第7章
Windows及Linux系统的安全

中国科学技术大学

曾凡平 billzeng@ustc.edu.cn

主要内容

7.1 计算机系统的安全级别

7.2 Windows 系统的安全防护

7.3 入侵Windows系统

7.4 Linux(Unix) 的安全防护

7.5 入侵Linux系统

7.1 计算机系统的安全级别

- 美国的**TCSEC (Trusted Computer System Evaluation Criteria-**《**受信计算机系统评测标准**》)是用于评估**ADP(Automatic Data Processing)**系统内建安全控制效率的标准。

- TCSEC的全称是“DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA”，发表于1985年12月26日，文档代号为DoD 5200.28-STD。这个119页的文档将信息系统的安全等级划分为D、C、B和A四个等级，C和B又分成多个子级。

TCSEC的四个级别

- D为最小保护(MINIMAL PROTECTION)级
- C为自主保护(DISCRETIONARY PROTECTION)，分成2个子级：
  - C1: 自主安全保护(DISCRETIONARY SECURITY PROTECTION)
  - C2: 受控的访问保护(CONTROLLED ACCESS PROTECTION)
- B为强制保护级(MANDATORY PROTECTION)，其下分3个子级：
  - B1: 标签式安全保护(LABELED SECURITY PROTECTION)
  - B2: 结构化保护(STRUCTURED PROTECTION)
  - B3: 安全域(SECURITY DOMAINS)
- A: 经过验证的保护(VERIFIED PROTECTION)，只定义了A1：
  - A1: 经过验证的设计(VERIFIED DESIGN)

关于TCSEC

- 从TCSEC的B2级到A1级，TCSEC要求所有对**受信计算基（TCB）**的更改必须由**配置管理**进行控制。受信系统的配置管理包括在开发、维护和设计过程中，对TCB所有更改的识别、控制、记录和审计。

- TCSEC的主要目的是为受信系统的开发者提供配置管理概念，及其在受信系统开发和生命周期中所需的指导。TCSEC也为其它系统开发者提供配置管理重要性及其实施方式的指导。

ITSEC和ISO 15408

- 欧洲四国（英、法、德、荷）提出了评价满足保密性、完整性、可用性要求的信息技术安全评价准则（ITSEC, Information Technology Security Evaluation Criteria）后，美国又联合以上诸国和加拿大，并会同国际标准化组织（ISO）共同提出信息技术安全评价的通用准则（CC for ITSEC），CC (Common Criteria) 已经被技术发达的国家承认为代替TCSEC的评价安全信息系统的标准。

- 1999年12月，ISO接受CC 2.0版为ISO 15408标准，并正式颁布发行。

ISO/IEC 15408——CC for ITSEC

- ISO/IEC 15408 permits comparability between the results of independent security evaluations. ISO/IEC 15408 does so by providing **a common set of requirements** for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. These IT products may be implemented in hardware, firmware or software.

- The evaluation process establishes a level of confidence that the security functionality of these IT products and the assurance measures applied to these IT products **meet these requirements.** The evaluation results may help consumers to determine whether these IT products fulfil their security needs.

GB 17859-1999
计算机信息系统安全保护等级划分准则

- GB 17859-1999是我国计算机信息系统安全保护等级划分准则强制性标准，该标准给出了计算机信息系统相关定义，规定了计算机系统安全保护能力的五个等级。
- 计算机信息系统安全保护能力随着安全保护等级的增高，逐渐增强。

- http://www.gb688.cn/bzgk/gb/index

物联网相关的国家标准

- http://www.gb688.cn/bzgk/gb/index
- 截至2019年10月21日，发布了61个物联网相关标准，其中9项为物联网相关标准。

序号	标准号	标准名称
1	GB/T 37714-2019	公安物联网感知设备数据传输安全性评测技术要求
2	GB/T 36951-2018	信息安全技术 物联网感知终端应用安全技术要求
3	GB/T 37024-2018	信息安全技术 物联网感知层网关安全技术要求
4	GB/T 37025-2018	信息安全技术 物联网数据传输安全技术要求
5	GB/T 37044-2018	信息安全技术 物联网安全参考模型及通用要求
6	GB/T 37093-2018	信息安全技术 物联网感知层接入通信网的安全要求
7	GB/T 35317-2017	公安物联网系统信息安全等级保护要求
8	GB/T 35318-2017	公安物联网感知终端安全防护技术要求
9	GB/T 35592-2017	公安物联网感知终端接入安全技术要求

Windows及Unix系统的安全级别：C2级

- 早在1995年7月，Windows NT的第一版带服务包3的NT3.5就取得了美国**TCSEC**(受信计算机系统评测标准)标准的C2安全级；Windows2000及其后续版本(如2003，vista，2008，Windows7, windows10)的基础安全体系结构比Windows NT更加健壮，其安全性也能达到C2级的标准。
- 一般认为，Unix系统 (包括Linux) 比Windows系统更安全，因此也达到了C2级别。
- **ITSEC** (Information Technology Security Evaluation Criteria) 组织的**E3**级别，其等同于**C2**级；

C2安全级的关键要求

- 达到C2安全级的**4项关键要求是**：
  - 要求系统实现**安全登录机制**、**自主访问控制机制**、**安全审计机制**和**对象重用保护机制**。
  - 其中后者(**对象重用保护机制**)就是残留信息的处理机制，即：阻止一个用户利用或阅读另一个用户已删除的数据，或访问另一个用户曾经使用并释放的内存。

Windows系统的安全机制

- NT序列的系统不仅实现了这些机制，同时还实现了两项B安全级的要求：
  - 一是**信任路径功能**，用于防止用户登录时被特洛伊木马程序截获用户名和密码；
  - 二是**信任机制管理**，支持管理功能的单独账号，例如，给管理员的分离账号、可用于备份计算机的用户账号和标准用户等。
- 当今流行的操作系统满足C2级的设计要求，然而由于实现、配置或用户使用等方面的原因，Windows和Unix仍然不能保证高的安全性，不可避免地会存在诸多脆弱性，从而可以被利用而危害信息系统的安全。

7.2 Windows 系统的安全防护

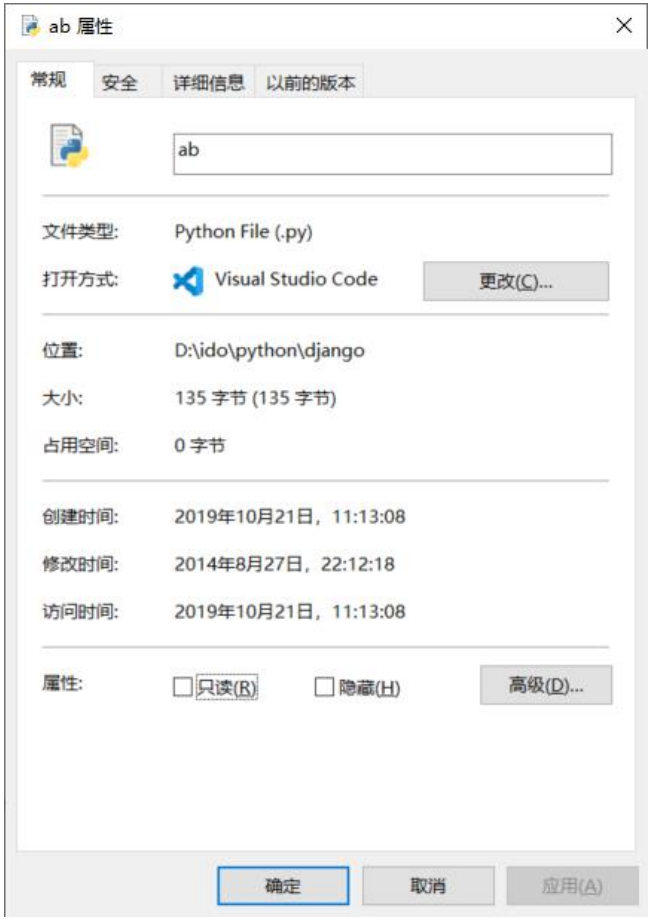
- Windows操作系统采用了符合C2安全等级的众多安全机制，其中最重要的有：
  1. 对象的保护机制
  2. 安全审计
  3. 用户管理安全机制
- 这些安全机制大多可以通过操作系统提供的“本地安全策略”进行配置。我们以Windows 2003为例，列举一些常用的安全防护措施。

1. 使用NTFS

- NTFS（NT文件系统）可以对文件和目录使用ACL（存取控制表），ACL可以管理共享目录的合理使用，而FAT（文件分配表）和FAT32却只能管理共享级的安全。

- 此外，通过ACL还可以设置用户以及组用户对于文件和目录的访问权限，如图7-1所示。

图7-1 文件和目录的访问权限



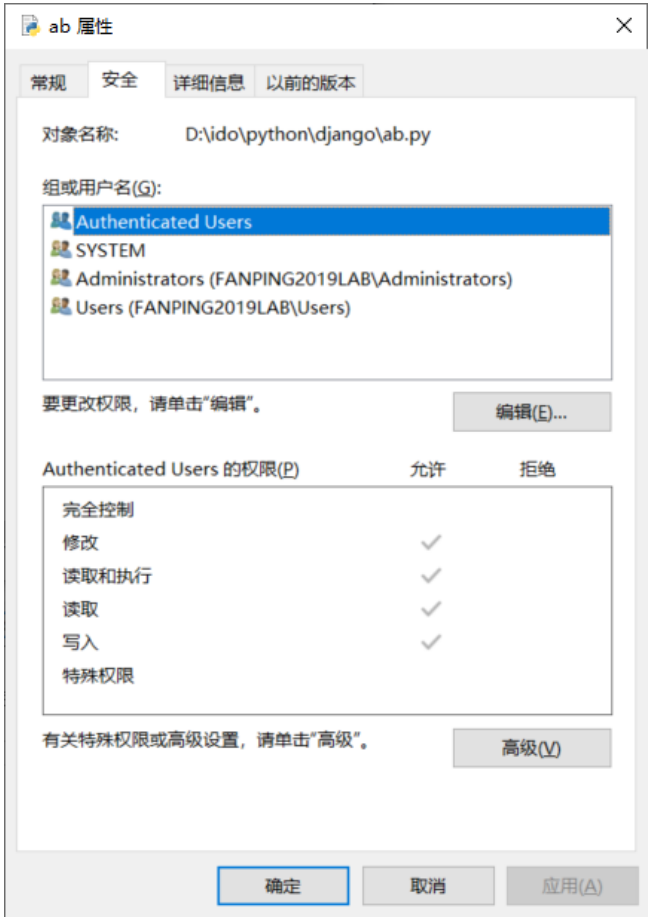
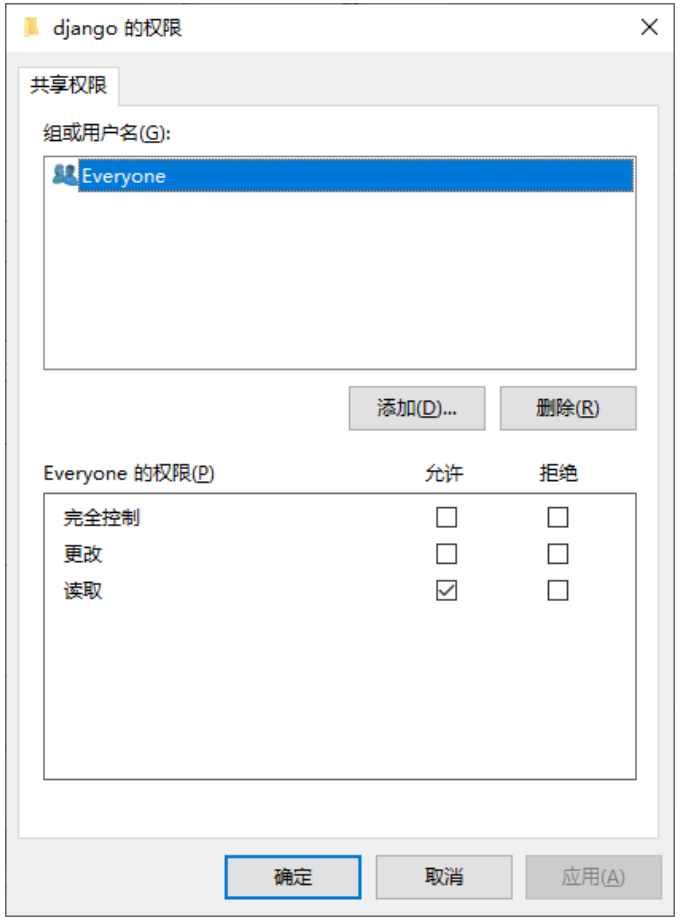


