第 3 章 操作系统的安全配置

学习目标：

- 掌握 Linux 操作系统的设置。
- 掌握 Windows 10 操作系统的安全设置。

目前服务器常用的操作系统有三类：UNIX、Linux 和 Windows 系列。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，其目的是建立不受任何商品化软件版权制约的、全世界都能自由使用的 UNIX 兼容产品。Linux 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。他的目标是想设计一个代替 Minix(由一位名叫 Andrew Tannebaum 的计算机教授编写的一个免费操作系统)的操作系统，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，源代码包的文件为 coreutils，可以通过命令查找，获取源代码的步骤如下(以 Ubuntu Linux 为例)。

(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，其中，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,看到主文件名字是命令(如ls)扩展名为.c的文件,可以使用cat命令显示命令ls的源代码ls.c。

```
cat ls.c
```

Linux是在共用许可证GPL(General Public License)保护下的自由软件,有很多发行版,如Ubuntu Linux、Red Hat Linux、Debian Linux、红旗Linux等。Linux的流行是因为它具有以下优点。

(1) 完全免费。

(2) 完全兼容POSIX 1.0标准,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

以下安全配置以Ubuntu Linux操作系统为例。

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)应分开到不同的磁盘分区。

(2) 以上各目录应充分考虑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,如表3-1所示。

表3-1　建立分区的要求

设备	分区类型	文件系统	挂载点	分区大小
/dev/sda1	主分区(引导分区)	Ext4	/boot	510MB
/dev/sda5	逻辑分区(系统分区)	Ext4	/	10240MB
/dev/sda6	交换分区	swap	swap	1023MB
/dev/sda7	个人文件分区	Ext4	/home	9696MB

2. 账户安全

(1) 锁定系统中多余的自建账号。

```
#cat /etc/passwd          查看用户名
#cat /etc/shadow          查看用户的口令(加密后的口令)
#passwd -l <用户名>       锁定不必要的账号
#passwd -u <用户名>       解锁需要恢复的账号
```

查看账户、口令文件,确认不必要的账号锁定。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:

```
#vi /etc/login.defs          编辑密码策略的配置文件
PASS_MAX_DAYS 90             新建用户的密码最长使用天数为 90 天
PASS_MIN_DAYS 0              新建用户的密码最短使用天数为 0 天
PASS_WARN_AGE 7              新建用户的密码到期提前提醒天数为 7 天
PASS_MIN_LEN 6               最小密码长度为 6
PASS_MAX_LEN 9               最大密码长度为 9
#cat /etc/login.defs|grep PASS      查看密码策略设置,如图 3-1 所示
```

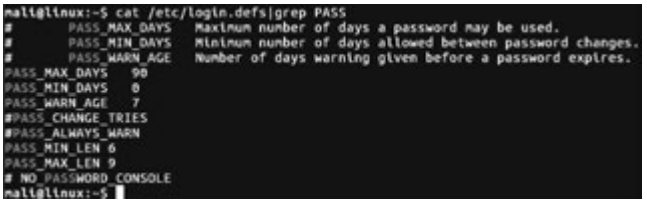

图 3-1 查看密码策略设置

(3) 禁止普通用户 su 至 root。

```
#nano /etc/pam.d/su
```

编辑/etc/pam.d/su 文件,在文件中看到 auth required pam_wheel.so deny group=nosuo 是以#开头,即#auth required pam_wheel.so deny group=nosuo,说明它已经被注释掉了,任何用户都可以转到 root 用户。去掉#,将其修改为 auth required pam_wheel.so group=sudo,只有属于 sudo 组的用户,才可以从 su 转到 root,如图 3-2 所示,其他用户不能转到 root,如图 3-3 所示。

图 3-2 修改 su 文件

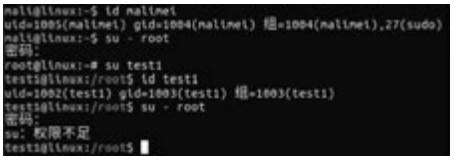

图 3-3 验证普通用户不能转到超级用户

(4) 检查 shadow 中的空口令账号。

检查方法:

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

检查到空口令的账号后,对空口令账号进行锁定,或增加密码。

(5) 账户登录失败锁定次数、锁定时间的设置。

#cat /etc/pam.d/common-auth 查看有无 auth required pam_tally.so 条目的设置,如果没有,编辑/etc/pam.d/common-auth 文件,普通用户设置密码连续错误 3 次锁定,锁定

时间为 60 秒，超级用户锁定时间为 10 秒，如图 3-4 所示。验证如图 3-5 所示，密码连续输错，锁定 60 秒后，密码输入正确，用户可以登录。

```
#nano /etc/pam.d/common - auth
```

图 3-4　修改 common-auth 文件

图 3-5　密码输入正确即可登录

(6) 修改账户 TMOUT 值，设置自动注销时间，在设置时间内，不操作自动退出。

```
#cat /etc/profile 查看有无 TMOUT 的设置
#nano /etc/profile
```

TMOUT＝600 无操作 600 秒后自动退出，锁屏。

(7) 设置 Bash 保留历史命令的条数。

```
#cat /etc/profile|grep HISTSIZE= 内存中保留的历史命令的数量
#cat /etc/profile|grep HISTFILESIZE= 写入历史文件的命令数量
#nano /etc/profile
```

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

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，如图 3-6 所示。

使用命令开启 sshd 服务：

```
#service sshd start
```

图 3-6　查看 sshd 服务

(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
#nano /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
#nano /etc/ssh/sshd_config
```

设置 PermitRootLogin 为 no，如图 3-7 所示。

图 3-7 设置禁止 root 远程登录

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 到 root。

(4) 限定信任主机。

检查方法:

```
#cat /etc/hosts.allow  查看允许登录服务器的主机 IP 地址或 IP 地址段
#nano /etc/hosts.allow  编辑删除不允许登录的主机 IP 地址
```

(5) 防止误使用 Ctrl+Alt+Del 组合键重启系统。

```
#nano /etc/init/ control-alt-delete.conf  编辑文件
```

在行开头添加注释符号"#":

#exec shutdown -r now "Control-Alt-Delete pressed",如图 3-8 所示。

图 3-8 禁止使用 Ctrl+Alt+Del 组合键

(6) 资源限制。

对系统上所有的用户设置资源限制可以防止 DoS 类型攻击(denial of service attacks)如最大进程数、内存数量等。例如对所有用户的限制:

