第3章　操作系统安全配置

学习目标：

- 掌握 Linux 操作系统的设置。
- 掌握 Windows 2008 Server 操作系统的设置。

目前服务器常用的操作系统有三类：UNIX、Linux 和 Windows 2000/2003/2008 Server。这些操作系统都是符合 C2 级安全级别的操作系统，但是都存在不少漏洞，如果对这些漏洞不了解，不采取相应的安全措施，就会使操作系统完全暴露给入侵者。

3.1　Linux 操作系统

3.1.1　Linux 操作系统介绍

Linux 是一套可以免费使用和自由传播的类 UNIX 操作系统，主要用于基于 Intel x86 系列 CPU 的计算机上。这个系统是由全世界各地的成千上万的程序员设计和实现的，其目的是建立不受任何商品化软件的版权制约的、全世界都能自由使用的 UNIX 兼容产品。Linux 最早开始于一位名叫 Linus Torvalds 的计算机业余爱好者，当时他是芬兰赫尔辛基大学的学生，目的是想设计一个代替 Minix(是由一位名叫 Andrew Tannebaum 的计算机教授编写的一个操作系统示教程序)的操作系统。这个操作系统可用于 386、486 或奔腾处理器的个人计算机上，并且具有 UNIX 操作系统的全部功能。Linux 是一个免费的操作系统，用户可以免费获得其源代码，并能够随意修改。

例如，搜索 ls 命令源码，源代码包的文件名为 coreutils，可以通过命令查找，获取源代码的步骤如下。

(1) 先搜索命令所在包，命令如下：

```
# which ls
```

执行结果如下：

```
/bin/ls
```

(2) 用命令搜索该软件所在包，代码如下：

```
# dpkg -S /bin/ls
```

执行结果如下：

```
coreutils: /bin/ls
```

(3) 下载包，包的名字为 coreutils-XXX.tar.gz，XXX 表示版本号。

(4) 安装解压包:

```
# tar - xzvf coreutils - XXX.tar.gz
```

(5) 显示文件名字,看到主文件名字为命令(如 ls)扩展名为.c 的文件。

Linux 是在共用许可证(General Public License,GPL)保护下的自由软件,也有多种版本,如 Red Hat Linux、Slackware,以及国内的 Xteam Linux、红旗 Linux 等。Linux 的流行是因为它具有许多优点,如下。

(1) 完全免费。

(2) 完全兼容 POSIX 1.0 标准,为一个 POSIX 兼容的操作系统编写的程序,可以在任何其他的 POSIX 操作系统(即使是来自另一个厂商)上编译执行。

(3) 多用户、多任务。

(4) 良好的界面。

(5) 丰富的网络功能。

(6) 可靠的安全、稳定性能。

(7) 支持多种平台。

3.1.2 Linux 安全配置

1. 磁盘分区

如果是新安装系统,对磁盘分区应考虑安全性。

(1) 引导分区(/boot)、系统分区(/)、交换分区(swap)、用户目录(/home)应分开放到不同的磁盘分区。

(2) 应充分考虑以上各目录所在分区的磁盘空间大小,避免因某些原因造成分区空间用完而导致系统崩溃,交换分区为物理内存的 2 倍。

2. 账户安全

(1) 锁定系统中多余的自建账号。

使用命令 passwd -l <用户名>锁定不必要的账号。

使用命令 passwd -u <用户名>解锁需要恢复的账号。

执行命令如下:

```
#cat /etc/passwd
#cat /etc/shadow
```

查看账户、口令文件,与系统管理员确认不必要的账号。对于一些保留的系统伪账户如 bin, sys,adm,uucp,lp, nuucp,hpdb, www, daemon 等可根据需要锁定登录。

(2) 设置系统口令策略。

使用命令如下:

```
#cat /etc/login.defs|grep PASS      查看密码策略设置
#vi /etc/login.defs                 修改配置文件
PASS_MAX_DAYS 90                    #新建用户的密码最长使用天数 90 天
PASS_MIN_DAYS 0                     #新建用户的密码最短使用天数 0 天
PASS_WARN_AGE 7                     #新建用户的密码到期提前提醒天数 7 天
```

```
PASS_MIN_LEN 9                    #最小密码长度 9
```

(3) 限制能够 su 为 root 的用户。

检查方法：

```
#cat /etc/pam.d/su,查看是否有 auth required /lib/security/pam_wheel.so 这样的配置条目。
备份方法：#cp -p /etc/pam.d /etc/pam.d_bak
加固方法：#vi /etc/pam.d/su
```

在头部添加：

```
auth required /lib/security/pam_wheel.so group=wheel
```

这样，只有 wheel 组的用户可以 su 到 root。

(4) 检查 shadow 中空口令账号。

检查方法：

```
#awk -F: '($2 == "") { print $1 }' /etc/shadow
```

对空口令账号进行锁定，或要求增加密码。

(5) 设置账户锁定登录失败锁定次数、锁定时间。

```
#cat /etc/pam.d/system-auth 查看有无 auth required pam_tally.so 条目的设置。
#vi /etc/pam.d/system-auth
```

auth required pam_tally.so onerr=fail deny=6 unlock_time=300 设置输入密码连续错误 6 次锁定，锁定时间 300s

(6) 修改账户 TMOUT 值，设置自动注销时间。

```
#cat /etc/profile 查看有无 TMOUT 的设置。
#vi /etc/profile
TMOUT=600 无操作 600s 后自动退出.
```

(7) 设置 Bash 保留历史命令的条数。

```
#cat /etc/profile|grep HISTSIZE=
#cat /etc/profile|grep HISTFILESIZE=  查看保留历史命令的条数。
      #vi /etc/profile
```