图7-2 对共享目录设置权限



2. 防止穷举法猜测口令

- 设置口令错误禁止账号机制：例如3次口令输入错误后就禁止该账号登录。
- **将系统管理员账号的用户名由原先的“Administrator”改为一个无意义的字符串。**这样企图入侵的非法用户不但要猜准口令，还要先猜出用户名，这样就大大的增大了口令攻击的难度。
- 用于提供Internet服务的公共计算机不需要也不应该有除了系统管理用途之外的其它用户账号。因此，应该废止Guest账号，移走或限制所有的其它用户账号。
- 封锁联机系统管理员账号。这种封锁只对由网络过来的非法登录起作用，账号一旦被封锁掉，系统管理员还可以通过本地登录重新设置封锁特性。

3.使用高强度的密码（口令）

- 密码是防止非法登陆到Windows系统的第一道关卡，用户应该选用不容易被猜测的密码，以防止密码攻击。用户选择的密码应该包含字母、数字、特殊符号等。
- 密码应该在隔一段时间后更换。如果长时间不改变密码，则非法用户有足够的时间试探密码或通过窥视你击键动作来猜测密码。
- 不同的系统使用不同的密码。如果多个资源共享一个密码，则一旦某个系统密码被泄露，所有的资源都会受到威胁。

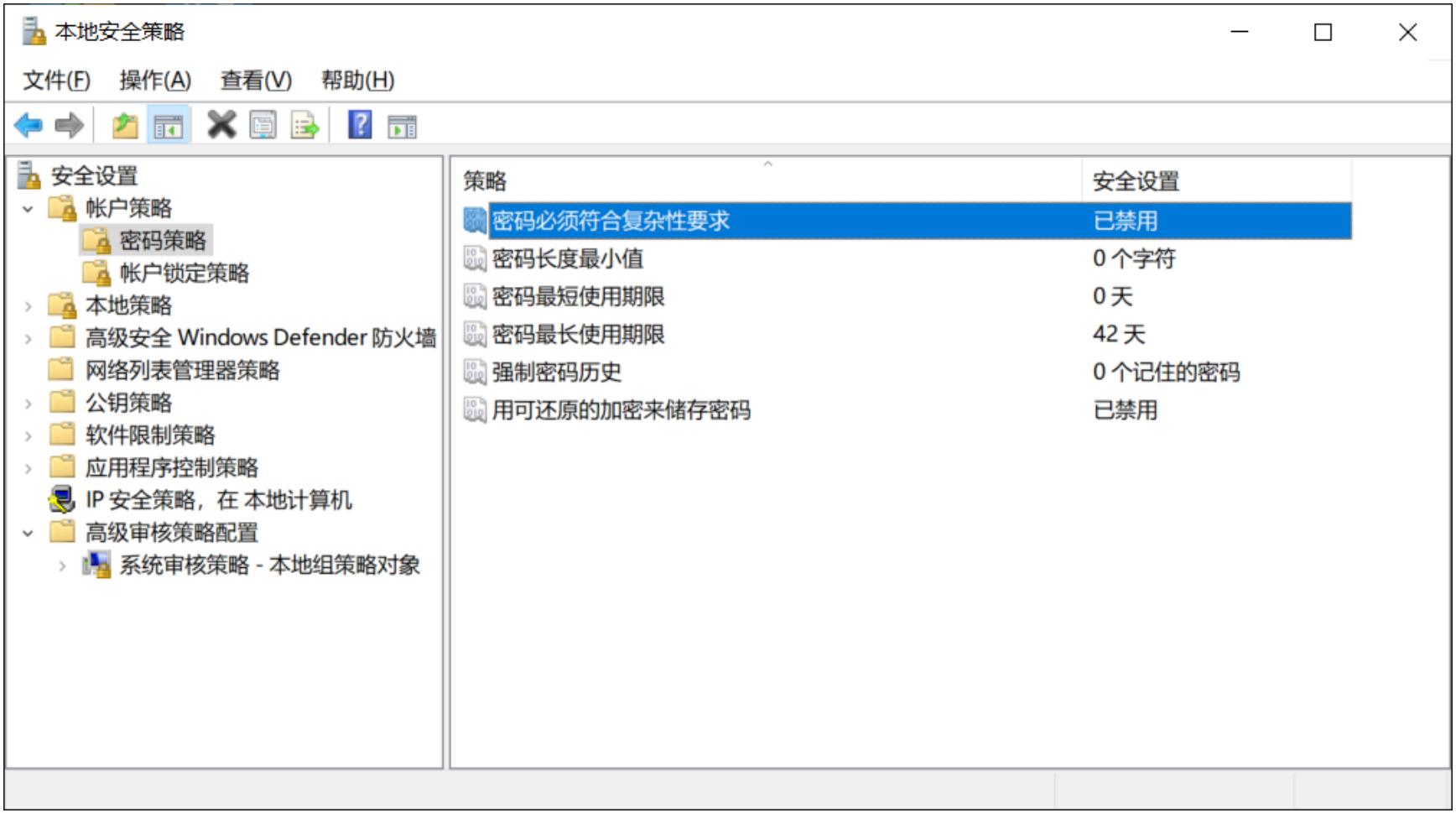


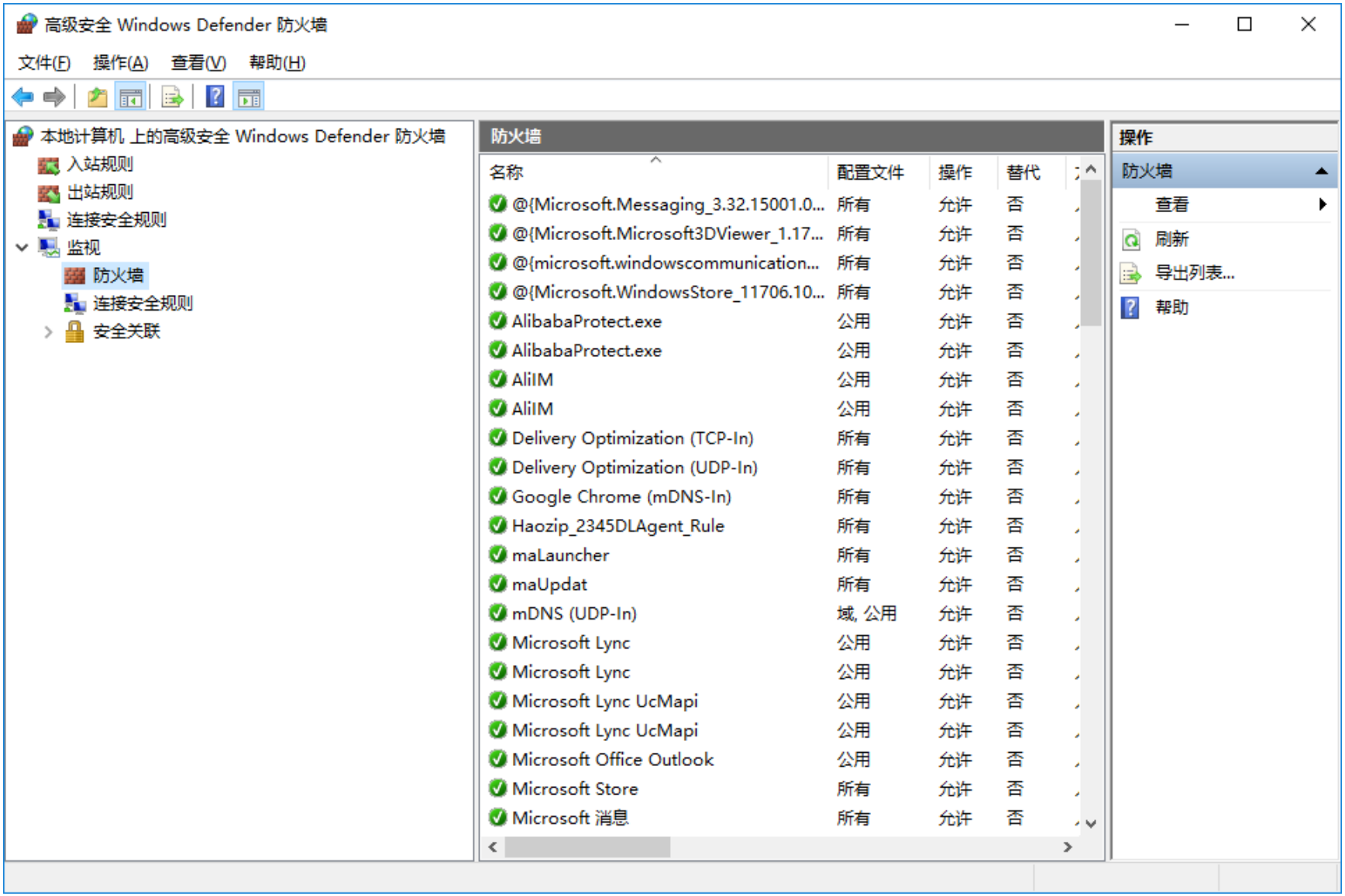
图7-4 激活“密码必须符合复杂性要求”

用户选择密码应避免以下情况

- (1) **纯数字的密码**。特别是123456、或者888888这样的数字，过短的密码显然是不安全的。
- (2) **以你或者有关人的相关信息构成的密码**。比如生日、电话、学号、姓名的拼音或者缩写、单位的拼音或者英文简称等等。
- (3) **长时间不变的密码**。非法用户有足够的时间试探密码或通过窥视你击键动作来猜测密码。
- (4) **多个资源共享一个密码**。这是一种把所有鸡蛋都放在一个篮子里的情况，一旦你的一个密码泄露，你所有的资源都受到威胁。