```
#nano /etc/security/limits.conf
```

* hard rss 5000 限制单个用户内存使用为 5MB

* hard nproc 20 限制单个用户可用的最大进程数为 20,如图 3-9 所示。

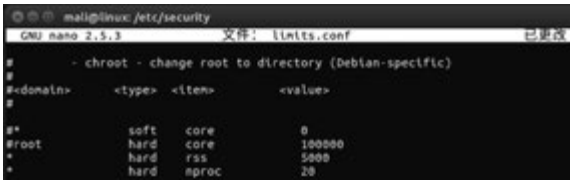

图 3-9 配置可使用的内存和最大进程数

3.1.3 Linux 下建议使用的常用网络服务应用程序

1. 文件传输

在 Linux 系统中,有许多不同的 FTP 工具可供选择,每个工具都有其独特的优势和

用途。

以下是一些常见的 FTP 工具以及它们的特点。

(1) vsftpd：vsftpd 是一个非常流行的 FTP 服务器程序，它非常安全和稳定，并具有高性能。它支持虚拟用户，可限制用户访问的目录，并提供许多配置选项。

(2) ProFTPD：ProFTPD 是另一个流行的 FTP 服务器程序，它具有高度可配置性和灵活性。它支持虚拟用户，具有强大的权限控制功能，并且可以通过模块进行扩展。

(3) Pure-FTPd：Pure-FTPd 是一个轻量级的 FTP 服务器程序，它具有简单的配置和易于使用的界面。它支持虚拟用户和匿名访问，并具有一些安全功能，如防止恶意攻击和破解密码。

(4) FileZilla：FileZilla 是一个流行的跨平台 FTP 客户端，它提供了用户友好的界面和易于使用的功能。它支持多个并发连接，具有文件传输队列和断点续传功能，并且可以通过插件进行扩展。

(5) lftp：lftp 是一个命令行 FTP 客户端，它具有丰富的功能和高级的自动化功能。它支持多线程文件传输，支持断点续传，可以进行脚本编写和自动化任务，并支持 FTP、FTPS 和 SFTP 协议。

2. 远程登录

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 和 UNIX 平台上有很多免费的客户端软件，如 Putty。Putty 是一个免费的开源软件，用户可以自由下载和使用，并且其源代码完全开放，用户可以对其进行修改和扩展。Putty 支持 SSH、Telnet、SCP (Secure Copy Protocol)和 SFTP(SSH File Transfer Protocol)等多种协议，使得用户可以通过不同的网络协议进行远程连接和管理。操作简单、配置灵活、体积小。支持多种加密协议，如 3DES、AES、Blowfish、DES 和 RC4。

3. 邮件服务器

Postfix：Postfix 是一个现代化的替代 Sendmail 的邮件传输代理(MTA)，设计简单、安全，易于配置和管理。它支持虚拟域、SASL 验证、TLS 加密等先进的特性，适合用于大规模邮件发送环境。

Qmail：Qmail 是另一种常用的 Sendmail 替代品，它提供了类似 Sendmail 的功能，但通常被认为更安全、更稳定。Qmail 的配置相对简单，适合中小型邮件服务器使用。

Exim：Exim 是一个广泛使用的邮件传输代理，支持多种操作系统和平台。它具有高度的可配置性和灵活性，适合需要高度定制的邮件服务器环境。

这些替代软件都能提供类似 Sendmail 的功能，但在安全性、稳定性和易用性方面各有优势，用户可以根据具体需求选择合适的替代软件。

4. sudo

sudo 命令的主要作用是允许系统管理员授权普通用户执行一些或全部的 root 命令。这意味着普通用户可以在权限范围内执行需要高级权限的操作，而不需要知道 root 用户的密码。sudo 命令通过 sudoers 配置文件来管理这些权限，允许系统管理员集中地控制哪些用户可以在哪些主机上执行哪些命令。sudo 的配置文件通常是/etc/sudoers，只有超级用户可以编辑。配置文件中定义了哪些用户和组可以执行哪些命令。sudo 命令常用于需要

高级权限的操作,如系统重启(reboot)、关机(halt)等。通过 sudo,系统管理员可以精细控制哪些操作由普通用户执行,从而提高系统的安全性和管理的便利性。

5. named

在 Linux 系统中,可以使用 named 命令来管理和配置 DNS 服务器。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>
```

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 到 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) 对于重要的信息,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) 去掉对操作并非至关重要又极少使用的程序。

(12) 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子目录和文件的名字,而用户仍可执行。

(13) 将系统软件升级为最新版本。

3.2 Windows 10 操作系统

Windows 10 作为微软推出的经典操作系统,其核心特点包括现代化的界面设计、卓越的兼容性、多层次安全防护及创新功能集成。该系统通过结合传统操作逻辑与新技术优化,在性能、多设备协同和用户体验方面展现出独特优势,是目前主流的操作系统之一。

Windows 10 共有家庭版、专业版、企业版、教育版、专业工作站版、物联网核心版 6 个版本。

3.2.1 Windows 10 的特点

(1) 生物识别技术。

Windows 10 所新增的 Windows Hello 功能带来一系列对于生物识别技术的支持。除了常见的指纹扫描之外,系统还能通过面部或虹膜扫描来让用户进行登录。

