第 14 章　网络安全管理

网络安全管理涉及设备安全、系统安全、数据安全、应用安全等方面的内容。在实际应用中，应加强服务器的网络安全管理，以保证网络安全、正常、高效地运行。

14.1　安全配置向导

在运行 Windows Server 2003 操作系统的服务器计算机中，可以使用“安全配置向导”对系统进行安全配置，即创建一个安全策略，此安全策略基于服务器角色配置服务和网络安全，并配置审核和注册表设置，从而提高服务器的安全性。

14.1.1　安装“安全配置向导”组件

可以使用 Windows Server 2003 系统中的“添加或删除程序”安装“安全配置向导”组件，其操作步骤如下：

(1)执行“开始”→“控制面板”→“添加或删除程序”命令，弹出“添加或删除程序”窗口，如图 14-1 所示。

图 14-1　“添加或删除程序”窗口

(2)单击“添加/删除 Windows 组件”按钮,弹出“Windows 组件向导”对话框,如图 14-2 所示,在“组件”列表框中选中“安全配置向导”复选框。

(3)单击“下一步”按钮,弹出“正在配置组件”对话框,如图 14-3 所示。

图 14-2 “Windows 组件向导”对话框

图 14-3 “正在配置组件”对话框

(4)配置完成组件后,弹出“完成‘Windows 组件向导’”对话框,如图 14-4 所示,单击“完成”按钮,完成“安全配置向导”组件的安装。

图 14-4 “完成‘Windows 组件向导’”对话框

14.1.2 创建安全策略

“安全配置向导”组件安装完成后,应使用其进行安全策略配置,以提高服务器的安全性,创建安全策略的操作步骤如下:

(1)执行“开始”→“所有程序”→“管理工具”→“安全配置向导”命令,弹出“欢迎使用安全配置向导”对话框,如图 14-5 所示。

(2)单击“下一步”按钮,弹出“配置操作”对话框,如图 14-6 所示,选中“创建新的安全策略”单选按钮。

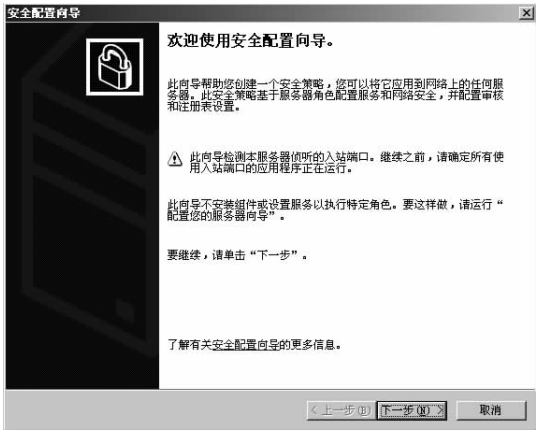

图 14-5　“欢迎使用安全配置向导”对话框

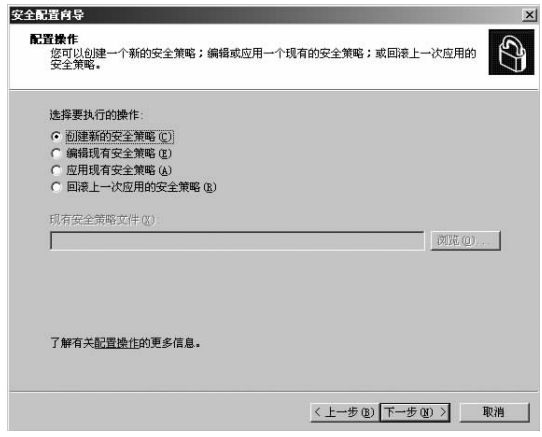

图 14-6　“配置操作”对话框

(3)单击“下一步”按钮，弹出“选择服务器”对话框，如图 14-7 所示。可以在“服务器”文本框中输入要配置的服务器名称，也可以单击“浏览”按钮，在弹出的“选择计算机”对话框中选择服务器计算机。

