TREND MICRO™

高职高专技能教育系列教材
趋势科技认证信息安全专员(TCSP)教材

网络安全与病毒防范
实验指导手册

趋势科技(中国)有限公司／组编
马宜兴／主编

上海交通大學出版社
SHANGHAI JIAO TONG UNIVERSITY PRESS

网络安全与病毒防范实验指导手册

主编　马宜兴
编写　沈　赟
　　臧兆伟

上海交通大学出版社

内 容 提 要

本书是趋势科技认证信息安全专员的补充课程教材，学校可以根据实际情况选择性安排教学课时和内容。教材旨在加深学员信息安全意识，使学员更深刻地理解信息安全威胁，而非要求学员掌握确切的攻击技术。授课教师应该严格遵守实验要求，控制相关风险。

本书既适用于普通本科院校、高职高专院校计算机及相关专业的教学，又是初学者轻松跨入信息安全领域的钥匙，也是专业信息安全人士的有效参考书籍。

图书在版编目（CIP）数据

网络安全与病毒防范实验指导手册 / 马宜兴主编. ——上海：上海交通大学出版社，2011
ISBN 978-7-313-07563-5

Ⅰ. ①网… Ⅱ. ①马… Ⅲ. ①计算机网络－安全技术－手册 ②计算机病毒－防治－手册 Ⅳ. ①TP393.08-62 ②TP309.5-62

中国版本图书馆 CIP 数据核字（2011）第 180731 号

网络安全与病毒防范实验指导手册
马宜兴 主编
上海交通大学出版社出版发行
（上海市番禺路 951 号 邮政编码 200030）
电话：64071208 出版人：韩建民
上海交大印务有限公司印刷 全国新华书店经销
开本：787mm×1092mm 1/16 印张：7.25 字数：174 千字
2011 年 9 月第 1 版 2011 年 9 月第 1 次印刷
印数：1—3030
ISBN 978-7-313-07563-5/TP 定价：19.00 元

实 验 说 明

本课程是趋势科技认证信息安全专员的补充课程，学校可以根据实际情况选择性安排教学课时和内容。

本课程旨在加深学员信息安全意识，使学员更深刻地理解信息安全威胁，而非要求学员掌握确切的攻击技术。授课教师应该严格遵守实验要求，控制相关风险。

趋势科技不提供实验课程所涉及的工具，某些免费软件建议仅限教师演示用，其相关权利也归各自公司所有，使用时应遵守其规定。学员不得以任何途径获得和传播这些工具。

教师在授课演示时务必做到：

1．在隔离的网络环境下演示；

2．控制实验环境，工具和演示代码不带出实验室。

对于不遵循实验要求而产生的安全问题，一律与趋势科技无关。

目　录

※ 基础篇 ※

※ 攻防篇 ※

※ 病毒篇 ※

※ 进阶篇（选修）※

基　礎　篇

实验 1　熟悉常见的系统命令

【实验目的】

掌握常见的系统命令的使用方法。

【知识点】

随着微软 Windows 操作系统基于图形用户界面应用程序的普及，普通用户已逐渐淡忘了 DOS 时代只能依靠输入命令同计算机交互的方式；但是命令行依然有它独特的价值，而 Windows 命令行中也提供了一些实用小工具，尤其适用于判断和处理系统网络问题。

【实验准备】

1．硬件：装有 Windows 操作系统的计算机若干，已连入局域网。

2．软件：FTP，Telnet 帐户。

【注意事项】

无。

【实验步骤】

1．从开始菜单里选择“运行”，输入“cmd”，进入命令行环境。

2．在命令行环境下依次测试以下命令。

1）**ipconfig 命令**

它是调试计算机网络的常用命令，通常用户使用它显示计算机中网络适配器的 IP 地址、子网掩码及默认网关。见图 1-1。

```
C:\>ipconfig/all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : trend-lab
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : VMware Accelerated AMD PCNet Adapter

        Physical Address. . . . . . . . . : 00-0C-29-D0-18-8F
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 10.28.132.111
        Subnet Mask . . . . . . . . . . . : 255.255.255.128
        Default Gateway . . . . . . . . . : 10.28.132.1
        DNS Servers . . . . . . . . . . . : 10.28.132.20
                                            10.28.128.8
                                            10.64.1.55
        Primary WINS Server . . . . . . . : 10.28.132.20
        Secondary WINS Server . . . . . . : 10.28.128.8
                                            10.64.1.55
```