(2) 平板模式。

Windows 10 提供了针对触控屏设备优化的功能,同时还提供了专门的平板电脑模式,

开始菜单和应用都将以全屏模式运行。如果设置得当，系统会自动在平板电脑与桌面模式间切换。

(3) 多桌面。

如果用户没有多显示器配置，但依然需要对大量的窗口进行重新排列，那么 Windows 10 的虚拟桌面应该可以帮到用户。在该功能的帮助下，用户可以将窗口放进不同的虚拟桌面当中，并在其中进行轻松切换。使原本杂乱无章的桌面也变得整洁起来。

(4) 贴靠辅助。

Windows 10 不仅可以让窗口占据屏幕左右两侧的区域，还能将窗口拖曳到屏幕的四个角落使其自动拓展并填充 1/4 的屏幕空间。在贴靠一个窗口时，屏幕的剩余空间内还会显示出其他开启应用的缩略图，单击之后可将其快速填充到这块剩余的空间当中。

(5) 通知中心。

用户可以方便地查看来自不同应用的通知，此外，通知中心底部还提供了一些系统功能的快捷开关，比如平板模式、便签和定位等。

(6) 命令提示符窗口升级。

在 Windows 10 中，用户不仅可以对 CMD 窗口的大小进行调整，还能使用辅助粘贴等熟悉的快捷键。

(7) 新的 Edge 浏览器。

Edge 浏览器虽然尚未发展成熟，但它的确带来了诸多的便捷功能，比如和 Cortana 的整合以及快速分享功能。

(8) 计划重新启动。

在 Windows 10 中，系统会询问用户希望在多长时间之后进行重启。

(9) 兼容性增强。

只要能运行 Windows 7 操作系统，就能更加流畅地运行 Windows 10 操作系统。针对固态硬盘、生物识别、高分辨率屏幕等硬件都进行了优化支持与完善。

(10) 新技术融合。

在易用性、安全性等方面进行了深入的改进与优化。针对云服务、智能移动设备、自然人机交互等新技术进行融合。

3.2.2　Windows 10 的安全配置

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。设置账户已禁用，如图 3-10 所示。

2. 管理员账号改名

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，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 3-11 所示。

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，

图 3-10　设置 Guest 账户禁用

图 3-11　修改 Administrator 账号

什么事也干不了的那种,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,并且可以借此发现它们的入侵企图。可以将该用户隶属的组修改成 Guests 组,如图 3-12 所示。

4. 安全策略

利用 Windows 10 的安全配置工具来配置安全策略,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 3-13 所示,可以配置安全策略:账户策略、本地策略、高级安全 Windows 防火墙、网络列表管理策略、公钥策略、软件限制策略等,在默认情况下,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“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,在弹出的右键菜单中选择“创建 IP 安全策略”命令,将弹出

图 3-12　修改用户隶属的组

图 3-13　安全策略界面

IP 安全策略向导，如图 3-14 所示。

（2）单击“下一步”按钮，填写名称“禁用 80 端口策略”，然后单击“下一步”按钮，继续下一步，点击完成。

（3）系统弹出“属性”对话框。取消右下角“使用添加向导”的勾选，再点击“添加”，弹出“新规则属性”对话框，点击“添加”，弹出“IP 筛选列表”，填写名称“禁用 80 端口”，单击“添加”，弹出“IP 筛选器属性”。

图 3-14 创建本地安全策略

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

(5) 在"新规则属性"对话框中,选中"禁用 80 端口",单击左侧的单选框,表示已经激活。在"筛选器操作"选项卡中,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",单击 "确定"。接着单击"新筛选器操作"左边的单选框,然后单击"关闭"。

(6) 最后进入"显示 80 端口属性",在"禁用 80 端口策略"左边打勾,按确定关闭对话框。鼠标右击"禁用 80 端口",然后选择"分配"。

6. 开启审核策略

安全审核是 Windows 10 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)的入侵的时候,都会被安全审核记录下来。很多管理员在系统被入侵了几个月都不知道,直到系统遭到破坏。表 3-2 的这些审核是必须开启的,其他的可以根据需要增加。