(4)单击“下一步”按钮，弹出“正在处理安全配置数据库”对话框，如图 14-8 所示。

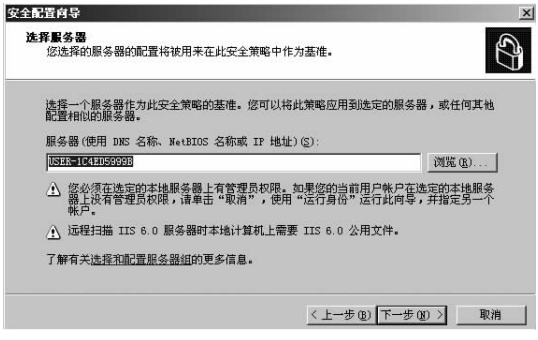

图 14-7　“选择服务器”对话框

图 14-8　“正在处理安全配置数据库”对话框

提示:单击“查看配置数据库”按钮，可以在弹出的如图 14-9 所示的对话框中查看安全配置数据库的内容。

图 14-9　安全配置数据库

(5)单击“下一步”按钮,弹出“基于角色的服务配置”对话框,如图 14-10 所示。

(6)单击“下一步”按钮,弹出“选择服务器角色”对话框,如图 14-11 所示。在“为选定的服务器选择要执行的服务器角色”列表框中选择服务器角色。

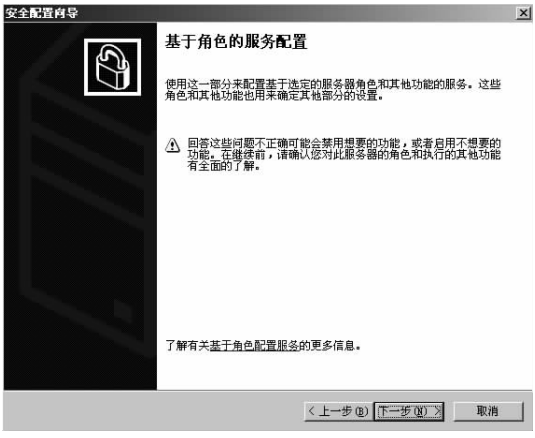

图 14-10 “基于角色的服务配置”对话框

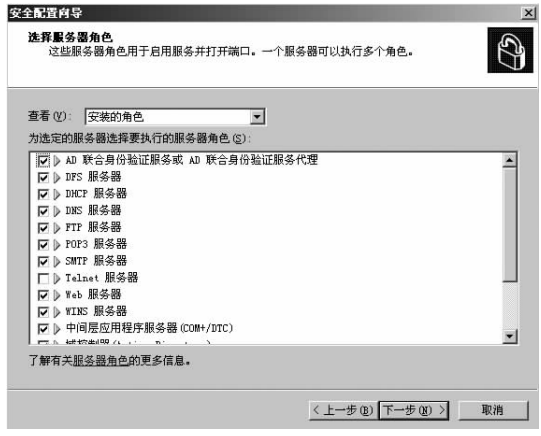

图 14-11 “选择服务器角色”对话框

(7)单击“下一步”按钮,弹出“选择客户端功能”对话框,如图 14-12 所示,根据客户端要求选择需要的功能。

(8)单击“下一步”按钮,弹出“选择管理和其他选项”对话框,如图 14-13 所示,选择用于管理服务器的选项。

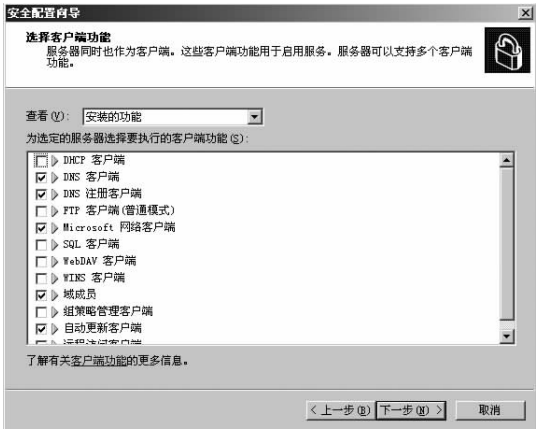

图 14-12 “选择客户端功能”对话框

图 14-13 “选择管理和其他选项”对话框

(9)单击“下一步”按钮,弹出“选择其他服务”对话框,如图 14-14 所示,选择需要的其他服务。

(10)单击“下一步”按钮,弹出“处理未指定的服务”对话框,如图 14-15 所示,选中“不更改此服务的启动模式”单选按钮。

图 14-14　“选择其他服务”对话框

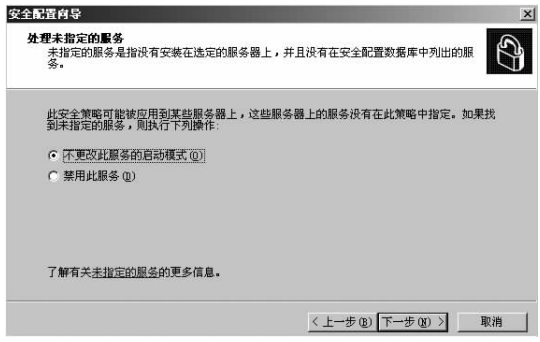

图 14-15　“处理未指定的服务”对话框

(11)单击“下一步”按钮,弹出“确认服务更改”对话框,如图 14-16 所示,如果需要更改设置,则单击“上一步”按钮。

(12)单击“下一步”按钮,弹出“网络安全”对话框,如图 14-17 所示。

图 14-16　“确认服务更改”对话框

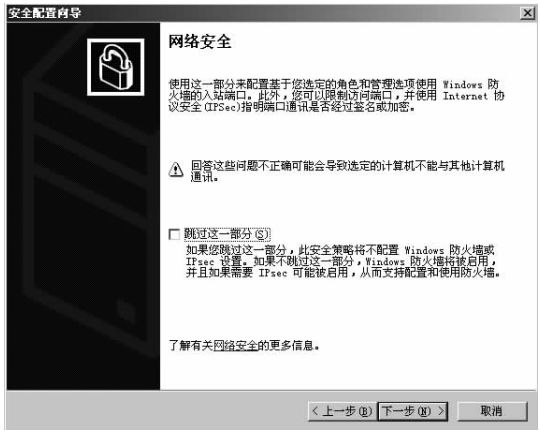

图 14-17　“网络安全”对话框

(13)单击“下一步”按钮,弹出“打开端口并允许应用程序”对话框,如图 14-18 所示,选择要打开的端口。

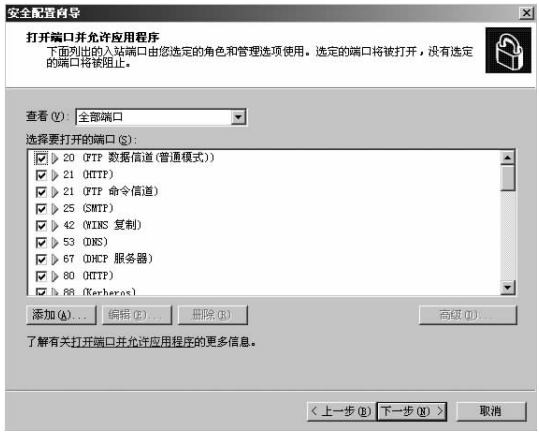

图 14-18　“打开端口并允许应用程序”对话框

(14)单击“下一步”按钮,弹出“确认端口配置”对话框,如图 14-19 所示,如果需要更改,则单击“上一步”按钮。

(15)单击“下一步”按钮,弹出“注册表设置”对话框,如图 14-20 所示。

图 14-19 “确认端口配置”对话框

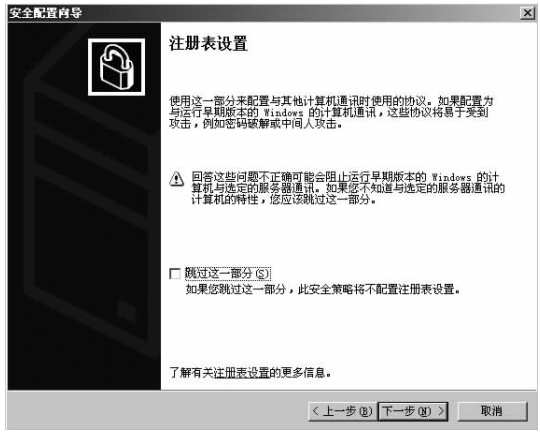

图 14-20 “注册表设置”对话框

(16)单击“下一步”按钮,弹出“要求 SMB 安全签名”对话框,如图 14-21 所示。选中“所有连接到它的计算机满足下列最低操作系统要求”复选框和“它有剩余的处理器能力,可以用来给文件和打印通讯签名”复选框。

(17)单击“下一步”按钮,弹出“要求 LDAP 签名”对话框,如图 14-22 所示,选中“Windows 2000 Service Pack 3 或更新”复选框。

图 14-21 “要求 SMB 安全签名”对话框

图 14-22 “要求 LDAP 签名”对话框

(18)单击“下一步”按钮,弹出“出站身份验证方法”对话框,如图 14-23 所示,选中“域账户”复选框。

(19)单击“下一步”按钮,弹出“出站身份验证使用域账户”对话框,如图 14-24 所示。选中“Windows NT 4.0 Service Pack 6a 或更新的操作系统”复选框和“与选定的服务器的时钟进行了同步的时钟”复选框。

