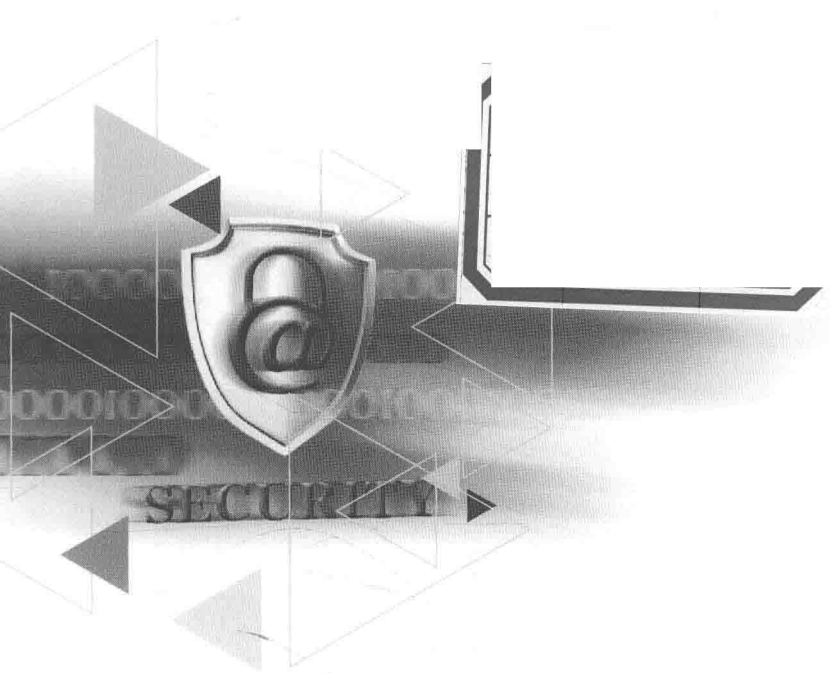

# 主流操作系统安全实验教程

王　鹃　张焕国　主编

WUHAN UNIVERSITY PRESS
武汉大学出版社




# 主流操作系统安全实验教程

王 鹃 张焕国 主编

WUHAN UNIVERSITY PRESS
武汉大学出版社

**图书在版编目(CIP)数据**

主流操作系统安全实验教程/王鹃,张焕国主编. —武汉:武汉大学出版社,2016.11

ISBN 978-7-307-18885-3

Ⅰ.主… Ⅱ.①王… ②张… Ⅲ.操作系统—教材 Ⅳ.TP316

中国版本图书馆 CIP 数据核字(2016)第 288281 号

责任编辑:刘 阳 责任校对:汪欣怡 整体设计:马 佳

出版发行:**武汉大学出版社** (430072 武昌 珞珈山)

(电子邮件:cbs22@whu.edu.cn 网址:www.wdp.com.cn)

印刷:虎彩印艺股份有限公司

开本:787×1092 1/16 印张:8.75 字数:206 千字 插页:1

版次:2016 年 11 月第 1 版 2016 年 11 月第 1 次印刷

ISBN 978-7-307-18885-3 定价:24.00 元

# 前　言

本书是《主流操作系统安全》一书的实验教材，主要讲述了包括主流操作系统身份认证、访问控制、内核架构、驱动开发和内核漏洞等主题共 13 个实验。每个实验都包括实验目的、实验环境、实验要求、实验内容和步骤、实验报告及参考资料相关内容。

全书共分为 13 章，实验一为 Linux 系统的基本操作；实验二为 Linux 文件权限；实验三为 Linux 系统用户密码机制；实验四为操作系统内存分配及缓冲区溢出；实验五为 ALSR 及绕过方法；实验六为 Windows 内核架构及驱动开发；实验七为 Linux 内核架构；实验八为 Linux 基本访问控制实现机制；实验九为 Selinux 及源代码分析；实验十为 Capability 机制；实验十一为 Windows 操作系统内核漏洞实例；实验十二为 Linux 操作系统内核漏洞实例；实验十三为安卓 Rooting。

本书具有如下特点：内容组织从易到难，便于掌握；侧重操作系统攻防实践及基本技能的掌握；提供实验环境及参考代码。

本书由王鹃副教授、张焕国教授担任主编，王鹃制定了本书大纲、内容安排并指导文字写作；张焕国教授负责本书的统稿和审阅工作。其中，樊成阳参与了实验一~三的编写工作；何能斌参与了实验五、实验六和实验九的编写工作；文茹参与了实验四、实验十二的编写工作；洪智参与了实验七~八和实验十一的编写工作；张雨菡参与了实验九和实验十的编写工作。

感谢选修“主流操作系统安全”课程的学生们提出的意见和建议。

因为时间有限，有些内容本书未能全部覆盖。同时，由于作者的认识水平和领悟能力有限，书中难免存在缺点和疏漏，敬请各位专家以及广大读者批评指正。

**王鹃于武汉大学**

2016 年 11 月

# 目　录

# 第一部分　实验预备知识

## 第一节　主流操作系统安全实验的性质、任务与要求

### 一、主流操作系统安全实验的性质与任务

主流操作系统安全课程的学习目标是使学生能够深入了解和掌握目前主流操作系统，如 Windows、Linux 和安卓操作系统的安全架构、原理和机制，并结合操作系统内核攻防实践，使学生具备使用和设计操作系统安全架构和机制的基本方法和技能。