图 1-1

/all 该参数显示所有网络适配器（网卡、拨号连接等）的完整 TCP/IP 配置信息。与不带参数的用法相比，它的信息更全、更多，如 IP 是否动态分配、显示网卡的物理地址等。

2) **ping 命令**

它是用来检查网络是否畅通或者网络连接速度的命令。该命令所利用的原理：网络上的机器都有唯一确定的 IP 地址，当用户给某一目标 IP 地址发送一个数据包时，对方就要返回一个同样大小的数据包，根据返回的数据包，用户就能确定目标主机的存在，可以初步判断目标主机的操作系统等。

在命令行模式下输入“ping /h”即可得到 ping 的命令介绍，其他命令通过在命令名称后空格加“/h”也可得到相关使用帮助。见图 1-2。

```
C:\>ping /h
Bad option /h.

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] target_name

Options:
    -t              Ping the specified host until stopped.
                    To see statistics and continue - type Control-Break;
                    To stop - type Control-C.
    -a              Resolve addresses to hostnames.
    -n count        Number of echo requests to send.
    -l size         Send buffer size.
    -f              Set Don't Fragment flag in packet.
    -i TTL          Time To Live.
    -v TOS          Type Of Service.
    -r count        Record route for count hops.
    -s count        Timestamp for count hops.
    -j host-list    Loose source route along host-list.
    -k host-list    Strict source route along host-list.
    -w timeout      Timeout in milliseconds to wait for each reply.
```

图 1-2

-t 该参数表示将不间断向目标 IP 发送数据包，直到我们强迫其停止（Ctrl+C 进行终止），见图 1-3。

```
C:\>ping www.sina.com.cn -t

Pinging auriga.sina.com.cn [61.172.201.194] with 32 bytes of data:

Reply from 61.172.201.194: bytes=32 time=114ms TTL=239
Reply from 61.172.201.194: bytes=32 time=129ms TTL=239
Reply from 61.172.201.194: bytes=32 time=104ms TTL=239
Reply from 61.172.201.194: bytes=32 time=104ms TTL=239
Reply from 61.172.201.194: bytes=32 time=104ms TTL=239
Reply from 61.172.201.194: bytes=32 time=104ms TTL=239

Ping statistics for 61.172.201.194:
    Packets: Sent = 6, Received = 6, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 104ms, Maximum = 129ms, Average = 109ms
Control-C
^C
```

图 1-3

-l 该参数用来定义发送数据包的大小，默认为32字节，利用它可以最大定义到65500字节。见图1-4。

```
C:\>ping -l 300 www.sina.com.cn

Pinging libra.sina.com.cn [202.108.33.77] with 300 bytes of data:

Reply from 202.108.33.77: bytes=300 time=38ms TTL=51
Reply from 202.108.33.77: bytes=300 time=35ms TTL=51
Reply from 202.108.33.77: bytes=300 time=35ms TTL=51
Reply from 202.108.33.77: bytes=300 time=35ms TTL=51

Ping statistics for 202.108.33.77:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 35ms, Maximum = 38ms, Average = 35ms
```

图1-4

-n 该参数定义向目标IP发送数据包的次数，默认为3次。如果网络速度比较慢，定义1次即可。见图1-5。

```
C:\>ping -n 1 www.sina.com.cn

Pinging libra.sina.com.cn [202.108.33.74] with 32 bytes of data:

Reply from 202.108.33.74: bytes=32 time=36ms TTL=52

Ping statistics for 202.108.33.74:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 36ms, Maximum = 36ms, Average = 36ms
```

图1-5

这里time=36ms，表示从发出数据包到接受到返回数据包所用的时间是36ms，从这里可以判断网络连接速度的大小。从TTL的返回值可以初步判断被ping主机的操作系统，之所以说“初步判断”是因为这个值是可以修改的。