图 14-23　“出站身份验证方法”对话框

图 14-24　“出站身份验证使用域账户”对话框

(20)单击“下一步”按钮,弹出“入站身份验证方法”对话框,如图 14-25 所示。

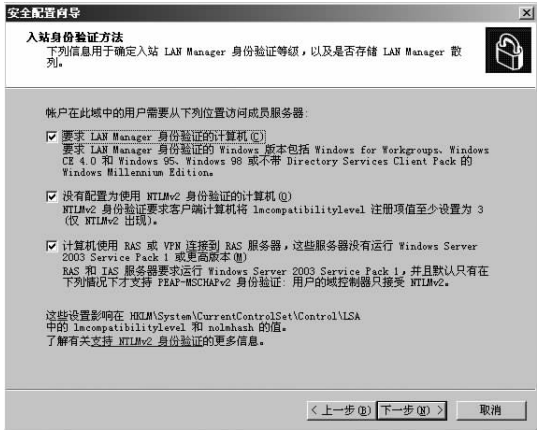

图 14-25　“入站身份验证方法”对话框

(21)单击“下一步”按钮,弹出“注册表设置摘要”对话框,如图 14-26 所示,如果需要更改设置,则单击“上一步”按钮。

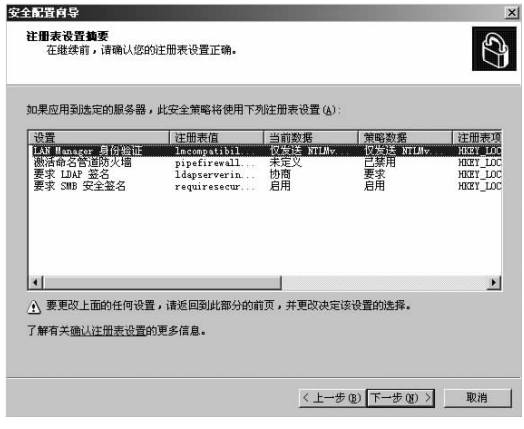

图 14-26　“注册表设置摘要”对话框

(22)单击“下一步”按钮,弹出“审核策略”对话框,如图 14-27 所示。

(23)单击“下一步”按钮,弹出“系统审核策略”对话框,如图 14-28 所示,选中“审核成功的操作”单选按钮。

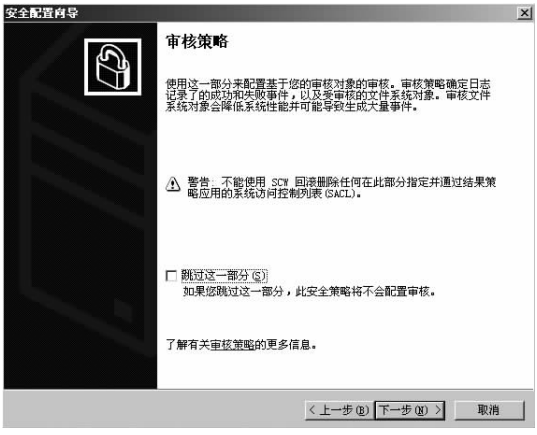

图 14-27 “审核策略”对话框

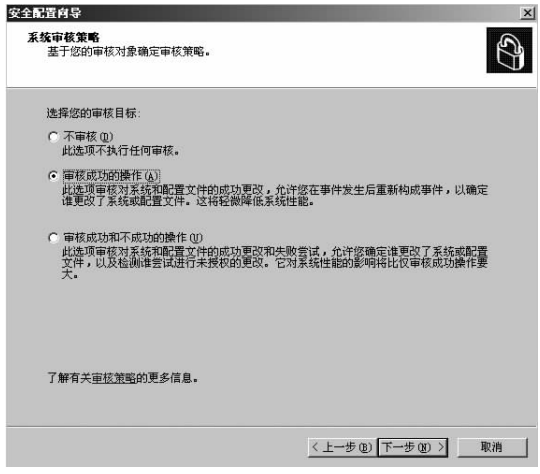

图 14-28 “系统审核策略”对话框

(24)单击“下一步”按钮,弹出“审核策略摘要”对话框,如图 14-29 所示,如果需要更改设置,则单击“上一步”按钮。

(25)单击“下一步”按钮,弹出“Internet 信息服务”对话框,如图 14-30 所示。

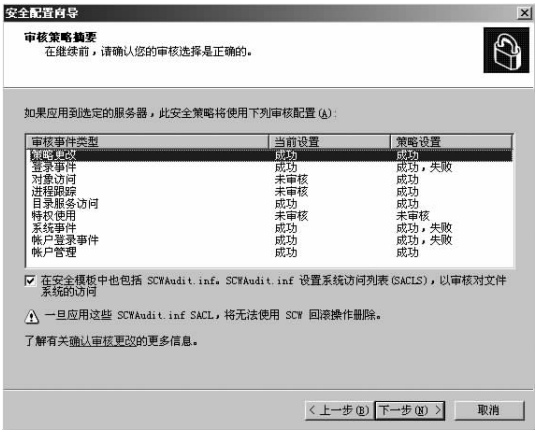

图 14-29 “审核策略摘要”对话框

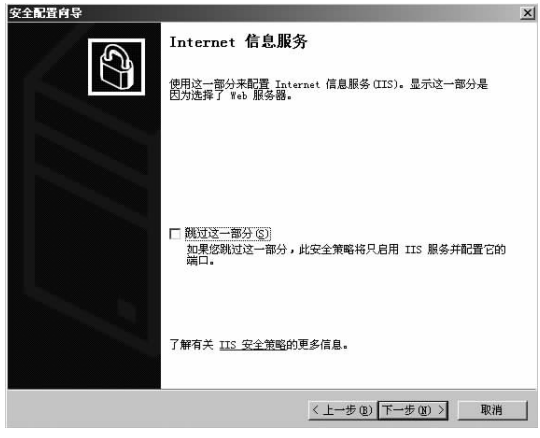

图 14-30 “Internet 信息服务”对话框

(26)单击“下一步”按钮,弹出“选择动态内容的 Web 服务扩展”对话框,如图 14-31 所示,选择服务器要求的 Web 服务扩展。

(27)单击“下一步”按钮,弹出“选择一个要保留的虚拟路径”对话框,如图 14-32 所示,选择要在服务器上保留的虚拟目录。

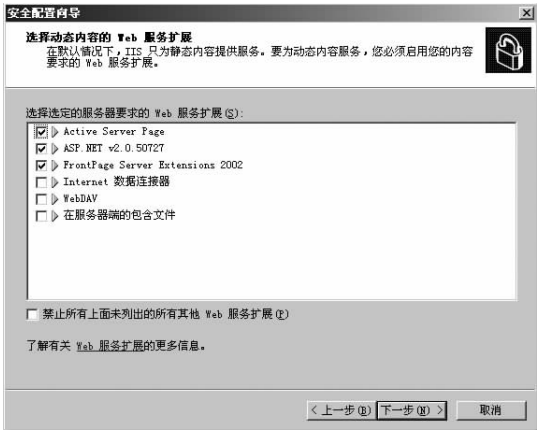

图 14-31　“选择动态内容的 Web 服务扩展”对话框

图 14-32　“选择一个要保留的虚拟路径”对话框

(28)单击“下一步”按钮，弹出“阻止匿名用户访问内容文件”对话框，如图 14-33 所示。

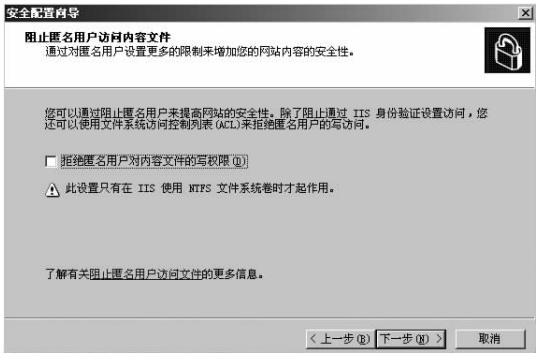

图 14-33　“阻止匿名用户访问内容文件”对话框

(29)单击“下一步”按钮，弹出“IIS 设置摘要”对话框，如图 14-34 所示，如果需要更改设置，则单击“上一步”按钮。

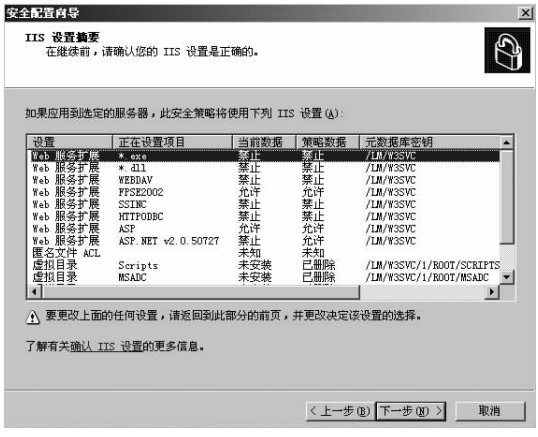

图 14-34　“IIS 设置摘要”对话框

(30)单击“下一步”按钮，弹出“保存安全策略”对话框，如图 14-35 所示。

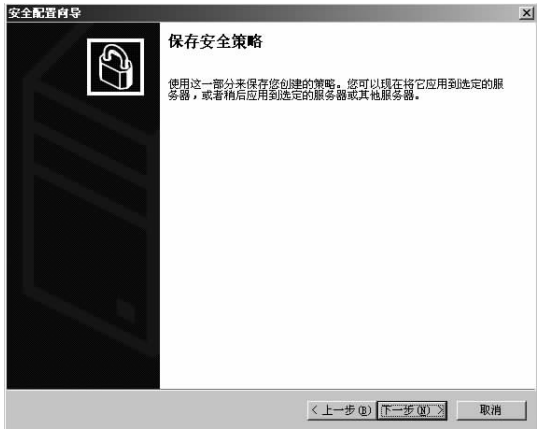

图 14-35 “保存安全策略”对话框

(31)单击“下一步”按钮，弹出“安全策略文件名”对话框，如图 14-36 所示，在“安全策略文件名”文本框中输入保存安全策略的文件名称。

图 14-36 “安全策略文件名”对话框

提示：• 在“安全策略文件名”对话框上单击“查看安全策略”按钮，可以在弹出的如图 14-37 所示的对话框中查看安全策略的内容。

图 14-37 安全策略的内容

· 在“安全策略文件名”对话框上单击“包括安全模板”按钮，弹出“包括安全模板”对话框，如图 14-38 所示，可以添加安全模板。

(32)单击“下一步”按钮，弹出“应用安全策略”对话框，如图 14-39 所示，选中“现在应用”单选按钮。

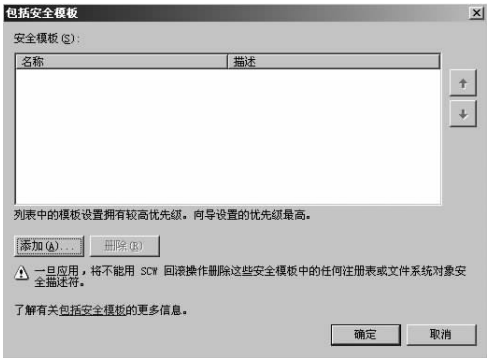

图 14-38　“包括安全模板”对话框

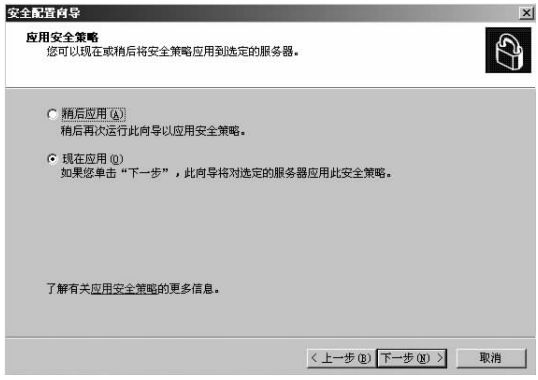

图 14-39　“应用安全策略”对话框

(33)单击“下一步”按钮，弹出“正在应用安全策略”对话框，如图 14-40 所示。

(34)弹出“正在完成安全配置向导”对话框，如图 14-41 所示，单击“完成”按钮，完成安全策略配置。

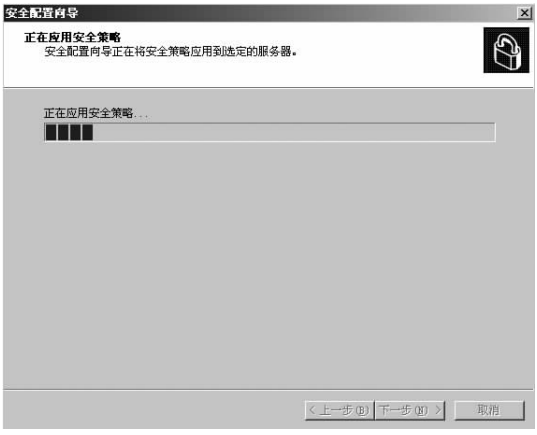

图 14-40　“正在应用安全策略”对话框

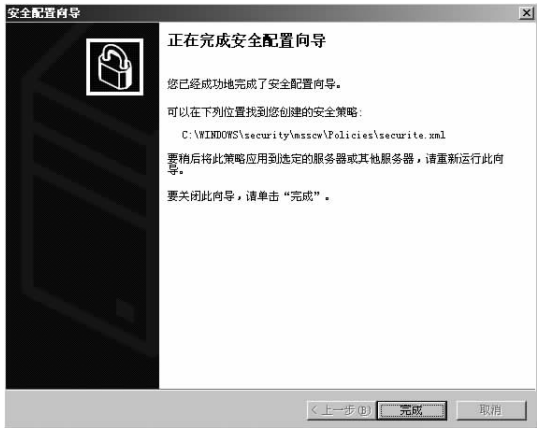

图 14-41　“正在完成安全配置向导”对话框

14.2　系统安全策略

通过在 Windows Server 2003 操作系统中禁用不必要的服务和端口，可以提高服务器的安全性。

14.2.1　设置服务

Windows Server 2003 系统提供的服务以后台程序的方式运行，减少系统运行的服务，可以提高系统运行效率，并避免受到攻击。

执行“开始”→“所有程序”→“管理工具”→“服务”命令，打开“服务”窗口，如图 14-42 所示。在右侧的详细信息列表中列出了服务器中的服务，可以查看服务的名称、内容描述、服务的状态(已启动或未启动)、启动类型(自动、手动和禁用)及该服务所提供的服务类型(本地系统或网络服务)。在启动类型中，自动模式是指系统运行时服务自动启动；手动模式是指只有在需要该服务时才手动启动它；禁用模式是指除非修改为自动模式或手动模式，否则在什么情况下都不能启动该服务。右击一个服务选项，可以通过在弹出的快捷菜单中选择相关命令来修改启动类型及启动或停止服务。

