中的异常改变、程序执行中的异常行为及物理形式的入侵信息四个方面。

2. 数据分析

数据分析是入侵检测的核心。它首先构建分析器,把收集到的信息经过预处理,建立一个行为分析引擎或模型,然后向模型中植入时间数据,在知识库中保存植入数据的模型。数据分析一般通过模式匹配、统计分析和完整性分析三种手段进行。前两种方法用于实时入侵检测,而完整性分析则用于事后分析。

3. 响应

入侵检测系统在发现入侵后会及时做出响应,包括切断网络连接、记录事件和报警等。响应一般分为主动响应(阻止攻击或影响进而改变攻击的进程)和被动响应(报告和记录所检测出的问题)两种类型。主动响应由用户驱动或系统本身自动执行,可对入侵者采取行动(如断开连接)、修正系统环境或收集有用信息；被动响应则包括报警和通知、简单网络管理协议(SNMP)陷阱和插件等。另外,还可以按策略配置响应,可分别采取立即、紧急、适时、本地的长期和全局的长期等行动。

入侵检测工具常用 BlackICE,具体使用参见第 9 章实验 13。

5.2.6 防火墙和入侵检测系统的区别和联系

1. 防火墙和入侵检测系统的区别

(1) 概念上的区别。

防火墙是设置在被保护网络(本地网络)和外部网络(主要是 Internet)之间的一道防御系统,以防止发生不可预测的、潜在的、破坏性的侵入。它可以通过检测、限制、更改跨越防火墙的数据流,尽可能对外部屏蔽内部的信息、结构和运行状态,以此来保护内部网络中的信息、资源等不受外部网络中非法用户的侵犯。

入侵检测系统是对入侵行为的发觉,通过从计算机网络或计算机的关键点收集信息并进行分析,从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。

总结：从概念上我们可以看出防火墙是针对黑客攻击的一种被动的防御，IDS则是主动出击寻找潜在的攻击者；防火墙相当于一个机构的门卫，受到各种限制和区域的影响，即凡是防火墙允许的行为都是合法的，而IDS则相当于巡逻兵，不受范围和限制的约束，这也造成了ISO存在误报和漏报的情况出现。

（2）功能上的区别。

防火墙的主要功能是过滤不安全的服务和非法用户：所有进出内部网络的信息都必须通过防火墙，防火墙成为一个检查点，禁止未授权的用户访问受保护的网络。

① 控制对特殊站点的访问：防火墙可以允许受保护网络中的一部分主机被外部网访问，而另一部分则被保护起来。

② 作为网络安全的集中监视点：防火墙可以记录所有通过它的访问，并提供统计数据，提供预警和审计功能。

入侵检测系统的主要任务有：

（1）监视、分析用户及系统活动。

（2）对异常行为模式进行统计分析，发现入侵行为规律。

（3）检查系统配置的正确性和安全漏洞，并提示管理员修补漏洞。

（4）能够实时对检测到的入侵行为进行响应。

（5）评估系统关键资源和数据文件的完整性。

（6）操作系统的审计跟踪管理，并识别用户违反安全策略的行为。

总结：防火墙只是防御为主，通过防火墙的数据便不再进行任何操作，IDS则进行实时的检测，发现入侵行为即可做出反应，是对防火墙弱点的修补；防火墙可以允许内部的一些主机被外部访问，IDS则没有这些功能，只是监视和分析用户和系统活动。

2. 防火墙和入侵检测系统的联系

（1）IDS是继防火墙之后的又一道防线，防火墙是防御，IDS是主动检测，两者结合有力地保证了内部系统的安全。

（2）IDS实时检测可以及时发现一些防火墙没有发现的入侵行为，发现入侵行为的规律，这样防火墙就可以将这些规律加入规则集之中，提高防火墙的防护力度。

习　题　5

一、填空题

1. 常见的防火墙有三种类型：_____、_____、_____。

2. 创建一个防火墙系统一般需要六步：_____、_____、_____、_____、_____、_____。

3. 常见的防火墙系统一般按照四种模型构建：_____、_____、_____、_____。

4. 入侵检测的三个基本步骤是_____、_____、_____。

5. 入侵检测系统分为_____、_____、_____三种。

二、简答题

1. 简述防火墙的分类,并说明分组过滤防火墙的基本原理。
2. 常见防火墙模型有哪些？比较它们的优缺点。
3. 什么是入侵检测系统？简述入侵检测系统目前面临的挑战。
4. 简述入侵检测常用的方法。