4. 正确设置防火墙

Windows 10的防火墙和网络保护



Windows10 中的防火墙设置

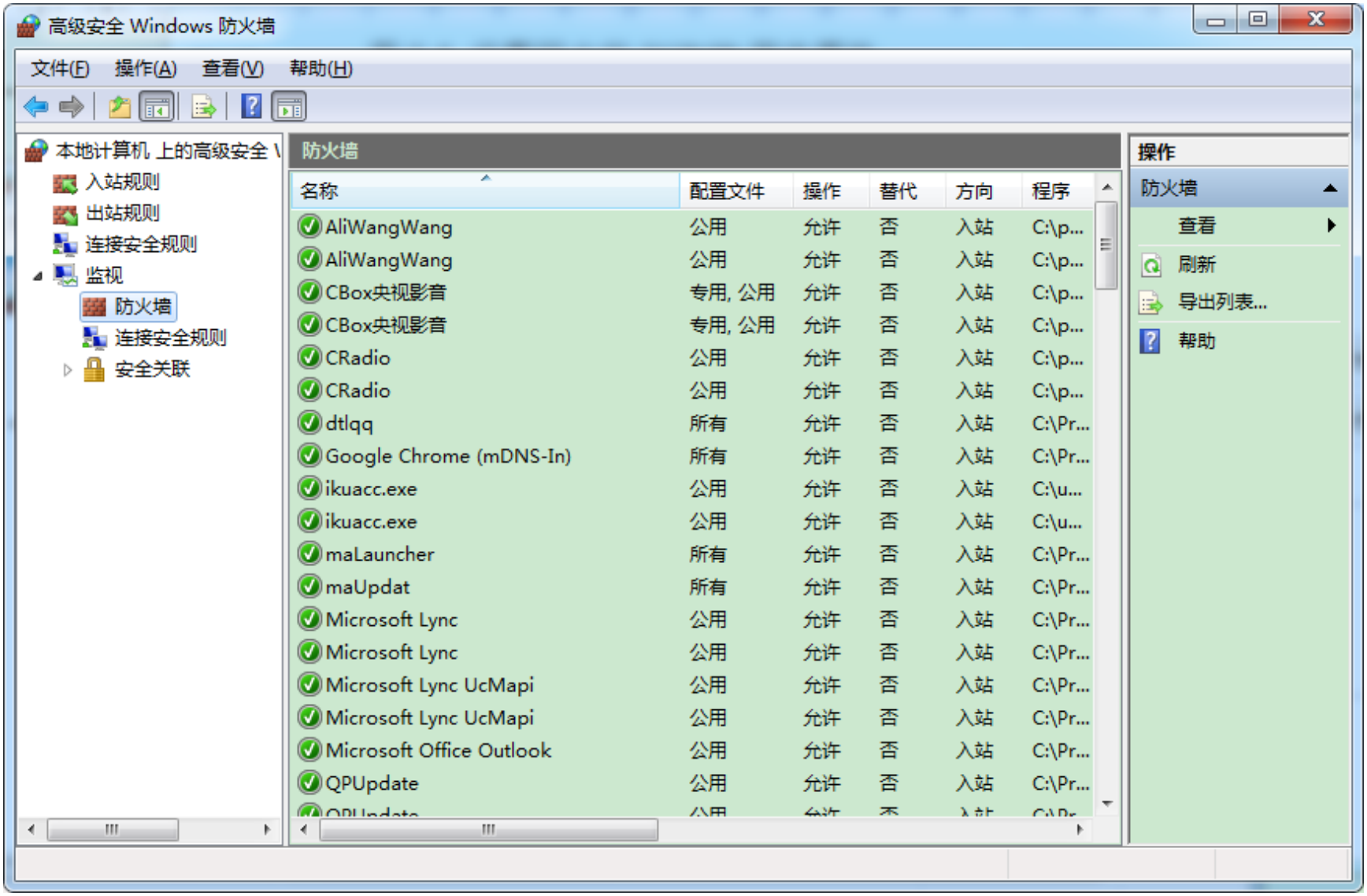


图7-6 Windows7和Windows8中的防火墙设置

在Windows2003中，正确设置网卡的TCP/IP筛选属性

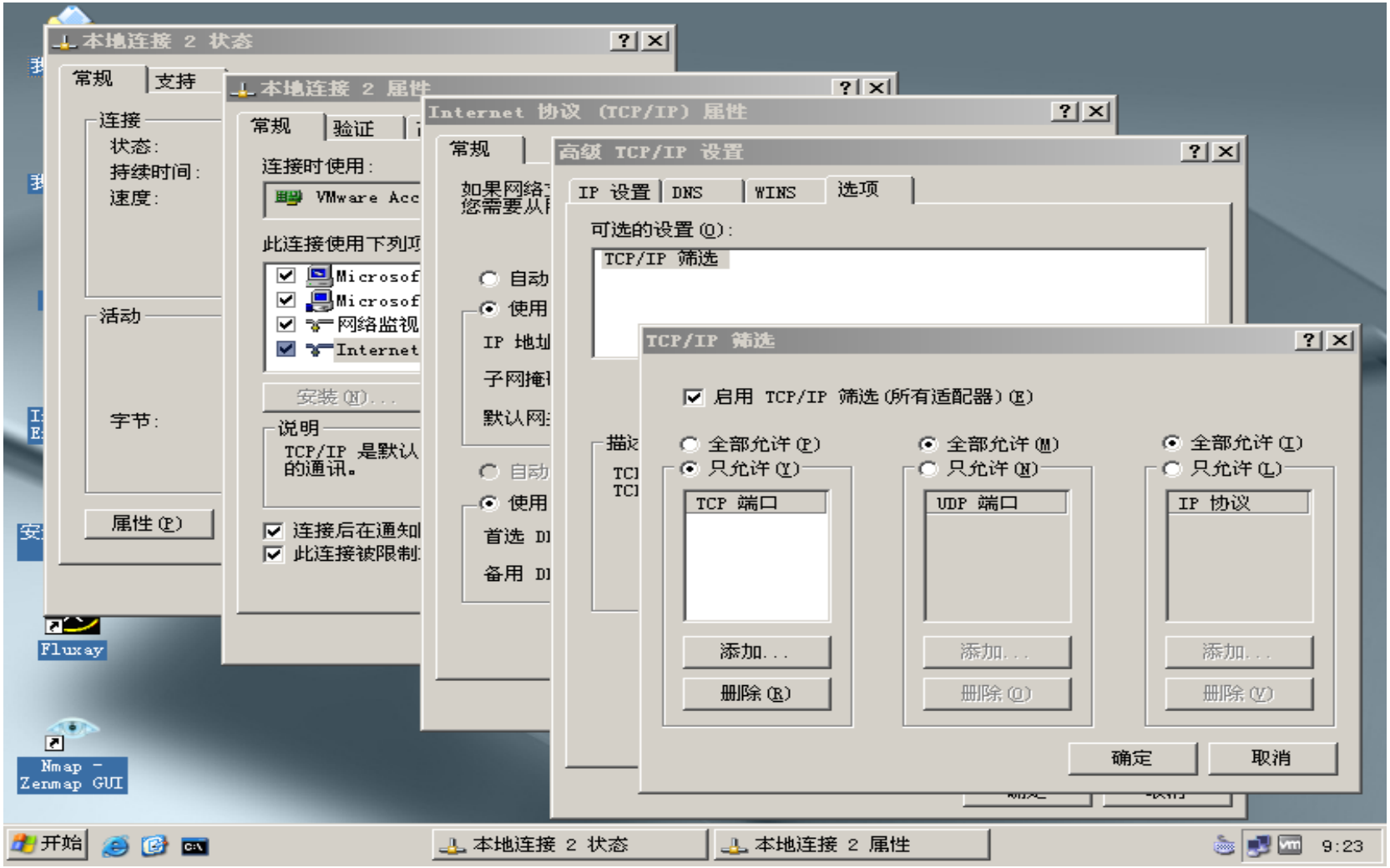


图7-5 设置网卡的TCP/IP筛选属性

5. 路由和远程访问中的限制

- Windows2003除了设置网卡属性外还有两处可以进行网络上的限制：一个是路由和远程访问，另一个是IPSEC的安全策略。其中第二种方法太麻烦而且设置比较复杂。
- 通过路由和远程访问可以实现基于包过滤的防火墙(Windows2003)，如图7-7所示。

演示（禁止ICMP）

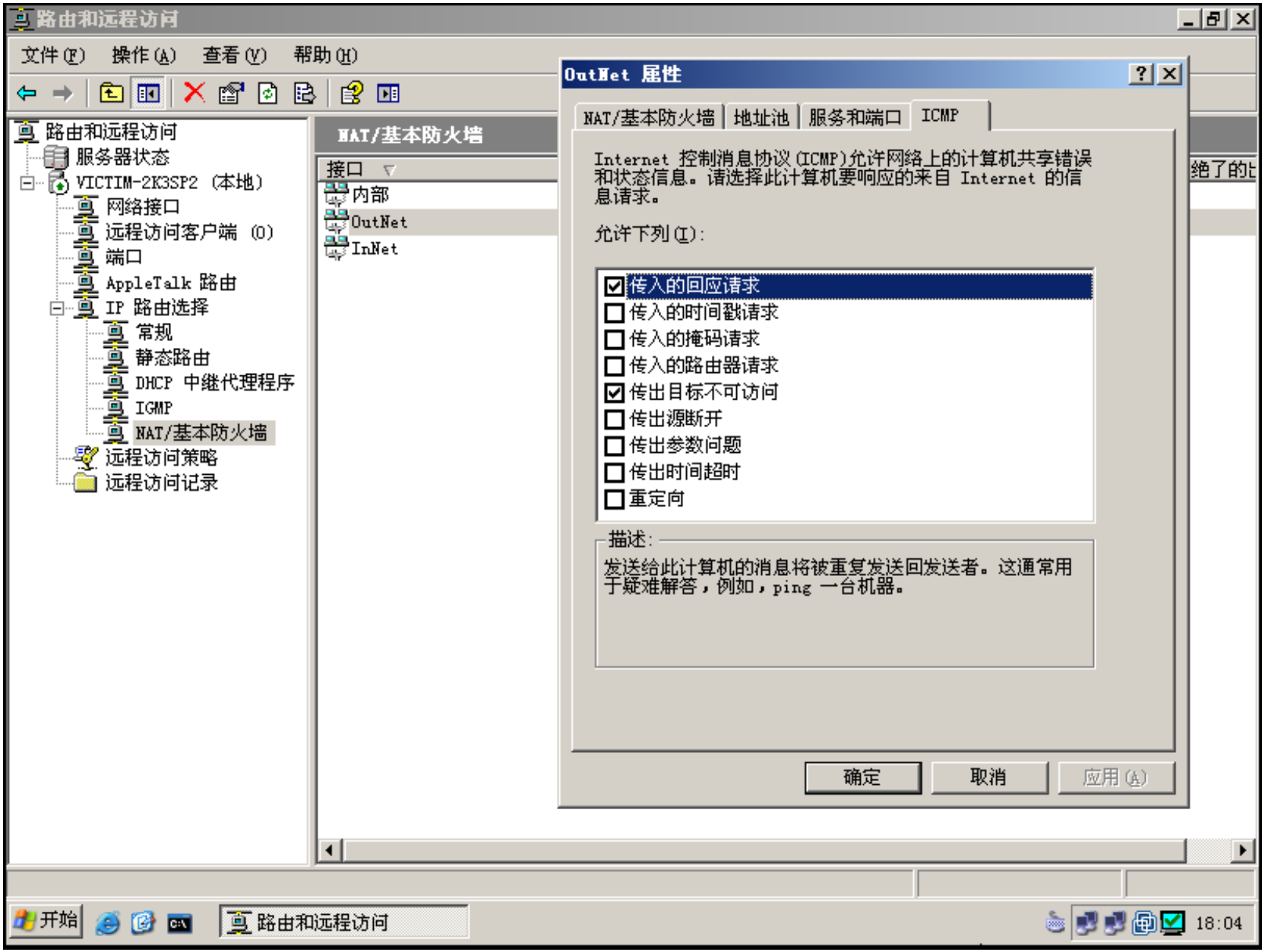

路由和远程访问
文件(F) 操作(A) 查看(V) 帮助(H)
路由和远程访问
服务器状态
VICTIM-2K3SP2 (本地)
网络接口
远程访问客户端 (0)
端口
AppleTalk 路由
IP 路由选择
常规
静态路由
DHCP 中继代理程序
IGMP
NAT/基本防火墙
远程访问策略
远程访问记录
NAT/基本防火墙
接口
内部
OutNet
InNet
OutNet 属性
NAT/基本防火墙
地址池
服务和端口
ICMP
Internet 控制消息协议(ICMP)允许网络上的计算机共享错误和状态信息。请选择此计算机要响应的来自 Internet 的信息请求。
允许下列(I):
传入的回应请求
传入的时间戳请求
传入的掩码请求
传入的路由器请求
传出目标不可访问
传出源断开
传出参数问题
传出时间超时
重定向
描述:
发送给此计算机的消息将被重复发送回发送者。这通常用于疑难解答，例如，ping 一台机器。
确定
取消
应用(A)
开始
路由和远程访问
18:04

图7-7 正确设置防火墙

6. 系统安全策略

- Windows 2003提供了许多本地安全策略，然而许多策略是默认禁用的，用户可以根据需要启用合适的安全策略。比如可以通过“用户权限分配”中的“禁止本地登录”选项禁止用户从本地登录，如图7-8所示。