表 3-2 开启审核策略的设置

策 略	安 全 设 置
审核策略更改	成功,失败
审核登录事件	成功,失败
审核对象访问	成功,失败
审核进程跟踪	成功,失败
审核目录服务访问	成功,失败
审核特权使用	成功,失败

续表

策　　略	安 全 设 置
审核系统事件	成功,失败
审核账户登录事件	成功,失败
审核账户管理	成功,失败

审核策略在默认情况下都是没有开启的,如图 3-15 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 3-16 所示。

图 3-15　审核策略的默认设置

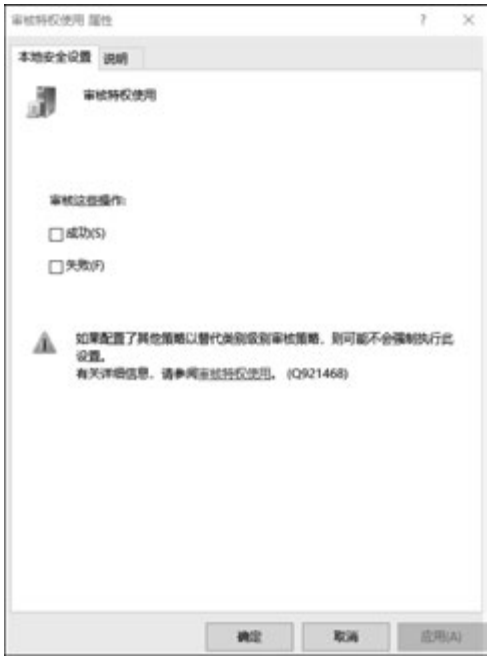

图 3-16　审核策略的设置

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,设置如图 3-17 所示,这部分包含以下四方面。

图 3-17 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。有效范围从 0 到 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 至 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,失败的密码尝试计入失败的登录尝试次数中。默认值为 0。

(3) 重置账户锁定计数器。

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 到 99 999 分钟之间。

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 到 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。

(4) 允许管理员账户锁定。此安全设置决定内置管理员账户是否受账户锁定策略约束。

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等,如图 3-18 所示。

(1) 放宽最小密码长度的原有限制。

此设置控制最小密码长度设置是否可以超出原有的限制 14,如果未定义此设置,则可将最小密码长度配置为不超过 14,如果已定义并禁用此设置,则可将最小密码长度配置为不超过 14,如果已定义并启用此设置,则可将最小密码长度配置为大于 14。

图 3-18　密码策略的设置

(2) 密码必须符合复杂性要求。

默认是已禁用,此安全设置确定密码是否必须符合复杂性要求。如果启用此策略,密码必须符合最低要求: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,至少有六个字符长。

密码必须包含以下四类字符中的三类:

英文大写字母(A～Z);

英文小写字母(a～z);

10 个基本数字(0～9);

非字母字符(例如 !、$、#、%)。

(3) 最小密码长度。

该安全设置确定了用户账户密码可以包含的最少字符数,此设置的最大值与放宽最小密码长度限制设置的值相关。如果未定义放宽最小密码长度限制设置,则可将此设置配置为 0 到 14。

(4) 密码最短使用期限。

此设置确定在用户更改某个密码之前必须使用该密码一段时间(以天为单位)。可以设置一个介于 1 和 998 的值,或者将天数设置为 0,允许立即更改密码。

(5) 密码最长使用期限。

此设置确定在系统要求用户更改某个密码之前可以使用该密码的期间(以天为单位)。可以将密码设置为在某些天数(介于 1 到 999)后到期,或者将天数设置为 0,指定密码永不过期。如果密码最长使用期限介于 1 和 999,密码最短使用期限必须小于密码最长使用期限。如果将密码最长使用期限设置为 0,则可以将密码最短使用期限设置为介于 0 和 998 的任何值。