通常利用ping命令可以快速查找网络故障，可以快速判断服务器连接速度。如果目标服务器安全防护性能差且出口带宽窄，也可能被攻击者通过ping进行攻击。

3) **nbtstat** 命令

该命令使用TCP/IP上的NetBIOS显示协议统计和当前TCP/IP连接，使用此命令可以得到远程主机的NETBIOS信息，比如用户名、所属的工作组、网卡的MAC地址等。下面介绍此命令的几个基本参数。

进行实验前，需要在“本地连接”属性里“安装”，选择“协议”，确保安装了以下选项（图1-6）。

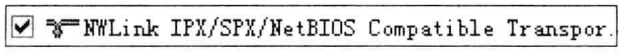

图1-6

-a 使用该参数，只要你知道远程主机的机器名称，就可以得到它的 NETBIOS 信息。

-A 使用该参数，也可以得到远程主机的 NETBIOS 信息，但需要知道远程主机的 IP。

-n 列出本地机器的 NETBIOS 信息。

攻击者当得到了对方的 IP 或者机器名的时候，就可以使用 nbtstat 命令来进一步得到对方的信息，增加了攻击者入侵的成功系数。

4) **netstat 命令**

这是一个用来查看网络状态的命令，操作简便功能强大。

-a 该参数用来查看本地机器的所有开放端口，可以有效发现和预防木马，可以知道机器所开的服务等信息。见图 1-7。

```
C:\>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    trend-lab:epmap        trend-lab:0            LISTENING
  TCP    trend-lab:microsoft-ds  trend-lab:0           LISTENING
  TCP    trend-lab:netbios-ssn  trend-lab:0            LISTENING
  TCP    trend-lab:1034         10.28.132.110:smtp     ESTABLISHED
  TCP    trend-lab:1038         220.181.47.73:ftp      ESTABLISHED
  TCP    trend-lab:1040         220.181.47.73:ftp      ESTABLISHED
  TCP    trend-lab:1026         trend-lab:0            LISTENING
  TCP    trend-lab:1026         trend-lab:1038         ESTABLISHED
  UDP    trend-lab:microsoft-ds  *:*
  UDP    trend-lab:isakmp       *:*
  UDP    trend-lab:1025         *:*
  UDP    trend-lab:4500         *:*
  UDP    trend-lab:ntp          *:*
  UDP    trend-lab:netbios-ns   *:*
  UDP    trend-lab:netbios-dgm  *:*
  UDP    trend-lab:1900         *:*
  UDP    trend-lab:ntp          *:*
  UDP    trend-lab:1900         *:*
```

图 1-7

从图 1-7 可以看出本地机器正向远程计算机建立起了 SMTP 连接和 FTP 连接。

-r 该参数列出当前的路由信息，告诉用户本地机器的网关、子网掩码等信息。

5) **tracert 命令**

该命令跟踪路由信息，使用此命令可以查出数据从本地机器传输到目标主机所经过的所有途径，这对用户了解网络布局和结构很有帮助。见图 1-8。

```
C:\>tracert 10.28.133.1

Tracing route to 10.28.133.1 over a maximum of 30 hops

  1    12 ms     2 ms     2 ms  10.28.132.1
  2     2 ms     3 ms     3 ms  10.28.133.1

Trace complete.
```

图 1-8

图 1-8 说明数据从本地机器传输到 10.28.133.1 的机器上，中间经过了 10.28.132.1 作为中转，说明这两台机器是不在同一段局域网内。

6) **net 命令**

该命令是网络命令中最重要的一个，必须透彻掌握它的每一个子命令的用法，首先让我们来看一看它都有哪些子命令，键入 net /h。

net view 使用此命令查看远程主机的所有共享资源。

命令格式：net view \\<IP>

net use 使用此命令建立远程目标到本地计算机的影射。

C:\net use \\192.168.1.99\ipc$ "pass" /user:"admin"

C:\Net use z: \\192.168.1.99\C$ "aaa" /user: "bbb"