演示（windows2003）

（禁止从本地登录）

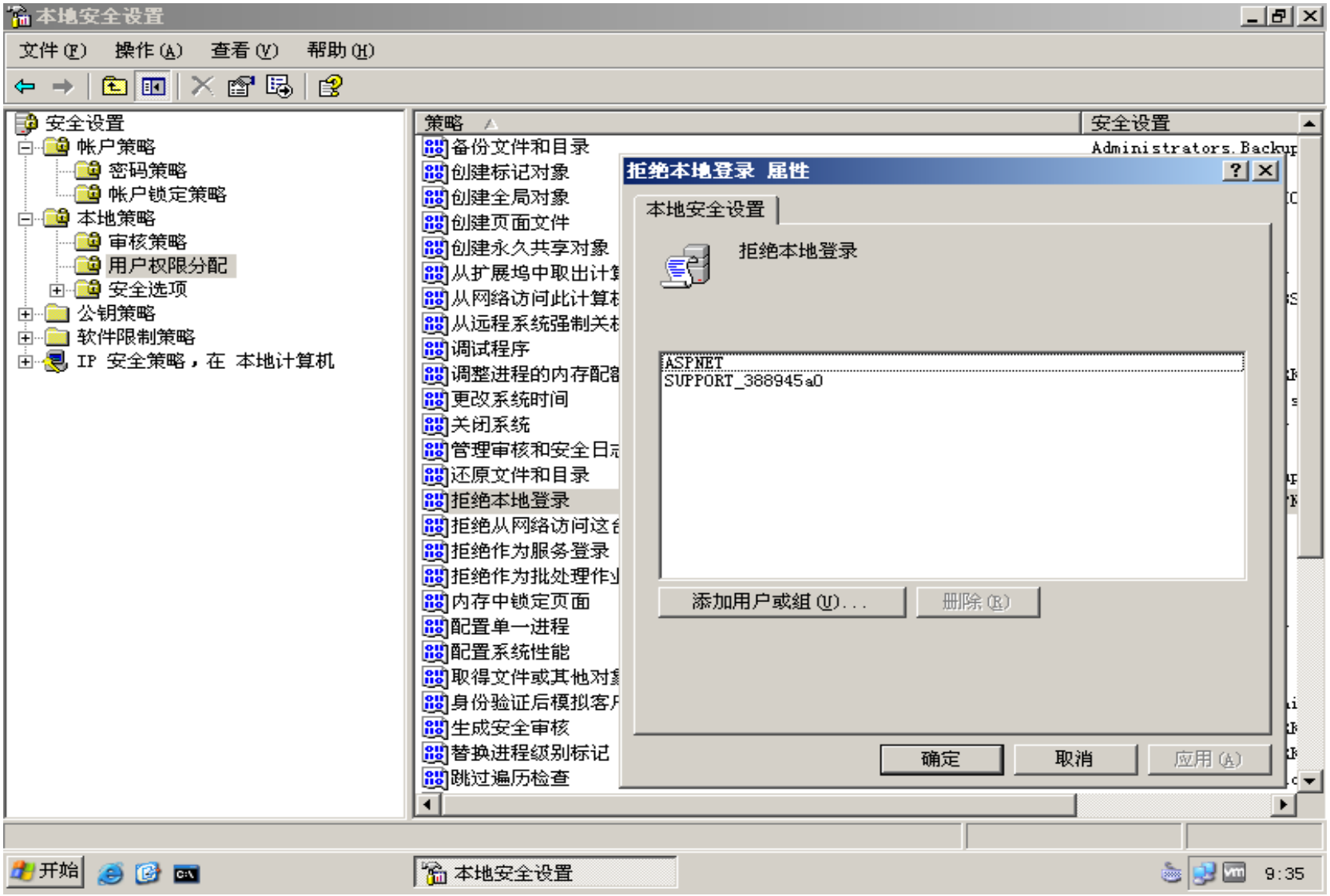


图7-8 拒绝某些用户从本地登录

7.重要文件的权限设置

- 默认情况下很多文件是每个人都可以访问的。为了提高安全性，对于一些容易被攻击者利用的文件应该严格设置它的访问权限。比如cmd.exe是远程缓冲区溢出攻击后经常要执行的可执行文件，应该设置权限以禁止普通用户执行，如图7-9所示。

演示（Windows2003）

（禁止CMD）

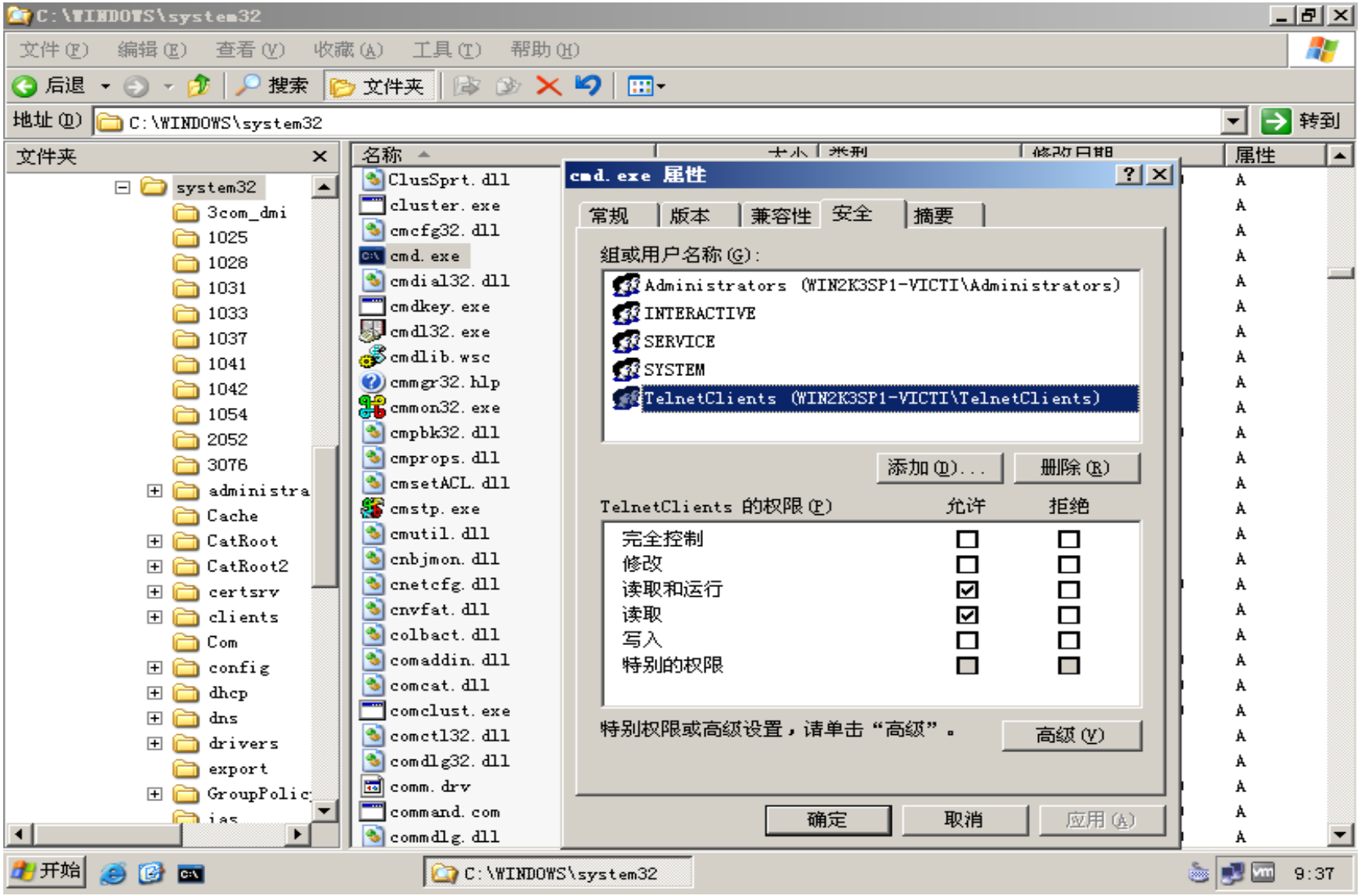


图7-9 正确设置重要文件的权限

8. 安装第三方安全软件，及时打上补丁

- 开通操作系统提供的自动更新服务，以便及时打上漏洞补丁。
- 还有就是安装第三方安全软件，比如腾讯电脑管家、金山毒霸、360安全套件等。尽量选择国产软件，因为国产安全软件更切合国人的工作习惯，且技术水平不比国外软件差。

9. 断开重要的工作主机与外部网络的连接

- 这是最安全的、也是最无奈的方法。如果实在无法做到物理隔离，可以考虑以下方法：

(1)用路由器隔离内部网络与外部网络；

(2)用(VMWare或VirtualBox)虚拟机访问互联网；

(3)主机设置访问控制：

1) 禁止访问互联网
2) 禁止USB端口（禁用U盘）
3) 设置内部ftp以分享资料。

Windows 10 安全性概述

- Windows 10 旨在抵御各种攻击平台上的已知安全威胁和新兴安全威胁。Windows 10 执行的安全性工作有三大类：

(1) 身份标识和访问控制

- 已进行了大幅度地扩展，从而简化和增强用户身份验证的安全性。这些功能包括 Windows Hello 和 Microsoft Passport，它们能更好地通过易于部署和易于使用的多因素身份验证 (MFA) 保护用户身份。另一个新增功能是 Credential Guard，该功能使用基于虚拟化的安全 (VBS) 来帮助保护 Windows 身份验证子系统和用户凭据。

(2) 信息保护

- 即保护闲置信息、使用的信息，以及传输的信息。
- 除了 BitLocker 和 BitLocker To Go 可用于保护闲置数据外，Windows 10 还包括具有企业数据保护的文件级加密，该功能不仅可用于执行数据分离和包含，还可以在退出公司网络后对数据进行加密（如果将该功能与 Rights Management Services 结合使用）。
- Windows 10 还可以使用虚拟专用网络 (VPN) 和 Internet 协议安全来帮助保护数据安全。

(3) 防恶意软件

- 包括可以使关键的系统和安全组件免遭威胁的体系结构更改。
- Windows 10 中有几项新功能可帮助减轻由恶意软件造成的威胁，包括 VBS、Device Guard、Microsoft Edge 和全新版本的 Windows Defender。
- 此外，来自 Windows 8.1 操作系统的许多反恶意软件功能（包括用于应用程序沙盒的 AppContainers，以及大量启动保护功能，如受信任启动）已在 Windows 10 中得到了沿用和改进。
- 详情见以下链接：

  https://technet.microsoft.com/zh-cn/library/mt601297(v=vs.85).aspx

7.3 入侵Windows系统

- 虽然Windows系统的设计符合C2安全级别的要求，但是由于系统是由人设计的，不可能完全避免错误；同时，在系统配置和使用过程中也可能存在失误。所以，存在入侵Windows系统的可能。

- 在此介绍几种入侵Windows系统的常用方法。

7.3.1 口令破解

- 破解口令是攻击Windows系统最常见的方法之一。只要能获得一个有效的用户名/口令字组合，则能在目标系统中获得一个立足点，以发起其它攻击。口令的破解利用了社交工程和心理学。
- **据统计，拥有最高权限的 Administrator 账户的口令字是很少被修改的**，不仅如此，有不少系统管理员还会把同样的口令字用在多个不同的服务器以及他们自己的工作站上。供数据备份工作使用的账户和各种服务账户的口令字被频繁修改的可能性也不大。这些账户都有着相当高的权限，口令字却不经常修改，所以是“猜测口令字”攻击的理想目标。

口令破解

- 另外，很多人喜欢用与自己相关的信息作为密码，比如：生日、身份证号的后6位、学号或工资号、实验室门牌号、电话号码等。从安全的角度考虑，尽量避免使用这些密码。
- 以人工方式猜测密码比较耗时费力，为此可以将常用的“用户名/密码”的组合存入一个文件，再利用操作系统的命令或工具自动进行破译，这种攻击方式称为字典攻击。字典攻击的关键在于建立高效的密码字典。NAT(NetBIOS Auditing Tool), SMBGrind, enum是Windows环境的著名密码破解工具。