图 14-42 “服务”窗口

为提高服务器的安全性，可以根据需要禁用以下服务：

- Automatic Updates 服务：会自动更新系统，在需要手动安装 Windows 补丁时应将其停止。
- Messenger 服务和 Alerter 服务：会被垃圾信息发送者或黑客使用。
- Remote Register 服务：用于远程操作注册表，有较大的风险。
- Security Center 服务：用于内置防火墙，如果使用第三方防火墙，可以将其停止使用。
- Telnet 服务：在网络传输中使用明码传递 ID 和密码，应将其禁用。
- NetBIOS 服务：提供网络文件或打印共享的协议，可能会被黑客利用来获取磁盘资源。
- Task Scheduler 服务：用于在计算机上配置和制定自动任务的日程，如果不需要系统自动备份，应将其停止。
- Wirelss Zero Configuration 服务：如果不使用无线连接，则应将其停止。

14.2.2 设置端口

禁用服务器上不必要的端口，可以有效提高服务器的安全性。在 Windows Server 2003 系统中可以通过禁用不必要的服务来禁用相关的端口，还可以使用 TCP/IP 筛选功能过滤端口，设置端口的操作步骤如下：

(1)右击“网上邻居”图标，在弹出的快捷菜单中选择“属性”命令，打开“网络连接”窗口。

(2)在“网络连接”窗口中右击“本地连接”图标，在弹出的快捷菜单中选择“属性”命令，

弹出“本地连接属性”对话框，如图 14-43 所示。

(3)在“本地连接属性”对话框的“此连接使用下列项目”列表框中选中“Internet 协议(TCP/IP)”选项，单击“属性”按钮，弹出“Internet 协议(TCP/IP)属性”对话框，如图 14-44 所示。

图 14-43　“本地连接属性”对话框

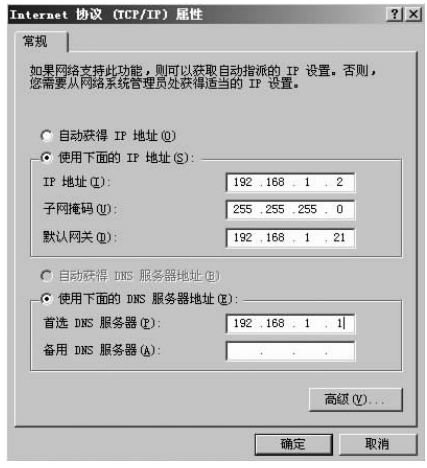

图 14-44　“Internet 协议(TCP/IP)属性”对话框

(4)单击“高级”按钮，弹出“高级 TCP/IP 设置”对话框，选择“选项”选项卡，如图 14-45 所示。

(5)单击“属性”按钮，弹出“TCP/IP 筛选”对话框，如图 14-46 所示。

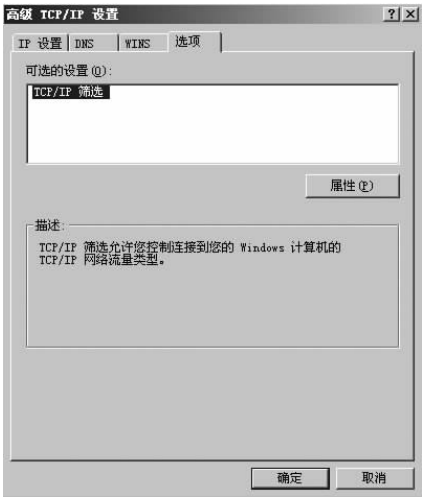

图 14-45　“选项”选项卡

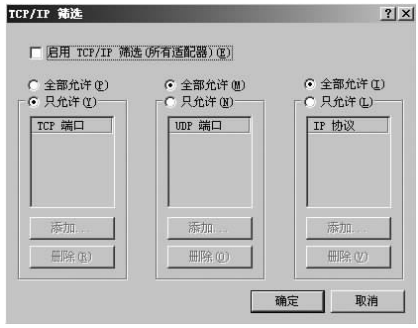

图 14-46　“TCP/IP 筛选”对话框

(6)选中“启用 TCP/IP 筛选(所有适配器)”复选框，然后配置 TCP 端口和 UDP 端口。以设置 TCP 端口为例，选中 TCP 端口对应的“只允许”单选按钮，然后单击其对应的“添加”按钮，弹出“添加筛选器”对话框，如图 14-47 所示。在“TCP 端口”文本框中输入允许开放的 TCP 端口号，单击“确定”按钮，将其添加到“TCP/IP 筛选”对话框的“TCP 端口”列表框中。

图 14-47 “添加筛选器”对话框

下列端口必要时可以禁用:

- 137、138 端口:NetBIOS 中 UDP 用的端口。
- 445、139 端口:SMB 用的端口。
- 443 端口:支持 SSL 的 HTTPS 请求的端口。
- 4899 端口:远程控制服务端的监听端口。
- 135 端口:用于启动与远程计算机连接的端口。

14.3 网络防火墙

防火墙作为网络安全的一种防护手段,在网络系统中得到了广泛的使用,并对网络的安全起到了一定的保护作用。

14.3.1 防火墙简介

防火墙(Firewall)是在两个网络之间执行访问控制策略的一个或一组系统,包括硬件和软件。防火墙遵循一种允许或阻止业务往来的网络通信安全机制,提供可控的过滤网络通信,只允许授权的通信,目的是保护网络不被他人侵扰。通常,防火墙就是位于内部网络或 Web 站点与因特网之间的一个路由器或一台计算机,又称堡垒主机,它是对所有网络通信流进行过滤的节点。

防火墙通过审查经过堡垒主机的每一个数据包,判断它是否匹配事先设置的过滤规则。如果满足,根据控制机制做出相应的动作;如果不满足,则将数据包丢弃,从而保护网络的安全。

通过使用防火墙,可以实现以下功能:

(1)隐藏内部网络。防火墙为用户的网络创建了一个可保护的边界,并且隐藏了内部网络的一些信息以增加保密性能。因此,当入侵者从外部测试本地网络时,入侵者只能看到防火墙,内部网络的拓扑、布局等信息都将被屏蔽。防火墙通过提高认证功能和对网络加密来限制网络信息在外部传输过程中的暴露,同时可以限制从外部发动的攻击。

(2)控制外部网络用户对内部网络的访问。该功能也分为两个方面,一方面是只允许外部用户访问本地网络中的某些主机;另一方面只允许外部用户中指定的用户访问本地网络。前者通过控制本地 IP 来实现,后者通过控制外部 IP 来实现。

(3)控制内部网络对外部网络的访问。该功能分为两个方面:一方面可以控制内部网络用户对外部一些非法或者受限网络的访问;另一方面控制内部网络用户是否可以连接到外部网络。前者通过对外部 IP 或者网址的控制来实现,后者通过对内部用户的 IP 控制来实现。

(4)监视网络安全,提供安全日志并预警。这是防火墙最主要的作用之一,根据防火墙

提供的日志，可以判断是否有异常的连接请求，对于可疑的问题，如多次连续的失败记录等，应注意是否是入侵者的试探性攻击。

(5)缓解 IP 地址空间短缺问题。内部网络在连接到 Internet 时，可能会获得比较少的几个外部网络 IP 地址，可以通过防火墙的 NAT 功能，将有限的 IP 地址动态或静态地与内部的 IP 地址对应起来，这种办法可以缓解地址空间短缺的问题。

(6)引出 DMZ(Demilitarized Zone，非军事区)区域，可设置各种服务器。从防火墙可以连接到一个单独的网段上，即非军事化区域，并在此部署 WWW 服务器和 FTP 服务器，将其作为向外部发布内部信息的地点。

(7)对内部用户的 Internet 使用进行审计和记录。防火墙是审计和记录 Internet 使用情况的一个最佳地点。管理员可以通过防火墙对 Internet 的使用情况进行了解，查出潜在的带宽瓶颈位置，并及时对 Internet 的使用情况进行调整。

除了上面的基本功能外，现在很多防火墙还具备一些流量控制和抵御 DoS 攻击的特殊功能。

14.3.2　防火墙的类型

根据实现的设备可以将防火墙分为硬件防火墙和软件防火墙；根据防范的方法和侧重点的不同，可以将防火墙分为多种类型，但总体上可以分为包过滤防火墙、代理服务型防火墙和主动监测防火墙等。