修改 HISTSIZE=5 和 HISTFILESIZE=5 即保留最新执行的 5 条命令。

3. 设置合理的初始文件权限

```
#cat /etc/profile 查看 umask 的值。
#vi /etc/profile
umask=027
```

修改新建文件的默认权限，如果该服务器是 Web 应用，则此项应谨慎修改。

4. 网络访问控制

(1) 使用 SSH 进行管理。

```
#ps - aef | grep sshd 查看有无此服务。
```

使用命令开启 ssh 服务:

```
#service sshd start
```

(2) 设置访问控制策略,限制能够管理本机的 IP 地址。

```
#cat /etc/ssh/sshd_config 查看有无 AllowUsers 的语句。
#vi /etc/ssh/sshd_config 添加以下语句。
AllowUsers *@10.138.*.* 此句意为: 仅允许 10.138.0.0/16 网段所有用户通过 SSH 访问。
#service sshd restart 保存后重启 SSH 服务。
```

(3) 禁止 root 用户远程登录。

```
#cat /etc/ssh/sshd_config 查看 PermitRootLogin 是否为 no。
#vi /etc/ssh/sshd_config
PermitRootLogin = no
service sshd restart 保存后重启 SSH 服务。
root 用户无法直接远程登录,需要用普通账号登录后 su。
```

(4) 限定信任主机。

检查方法:

```
#cat /etc/hosts.allow 查看其中的主机。
#vi /etc/hosts.allow 删除其中不必要的主机。
```

注意:在多机互备的环境中,需要保留其他主机的 IP 可信任。

(5) 防止误使用 Ctrl+Alt+Del 重启系统。

```
#vi /etc/inittab 编辑文件。
```

在行开头添加注释符号"#":

```
#ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

(6) 资源限制。

对你的系统上所有的用户设置资源限制可以防止 DoS 类型攻击如最大进程数、内存数量等。例如,对所有用户的限制:

```
#vi /etc/security/limits.conf 加:
* hard rss 5000
* hard nproc 20
```

也必须编辑/etc/pam.d/login 文件加上 session required /lib/security/pam_limits.so 这一行。

上面的命令限制进程数为 20,且限制内存使用为 5M。

3.1.3 Linux 下建议替换的常见网络服务应用程序

1. WuFTPD

WuFTD 从 1994 年就开始不断地出现安全漏洞,黑客很容易就可以获得远程 root 访问的权限,而且很多安全漏洞甚至不需要在 FTP 服务器上有一个有效的账号。最近,WuFTP 也是频频出现安全漏洞。

WuFTD 最好的替代程序是 ProFTPD。ProFTPD 很容易配置，在多数情况下速度也比较快，而且它的源代码也比较干净（缓冲溢出的错误比较少）。有许多重要的站点使用 ProFTPD。sourceforge.net 就是一个很好的例子（这个站点共有 3 000 个开放源代码的项目，其负荷并不小）。一些 Linux 的发行商在它们的主 FTP 站点上使用的也是 ProFTPD，只有两个主要 Linux 的发行商（SuSE 和 Caldera）使用 WuFTPD。

2. Telnet

Telnet 是非常不安全的，它用明文来传送密码。它的安全的替代程序是 OpenSSH。

OpenSSH 在 Linux 上已经非常成熟和稳定了，而且在 Windows 平台上也有很多免费的客户端软件。Linux 的发行商应该采用 OpenBSD 的策略：安装 OpenSSH 并把它设置为默认的，安装 Telnet 但是不把它设置成默认的。对于不在美国的 Linux 发行商，很容易就可以在 Linux 的发行版中加上 OpenSSH。美国的 Linux 发行商就要想一些别的办法了（例如，Red Hat 在德国的 FTP 服务器上（ftp.redhat.de）就有最新的 OpenSSH 的 rpm 软件包）。

Telnet 是不安全的程序。要保证系统的安全必须用 OpenSSH 这样的软件来替代它。

3. Sendmail

最近这些年，Sendmail 的安全性已经提高了很多（以前它通常是黑客重点攻击的程序）。然而，Sendmail 还是有一个很严重的问题。一旦出现了安全漏洞（例如，最近出现的 Linux 内核错误），Sendmail 就是被黑客重点攻击的程序，因为 Sendmail 是以 root 权限运行而且代码很庞大容易出问题。

几乎所有的 Linux 发行商都把 Sendmail 作为默认的配置，只有少数几个把 Postfix 或 Qmail 作为可选的软件包。但是，很少有 Linux 的发行商在自己的邮件服务器上使用 Sendmail。SuSE 和 Red Hat 都使用基于 Qmail 的系统。

Sendmail 并不一定会被别的程序完全替代。但是它的两个替代程序 Qmail 和 Postfix 都比它安全、速度快，而且特别是 Postfix 比它容易配置和维护。

4. su

su 是用来改变当前用户的 ID，转换成别的用户。可以以普通用户登录，当需要以 root 身份做一些事的时候，只要执行“su”命令，然后输入 root 的密码。su 本身是没有问题的，但是它会让人养成不好的习惯。如果一个系统有多个管理员，必须都给他们 root 的口令。su 的一个替代程序是 sudo。sudo 允许用户设置哪个用户哪个组可以以 root 身份执行哪些程序。还可以根据用户登录的位置对他们加以限制（如果有人“破”了一个用户的口令，并用这个账号从远程计算机登录，可以限制他使用 sudo）。Debian 也有一个类似的程序叫 super。使用 root 账号并让多个人知道 root 的密码是不安全的，这就是 www.apache.org 被入侵的原因，因为它有多个系统管理员，他们都有 root 的特权，这样的系统是很容易被入侵的。

5. named

大部分 Linux 的发行商都解决了这个问题。named 以前是以 root 运行的，因此当 named 出现新的漏洞的时候，很容易就可以入侵一些很重要的计算机并获得 root 权限。现在只要用命令行的一些参数就能让 named 以非 root 的用户运行。而且，现在绝大多数

Linux 的发行商都让 named 以普通用户的权限运行。命令格式通常为:

```
named -u <user name>; -g <group name>;
```

3.1.4 Linux 下的安全守则

(1) 删除系统所有默认的账号和密码。

(2) 在用户合法性得到验证前不要显示公司题头、在线帮助以及其他信息。

(3) 关闭"黑客"可以攻击系统的网络服务。

(4) 使用 6～8 位的字母数字混合式密码。

(5) 限制用户尝试登录到系统的次数。

(6) 记录违反安全性的情况并对安全记录进行复查。

(7) 对于重要信息,上网传输前要先进行加密。

(8) 重视专家提出的建议,安装他们推荐的系统"补丁"。

(9) 限制不需密码即可访问的主机文件。

(10) 修改网络配置文件,以便将来自外部的 TCP 连接限制到最少数量的端口。不允许诸如 tftp,sunrpc,printer,rlogin 或 rexec 之类的协议。

(11) 用 upas 代替 sendmail。sendmail 有太多已知漏洞,很难修补完全。

(12) 去掉对操作并非至关重要又极少使用的程序。

(13) 使用 chmod 将所有系统目录变更为 711 模式。这样,攻击者们将无法看到它们当中有什么东西,而用户仍可执行。

(14) 只要可能,就将磁盘安装为只读模式。其实,仅有少数目录需读写状态。

(15) 将系统软件升级为最新版本。老版本可能已被研究并被成功攻击,最新版本一般包括了这些问题的补救。

3.2 Windows Server 2008 操作系统

Windows Server 2008 是微软公司一个服务器操作系统的名称。Windows Server 2008 发行了多种版本,以支持各种规模的企业对服务器不断变化的需求。Windows Server 2008 共有包括 Standard Edition、Enterprise Edition、DataCenter Edition、Web Server Edition 等 8 种版本,每个版本均有 32 位和 64 位两种编码。Windows 2003 对硬件的最低要求不高,和 Windows Server 2003 相仿。

3.2.1 Windows Server 2008 的特点

1. 控制力

使用 Windows Server 2008,IT 专业人员能够更好地控制服务器和网络基础结构,从而可以将精力集中在处理关键业务需求上。增强的脚本编写功能和任务自动化功能(例如,Windows PowerShell)可帮助 IT 专业人员自动执行常见 IT 任务。通过服务器管理器进行的基于角色的安装和管理简化了在企业中管理与保护多个服务器角色的任务。服务器的配

置和系统信息是从新的服务器管理器控制台这一集中位置来管理的。IT 人员可以仅安装需要的角色和功能，向导会自动完成许多费时的系统部署任务。增强的系统管理工具（例如，性能和可靠性监视器）提供有关系统的信息，在潜在问题发生之前向 IT 人员发出警告。在 Windows Server 2008 中，所有的电源管理设置已被组策略启用，这样就潜在地节约了成本。控制电源设置通过组策略可以大量节省公司金钱。比如，可以通过修改组策略设置中特定电源的设置，或通过使用组策略建立一个定制的电源计划。

2. 保护

Windows Server 2008 提供了一系列新的和改进的安全技术，这些技术增强了对操作系统的保护，为企业的运营和发展奠定了坚实的基础。Windows Server 2008 提供了减小内核攻击面的安全创新（例如 PatchGuard），因而使服务器环境更安全、更稳定。通过保护关键服务器服务使之免受文件系统、注册表或网络中异常活动的影响，Windows 服务强化有助于提高系统的安全性。借助网络访问保护（NAP）、只读域控制器（RODC）、公钥基础结构（PKI）增强功能、Windows 服务强化、新的双向 Windows 防火墙和新一代加密支持，Windows Server 2008 操作系统中的安全性也得到了增强。

3. 灵活性