7.3.2 利用漏洞入侵Windows系统

- 漏洞通常指可以被利用的目标系统缺陷。由于软件是人设计的，操作系统和运行其上的应用软件不可避免地存在许多漏洞。利用漏洞入侵windows系统是最基本的入侵方法。
- Windows系统由于其很高的市场占有率，其安全漏洞的挖掘和利用一直是黑客和特权部门关注的焦点。截至2019年10月21日，“绿盟科技”的漏洞库(http://www.nsfocus.net)收集了6889条windows系统及应用软件的漏洞，其中602个远程进入系统类漏洞，5851个本地越权漏洞。 。由此可见，可被利用的漏洞是非常多的。

入侵实例：中文版输入法漏洞入侵

- Windows2000简体中文版存在着输入法漏洞，可以使本地用户绕过身分验证机制进入系统内部。
- 经测试，利用远程桌面连接到Windows2000简体中文版的终端服务时仍然存在这一漏洞，因此这一漏洞使终端服务成为Windows2000的木马。也就是说，远程用户可以利用该漏洞进入系统。

- 下面介绍利用该漏洞的几个步骤。

(1) 获得管理员账号

- 先对一个网段进行扫描，扫描端口设为3389，运行客户端连接管理器(远程桌面)，将扫描到的任一地址加入，设置好客户端连接管理器，然后与服务器连结。几秒钟后，屏幕上显示出Windows2000登录界面（如果发现是英文或繁体中文版则无法入侵），**用Ctrl+Shift键快速切换输入法至“全拼”**，这时在登录界面左下角将出现输入法状态条（如果没有出现，请耐心等待，因为数据在网络上传输需要时间）。

- 然后右键点击状态条上的微软徽标，弹出“帮助”（如果发现“帮助”呈灰色，放弃，因为对方可能已经修补这个漏洞），打开“帮助”一栏中“操作指南”，在最上面的任务栏点击右键，会弹出一个菜单，打开“跳至URL”。此时将出现Windows2000的系统安装路径和要求我们填入的路径的空白栏。比如，该系统安装在C盘上，就在空白栏中填入“c:\winnt\system32”。

- 然后按“确定”，于是我们就**成功地绕过了身份验证，进入了系统的SYSTEM32目录**。

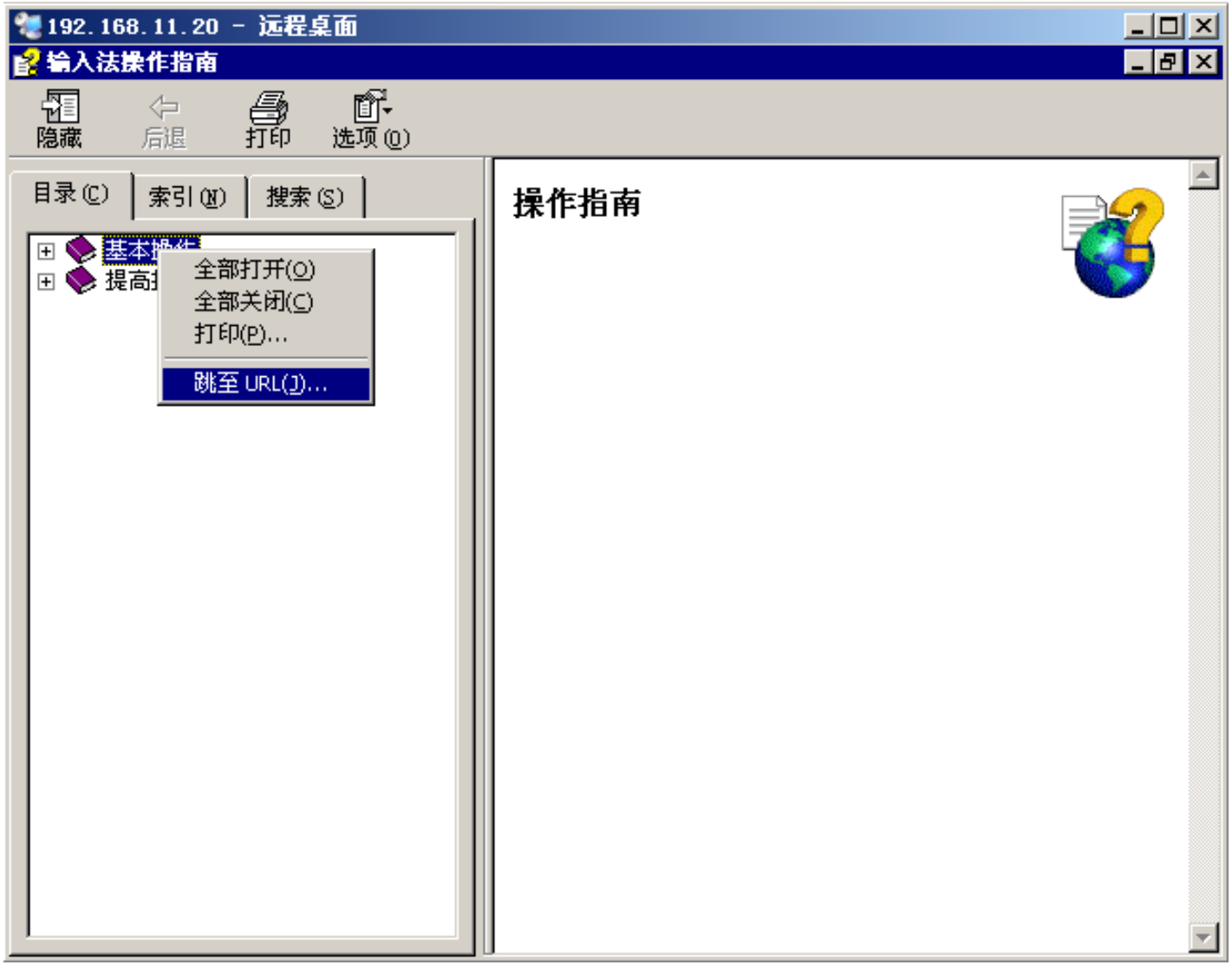
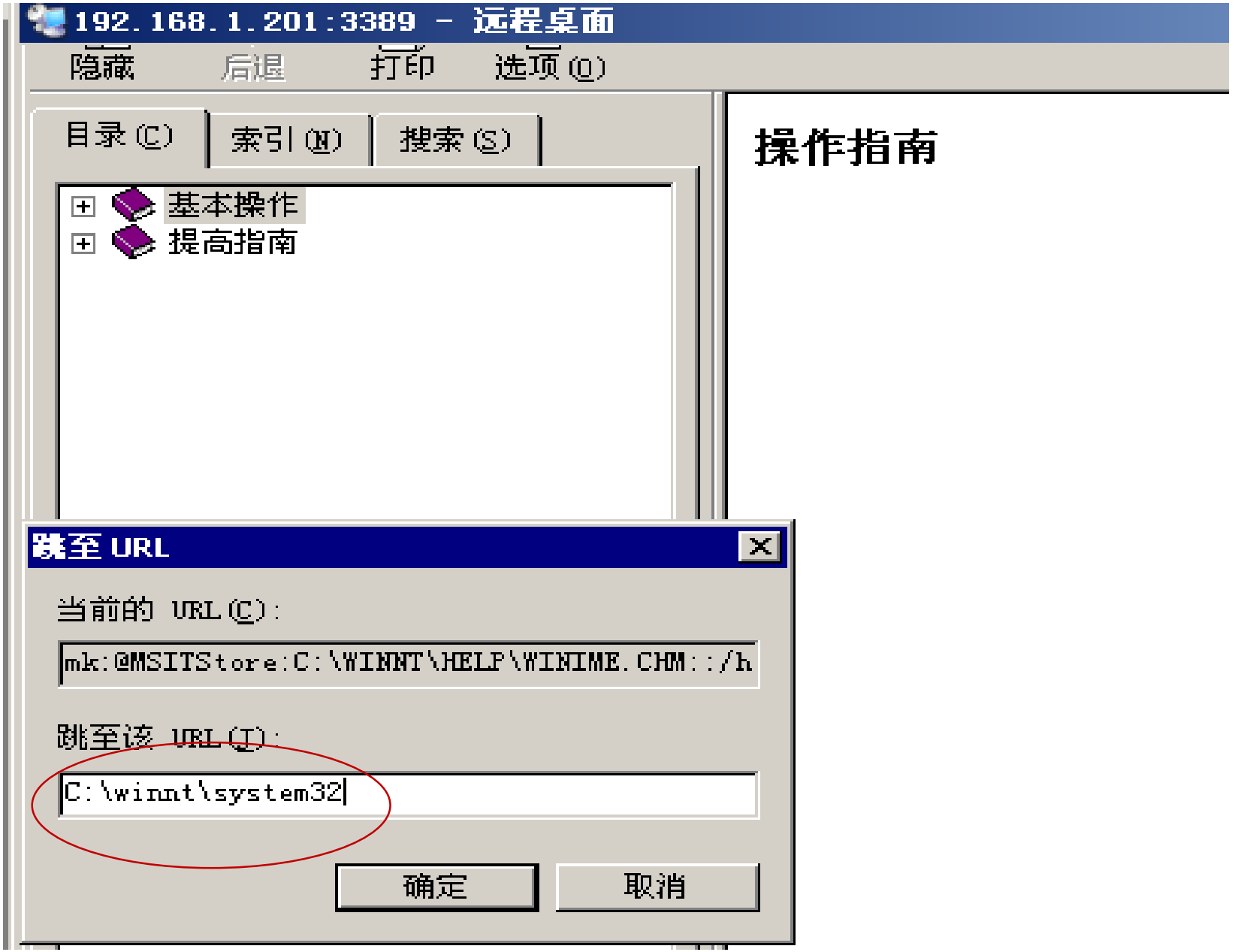


图7-10 打开“跳至URL”


192.168.1.201:3389 - 远程桌面
隐藏
后退
打印
选项(O)
目录(C)
索引(N)
搜索(S)
基本操作
提高指南
操作指南
跳至 URL
当前的 URL(C):
mk:@MSITStore:C:\WINNT\HELP\WINIME.CHM::/h
跳至该 URL(J):
C:\winnt\system32
确定
取消