1. 包过滤防火墙

数据包过滤(Packet Filtering)技术是在网络层对数据包进行选择，选择的依据是系统内设置的过滤逻辑，也称为访问控制表(Access Control List，ACL)。访问控制表通过检查数据流中每个数据包的源地址、目的地址、所用的端口号和协议状态等因素或它们的组合来确定是否允许该数据包通过。

2. 代理服务型防火墙

应用代理服务型防火墙(Proxy Service)也称链路级网关或 TCP 通道。它是针对数据包过滤和应用网关技术存在的缺点而引入的防火墙技术，其特点是将所有跨越防火墙的网络通信链路分为两段。当代理服务器接收到用户对某个站点的访问请求后就会检查该请求是否符合控制规则，如果规则允许用户访问该站点，代理服务器就会代替用户去访问，并取回所需信息，然后再转发给用户。内外用户的访问都是通过代理服务器上的“链接”来实现的，从而起到了隔离防火墙内外计算机系统的作用。

3. 主动监测防火墙

为了在开放网络服务的同时也提供安全保证，必须能够监测网络情况，当出现网络攻击时能立即报警或切断相关的连接。主动监测技术就是基于这种思路发展起来的，它有一个用于维护记录各种攻击模式的数据库，并在网络中时刻运行一个监测程序进行监控，一旦发现网络中存在与数据库中的某个模式匹配的活动时，就能推断可能出现网络攻击。主动监测技术也存在另外一个安全隐患，即 DoS 攻击，如果入侵者利用伪造的合法 IP 地址进行网络攻击，网络将自动切断连接，从而使合法的用户无法正常使用网络服务，也就形成了拒绝服务攻击。

14.3.3 防火墙产品介绍

1.硬件防火墙

1)Quidway Eudemon(守护神)300 防火墙

华为技术有限公司成立于 1988 年,是由员工持股的高科技民营企业。华为从事通信网络技术与产品的研究、开发、生产与销售,专门为电信运营商提供光网络、固定网、移动网和增值业务领域的网络解决方案,是中国电信市场的主要供应商之一,并已成功进入全球电信市场。

Quidway Eudemon 300 是华为公司推出的基于网络处理器 NP 技术的硬件高速状态防火墙,采用先进的动态检测技术(ASPF),具备电信级高性能和高可靠性,为用户网络提供全面的安全保护,同时还具备强大的虚拟专用网(VPN)功能、地址转换(NAT)功能以及 P2P 业务控制与带宽管理功能,普遍适用于大、中型企业及其分支机构。

Quidway Eudemon 300 产品的特点是:拥有强大的防范 DoS/DDoS 攻击能力,提供丰富的安全业务和灵活组网能力,拥有高性能的 VPN 网关,具备强大的 NAT 业务能力,可实现灵活的 P2P 等流量识别和带宽管理。

2)Cisco PIX515ERBUN 防火墙

思科公司是世界领先的 Intranet 和 Internet 网络互联厂商,其设备和软件产品主要用于连接计算机网络系统,其网络互联解决方案已为众多用户提供了更为快捷有效的信息交换途径,降低了用户开销,提高了工作效率,并进一步拉近了用户与其客户、商业伙伴和公司职员之间的距离。

思科公司的防火墙产品 Cisco PIX515ERBUN 是一个百兆企业级防火墙,内置的 CPU 为 Intel Celeron,频率为 433MHz,内存容量为 32MB,闪存容量为 16MB,并发连接数为 13 000,网络吞吐量达到 190Mb/s。该防火墙能够提供空前的安全保护能力,其保护机制的核心是能够提供面向静态连接防火墙功能的自适应安全算法(ASA)。

PIX515 系列防火墙具有无限软件捆绑的特点,它可以同时处理 50 000 余个连接,吞吐量高达 170Mb/s。支持多达 3 个以太网接口的 PIX515ERBUN 是一种具有特别高性价比的解决方案,适合那些选择在防火墙之外托管自己的网站或者通过 Internet 服务提供商(ISP)托管网站,并且需要较合理性价比防火墙解决方案的小型公司以及那些仅需要与自己企业网进行双向通信的远程站点,或由企业网在自己的企业防火墙上提供所有的 Web 服务的情况。

2.软件防火墙

1)Microsoft ISA Server 软件防火墙

Microsoft ISA Server 企业级防火墙是由全球最大的软件公司微软公司发布的软件防火墙。作为 Microsoft Windows Server System 成员之一的 ISA Server 2004 企业级防火墙是一个安全、易于使用且经济高效的解决方案,可帮助 IT 专业人员抵御不断涌现的新安全威胁。Microsoft ISA Server 2004 是一个应用层防火墙、VPN 和 Web 高速缓冲产品,旨在改善用户的网络安全,实现了对应用层攻击的防护。当数据过来后,ISA Server 2004 企业级防火墙会将应用层内容打开,同时对包头部分以及应用层内容进行检测,如果发现与已知攻击代码相符,立刻将该数据流作为不合法数据流进行阻止,严禁攻击数据流发送到服务器,从而能够比较有效地防护这种伪装起来的攻击,使得 ISA Server 2004 实现高级防护,最

大限度地保护应用程序。

Microsoft ISA Server 软件防火墙也有不足之处，由于它是在应用层对网络包进行检查，安装该防火墙之后，会对网络传输速度有所影响，造成网络资源的消耗和信息流通的阻碍。Microsfot ISA Server 企业级防火墙目前只支持 Windows 操作系统，采用 Server/Client 模式。

2）CheckPoint 软件防火墙

美国 CheckPoint 公司开发的软件防火墙 CheckPoint Firewall1 是一个综合的、模块化的安全产品，基于策略的解决方案能够让管理员指定网络访问按部署的时间段进行控制，它能够将处理任务分散到一组工作站上，从而减轻相应防火墙服务器、工作站的负担。

CheckPoint Firewall1 防火墙的操作在操作系统的核心层，而不是在应用程序上进行，这能让防火墙系统达到最高的性能、最佳的扩展与升级，它支持基于 Web 的多媒体和 UDP 应用程序，采用多重验证模板和方法，使网络管理员可以简单地验证客户端、会话和用户对网络的访问。CheckPoint 架构不依赖硬件，因此，在理论上，防火墙的功能是可以无限扩充的，它能给客户更多的控制和定制功能。同时，它是一个跨平台防火墙系统，目前支持 Windows 98/NT/2000/XP/2003、Sun OS、SunSolaris、IBM AIX、HPUN、FreeBSD 以及各类 Linux 系统。就目前来讲，CheckPoint Firewall1 是全球认可的软件防火墙产品，但是，价格偏高是该产品的一个不足之处。

14.4　入侵检测

入侵（Intrusion）不仅包括发起攻击的人取得超出范围的系统控制权，还包括收集漏洞信息，造成拒绝访问等对计算机造成危害的行为。

入侵检测（Intrusion Detection）即对入侵行为的发觉。它收集计算机网络或计算机系统中的若干关键点的信息并对其进行分析，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。

入侵检测系统（Intrusion Detection System，IDS）是指任何有能力检测系统或网络状态改变的系统或系统的集合，它能发送警报或采取预先设置好的行动来帮助保护网络。IDS 可以是一台简单的主机，例如，Unix/Linux 系统中的 TCPdump 程序可以用来获取网络状态；也可以是一个复杂的系统，使用多台主机来帮助捕获、处理并分析网络流量，例如，Linux 系统中的网络入侵检测系统 Snort IDS 等。

14.4.1　入侵检测方法

根据对收集到的信息进行识别和分析所采用的原理不同，可以将入侵检测分为异常入侵检测和误用入侵检测。

1. 异常入侵检测技术

异常入侵检测（Anomaly Detection）技术是指运行在系统层或应用层的监控程序，通过将当前主体的活动情况和用户轮廓进行比较来监控用户的行为。所谓用户轮廓，通常是各种行为参数及其阈值的集合，一般用于描述正常行为的范围。当当前主体的活动与正常行为有重大偏离时即被认为是入侵行为。

如果系统错误地将异常活动定义为入侵则称为错报(False Positive),如果系统未能检测出真正的入侵行为则称为漏报(False Negative)。对异常检测的理论研究包括统计异常检测、基于特征选择异常检测、基于贝叶斯网络异常检测、基于神经网络异常检测、基于机器学习异常检测、基于人工免疫异常检测等。

异常检测只能识别出那些与正常过程有较大偏差的行为,而无法知道具体的入侵情况。由于对各种网络环境的适应性不强,且缺乏精确的判定准则,异常检测经常会出现错报和漏报情况。

2.误用入侵检测技术

误用入侵检测(Misuse Detection)的前提是必须先提取已知入侵行为的特征,建立入侵特征库,然后将当前用户或系统行为与入侵特征库中的记录进行匹配,如果相匹配就认为当前用户或系统行为是入侵,否则入侵检测系统认为是正常行为。很显然,如果正常行为与入侵特征相匹配,则入侵检测系统发生错报,而如果没有入侵特征与某种新的攻击行为相匹配,则 IDS 系统发生漏报。