Windows Server 2008 的设计允许管理员修改其基础结构来适应不断变化的业务需求，同时保持了此操作的灵活性。它允许用户从远程位置（如远程应用程序和终端服务网关）执行程序，这一技术为移动工作人员增强了灵活性。Windows Server 2008 使用 Windows 部署服务（WDS）加速对 IT 系统的部署和维护，使用 Windows Server 虚拟化（WSv）帮助合并服务器。对于需要在分支机构中使用域控制器的组织，Windows Server 2008 提供了一个新配置选项：只读域控制器（RODC），它可以防止在域控制器出现安全问题时暴露用户账户。

3. 自修复系统

从 DOS 时代开始，文件系统出错就意味着相应的卷必须下线修复，而在 Windows Server 2008 中，一个新的系统服务在后台默默工作，检测文件系统错误，并且可以在无须关闭服务器的状态下自动将其修复。有了这一新服务，在文件系统发生错误的时候，服务器只会暂时停止无法访问的部分数据，整体运行基本不受影响，所以 CHKDSK 基本就可以退休了。

4. Session 创建

如果有一个终端服务器系统，或者多个用户同时登录了家庭系统，这些就是 Session。在 Windows Server 2008 之前，Session 的创建都是逐一操作的，对于大型系统而言就是个瓶颈，比如周一清晨数百人返回工作的时候，不少人就必须等待 Session 初始化。Vista 和 Windows Server 2008 加入了新的 Session 模型，可以同时发起至少 4 个 Session，而如果服务器有 4 颗以上的处理器，还可以同时发起更多 Session。举例来说，如果家里有一个媒体中心，那各个家庭成员就可以同时在各自的房间里打开媒体终端，同时从 Vista 服务器上得到视频流，而且速度不会受到影响。

5. 快速关机服务

Windows 的一大历史问题就是关机过程缓慢。在 Windows XP 里，一旦关机开始，系

统就会开始一个 20s 的计时,之后提醒用户是否需要手动关闭程序,而在 Windows Server 里,这一问题的影响会更加明显。到了 Windows Server 2008,20s 的倒计时被一种新服务取代,可以在应用程序需要被关闭的时候随时、一直发出信号。开发人员开始怀疑这种新方法会不会过多地剥夺应用程序的权利,但他们已经接受了它,认为这是值得的。

6. UAC

Windows Server 2008 操作系统和 Windows Vista 类似同样附带了 UAC(User Account Control,用户账户控制),可以有效降低服务器的风险。但是通过 Vista 地带适用 Windows 2008 的系统管理员账户并没有受到像 Vista 一样的限制。

7. 安全

Windows Server 2008 的 IE7 具有"增强的安全配置",必须通过用户手动审核才可以打开相关的网站,与 Windows Vista 相比安全了许多。

3.2.2 Windows Server 2008 安全配置

1. 停止 Guest 账号

在计算机管理的用户里面把 Guest 账号停用,任何时候都不允许 Guest 账号登录系统。为了保险起见,最好给 Guest 加一个复杂的密码,可以打开记事本,在里面输入一串包含特殊字符、数字、字母的长字符串,用它作为 Guest 账号的密码,并且修改 Guest 账号的属性,设置拒绝远程访问,如图 3-1 所示。

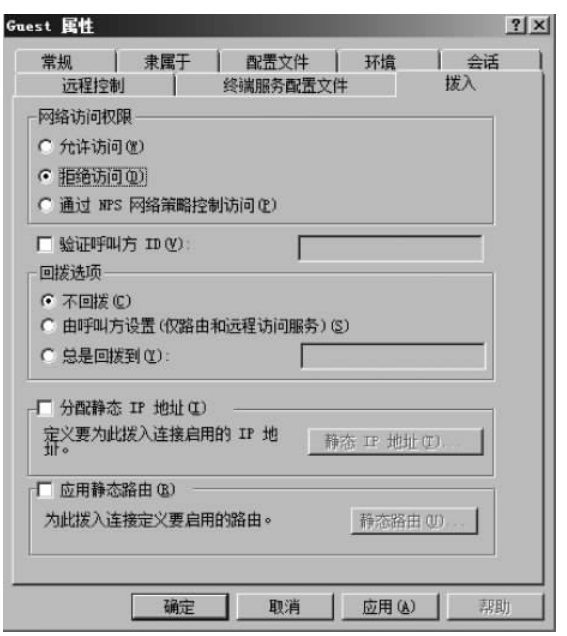

图 3-1 设置 Guest 账号属性

2. 管理员账号改名

Windows 2008 中的 Administrator 账号是不能被停用的,这意味着别人可以一遍又一遍地尝试这个账户的密码。把 Administrator 账户改名可以有效地防止这一点。不要使用

Admin 之类的名字，改了等于没改，应尽量把它伪装成普通用户，比如改成 guestone。具体操作的时候只要选中账户名改名就可以了，如图 3-2 所示。

图 3-2　修改 Administrator 账号

3. 陷阱账号

所谓的陷阱账号是创建一个名为“Administrator”的本地账户，把它的权限设置成最低，什么事也干不了，并且加上一个超过 10 位的超级复杂密码，这样可以让那些企图入侵者忙上一段时间了，并且可以借此发现他们的入侵企图。可以将该用户隶属的组修改成 Guests 组，如图 3-3 所示。

图 3-3　修改用户隶属的组

4. 安全策略