注意:安全最佳操作是将密码设置为 30 到 90 天后过期,具体取决于你的环境。这样,攻击者用来破解用户密码以及访问网络资源的时间将受到限制。默认值:42。

(6) 强制密码历史。

此设置确定再次使用某个旧密码之前必须与某个用户账户关联的唯一新密码数。该值

必须介于0个和24个密码之间。此策略使管理员能够通过确保旧密码不被连续重新使用来增强安全性。默认值:在域控制器上为24。在独立服务器上为0。

(7) 用可还原的加密来存储密码。

此设置确定操作系统是否使用可还原的加密来存储密码。此策略为某些应用程序提供支持,这些应用程序使用的协议需要用户密码来进行身份验证。使用可还原的加密储存密码与存储纯文本密码在本质上是相同的。因此,除非应用程序需求比保护密码信息更重要,否则绝不要启用此策略。通过远程访问或Internet身份验证服务(IAS)使用质询握手身份验证协议(CHAP)验证时需要设置此策略。在Internet信息服务(IIS)中使用摘要式身份验证时也需要设置此策略。默认值:禁用。

(8) 最小密码长度审核。

此设置确定了发出密码长度审核警告事件的最小密码长度。可以设置为1到128。仅当尝试确定在环境中增加最小密码长度设置的潜在影响后,才能启用和配置此设置。如果未定义此设置,则不会发出审核事件。如果定义了此设置并且该设置小于或等于最小密码长度设置,则不会发出审核事件。如果定义了此设置并且该设置大于最小密码长度设置,且新账户密码的长度小于此设置,则会发出审核事件。

9. 关机时清除文件

页面文件也就是调度文件,是Windows 10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。一些第三方的程序可以把一些没有的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3-19所示。

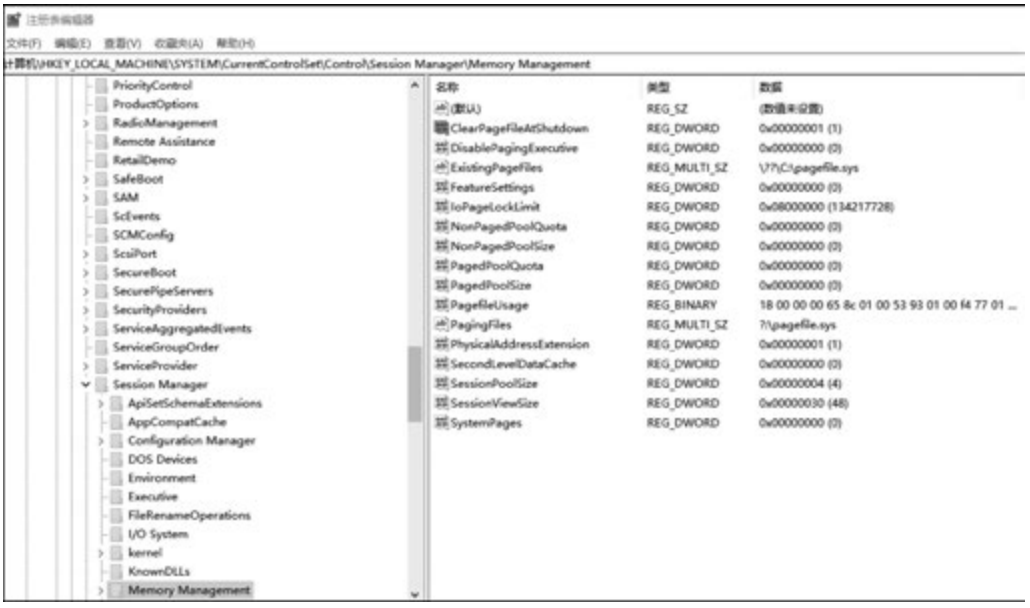

图3-19 关机时清除文件的设置

10. 拒绝网络病毒藏于临时文件中

现在 Internet 网络上的病毒疯狂肆虐，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，那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，我们可以按照下面的操作设置 Windows 10 系统的软件限制策略。