这里的第一个命令表示与 192.168.1.99 建立一个 IPC$连接，第二个命令表示将 192.168.1.99 的 C 盘影射成本机的 Z:\盘。建立了 IPC$连接并且影射后，就可以从本地机向目标机器拷贝文件了。

net start/stop 使用此命令来启动或停止主机上的服务。

命令格式：net start <servername>或 net stop <servername>。

Net user 使用此命令查看和帐户有关的情况，包括新建帐户、删除帐户、查看特定帐户、激活帐户、帐户禁用等。键入不带参数的 net user，可以查看所有用户，包括已经禁用的。

net user u1 123 /add 新建一个用户名为 u1，密码为 123 的帐户，默认为 user 组成员。

net user u2 /del 将用户名为 u2 的用户删除。

net user u3 /active:no 将用户名为 u3 的用户禁用。

net user u4 /active:yes 激活用户名为 u4 的用户。

net user u5 查看用户名为 u5 的用户情况。

net localgroup 使用此命令查看所有和用户组有关的信息和进行相关操作。

net time 使用此命令查看远程主机当前的时间，可以和 Windows 的计划任务命令配合启动程序任务。

命令格式：net time \\<IP>。

7) **at 命令**

该命令的作用是安排在特定日期或时间执行某个特定的命令和程序（需要 Task Schedule 是启动状态下）。当用户知道了远程主机的当前时间，就可以利用此命令让其在以后的某个时间执行某个程序和命令。

命令格式：at <time> <command> \\<computer>。

8) **ftp 命令**

ftp 是用来与服务器之间进行文件传输的协议，网络上很多服务器都提供 ftp 服务。在命令行键入 ftp，出现 ftp 的提示符，这时候可以键入 help 来查看帮助，下面介绍几个简单的命令。

先是登陆过程，使用 open 命令，格式：open <ftp_IP> <ftp_port>。一般 ftp 端口默认是 21，可以省略。接着就是输入合法的用户名和密码进行登陆了。

接下来介绍具体命令的使用方法：

dir 跟 DOS 命令一样，用于查看服务器的文件。

cd 进入某个文件夹。

get 下载文件到本地机器。

put 上传文件到远程服务器。这就要查看远程 ftp 服务器是否授予你可写的权限，如果授权了，就可以进行文件上传。

delete 删除远程 ftp 服务器上的文件。这也必须保证你有可写的权限。

bye 退出当前连接。

quit 退出当前连接。

9) **telnet 命令**

远程登录命令，它操作简单，熟悉命令行操作，登录后如同使用自己的计算机一样。首先键入 telnet，再键入 help 可以查看帮助信息。

在提示符下键入 open <IP>，这时就出现了如图 1-9 所示的登录窗口。

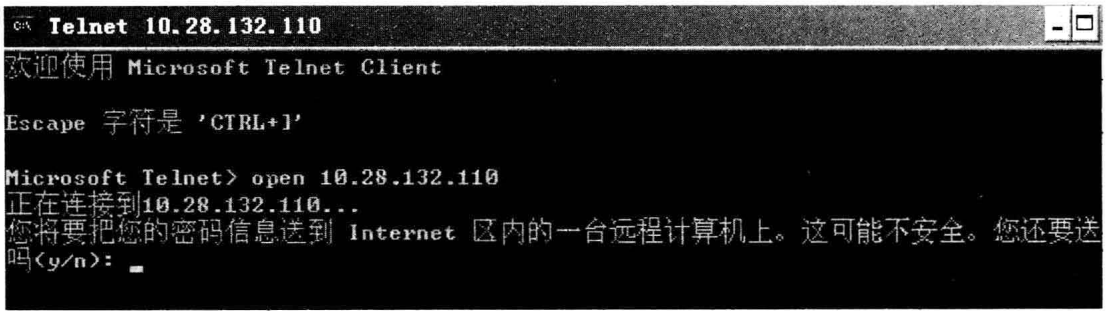

图 1-9

在安全提示后输入“y”，然后按照提示输入合法的用户名和密码。当验证了用户名和密码后就成功建立了 telnet 连接，此时在远程主机上就具有了和此用户一样的权限。

【实验结果】

保证每个命令都能执行成功。

实验 2　远程桌面管理工具的使用

【实验目的】

通过实验了解远程工具的功能，深入了解远程控制在恶意程序中的使用可造成的巨大危害。

【知识点】

远程桌面连接功能可以用于计算机的远程连接和操控，在被连接的计算机上可以安装软件、运行程序，所有的一切都好像是直接在该计算机上操作一样。通过该功能，网络管理员可以在远程办公室安全地控制机房的服务器，而且由于该功能是系统内置的，所以比其他第三方远程控制工具使用更方便，更灵活。