利用 Windows 2008 的安全配置工具来配置安全策略，微软提供了一套基于管理控制台的安全配置和分析工具，可以配置服务器的安全策略。在管理工具中可以找到“本地安全策略”，主界面如图 3-4 所示，可以配置 6 类安全策略：账户策略、本地策略、高级安全 Windows 防火墙、公钥策略、软件限制策略和 IP 安全策略。在默认的情况下，这些策略都是没有开启的。

5. 设置本机开放的端口和服务

(1) 单击“控制面板”→“管理工具”，打开“本地安全策略”。在左边栏单击“IP 安全策略，在本地计算机”，然后在右边的空白处右击，选择“创建 IP 安全策略”，将弹出“IP 安全策略向导”窗口，如图 3-5 所示。

图 3-4 安全策略界面

图 3-5 创建本地安全策略

(2) 单击“下一步”按钮,填写名称“禁用 80 端口策略”,然后下一步,不要改动,继续下一步,单击“完成”按钮。

(3) 系统弹出“属性”对话框。取消右下角“使用添加向导”的勾选,然后再单击“添加”,随后弹出“新规则属性”对话框,单击“添加”,又弹出了“IP 筛选列表”,填写名称“禁用 80 端口”,在页面中取消“使用添加向导”的勾选,然后单击“添加”,将弹出“IP 筛选器属性”。

(4) 进入“筛选器属性”对话框,源地址选择“任何 IP 地址”,目标地址选择“我的 IP 地址”。接下来单击“协议”标签,在“选择协议类型”中选择 TCP,到此端口填“80”,接着单击“描述”标签,填写描述“禁用 80”,单击“确定”按钮。

(5) 在“新规则属性”对话框中,选中“禁用 80 端口”然后单击其左边的复选框,表示已经激活。然后单击“筛选器操作”标签,取消“使用添加向导”的勾选,单击“添加”按钮,在“新筛选器操作属性”的“安全方法”选项卡中,选择“阻止”,然后单击“确定”按钮。接着单击“阻止操作”左边的复选框,然后单击“确定”按钮。

(6) 最后打开“新 IP 安全策略属性”对话框,在“禁用 80 端口策略”左边打勾,确定关闭对话框。在“本地安全策略”窗口中,鼠标右击新添加的 IP 安全策略,然后选择“分配”。

6. 开启审核策略

安全审核是 Windows 2008 最基本的入侵检测方法。当有人尝试对系统进行某种方式

(如尝试用户密码,改变账户策略和未经许可的文件访问等)入侵的时候,都会被安全审核记录下来。很多的管理员在系统被入侵了几个月后都不知道,直到系统遭到破坏。表 3-1 的这些审核是必须开启的,其他的可以根据需要增加。

表 3-1　开启审核策略的设置

策　略	安全设置	策　略	安全设置
审核策略更改	成功,失败	审核特权使用	成功,失败
审核登录事件	成功,失败	审核系统事件	成功,失败
审核对象访问	成功,失败	审核账户登录事件	成功,失败
审核进程跟踪	成功,失败	审核账户管理	成功,失败
审核目录服务访问	成功,失败		

审核策略在默认的情况下都是没有开启的,如图 3-6 所示。双击审核列表的某一项,出现设置对话框,将复选框“成功”和“失败”都选中,如图 3-7 所示。

图 3-6　审核策略的默认设置

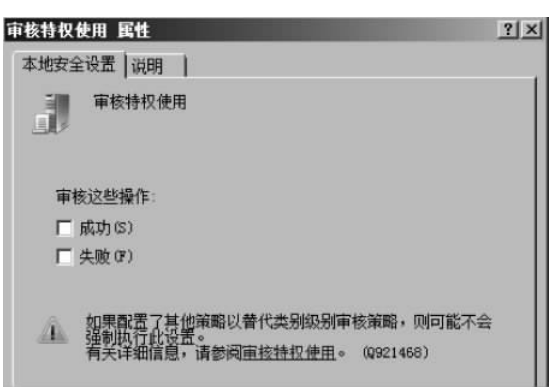

图 3-7　审核策略的设置

7. 开启账户策略

账户锁定策略用于域账户或本地用户账户,它们确定某个账户被系统锁定的情况和时间长短,可以有效地防止字典式攻击,其设置如图 3-8 所示,这部分包含以下三个方面。

图 3-8 账户锁定策略的设置

1) 账户锁定时间

该安全设置确定锁定的账户在自动解锁前保持锁定状态的分钟数。有效范围为 0～99 999 分钟。如果将账户锁定时间设置为 0,那么在管理员明确将其解锁前,该账户将被锁定。如果定义了账户锁定阈值,则账户锁定时间必须大于或等于重置时间。

默认值:无。因为只有当指定了账户锁定阈值时,该策略设置才有意义。

2) 账户锁定阈值

该安全设置确定造成用户账户被锁定的登录失败尝试的次数。无法使用锁定的账户,除非管理员进行了重新设置或该账户的锁定时间已过期。登录尝试失败的范围可设置为 0～999 之间。如果将此值设为 0,则将无法锁定账户。

对于使用 Ctrl+Alt+Delete 组合键或带有密码保护的屏幕保护程序锁定的工作站或成员服务器计算机上,失败的密码尝试计入失败的登录尝试次数中。