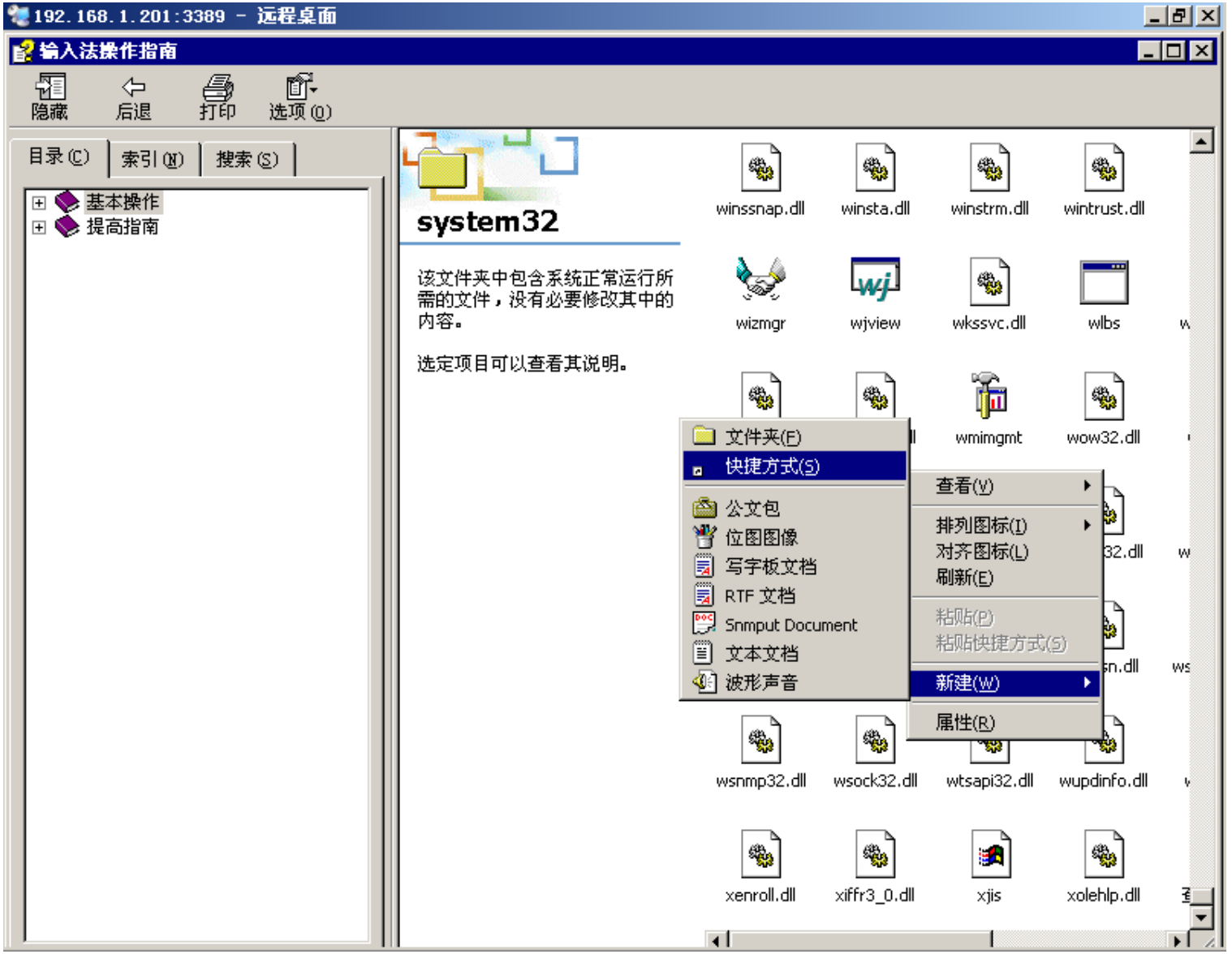


图7-11 绕过Windows2000的身份验证，进入系统的SYSTEM32目录

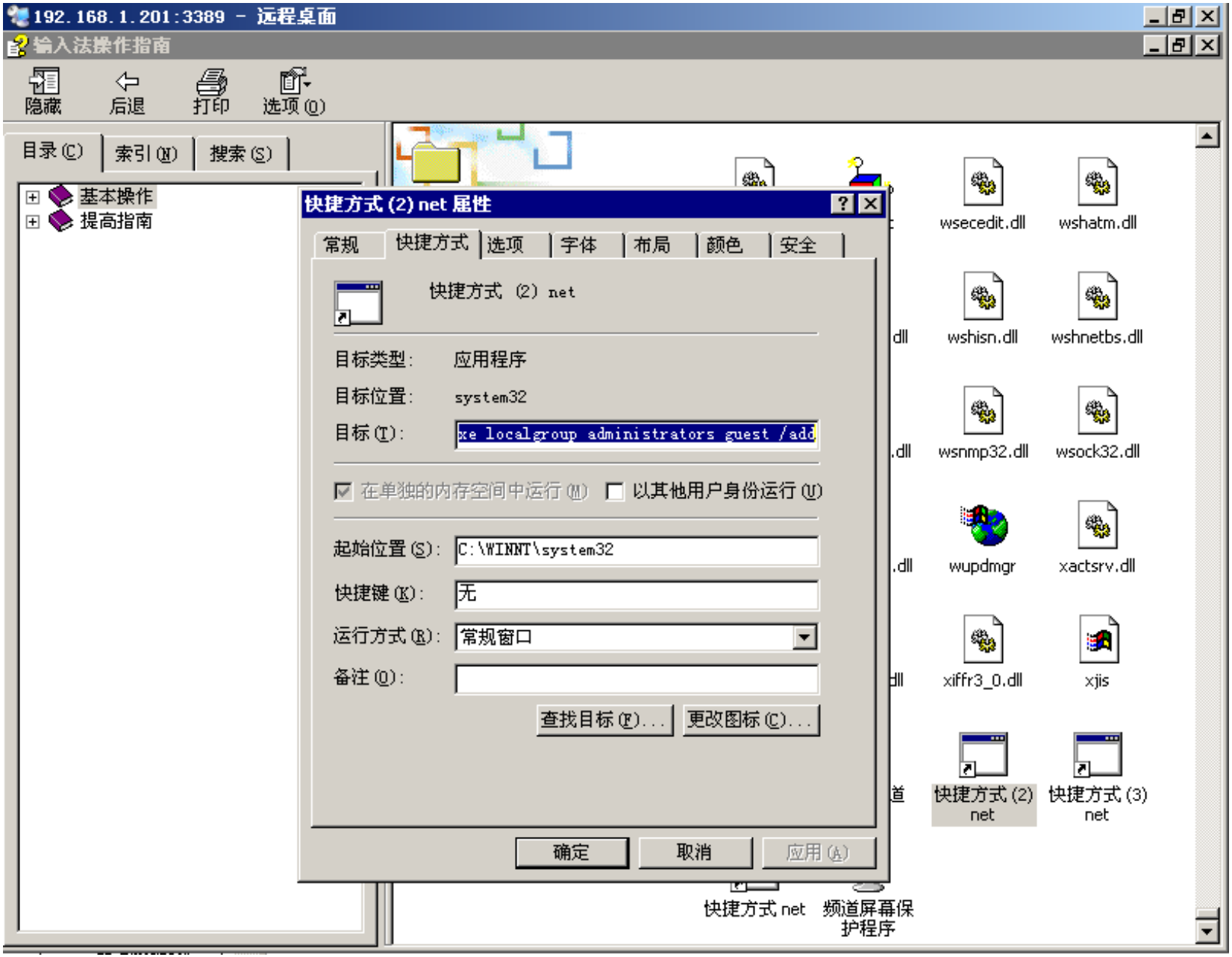
获得一个账号

- 现在我们要获得一个账号，成为系统的合法用户。在该目录下找到“net.exe”，为“net.exe”创建一个快捷方式，右键点击它，在“属性”—“目标”—c:\winnt\system32\net.exe后面空一格，填入“**user guest /active:yes**”点“确定”。

- 这一步骤目的在于用net.exe激活被禁止使用的guest账户，当然也可以利用“user 用户名　密码 / add”，创建一个新账号，但容易引起网管怀疑。

- 运行该快捷方式，此时你不会看到运行状态，但guest用户已被激活。然后又修改该快捷方式，填入“user guest 密码”，运行(open)，于是guest便有了密码。

- 最后，再次修改，填入”localgroup administrators guest /add”，将guest变成系统管理员。


192.168.1.201:3389 - 远程桌面
输入法操作指南
隐藏
后退
打印
选项(O)
目录(C)
索引(N)
搜索(S)
基本操作
提高指南
快捷方式 (2) net 属性
常规
快捷方式
选项
字体
布局
颜色
安全
快捷方式 (2) net
目标类型: 应用程序
目标位置: system32
目标(T): xe localgroup administrators guest /add
在单独的内存空间中运行(M)
以其他用户身份运行(U)
起始位置(S): C:\WINNT\system32
快捷键(K): 无
运行方式(R): 常规窗口
备注(O):
查找目标(F)...
更改图标(C)...
确定
取消
应用(A)
wsecedit.dll
wshatm.dll
wshisn.dll
wshnetbs.dll
wsnmp32.dll
wsock32.dll
wupdmgr
xactsrv.dll
xiffr3_0.dll
xjis
快捷方式 (2) net
快捷方式 (3) net
快捷方式 net
频道屏幕保护程序

(2) 创建跳板：

- 登录终端服务器，以”guest”身份进入，此时guest已是系统管理员，拥有一切权限。
- 可以做你任何想做的事，至此，你已经拥有一台跳板机。

(3) 扫除脚印

- 删除为net.exe 创建的快捷方式，删除winnt\system32\logfiles下的日志文件。

7.3.3 利用黑客工具进行入侵

- 互联网上有很多免费的黑客工具，可以用来入侵有漏洞的目标操作系统。一般而言，当一个漏洞被公布以后，在几周之内就会出现免费的漏洞利用工具。
- 为了保证系统的安全，及时为系统打上补丁是非常重要的。
- 例如：MSRPC漏洞利用工具

  演示：用Kaht2.exe入侵windows2000

演示：用Kaht2.exe入侵windows2000

- Kaht2是针对MSRPC（微软远程过程调用）的DCOM（分布式组件对象模型）漏洞的黑客利用工具。如果Kaht2扫描到一个有漏洞的目标系统(windows2000)，就会在攻击者的机器上获得一个以**SYSTEM权限**运行的命令行窗口。
- 从 http://www.securityfocus.com/bid/8205/exploit 可以下载攻击代码。
- 在攻击者的机器上运行以下命令
  - Kaht2 192.168.86.101 192.168.86.103