【实验准备】

硬件：装有 Windows 操作系统的计算机 2 台，已连入局域网。

【注意事项】

1. 了解远程桌面管理工具所使用的端口：3389。

2. 两台计算机之间的上述端口可以通信。

【实验步骤】

1. 在将被管理的远程计算机上，右键“我的电脑”-“系统属性”，选择“远程”面板，选择“允许用户远程连接到此计算机，点击“选择远程用户”，添加允许远程连接的用户对象，确定并应用设置。见图 2-1。

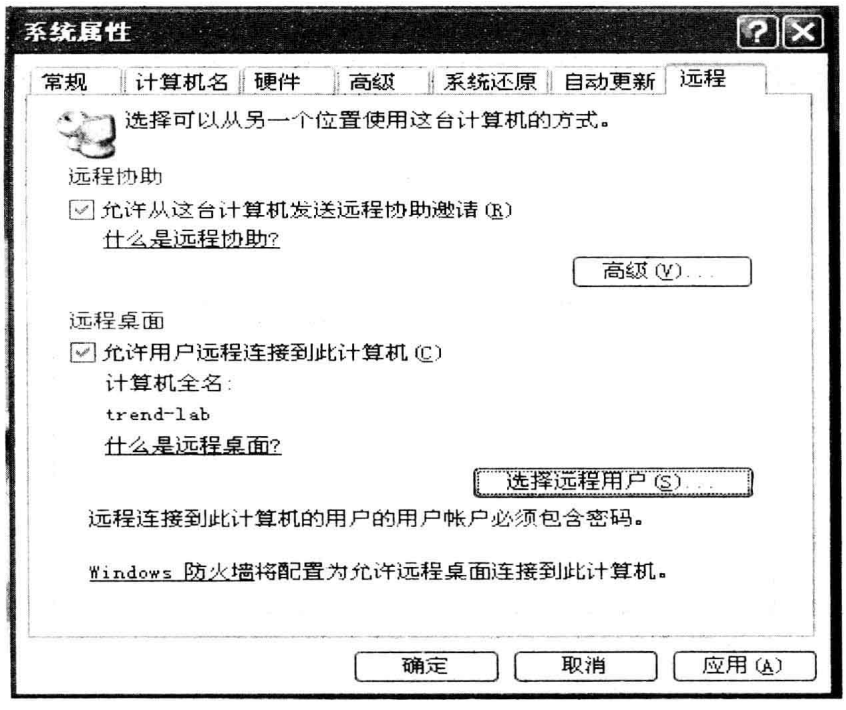

图 2-1

2. 在本地计算机上，从开始菜单选择“运行”，输入“mstsc”，输入远程计算机的 IP 地址，选择“连接”后，将出现远程计算机的登录界面。见图 2-2。

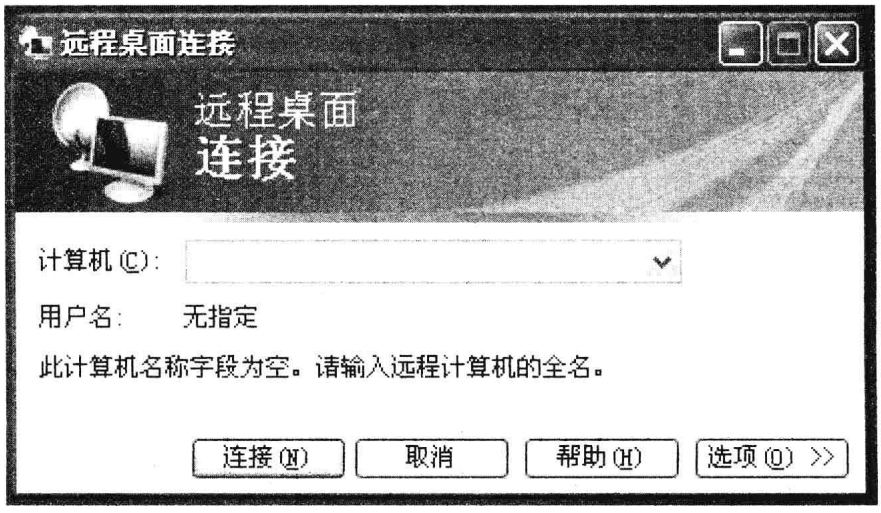

图 2-2

3．接下来就可以像在本地一样，对远程计算机进行设置操作了。

【实验结果】

可以成功地连接到远程计算机，并对远程计算机进行控制操作。

【课后思考】

在远程桌面连接计算机登录界面中有一个“选项”按钮，能否通过该设置来调整显示在本地的远程桌面的大小？