按 Win＋R 首先打开 Windows 10 系统的“运行”窗口，在弹出的系统运行对话框中，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，按右键选择“新建路径规则”命令，打开如图 3-20 所示的设置对话框；单击其中的“浏览”按钮，从弹出的文件选择对话框中选中 Windows 10 系统的临时文件夹，同时再将“安全级别”参数设置为“不允许”，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。

图 3-20　将“安全级别”参数设置为“不允许”

11. 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 10 服务器系统的运行稳定性，我们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。

(1) 以管理员身份登录进入 Windows 10 系统,在运行窗口输入字符串命令"gpedit.msc",按回车键后,进入对应系统的控制台窗口。

(2) 选中该控制台左侧列表中的"计算机配置"节点选项,并从目标节点下面逐一选择"Windows 设置"→"安全设置"→"高级安全 Windows Defender 防火墙"→"高级安全 Windows Defender 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。

(3) 按右键选择"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,单击"下一页"按钮再将"所有程序"项目选中,单击"下一页"按钮在协议类型列表中选中"ICMPv4",如图 3-21 所示。

图 3-21 在协议类型列表中选中"ICMPv4"

单击"下一页"按钮,选择此规则应用于任何 IP 地址,单击"下一页"按钮,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合的名称。完成上面的设置任务后,将 Windows 10 系统重新启动,Windows 10 系统以后就不会轻易受到来自外网的非法 ping 测试攻击了。

12. 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 10 系统的资源,最终达到搞垮服务器系统的目的,为此,在实际管理 Windows 10 系统的过程中,一旦我们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 10 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。

(1) 在 Windows 10 系统桌面中依次单击"开始"→"运行"选项,在弹出的系统运行对话框中输入"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。

（2）选中组策略控制台窗口左侧位置处的“用户配置”节点分支，并用鼠标逐一选择目标节点分支下面的“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 3-22 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 10 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 3-22　设置删除所有用户远程访问连接为“已启用”

13. 防火墙的设置

Windows 10 内置的防火墙可以对流经它的网络通信进行扫描，这样能够过滤掉一些攻击，以免其在目标计算机上被执行。其还可以关闭不使用的端口。而且它还能禁止特定端口的流出通信，封锁特洛伊木马。最后，它可以禁止来自特殊站点的访问，从而防止来自不明入侵者的所有通信。入侵者必须首先穿越防火墙的安全防线，才能接触目标计算机。管理员可以将防火墙配置成许多不同保护级别，从而保护主机系统不受安全威胁，防火墙设置如图 3-23 所示。

图 3-23　高级防火墙设置

习 题 3

一、填空题

1. 一套可以免费使用和自由传播的类 UNIX 操作系统是_____。

2. 在 Linux 系统中使用_____命令锁定账号。

3. 在 Ubuntu Linux 中,禁止普通用户 su 到 root,应编辑的文件是_____。

4. 在 Ubuntu Linux 中,修改账户登录失败锁定次数、锁定时间的设置,应编辑的文件是_____。

5. 在 Ubuntu Linux 中,为了防止 DoS 类型攻击(denial of service attacks),设置用户最大进程数、内存数量等,应编辑的文件是_____。

6. 在 Windows 10 中,所谓的陷阱账号是创建一个名为_____的本地账户,把它的权限设置成最低。

7. 在 Windows 10 中写出六个配置安全策略,它们是_____、_____、_____、_____、_____、_____。

8. 账户锁定策略包含_____、_____、_____、_____四方面的设置。

9. 密码策略包含_____、_____、_____、_____、_____、_____、_____、_____八方面的设置。

10. 禁止来自外网的非法 ping 攻击,运行界面输入的命令是_____。

二、操作题

1. Ubuntu Linux 操作系统的安全配置。

2. Windows 10 操作系统的安全配置。

三、简答题

1. 简述 sudo 命令的主要作用。

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。