从误用入侵检测技术的检测方式可以看出,其缺点是漏报率会增加,因为当新的入侵行为出现或入侵特征发生细微变化时,误用检测技术将无法检测出入侵行为。

14.4.2 入侵预防措施

1.入侵预防问题

随着网络安全技术的发展以及用户需求的升级,产生了入侵防御系统(Intrusion Prevention System,IPS)。IPS 是一种主动的、积极的入侵防范与阻止系统,它部署在网络的进出口处,当它检测到攻击企图后,会自动地将攻击包丢掉或采取措施将攻击源阻断。举一个简单的例子,IDS 就如同火灾预警装置,火灾发生时,它会自动报警,但无法阻止火灾的蔓延,必须由人来进行灭火。而 IPS 就像智能灭火装置,当它发现有火灾发生后,会主动采取措施灭火,中间不需要人的干预。

可以将 IPS 简单地理解为防火墙加上入侵检测系统,但并不是说 IPS 可以代替防火墙或入侵检测系统。防火墙是粒度比较粗的访问控制产品,它在基于 TCP/IP 协议的过滤方面表现出色,而且在大多数情况下可以提供网络地址转换、服务代理、流量统计等功能,甚至有的防火墙还能提供 VPN 功能。

IPS 和防火墙比较起来,其功能比较单一,它只能串联在网络上(类似于通常所说的网桥式防火墙),对防火墙所不能过滤的攻击进行过滤。这样一个两级的过滤模式,可以最大限度地保证系统的安全。一般来说,企业用户关注的是自己的网络能否避免被攻击,对于能检测到多少攻击并不是很热衷。但这并不是说入侵检测系统就没有用处,在一些专业机构或对网络安全要求比较高的地方,入侵检测系统和其他审计跟踪产品结合,可以提供针对企业信息资源的全面的审计资料,这些资料对攻击还原、入侵取证、异常事件识别、网络故障排除等方面都有很重要的作用。

2.IPS 的工作原理

真正的入侵防御系统与传统的入侵检测系统的关键区别在于自动阻截和在线运行,两者缺一不可。防御工具(软/硬件方案)必须设置相关策略,以对攻击自动做出响应,而不仅仅是在恶意通信进入时向网络主管发出警告。要实现自动响应,系统就必须在线运行。

当黑客试图与目标服务器建立会话时，所有数据都会经过 IPS 传感器，传感器位于活动数据路径中。传感器检测数据流中的恶意代码，核对策略，在未转发到服务器之前将信息包或数据流阻截。由于是在线操作，因而能保证处理方法适当而且可预知。

14.5　病毒防范

计算机病毒是人为制造的程序，它的运行是非法入侵。

随着操作系统的发展和 Internet 的流行，病毒技术的发展经历了由 DOS 向 Windows 及 Internet 网络发展的过程。

DOS 是一个安全性较差的操作系统，所以在 DOS 时代，计算机病毒的种类繁多。目前 DOS 病毒已经大大减少，一方面是因为基于 DOS 平台的软件越来越少，另一方面是因为 DOS 模式下的病毒基本上可以被杀毒软件检测出来。

伴随着 Windows 操作系统的出现，产生了大量基于 Windows 平台的计算机病毒。Internet 的出现和流行，使得病毒的传播途径更为多元化，而网络已成为最重要的病毒传播途径。

14.5.1　常见的计算机病毒

1. 木马病毒

木马病毒的名称来源于古希腊的特洛伊木马神话，它是把自己伪装在正常程序内部的病毒，这种病毒的伪装性强，通常使用户很难判断它到底是合法程序还是木马。木马病毒带有黑客性质，它有强大的控制和破坏能力，可窃取密码、控制系统、操作文件等。

木马病毒由客户端和服务器端两个执行程序组成，客户端程序是攻击者向远程计算机植入木马的执行程序，以达到远程控制此计算机的目的；服务器程序是被植入的木马程序。木马病毒的设计者为了防止木马病毒被发现，采用多种手段隐藏木马。木马病毒入侵目标计算机后，会把目标计算机的 IP 地址、木马端口等信息发送给入侵者，从而使入侵者利用这些信息来控制目标计算机。木马病毒的类型包括 EXE 文件执行类木马、进程插入式木马和 Rootkit 类木马。

2. 宏病毒

宏是一系列由用户编写或录制的命令和指令，用来实现任务执行的自动化。

宏病毒是使用 Word 的 VBA 编程接口编写的具有病毒特征的宏集合。它以二进制文件加密压缩格式存入 .doc 或 .dot 文件中，通过小文档或模板进行大量自我复制及传播，危害性大。一旦运行宏病毒，相应的 Normal 模板会被传染，所有打开的 Word 文档都会在自动保存时被传染。多数宏病毒包含 AutoExec、AutoOpen 和 AutoNew 等自动宏，通过这些自动宏，病毒取得文档(模板)操作权。宏病毒的种类很多，版本也各不相同，所以查杀各类宏病毒的关键是恢复文件参数。

3. 脚本病毒

脚本病毒通常是用 JavaScript 或者 VBScript 代码编写的恶意代码病毒。JavaScript 脚本病毒通过网页进行传播，一旦用户运行了带有病毒的网页，病毒就会修改 IE 首页及注册表等信息，给用户使用计算机带来不便。

VBS 脚本病毒是使用 VBScript 编写的,以宏病毒和新欢乐时光病毒为典型代表。VBS 脚本病毒编写简单,破坏力大,感染力强。这类病毒通过 .htm 文档、E-mail 附件或其他方式传播,因此,其传播范围很大。

4. PE 病毒

PE(Portable Executable)病毒是指所有感染 Windows 操作系统中 PE 文件的病毒。PE 病毒大多数采用 Win 32 汇编语言编写。该病毒感染普通 PE 文件(如 EXE 文件)并把自己的代码加到 EXE 文件尾部,修改原程序的入口点以指向病毒体,PE 病毒没有 .data 段,变量和数据全部放在 .code 段,病毒本身没有什么危害,但被感染的文件可能被破坏。

5. 蠕虫病毒

蠕虫病毒是一种能自我复制的程序,并能通过计算机网络进行传播,它消耗大量系统资源,使其他程序运行减慢甚至停止,最后导致系统和网络瘫痪。蠕虫病毒的传染目标是互联网内的所有计算机,其传播方式分为两类:一类是利用系统漏洞主动进行攻击,另一类是通过网络服务传播。

6. 恶意网页病毒

网页病毒主要是利用软件或系统操作平台等的安全漏洞,通过执行嵌入在网页 HTML(超文本标记语言)内的 Java Applet 小应用程序、JavaScript 脚本语言程序或 ActiveX 控件,强行修改用户操作系统的注册表设置及系统实用配置程序,或非法控制系统资源,盗取用户文件,或恶意删除硬盘文件、格式化硬盘。这种网页病毒容易编写,使用户防不胜防,最好的防范措施是选用有网页监控功能的杀毒软件。

14.5.2 计算机病毒的共同特征

计算机病毒的共同特征是隐蔽性、传染性、触发性、破坏性和潜伏性。

1. 隐蔽性

大多数计算机病毒是代码设计得非常短小的程序。它通常把自己隐蔽在系统的正常程序中,以防止用户发现。隐蔽性是病毒的反侦察特性。

2. 传染性

传染性是病毒的最基本特征。计算机病毒有很强的再生机制,病毒程序一旦加到运行的程序体上,就能感染其他程序,并且迅速扩散到整个计算机系统,当在网络中进行数据交换时,也将使病毒在网上传播。是否具有传染性是判别一个程序是否为计算机病毒的最重要的条件。

3. 触发性

触发性又叫激发性,它指的是病毒在某种激活的情况下产生的破坏。大多数病毒都在进入系统后有一段时间的潜伏期,当达到病毒的触发条件时,病毒就被激活了。使计算机病毒触发的条件主要有 3 个:利用系统时钟提供的时间作为触发器、利用病毒体自带的计数器作为触发器、利用计算机内执行的某些特定操作作为触发器。

4. 破坏性

病毒指的是带有破坏性质的恶意程序,所以病毒对系统的破坏程度成为其重要的衡量方式。根据计算机病毒破坏能力的不同,将其分为良性病毒和恶性病毒。恶性病毒指的是一旦病毒感染系统就立即爆发,造成系统的破坏。良性病毒是指不包含立即直接破坏的代码,它的特征不很明显,但是当系统大量感染的时候,会大量占用系统资源,导致系统中断和

网络瘫痪。

5.潜伏性

计算机病毒入侵系统后，一般不立即发作，而是具有一定的潜伏期。一般在潜伏期中，病毒进行大量的复制，直到用户触发时，才显现出其强大的破坏性。

14.5.3　计算机病毒的新特点

计算机病毒在不断地发展，它具有如下新特点：

(1)具有较强的诱惑性和欺骗性。有些病毒结合大量的钓鱼工具实现病毒和黑客的结合，病毒出现频率高，变种快，不容易被发现和清除。

(2)传播途径多，扩散速度快。很多病毒通过系统漏洞、局域网、网页、邮件等方式进行传播，扩散速度极快。

(3)病毒与其他技术相融合。某些病毒集普通病毒、蠕虫、木马和黑客等技术于一身，具有混合型特征，破坏性极强。

(4)多态性病毒越来越多，宏病毒泛滥。病毒可以进入各种系统平台，病毒机理错综复杂。

(5)大量消耗系统和网络资源。计算机感染病毒后，可能导致系统崩溃，数据丢失。部分病毒具有反侦察能力，可以把用户系统上所有的 Ghost 备份文件删除，将杀毒软件和防火墙破坏。另外，可能阻止用户登录任何一个相关的安全处理站点。