默认值:0。

3) 复位账户锁定计数器

该安全设置确定在登录尝试失败计数器被复位为 0(即 0 次失败登录尝试)之前,尝试登录失败之后所需的分钟数。有效范围为 1～99 999 分钟。

如果定义了账户锁定阈值,则该复位时间必须小于或等于账户锁定时间。

默认值:无。因为只有当指定了“账户锁定阈值”时,该策略设置才有意义。

与“锁定”字段相同,设置该字段值时也应考虑到安全需求与有效用户访问需求之间的平衡。最好设置为 1～2 小时。该等待时间应足够长,足以强制黑客必须等待一个长于他们所希望的时间段后才能再次尝试登录。

8. 开启密码策略

密码对系统安全非常重要。本地安全设置中的密码策略在默认的情况下都没有开启,包括:密码长度最小值,密码最长使用期限,密码最短使用期限,强制密码历史记录,使用可还原的加密存储密码,密码必须符合复杂性要求,设置的结果如图 3-9 所示。

(1) 强制密码历史记录:防止用户创建与他们的当前密码或最近使用的密码相同的新密码。若要指定记住多少个密码,请提供一个值。例如,值为 1 表示仅记住上一个密码,值为 5 表示记住前 5 个密码,使用大于 1 的数字。

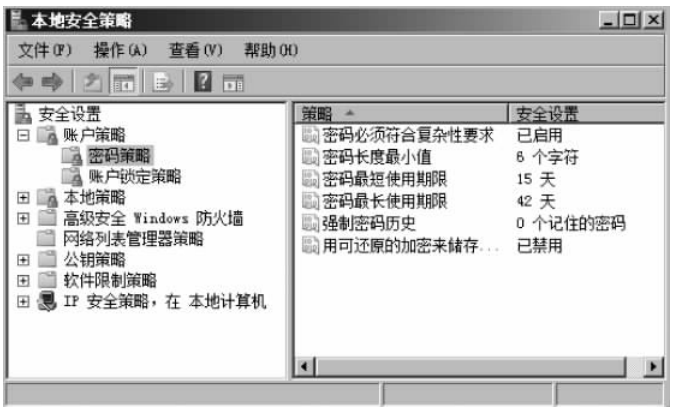

图 3-9　密码策略的设置

(2) 密码最长使用期限：设置密码有效天数的最大值。在此天数后，用户将必须更改密码。可设置 70 天的最长密码使用期限。将天数值设置得太高将给黑客破解密码提供延长窗口的机会；将天数值设置得太低将干扰用户，因为必须频繁地更改密码。

(3) 密码最短使用期限：设置在可以更改密码前必须通过的最短天数。将密码最短使用期限设置为至少一天。通过这样做，将要求用户一天只能更改一次密码，这将有助于强制使用其他设置。例如，如果记住了过去的 5 个密码，将确保在用户可以重新使用他们的原始密码前，必须至少经过 5 天。如果将密码最短使用期限设置为 0，则用户可以一天更改 6 次密码，并且在同一天就可以开始重新使用其原始密码。

(4) 密码长度最小值：指定密码可以具有的最少字符数。将密码设置为介于 8～12 个字符之间(假设它们也符合复杂性要求)。较长的密码比较短的密码更难破解(假定密码不是一个单词或普通短语)。但是，如果不担心办公室或家中的人使用自己的计算机，则不使用密码比使用容易猜到的密码能够更好地保护计算机不受黑客从 Internet 或其他网络攻击的侵害。如果不使用密码，Windows 将自动防止任何人从 Internet 或其他网络登录到自己的计算机。

(5) 密码必须符合复杂性要求，要求密码：

① 不能包含用户的账户名，不能包含用户姓名中超过两个连续字符的部分至少有 6 个字符长；

② 包含以下四类字符中的三类字符：英文大写字母(A～Z)、英文小写字母(a～z)、10 个基本数字(0～9)；

③ 非字母字符(例如 !、$、#、%)；

④ 在更改或创建密码时执行复杂性要求。

启用此设置。这些复杂性要求可以帮助创建强密码。

(6) 使用可还原的加密存储密码：存储密码而不对其加密，除非使用的程序要求这样，否则不要使用此设置。

9. 关闭默认共享

Windows Server 安装以后，系统会创建一些隐藏的共享，可以在 DOS 提示符下输入命令 net share 查看，如图 3-10 所示。

图 3-10 查看共享的磁盘

禁止这些共享,打开“管理工具”→“计算机管理”→“共享文件夹”→“共享”,在相应的共享文件夹上单击右键,选择“停止共享”即可,如图 3-11 所示。

图 3-11 停止共享的设置

10. 禁用 Dump 文件

在系统崩溃和蓝屏的时候,Dump 文件是一份很有用的资料,可以帮助查找问题。然而,它也能够给黑客提供一些敏感信息,比如一些应用程序的密码等。需要禁止它时,打开“控制面板”→“系统属性”→“高级”→“启动和故障恢复”,把“写入调试信息”改成“无”,如图 3-12 所示。

11. 关机时清除文件

页面文件也就是调度文件,是 Windows 2000 用来存储没有装入内存的程序和数据文件部分的隐藏文件。一些第三方程序可以把一些没有加密的密码存在内存中,页面文件中可能含有另外一些敏感的资料。要在关机的时候清除页面文件,可以编辑注册表,修改主键 HKEY_LOCAL_MACHINE 下的子键:

```
SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
```

把 ClearPageFileAtShutdown 的值设置成 1,如图 3-13 所示。

图 3-12　禁用 Dump 文件

图 3-13　关机时清除文件的设置

12. 限制使用迅雷进行恶意下载

在多人共同使用同一台计算机进行工作时，我们肯定不希望普通用户随意使用迅雷工具进行恶意下载，这样不但容易浪费本地系统的磁盘空间资源，而且也会大大消耗本地系统上的网带宽资源。而在 Windows Server 2008 系统环境下，限制普通用户随意使用迅雷工具进行恶意下载的方法有很多，例如，可以利用 Windows Server 2008 系统新增加的高级安全防火墙功能，或者通过限制下载端口等方法来实现上述控制目的，其实除了这些方法外，还可以巧妙地利用该系统的软件限制策略来达到这一目的，下面就是该方法的具体实现步骤。

首先以系统管理员权限登录进入 Windows Server 2008 系统，打开该系统的“开始”菜单，从中选择“运行”命令，在弹出的“运行”文本框中，输入“gpedit. msc”字符串命令，进入对应系统的组策略控制台窗口。

其次在该控制台窗口的左侧位置处,依次选中“计算机配置”→“Windows 设置”→“安全设置”→“软件限制策略”选项,同时用鼠标右击该选项,并执行快捷菜单中的“创建软件限制策略”命令。

接着在对应“软件限制策略”选项的右侧显示区域,双击“强制”组策略项目,在打开的设置对话框中选中其中的“除本地管理员以外的所有用户”选项,其余参数都保持默认设置,再单击“确定”按钮结束上述设置操作。

下面选中“软件限制策略”结点下面的“其他规则”选项,再用鼠标右击该组策略选项,从弹出的快捷菜单中选择“新建路径规则”命令,在其后出现的设置对话框中,单击“浏览”按钮选中迅雷下载程序,同时将对应该应用程序的“安全级别”参数设置为“不允许”,最后单击“确定”按钮执行参数设置保存操作。

重新启动 Windows Server 2008 系统,当用户以普通权限账号登录进入该系统后,普通用户就不能正常使用迅雷程序进行恶意下载了,不过当我们以系统管理员权限进入本地计算机系统时,仍然可以正常运行迅雷程序进行随意下载。

13. 拒绝网络病毒藏于临时文件

现在 Internet 上的病毒疯狂肆虐,一些“狡猾”的网络病毒为了躲避杀毒软件的追杀,往往会想方设法地将自己隐藏于系统临时文件夹,这样一来杀毒软件即使找到了网络病毒,也对它无可奈何,因为杀毒软件对系统临时文件夹根本无权“指手画脚”。为了防止网络病毒隐藏在系统临时文件夹中,可以按照下面的操作设置 Windows Server 2008 系统的软件限制策略。

首先打开 Windows Server 2008 系统的“开始”菜单,从中选择“运行”命令,在弹出的“运行”对话框中,输入组策略编辑命令“gpedit. msc”,单击“确定”按钮后,进入对应系统的组策略控制台窗口。

其次,在该控制台窗口的左侧位置处,依次选中“计算机配置”→“Windows 设置”→“安全设置”→“软件限制策略”→“其他规则”选项,同时用鼠标右键单击该选项,并执行快捷菜单中的“新建路径规则”命令,打开如图 3-14 所示的设置对话框;单击其中的“浏览”按钮,

图 3-14 将“安全级别”参数设置为“不允许的”

从弹出的选择文件对话框中，选中并导入 Windows Server 2008 系统的临时文件夹，同时再将“安全级别”参数设置为“不允许的”，最后单击“确定”按钮保存好上述设置操作，这样一来网络病毒日后就不能躲藏到系统的临时文件夹中了。

14. 禁止来自外网的非法 ping 攻击

巧妙地利用 Windows 系统自带的 ping 命令，可以快速判断局域网中某台重要计算机的网络连通性；可是，ping 命令在给我们带来实用性的同时，也容易被一些恶意用户所利用，例如，恶意用户要是借助专业工具不停地向重要计算机发送 ping 命令测试包时，重要计算机系统由于无法对所有测试包进行应答，从而容易出现瘫痪现象。为了保证 Windows Server 2008 服务器系统的运行稳定性，可以修改该系统的组策略参数，来禁止来自外网的非法 ping 攻击。

首先，以特权身份登录进入 Windows Server 2008 服务器系统，依次选择该系统桌面上的“开始”→“运行”命令，在弹出的“运行”对话框中，输入字符串命令“gpedit. msc”，按回车键后，进入对应系统的控制台窗口。

其次，选中该控制台左侧列表中的“计算机配置”结点选项，并从目标结点下面逐一选择“Windows 设置”、“安全设置”、“高级安全 Windows 防火墙”、“高级安全 Windows 防火墙——本地组策略对象”选项，再用鼠标选中目标选项下面的“入站规则”项目。

接着在对应“入站规则”项目右侧的“操作”列表中，选择“新规则”选项，此时系统屏幕会自动弹出新建入站规则向导对话框，依照向导屏幕的提示，先将“自定义”选项选中，再将“所有程序”项目选中，之后从“协议类型”列表中选中 ICMPv4，如图 3-15 所示。

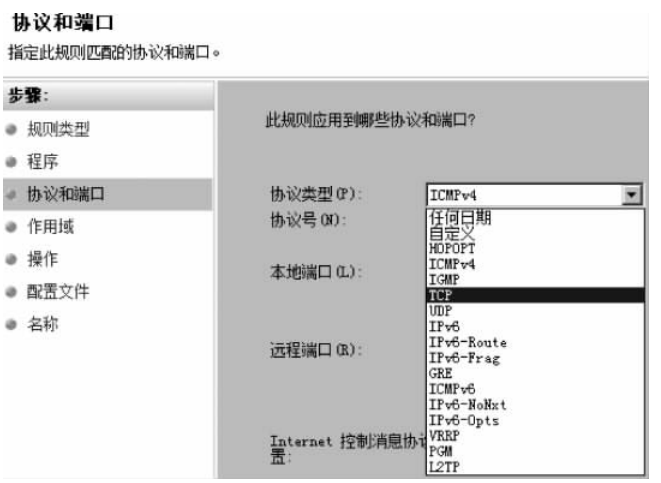

图 3-15　协议类型选择 ICMPv4

向导屏幕提示我们选择什么类型的连接条件时，可以选中“阻止连接”选项，同时依照实际情况设置好对应入站规则的应用环境，最后为当前创建的入站规则设置一个适当的名称。完成上面的设置任务后，将 Windows Server 2008 服务器系统重新启动一下，这样一来 Windows Server 2008 服务器系统日后就不会轻易受到来自外网的非法 ping 测试攻击了。