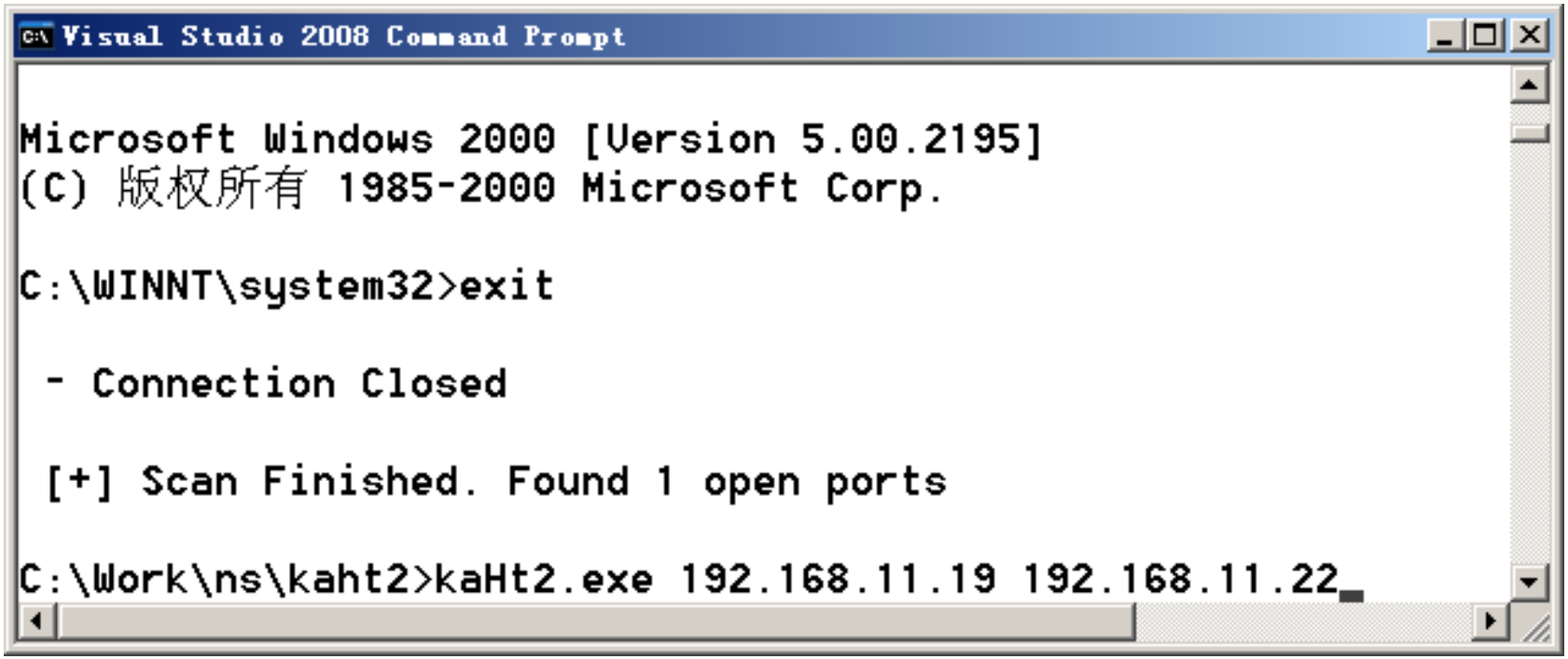


图7-12 用kaht2攻击Windows2000

则攻击者可以获得一个以SYSTEM权限运行的远程命令行窗口。SYSTEM权限是Windows系统上的最高权限，可以执行任何操作。

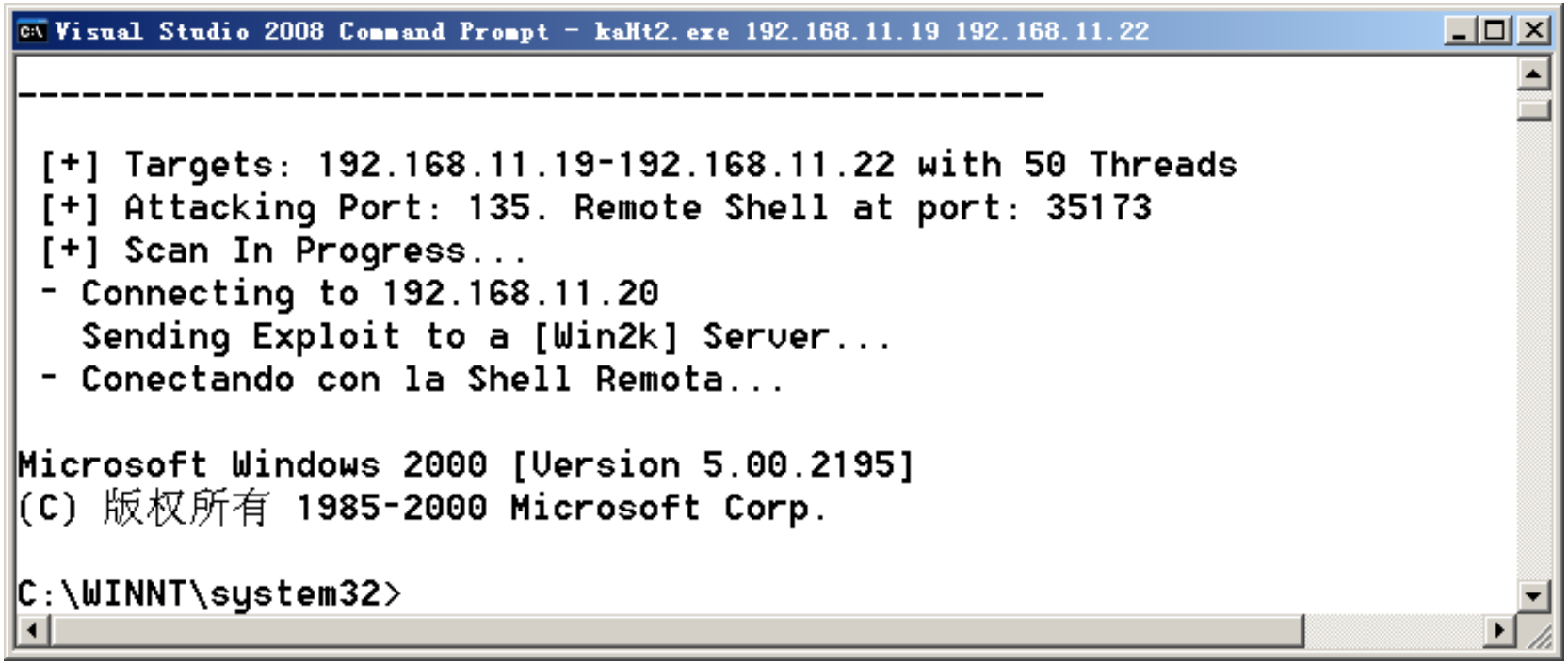


图7-13 攻击成功后在本地获得的远程命令窗口

7.4 Linux(Unix) 的安全机制及防护技术

- Linux是多用户多任务操作系统，内建了许多安全机制以保证系统的安全。由于Linux免费且开源，为了降低信息系统的建设成本，很多企业的服务器均以Linux为核心。

- 本节介绍Linux系统的安全机制及提高其安全防护能力的一些建议。

7.4.1 Linux的安全机制

(1) 用户和口令安全

- Linux是一个多用户操作系统，因此在任何时候都可以有多个用户登录到Linux机器上，而且他们中的每一个都可以同时多次登录。用户的类型以及怎样管理这些用户，对于系统安全而言是至关重要的。
- ***Linux* 用户可以分为三种不同的类型：**
  - ***root*（超级用户）**
  - 普通用户
  - 系统用户

(1) 用户和口令安全

- **root超级用户通常取名为root，它对整个系统有完全的控制权。**
- root可以存取系统的所有文件，同时只有root才能运行某些程序(例如root是惟一能够运行httpd(Apache Web服务器)的用户，因为httpd绑定端口80，该端口仅限root使用)。因此，**黑客要想完全控制系统，就要成为*root***。

- 请注意，**root的用户ID为0**。**每一个用户ID为0的用户，不论其用户名是什么，都是root**。

root超级用户

- 换句话说，如果你能通过某种方法把用户的ID号设置为0，则该用户就具有超级用户的权限，就是root超级用户。

- 早期的Linux系统(redhat9.0 及之前的版本)可以在创建新用户时指定UID=0；目前的Linux系统不允许直接指定UID，不能用这种方法创建UID=0的用户，但可以在获得root权限（比如通过缓冲区溢出攻击）后通过编辑口令文件来实现。

演示：将一个普通用户变成root

环境：Linux (Fedora 或 Ubuntu)

普通用户

- 普通用户是那些能登录到系统的用户，用于日常工作，如上网、写文档、开发软件等。
- 普通用户拥有一个主目录(没有主目录的用户不能登录系统)，对主目录拥有读写执行等权限。典型的普通用户对于其他用户的文件和目录只有受限的权限。
- Linux系统采用了自主访问控制策略，用户可以将主目录及子目录和文件的访问权授予其他用户。使用adduser命令添加的用户默认为一个普通用户。

系统用户

- 系统用户从不登录。这些账号用于特定的系统目的，不属于任何特定的人。这类用户不登录系统，通常也没有主目录(/etc/passwd文件中这些用户的主目录字段为空——有时使用“/”或某个不存在的目录。
- 因为这些用户不能登录，所以主目录字段不起作用)。此外，它们在/etc/passwd中所指定的shell也不是合法的登录shell，典型的例子是/bin/false（或/sbin/nologin）。
- 例如ftp，apache和lp。ftp用户用于处理匿名FTP访问，apache用户通常处理HTTP请求；lp处理打印功能。他们的Login Shell=/sbin/nologin。实际系统中所存在的系统用户取决于所安装的Linux发布和相关软件。

/etc/passwd文件

- 用户的信息存放在/etc/passwd文件中。在早期Linux系统中，加密后的用户口令也存放在/etc/passwd文件中。由于/etc/passwd文件对所有用户具有读权限，这样会带来口令破解风险，因此现代的Linux系统将加密后的口令存于/etc/shadow (影子) 文件中，只有root才具有访问权。
- /etc/passwd 中包含有用户的登录名，用户号，用户组号，用户注释，用户主目录和用户所用的shell程序。其中用户号(UID) 和用户组号(GID)用于Unix系统唯一地标识用户和同组用户及用户的访问权限。

/etc/passwd文件

- /在etc/shadow 中存放加密的口令，用于用户登录时输入的口令检验，符合则允许登录，否则拒绝用户登录。用户可用passwd命令修改自己的口令，不能直接修改 /etc/ shadow中的口令部分。

- /etc/passwd是一个文本文件，口令文件中每行代表一个用户条目，格式为：
- LOGNAME ： ***x*** ： UID ： GID ： USERINFO ： HOME ： SHELL
  - root:x:0:0:root:/root:/bin/bash
  - ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
  - hadoop:x:1000:1000:hadoop:/home/hadoop:/bin/bash

(2) 文件许可权

- 文件属性决定了文件的被访问权限，即谁能存取或执行该文件。用ls -l可以列出详细的文件信息，如:
- **-rwxrwxrwx**. 1 ns ns 7263 Mar 3 14:31 exit_asm
- -rw-rw-r--. 1 ns ns 140 Oct 6 15:49 exit_asm.c

- 包括了文件许可，文件联结数，文件所有者名，文件相关组名，文件长度，上次存取日期和文件名。其中文件许可分为四部分：
  - -：表示文件类型。
  - 第一个*rwx*：表示**文件属主**的访问权限。
  - 第二个*rwx*：表示文件**同组用户**的访问权限。
  - 第三个*rwx*：表示**其它用户**的访问权限。

执行许可位的特殊权限标志s和S

- 若某种许可被限制则相应的字母换为-。
- 在许可权限的执行许可位置上，可能是其它字母，s，S。s和S可出现在所有者和同组用户许可模式位置上，与特殊的许可有关，后面将要讨论。小写字（x，s）表示执行许可为允许，负号或大写字母（-，S）表示执行许可为不允许。
- 改变许可方式可使用 chmod 命令，并以新许可方式和该文件名为参数。新许可方式以3位8进制数给出，r为4，w为2，x为1。如rwxr-xr--为754。

(3) 目录许可

- 在Unix系统中，目录也是一个文件，用ls -l列出时，目录文件的属性前面带一个d，目录许可也类似于文件许可，用ls列目录要有读许可，在目录中增删文件要有写许可，进入目录或将该目录作路径分量时要有执行许可，故要使用任一个文件，必须有该文件及找到该文件的路径上所有目录分量的相应许可。
- **仅当要打开一个文件时，文件的许可才开始起作用**，而rm，mv 只要有目录的搜索和写许可，不需文件的许可，这一点应注意。

(4) 设置用户ID许可和同组用户ID许可

- 用户ID许可(SUID)和同组用户ID许可(SGID)可给予可执行的目标文件(只有可执行文件才有意义)。
- 当一个进程执行时就被赋于4个编号，以标识该进程隶属于谁、有什么权限，分别为实际和有效的UID（euid），实际和有效的GID（egid）。
- 有效的UID和GID一般和实际的UID和GID相同(即登录到系统的用户的UID和GID)，**有效的UID和GID用于系统确定该进程对于文件的存取许可**。
- 设置可执行文件的SUID许可将改变上述情况。

suid and sgid

- 当设置了SUID时，进程的euid为该可执行文件的所有者的euid，而不是执行该程序的用户的euid，因此，由该程序创建的进程都有与该程序所有者相同的存取许可。这样，程序的所有者将可通过程序的控制，在有限的范围内向用户发表不允许被公众访问的信息。同样，SGID是设置有效GID。

- 用chmod u+s 文件名和chmod u-s 文件名 来设置和取消SUID设置。用chmod g+s文件名和chmod g-s文件名来设置和取消SGID设置。当文件设置了SUID和SGID后，chown和chgrp命令将全部取消这些许可。

慎用 suid 和 sgid

- **要慎用 suid 和 sgid。**

- 如果某可执行文件是root创建的，如果设置了SUID，而该可执行文件又被赋予了其他普通用户的可执行权限，则该程序被任何用户运行时，对应的进程的euid是root，该进程可以访问任何文件。

- 因此，不要随意设置属主是root的可执行文件的suid，以避免安全问题。

演示
一个SUID程序危及安全的例子

```
#include <stdio.h>
#include <stdlib.h>
int main(int argc, char * argv[])
{
  FILE *fp;   char *line = NULL;
  size_t len = 0;  ssize_t read;
  fp = fopen("/etc/shadow", "r");
  if (fp == NULL){
    puts("Cannot open the file /etc/shadow");
    exit(EXIT_FAILURE);
  }
  while ((read = getline(&line, &len, fp)) != -1)
  {  printf("%s", line); }
  free(line);
  exit(EXIT_SUCCESS);
}
```