(6)产生移动系统中的病毒，可以感染手机等移动设备。

14.5.4　反病毒技术

1.病毒的预防措施

病毒的防范比病毒的查杀更加重要，建立一套强大的防范机制可以大大提高系统的安全性。计算机病毒的预防分为管理方法上的预防和技术上的预防两种，在一定程度上，这两种方法是相辅相成的。常用的预防措施如下：

(1)定义浏览器安全设置，在浏览网页时要谨慎，不要轻易下载 ActiveX 控件或 Java 脚本。

(2)使用比较复杂的密码。尽量选择难于猜测的密码，对不同的账号选用不同的密码。

(3)不要打开来历不明的电子邮件。

(4)经常备份重要数据。

(5)正确配置系统，减少病毒入侵。充分利用系统提供的安全机制，提高系统防范病毒的能力。

(6)慎用软盘、光盘等移动存储介质。

(7)定期检查敏感文件。对系统的敏感文件进行定期检查，保证及时发现已感染的病毒和黑客程序。

(8)选择安装优秀的防病毒软件和防火墙，定期对整个硬盘进行病毒检测、清除工作。

(9)安装最新的操作系统、应用软件的安全补丁程序。

(10)当计算机不使用时，不要接入互联网，一定要断掉连接。

(11)重要的计算机系统和网络一定要严格与互联网物理隔离，这种隔离包括离线隔离。

2. 常用的防病毒设置

1)设置文件和文件夹的查看方式

所有的 Windows 操作系统在默认情况下会隐藏已知文件类型的扩展名,这个特性可以被恶意程序编写者或黑客利用,将病毒程序用别的文件类型伪装起来。显示文件扩展名的方法为:在"文件夹选项"对话框中,选择"查看"选项卡,在"高级设置"列表框中取消选中"隐藏已知文件类型的扩展名"复选框,即可显示文件的扩展名。

在设置文件夹的查看方式时,推荐用户使用 Windows 传统风格的文件夹。因为如果在文件夹中显示常见任务选项,其中会包含一些脚本代码。设置文件夹的查看方式为 Windows 传统风格的方法为:在"文件夹选项"对话框中,选择"常规"选项卡,在"任务"选项区中选中"使用 Windows 传统风格的文件夹"单选按钮。

2)设置 IE 的安全级别

目前,很多病毒是随着用户浏览站点而下载的,所以进行 IE 的安全级别设置对维护系统安全非常重要。在默认情况下,IE 的安全级别设置为"中",但是某些病毒和恶意程序可以将这个级别改为"低",从而导致病毒的侵入。建议用户至少将安全级别设为"中",以降低被病毒感染的几率。在中度安全级别下,要运行一些包含不安全因素的程序时,IE 会发出警告。

设置 IE 安全级别的方法为:右击 IE 浏览器图标,在弹出的快捷菜单中选择"属性"命令,弹出"Internet 属性"对话框,选择"安全"选项卡,然后单击"默认级别"按钮,拖动滑块设置 IE 的安全级别。

3)禁止 Windows 的 Scripting Host 功能

为了有效防止脚本病毒在主机上运行,可以将 Windows 脚本文件类型删除,这样可以阻止 Visual Basic 的脚本病毒的运行。

双击"我的电脑"图标,在打开的窗口中执行"工具"→"文件夹选项"命令,弹出"文件夹选项"对话框,选择"文件类型"选项卡,选择 WSH 文件类型后单击"删除"按钮将其删除。

4)更新系统安全补丁

操作系统的安全漏洞成为病毒的一大攻击口,所以经常对系统进行自动更新可以及时安装补丁程序,更新安全补丁可以阻止黑客或某些恶意程序利用已知的安全漏洞对系统进行攻击。更新系统补丁的法为:在桌面上右击"我的电脑"图标,在弹出的快捷菜单中选择"属性"命令,弹出"系统属性"对话框,选择"自动更新"选项卡,在该选项卡中,用户可以决定系统的更新方式。当然,用户也可以从操作系统提供的更新站点下载并更新系统安全补丁。

5)Outlook 安全设置

电子邮件是病毒的一个重要传播源,所以如何设置邮件客户端软件的安全属性是关键。微软公司提供的电子邮件客户端软件有 Microsoft Outlook 和 Outlook Express,它们的功能基本相同,下面以 Outlook Express 的安全设置为例来介绍基本的电子邮件客户端软件的安全属性设置方法。

打开 Outlook Express 软件,选择"工具"→"选项"命令,弹出"选项"对话框,选择"安全"选项卡,选择要使用的 Internet Explorer 的安全区域为"受限站点区域",并选中"当别的应用程序试图用我的名义发送电子邮件时警告我"和"不允许保存或打开可能有病毒的附件"复选框。

关闭 Outlook Express 的预览窗口,因为预览窗口会自动打开邮件的附件,这将威胁到

用户的计算机安全，所以关闭预览功能可以进行 Outlook Explorer 的安全维护。打开 Outlook Explorer 软件，执行“查看”→“布局”命令，弹出“窗口布局属性”对话框，取消选中“显示预览窗格”复选框。

6）宏病毒保护设置

宏病毒是目前系统中常见的病毒，由于 Office 办公系列软件的大量使用，导致宏病毒成为当前的主要病毒。目前，在微软公司的 Office 系列软件中可以对宏进行安全设置，在 Word、Excel、PowerPoint 中的设置方式相同。打开某个 Office 软件，执行“工具”→“宏”→“安全性”命令，弹出“安全性”对话框，在“安全级”选项卡中设置宏的安全级别为“非常高”，这样系统就可以禁止运行来历不明的宏，从而有效阻止宏病毒。

7）设置安全密码

在操作系统和应用软件中，设置强壮的安全密码是非常必要的，一个强壮的安全密码，其长度至少应该为 8 位，且最好是大小写字母、数字、符号的组合。设置的密码不应该具有规律性，比如常见的单词，这些将很容易被破解。

3. 常见的病毒检测方法

目前，计算机病毒技术与计算机反病毒技术的矛盾越来越尖锐。病毒的危害使用户防不胜防，稍有不慎，病毒就会给用户造成严重后果。对计算机病毒的防范首先应该杜绝它的传染途径，对存储介质和网络都进行实时监控；其次要安装优秀的杀毒软件和防火墙，经常对系统进行病毒扫描和清除；同时还要建立系统备份和还原机制，以备不测。常见的反病毒技术有以下几种方式：

1）行为监测法

行为监测法是指利用病毒的特有行为特征来监测病毒的方法。通过利用操作系统底层接口技术，对系统中的所有文件或指定类型的文件进行实时的行为监控，一旦有病毒传染或病毒发作就及时报警，从而实现了对病毒的实时、永久、自动监控。

行为监测法可发现未知病毒，可非常准确地预报未知的多数病毒。但是这种方法可能误报警，且不能识别病毒名称。

2）特征代码法

特征代码法是通过扫描分析出病毒的特征病毒码并集中存放于病毒代码库文件中，将扫描对象与特征代码库比较，如有吻合则判断为感染了病毒。该技术实现起来简单有效、安全彻底，但查杀病毒滞后，并且庞大的特征代码库会造成查毒速度下降。它首先采集已知病毒样本，抽取特征代码，并将其归入病毒数据库。系统通过检查文件中是否含有病毒数据库中的病毒特征代码来判定文件是否感染病毒。

特征代码法准确快速，可识别病毒的名称，误报警率低，依据检测结果可做解毒处理。它的缺点是不能检测未知病毒，不能搜集已知病毒的特征代码，费用高，在网络上效率低、速度慢，并且不能检查多形性病毒，不能对付隐蔽性病毒。特征代码法在技术上需要不断更新程序版本，升级病毒特征代码。

3）校验和法

校验和法扫描病毒的原理是计算磁盘中的实际文件或系统扇区的 CRC 值（校验和），这些 CRC 值被杀毒软件保存到它自己的数据库中，在运行杀毒软件时，用备份的 CRC 值与当前计算的值比较，可以知道文件是否已经被修改或被病毒感染。

使用校验和法常常误报警，原因是病毒感染并非文件内容改变的唯一途径，还有可能是

正常程序引起的。文件校验和法不是最好的方法,它会影响文件的运行速度。不能识别病毒名称,不能对付隐蔽型病毒。校验和法对文件内容的变化太敏感,不能区分是否是由正常程序引起的变动。

4)虚拟执行法

对于多态性病毒,每次感染都改变其病毒密码,采用以上几种方式很难将病毒处理,所以提出虚拟执行技术。该技术通过虚拟执行方法查杀病毒,可以对付加密、变形、异型及病毒生产机生产的病毒。

采用虚拟执行技术查杀病毒时,在计算机虚拟内存中模拟出一个"指令执行虚拟机",在虚拟机环境中虚拟执行(不会被实际执行)可疑带毒文件。在执行过程中,从虚拟机环境内截获文件数据,如果含有可疑病毒代码,则杀毒后将其还原到原文件中,从而实现对病毒的查杀。