小提示：尽管通过 Windows Server 2008 服务器系统自带的高级安全防火墙功能可以实现很多安全防范的目的，不过稍微懂得一点儿技术的非法攻击者，就可以想办法修改防火

墙的安全规则,那样一来自行定义的各种安全规则可能会发挥不了任何作用。为了阻止非法攻击者随意修改 Windows Server 2008 服务器系统的防火墙安全规则,可以进行下面的设置操作。

首先打开 Windows Server 2008 服务器系统的"开始"菜单,选择"运行"命令,在弹出的"运行"文本框中执行"regedit"字符串命令,打开系统注册表控制台窗口;选中该窗口左侧显示区域处的 HKEY_LOCAL_MACHINE 选项,同时从目标分支下面选中 SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules 注册表子项,该子项下面保存有很多安全规则。

其次,打开注册表控制台窗口中的"编辑"下拉菜单,从中选择"权限"选项,打开权限设置对话框,单击该对话框中的"添加"按钮,从其后出现的账号选择框中选中 Everyone 账号,同时将其导入进来;再将对应该账号的"完全控制"权限调整为"拒绝",最后单击"确定"按钮执行设置保存操作,如此一来非法用户日后就不能随意修改 Windows Server 2008 服务器系统的各种安全控制规则了。

15. 禁止普通用户随意上网访问

通常 Windows Server 2008 系统都被安装到重要的计算机中,为了防止该计算机系统受到安全威胁,往往需要想办法限制普通用户在该系统中随意上网访问;但是如果简单关闭该系统的上网访问权限,又会影响特权用户正常上网,那么如何才能限制普通用户上网,而又不影响特权用户进行上网访问呢?其实很简单,可以按照下面的操作来修改 Windows Server 2008 系统的组策略参数。

首先,以普通权限的账号登录 Windows Server 2008 系统,打开对应系统中的 IE 浏览器窗口,单击其中的"工具"菜单项,从下拉菜单中选择"Internet 选项"命令,弹出 Internet 选项设置窗口。

其次,选择 Internet 选项设置窗口中的"连接"选项卡,进入连接选项设置页面,单击该设置页面中的"局域网设置"按钮,选中其后设置页面中的"为 LAN 使用代理服务器"选项,再任意输入一个代理服务器的主机地址以及端口号码,再单击"确定"按钮执行参数设置保存操作。

注销 Windows Server 2008 系统,换用具有特殊权限的用户账号重新登录进入 Windows Server 2008 系统,依次选择"开始"→"运行"命令,在其后出现的系统运行框中输入"gpedit.msc"命令,单击"确定"按钮后,进入对应系统的组策略控制台窗口。

选中该控制台窗口左侧位置处的"计算机配置"选项,再从目标结点下面依次展开"管理模板"→"Windows 组件"→Internet Explorer→"Internet 控制面板"子项,再双击目标子项下面的"禁用连接页"组策略项目,此时系统屏幕上会弹出如图 3-16 所示的目标组策略属性设置对话框,选中"已启用"选项,再单击"确定"按钮执行设置保存操作,这样一来,普通权限的用户日后在 Windows Server 2008 系统中尝试访问网络时,IE 浏览器会自动连接一个失效的代理服务器,那么 IE 浏览器自然也就不能正常显示网络页面内容了;而具有特殊权限的用户在 Windows Server 2008 系统中尝试进行网络访问时,IE 浏览器会直接显示出目标站点的内容,不需要通过代理服务器进行中转。

16. 断开远程连接恢复系统状态

很多时候,一些不怀好意的用户往往会同时建立多个远程连接,来消耗 Windows

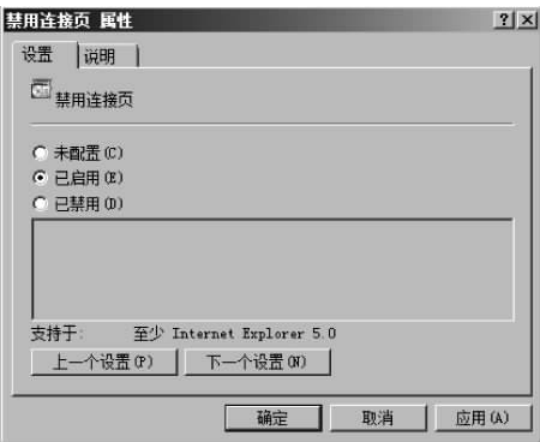

图 3-16　禁用连接页属性设置

Server 2008 服务器系统的宝贵资源，最终达到搞垮服务器系统的目的；为此，在实际管理 Windows Server 2008 服务器系统的过程中，一旦发现服务器系统运行状态突然不正常时，可以按照下面的办法强行断开所有与 Windows Server 2008 服务器系统建立连接的各个远程连接，以便及时将服务器系统的工作状态恢复正常。

首先，在 Windows Server 2008 服务器系统桌面中依次选择“开始”→“运行”选项，在弹出的“运行”对话框中，输入“gpedit. msc”命令，按回车键后，进入目标服务器系统的组策略控制台窗口。

其次，选中组策略控制台窗口左侧位置处的“用户配置”结点分支，并用鼠标逐一选择目标结点分支下面的“管理模板”→“网络”→“网络连接”组策略选项，之后双击“网络连接”分支下面的“删除所有用户远程访问连接”选项，在弹出的如图 3-17 所示的选项设置对话框中，选中“已启用”选项，再单击“确定”按钮保存好上述设置。这样一来，Windows Server 2008 服务器系统中的各个远程连接都会被自动断开，此时对应系统的工作状态可能会立即恢复正常。

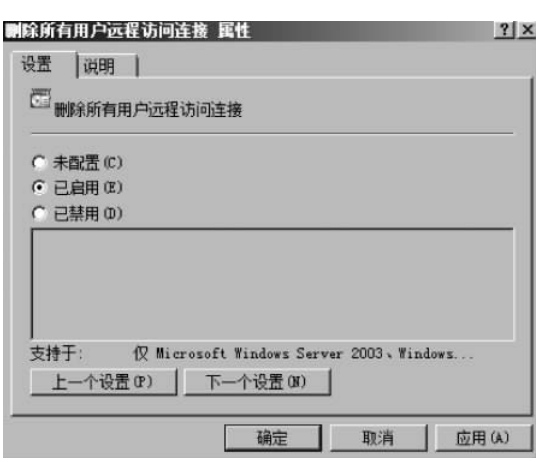

图 3-17　设置删除所有用户远程访问连接为“已启用”

习　题

一、填空题

1. 可以免费使用和自由传播,主要用于基于 Intel x86 系列 CPU 的计算机上的类 UNIX 操作系统是_____。

2. 在系统崩溃和蓝屏的时候,_____文件是很有用的资料,可以帮助查找问题。

3. 查看磁盘和文件共享的命令是_____。

4. 所谓的陷阱账号是创建一个名为_____的本地账号,把它的权限设置成最低。

二、简答题

1. 简述 Linux 安全配置方案。

2. 简述审核策略、密码策略和账户策略的含义,以及这些策略如何保护操作系统不被入侵。