- 将代码保存为demo.c

- [fanping@F16x32 c]$ gcc -o t demo.c
- [fanping@F16x32 c]$ ./t
- Cannot open the file /etc/shadow
- [fanping@F16x32 c]$ su
- 密码：
- [root@F16x32 c]# chown root t
- [root@F16x32 c]# chmod a+s t
- [root@F16x32 c]# exit
- exit
- [fanping@F16x32 c]$ ./t

- 将打印/etc/shadow的内容

7.4.2 Linux的安全防护

(1) 使用高强度的口令

- 口令是认证用户的主要手段。为了提高安全性，要保证口令的最小长度并限制口令的使用时间。现代的Linux系统如Ubuntu和Fedora系统默认采用了口令复杂化机制，拒绝接受长度过短和容易被破解的口令，还提供了自动生成复杂口令的功能。为安全起见，在设置口令时最好采用系统生成的口令，如图7-14所示。

图7-14 Ubuntu系统自动生成高强度的口令

图7-14 Ubuntu系统自动生成高强度的口令

(2) 用户超时注销

- 如果用户离开时忘记注销账户，则可能给系统安全带来隐患。为此需要设定锁屏时间，如图7-15所示。

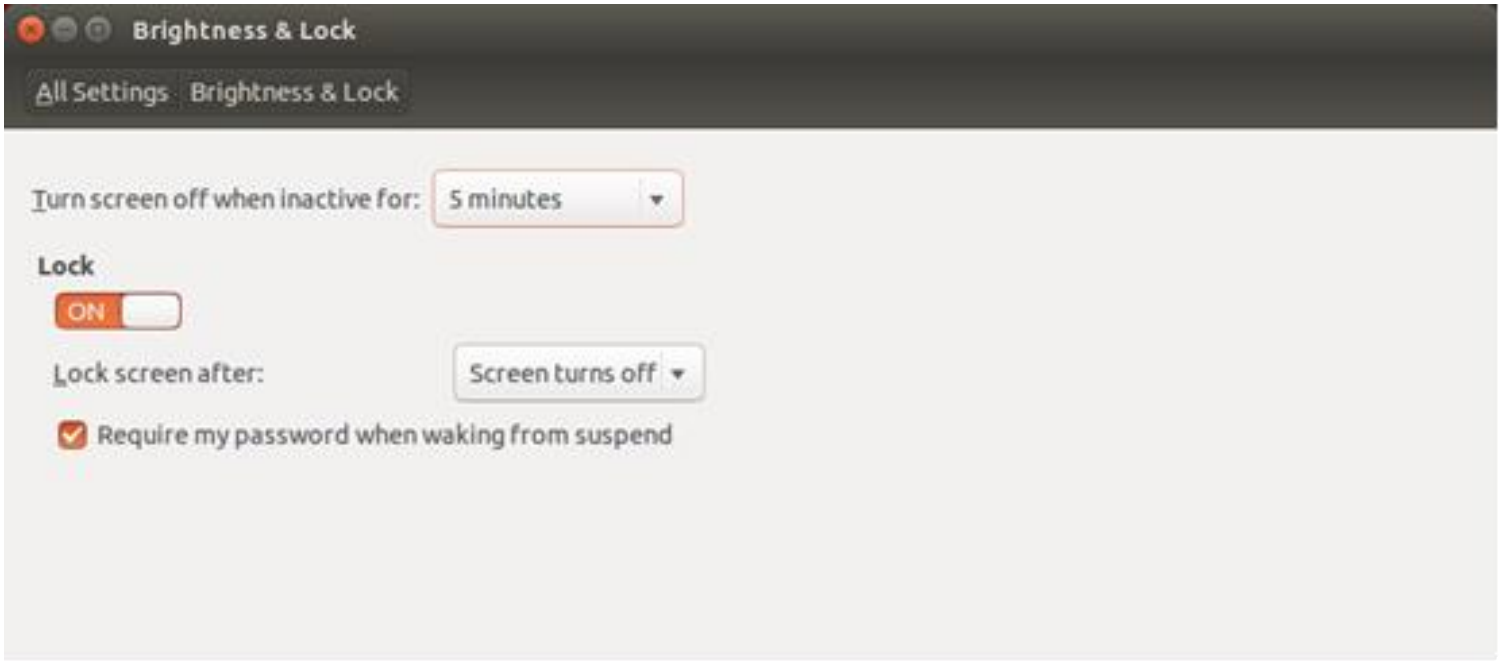


图7-15 Ubuntu系统中的锁屏设置

(3) 禁止访问重要文件

- 对于系统中的某些关键文件如services和lilo.conf等可修改其属性，防止意外修改和被普通用户查看。
- 首先改变文件属性为600：
  - # chmod 600 /etc/services
- 保证文件的属主为root，然后还可以将其设置为不能改变：# chattr +i /etc/services
  - 这样，对该文件的任何改变都将被禁止。
- 只有root重新设置复位标志后才能进行修改：
  - # chattr -i /etc/services

(4) 允许和禁止远程访问

- 在 Unix 中可通过 /etc/hosts.allow 和 /etc/hosts.deny 这2个文件允许和禁止远程主机对本地服务的访问。
- 通常的做法是：
  - (1)编辑hosts.deny文件，加入下列行：
    - # Deny access to everyone.
    - ALL: ALL@ALL
  - 则所有服务对所有外部主机禁止，除非由hosts.allow文件指明允许。
  - (2)编辑hosts.allow 文件，可加入下列行：
    - #Just an example:
    - ftp: aaa.aaa.aaa.aaa xxxxxx.com
  - 则将允许IP地址为aaa.aaa.aaa.aaa和主机名为xxxxxx.com的机器作为Client访问FTP服务。

(5) 限制Shell命令记录大小

- 默认情况下，bash shell会在文件$HOME/.bash_history中存放多达500条命令记录(根据具体的系统不同，默认记录条数不同)。系统中每个用户的主目录下都有一个这样的文件。

- 强烈建议限制该文件的大小。用户可以编辑/etc/profile文件，修改其中的选项如下：

  HISTFILESIZE=30或HISTSIZE=30

(6) 注销时删除命令记录

- 编辑/etc/skel/.bash_logout文件，增加如下行：

  rm -f $HOME/.bash_history

- 这样，系统中的所有用户在注销时都会删除其命令记录。
- 如果只需要针对某个特定用户，如root用户进行设置，则可只在该用户的主目录下修改/$HOME/.bash_history文件，增加相同的一行即可。

(7) 禁止不必要的SUID程序

- SUID可以使普通用户以root权限执行某个程序，因此应严格控制系统中的此类程序。

① 用find找出root所属的带s位的程序

② 禁止其中不必要的程序：

 # chmod a-s program_name

(8) 及时为系统的已知漏洞打上补丁

- 一般而言，一旦Unix系统被发现存在容易受到攻击的漏洞，全世界的各个Unix组织会很快发布相关的补丁，这时需要用户有时时更新系统补丁的意识，或者关闭相应的服务。

(9) 保证一些应用服务的安全

① 如果不是必须需要的服务，则应该设置关闭这些服务。

② 如果是必须使用的服务，则应该保证使用的服务程序是最新的版本。

③ 对于应用服务要提供口令认证，尽可能避免匿名登陆。

④ 另外，可以修改一些服务程序的版本信息，这样使得攻击者难以发现你的系统是否存在漏洞，从而降低遭受攻击的可能性。

7.5 入侵Linux系统

7.5.1 破解口令

- 如果能获得一对Linux系统的用户名/口令，则可以入侵Linux系统。
- 现代Linux系统的的加密口令是很难逆向破解的。通常的口令破解工具所采用的技术是**仿真对比**，利用与原口令程序相同的方法，通过对比分析，用不同的加密口令去匹配原口令。
- 目前已开发出许多口令破解工具，如下表所示。

工具名	下载地址
John the Ripper	http://www.openwall.com/john/
Brutus	http://www.hoobie.net/brutus/
ObiWan	http://www.phenoelit.org/fr/tools.html
THC-Hydra	http://www.thc.org/download.php?t=-r&f=hydra-4.5-src.tar.gz
pop.c	http://packetstorm.security.org/groups/ADM/ADM-pop.c
TeeNet	http://www.phenoelit.de/tn
Pwscan.pl	http://razor.bindview.com/tools/vlad/index.shtml (VLAD扫描软件的组件之一)
SNMPbrute	http://packetstormsecurity.org/Crackers/snmpbrute-fixedup.c

注意：某些工具可能已经移到别的网站

7.5.2 通过系统漏洞进行入侵

- 漏洞主要是指系统设计、应用服务、安全程序等方面存在的脆弱性(和缺陷)和人为的管理配置出现的系统的不安全因素，它们可被利用而造成对系统安全的危害。由于技术上的原因，安全漏洞问题将长期存在。
- 截至2019年10月21日，nsfocus收集了Linux系统的漏洞记录共 2868条，其中261个远程进入系统类漏洞，2398个本地越权漏洞。可见，Linux系统中的漏洞还是很多的，利用这些漏洞将危害系统的安全。

7.5.3几种典型的数据驱动攻击

- 数据驱动攻击是指向某个进程（远程或本地）发送将导致非预期结果的数据，从而入侵系统。

- 主要原因在于程序的设计者忽视了对输入数据的校验。

(1) 缓冲区溢出攻击

- 在某个用户或进程试图往一个缓冲区(即固定长度的数组)中放置比原初分配的空间还要多的数据的时候，就会出现缓冲区溢出条件(buffer overflow condition)。
- 这种情况与C语言特有的函数，例如strcpy()、strcat()、sprintf()等有关。正常的缓冲区溢出条件会导致段越界发生。然而精心利用这类情况，可以达到访问目标系统的目的。
- 目前已经有许多可根据缓冲区溢出漏洞自动产生shellcode的工具，比如hellkit-1.2.tar.gz。

- 由于缓冲区溢出攻击的危害巨大，已经开发了以下2种有效的防范措施：

- 1) 新版本的gcc在编译时默认使用了堆栈保护，即使会发生缓冲区溢出错误，造成的危害也仅限于破坏内存数据，不会发生执行攻击者代码的事件。
- 2) 现代操作系统可以禁止堆栈执行，从而阻止进程被劫持。

- 为了从根本上杜绝缓冲区溢出攻击，程序员应该对数据做边界检查，并进行较为充分的测试。

(2) 格式化字符串攻击

- 格式化字符串漏洞是格式化函数(包括printf()和sprintf())中的格式化参数与待输出的变量个数不匹配而导致的。攻击者利用该漏洞可以使进程崩溃、读写某个敏感变量的值，甚至能执行任意的代码。

- 防止格式化字符串攻击的根本在于程序员提高安全意识，避免从用户那里获得格式化参数，并对软件进行较为充分的测试。

(3) 输入验证攻击

- 如果进程没有确切地分析并验证所收到输入的有效性，则可能发生输入验证攻击。发生输入验证攻击的情况包括：
  1. 程序无法辨认语法上不正确的输入。
  2. 模块接受了无关的输入。
  3. 模块没有能够处理遗漏的输入域。
  4. 发生了域值相关性错误。
- SQL注入攻击就是典型的输入验证攻击。
- 为了防止输入验证攻击，程序员要认真检查输入，并测试所有的代码。

作业

1. 如何在windows2003中禁止某个用户从本地登录？写出实现的过程。
2. 在VirtualBox上运行Linux虚拟机时，如果安装了VirtualBox 的增强功能，那么虚拟机可以共享主机上的文件夹。然而要访问共享文件夹，必须将用户添加到vboxsf组，这可以用usermod命令实现。写出将用户alice添加到组vboxsf组的命令。

上机实践（不考核，自己练习）

1. 以windows2000为测试目标，利用中文输入法漏洞，增加账户test，并将其提升为管理员权限。

2. 查看linux系统的/etc/passwd文件，熟悉各个域的含义。