4.查杀病毒新技术

1)病毒免疫技术

病毒免疫是指加强自主访问控制和设置磁盘禁写保护区来实现病毒免疫的技术。由于用户应用软件的多样性和环境的复杂性,病毒免疫技术离广泛使用还有一段距离。

2)宏指纹技术

此项技术是基于 Office 复合文档 BIFF 格式精确查杀各类宏病毒的技术,它可以查杀所有在 Office 文档中存在的可知和未知的宏病毒,并且可以修复部分被破坏的 Office 文档。

3)未知病毒查杀技术

未知病毒查杀技术是继虚拟执行技术后的又一大技术突破,它结合了虚拟技术和人工智能技术,实现了对未知病毒的准确查杀。

4)嵌入式杀毒技术

嵌入式杀毒技术是对病毒经常攻击的应用程序或对象提供重点保护的技术,它利用操作系统或应用程序提供的内部接口来实现。它对使用频率高、使用范围广的应用软件提供被动式的防护。如对 MS Office、Outlook、IE、WinRAR、迅雷等应用软件进行的杀毒。

5.病毒处理的步骤

计算机病毒的处理包括防毒、查毒、杀毒 3 个方面。对于计算机病毒的实际防治能力和效果,也要从防毒能力、查毒能力和解毒能力 3 个方面来评判。

1)防毒

防毒是指根据系统特性,采取相应的系统安全措施预防病毒侵入计算机。防毒能力是指预防病毒侵入计算机系统的能力。通过采取防毒措施,应可以实时地监测经由光盘、软盘、硬盘不同目录之间,局域网、因特网(包括 FTP 方式、E-mail 方式、HTTP 方式或其他形式的文件下载等多种方式)之间进行的传输;能够在病毒入侵系统时发出警报,记录携带病毒的文件,即时清除其中的病毒;对网络而言,能够向网络管理员发送关于病毒入侵的信息,记录病毒入侵的工作站,必要时还要能够注销工作站,隔离病毒源。

2)查毒

查毒是指对于确定的环境,能够准确地报出病毒名称,该环境包括内存、文件、引导区(含主导区)、网络等。查毒能力是指发现和追踪病毒来源的能力。通过查毒应该能准确地

发现计算机系统是否感染病毒，并准确查找出病毒的来源，给出统计报告。查毒能力由查毒率和误报率来评判。

3）杀毒

将染毒文件的病毒代码摘除，使之恢复为可正常运行的文件，称为病毒的清除。清除病毒所采用的技术称为杀毒技术。

注意：依据病毒的种类及其破坏程度的不同，在计算机感染病毒后，有的可以清除，有的不能清除。

6. 病毒处理存在的问题

1）漏报

由于病毒技术的不断变化，很多未知新病毒、病毒变异、多形性病毒或者隐形病毒都将不能被杀毒软件检测到。由于病毒的特征码不断改变，压缩文件方式多样，病毒体加密解密方式改变（如循环加密等），病毒采用反跟踪技术和迷惑技术，内存高端和 XMS/EMS 区驻留，病毒技术避开检测技术等，漏报是病毒检测中经常见到的现象，所以要不断地升级杀毒软件的病毒库文件，隔一段时间就应该重新进行系统的安全扫描。

2）误报

误报是指把正常的系统文件报成病毒。由于杀毒软件的病毒特征码选择不合理，导致正常操作与非正常操作不能区分、判断失误，检测技术错误或者不妥，有时可能由于特殊干扰而导致杀毒软件做出错误推测。

3）错报

错报是指将一种病毒错报成另一种病毒。由于病毒的特征码交叉，病毒交叉感染、重复感染、病毒欺骗等往往会导致错报。

对杀毒系统而言，少许的漏报和误报是允许的，而错报可能会带来一定问题，但误报率超过一定范围，就会使用户对反病毒软件的质量与可靠性产生怀疑。

14.5.5　常用的杀毒软件

目前常用的杀毒软件可以分为两类：网络版和单机版。在网络环境中，通常使用网络版杀毒软件。网络版杀毒软件功能强大，易于管理。管理员可以远程查杀安装杀毒软件的客户端上的病毒，同时，管理员只需对服务器端的杀毒软件升级，客户端启动后就可以自动升级。

现在的杀毒软件一般都有实时查杀病毒的功能。系统启动后，杀毒软件就可以实时监视系统的运行情况，只要发现病毒，就会立即处理。下面介绍几个比较流行的杀毒软件。

1. Kaspersky

Kaspersky（卡巴斯基）杀毒软件来源于俄罗斯，是世界上顶级的网络杀毒软件。卡巴斯基杀毒软件具有超强的中心管理和杀毒能力，它强大的功能和局部的灵活性以及网络管理工具为自动信息搜索、中央安装和病毒防护控制提供最大的便利和最少的时间来建构用户的抗病毒分离墙。

2. PCcillin

PCcillin 是美国趋势科技公司出品的优秀杀毒软件。PCcillin 集个人防火墙、防病毒、防垃圾邮件等功能于一体，最大限度地提供对桌面机的保护，并不需要用户进行过多的操作。

3. McAfee VirusScan

McAfee VirusScan 是全球最畅销的杀毒软件之一，McAfee 防毒软件除了操作界面比较新颖外，也将 WebScanX 功能合在一起，杀毒性能稳定，操作方便。

4. Norton AntiVirus

Norton AntiVirus 是 Symantec 公司出品的优秀杀毒软件，它可帮助用户侦测上万种已知和未知的病毒。

5. AVG Anti Virus

AVG Anti Virus System 在功能上相当完善，可及时对任何存取文件侦测，防止计算机感染病毒。

6. BitDefender

BitDefender 具有功能强大的反病毒引擎以及互联网过滤技术，可以为用户提供即时信息保护。BitDefender 具备的功能主要有：防病毒保护、后台扫描与网络防火墙、保密控制、创建计划任务、自动快速升级模块、病毒隔离区。

7. F-Secure Anti-Virus

F-Secure AntiVirus 是一款功能强大的实时病毒监测和防护系统，支持所有的 Windows 平台，它集成了多个病毒监测引擎，如果其中一个发生遗漏，就会有另一个去监测。

8. AntiVirusKit

AntiVirusKit 具有超强的杀毒能力，具有病毒监控、E-mail 病毒拦截器、E-mail 防护、支持在线自动更新等功能，可以阻挡来自互联网的蠕虫病毒、黑客后门、特洛伊木马、拨号程序、广告软件、间谍软件等所有威胁，支持对压缩文件、电子邮件即时扫描，支持启发式病毒扫描，支持密码保护，有详细的日志，为计算机提供永久安全防护。AVK 最大的优点是只要病毒或木马录入病毒库，它能在病毒运行前拦截，因此不会出现中毒后再杀毒的情况。

9. 金山毒霸

金山毒霸是金山软件股份有限公司开发的高智能反病毒软件。金山毒霸独创双引擎杀毒技术，内置金山自主研发的杀毒引擎和俄罗斯著名杀毒软件 Dr. Web 的杀毒引擎，融合了启发式搜索、代码分析、虚拟机查毒等经业界证明已经成熟可靠的反病毒技术，使其在查杀病毒种类、查杀病毒速度、未知病毒防治等多方面达到世界先进水平。

10. 江民杀毒软件

江民杀毒软件是北京江民新科技术有限公司开发的计算机病毒处理软件。江民杀毒软件可有效清除 20 多万种已知计算机病毒，如蠕虫、木马、黑客程序、网页病毒、邮件病毒、脚本病毒等，可全方位主动防御未知病毒，并新增了流氓软件清理功能。

11. 瑞星杀毒软件

瑞星杀毒软件是北京瑞星科技股份有限公司出品的反病毒软件，它用于对已知病毒和黑客程序进行查找、实时监控和清除，恢复被病毒感染的文件或系统，保护计算机系统的安全。它能全面清除感染 DOS、Windows 系统的病毒以及危胁计算机安全的黑客程序。瑞星杀毒软件的更新速度非常快，几乎每天都有新的升级包。

12. 东方卫士

东方卫士是世纪长捷公司开发的免费杀毒软件，具有超强的易用性和实用性。东方卫士采用独创的自免疫智能反毒系统，通过对系统软件正常运行状态的记录，禁止病毒进行诸如复制、删除、格式化硬盘、破坏分区表、降低系统性能等操作，通过冻结病毒的传播和破坏

这两种特性，使病毒的隐蔽性发挥不了作用，能在完全不知病毒代码的情况下，解除新病毒及未知病毒的威胁，有效遏制各种病毒的传播。

本 章 小 结

本章介绍了如何通过在 Windows Server 2003 系统中使用安全配置向导、禁用不必要的服务和端口、安装网络防火墙来提高服务器的安全性，如何使用入侵检测技术防止服务器受到攻击，还介绍了目前常见的计算机病毒的种类、特征以及防病毒技术和常用杀毒软件。

习　题　14

1. 在运行 Windows Server 2003 操作系统的服务器计算机上安装并设置安全配置向导。
2. 简述 Windows Server 2003 系统中的两种系统安全策略。
3. 防火墙有哪几种类型？
4. 简述入侵检测方法。
5. 简述常见的计算机病毒及其特征。