实验 3　监听、开放或关闭服务端口

【实验目的】

利用端口有效地保证系统的安全性，掌握基本的对端口活动实现监控的技能，了解黑客攻击手段及安置后门的方法。

【实验准备】

1．硬件：装有 Windows 操作系统的计算机 2 台，已连入局域网。

2．软件：TCPView。

【注意事项】

1．实验过程中可以指导学员适时关闭防火墙以减少干扰因素。

2．确保实验机器安装有 FTP 和 IIS 服务。

【实验步骤】

1．无阻碍的网络环境：

由于远端计算机已安装有 IIS 服务和 FTP 服务，所以可以使用本地计算机访问远端计算机上的 HTTP 和 FTP 站点。

在本地计算机上，打开 IE 浏览器，在地址栏输入“http://<IP_remote>”，访问远端计算机上的 IIS 站点（该步骤使用到了 HTTP 协议默认端口：80）。见图 3-1。

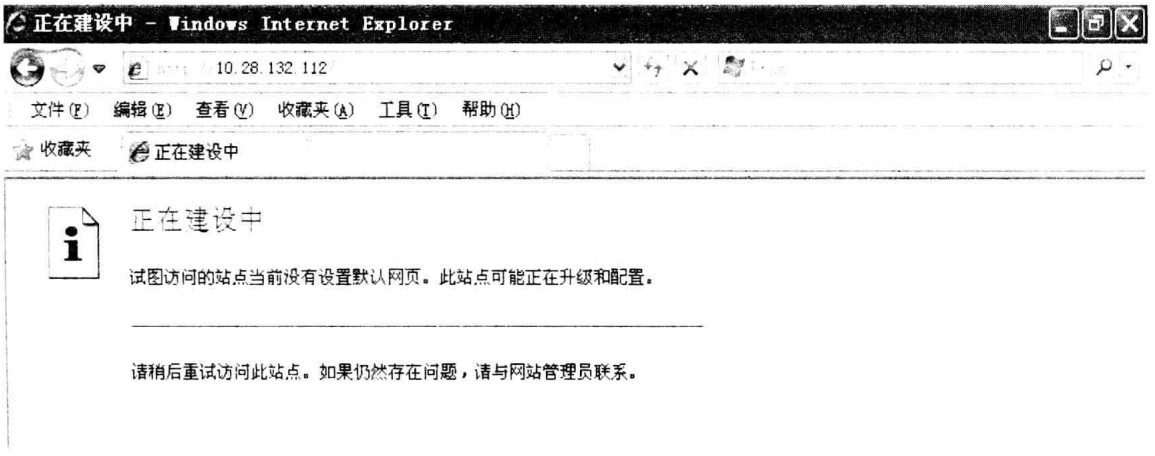

图 3-1

从开始菜单选择“运行”，输入“cmd”，进入命令行环境。输入“ftp <IP_remote>”，访问远端计算机上的 FTP 站点（该步骤使用到了 FTP 协议默认端口：21）。见图 3-2。