通过本课程的学习，学生在理论知识和实践技能上应达到以下要求：

(1)了解操作系统安全架构设计及原则；

(2)掌握 Linux 基本命令；

(3)熟悉应用程序内存分配原理及其安全防御措施；

(4)了解 Windows 操作系统的安全架构；

(5)熟悉 Windows 访问控制的实现机制；

(6)熟悉 Linux 操作系统的安全架构；

(7)熟悉 Linux 下访问控制实现机制；

(8)了解安卓操作系统的安全架构、原理和机制；

(9)了解和掌握对操作系统内核进行攻击的常用方法；

(10)熟悉各种调试工具的使用方法，如 Ollydbg、IDA pro、Windbg、Gdb 等。

主流操作系统安全是一门实践性较强的课程，因此我们精心组织了 13 个实验。这 13 个实验涵盖了操作系统的基本命令、主要安全机制、内核漏洞等内容。通过这 13 个实验，学生们能够掌握操作系统的基本使用方法和操作系统的攻防实战技能，并通过实验，能够深入理解操作系统的主要安全机制。

### 二、主流操作系统安全实验的一般要求

1. 实验前要求

为避免盲目性，参加实验者应对实验内容进行预习。要明确实验的目的和要求，掌握有关操作系统安全实验的基本原理，根据实验指导教程，拟出实验方法和步骤，观察实验数据，分析实验结果。

2. 实验中要求

(1)参加实验者要自觉遵守实验室规则。

(2)按实验方案认真实现。

(3)认真记录实验条件和所得数据，遇到问题应首先独立思考，耐心排除，并记录下解决的过程和方法。

(4)有疑问报告指导教师，等待处理。

(5)实验结束时，应将实验记录经指导教师审阅签字，清理现场。

3. 实验后要求

实验后要求学生认真写好实验报告，内容包括：

(1)列出实验条件，包括实验时间、地点及实验环境等。

(2)认真整理和处理测试的数据。

(3)对测试结果进行理论分析，做出简明扼要的结论。

(4)写出实验的心得体会及改进实验的建议。

## 第二节　实验主要涉及的操作系统类型

主流操作系统安全实验指导教程基于目前使用较广的操作系统，如 Windows 系统、Linux 系统和安卓系统。实验中需要准备相应版本的虚拟机操作系统镜像，在虚拟环境下进行相关实验。

### 一、Windows 操作系统

Windows 是目前主流的操作系统之一。Windows 系统包括客户机和服务器版本。主要的版本包括 Windows 95、Windows 98、Windows ME、Windows 2000、Windows 2003、Windows XP、Windows Vista、Windows 7、Windows 8、Windows 10 和 Windows Server 服务器操作系统，等等。本实验指导教程中涉及的主要是 Win XP 和 Win 7。

### 二、Linux 操作系统

Linux 系统是目前使用较多的开源操作系统。Linux 系统在服务器以及一些国产操作系统中使用较多。目前的主流版本包括 Ubuntu、CentOS、Fedora 和 OpenSuse 等。本实验指导教程中涉及的主要是 Ubuntu 和 Kali。

### 三、安卓操作系统

Android 是一种基于 Linux 的自由及开放源代码的操作系统，主要使用于移动设备，如智能手机和平板电脑，由 Google 公司和开放手机联盟领导及开发，目前包括从 Android 1.5 到 Nougat-Android 7.0 的多个版本。本实验指导教程中涉及的主要是 Android 4.2 版本。

# 第二部分　主流操作系统安全实验

## 实验一　Linux 系统的基本操作

### 一、实验目的

通过本次实验掌握 Linux 系统的基本命令及管理配置方法

### 二、实验环境

Ubuntu 12.04 虚拟机或 Kali 虚拟机

### 三、实验要求

(1)熟悉 Linux 管理的基本命令类型及要求
(2)掌握 Linux 运行环境的命令及使用格式
(3)掌握 Linux 系统的常用命令

### 四、实验内容和步骤

**1. 实验内容**

(1)Linux 系统的使用界面和各项功能
(2)目录操作
(3)文件操作命令
(4)系统询问与权限命令
(5)进程操作命令
(6)其他命令

**2. 实验步骤**

(1)Linux 命令格式
Linux 系统中 bash 命令的一般格式是：
命令名【选项】【处理对象】
例：$ ls -la mydir
使用 bash 命令时，应注意以下几点：

①命令名一般是小写英文字母，注意大小写有区别。

②格式中由方括号括起来的是可选的。

③选项是对命令的特别定义，以“-”开始。命令名，选项，处理对象三者之间用空格隔开。

④命令后加上“&”可使该命令后台执行。

⑤目录之间的分隔为(/)，区别于 DOS 中的(\)。

⑥Linux 系统的联机帮助对每个命令的准确语法都作了详细的说明。

(2)命令输入格式

在 shell 提示符“$”之后，可以输入相应的命令和参数，最后必须按 Enter 键予以确认。Shell 会读取该命令并予以执行。命令完成后，屏幕将再次显示提示符“$”。

(3)目录操作命令

Linux 文件系统采用树状目录管理结构，即只有一个根目录，其中含有下级子目录或文件信息。主目录往往位于/home 或/user 目录之下，例如/home/user。

路径名描述了文件系统通向任意文件的路径。有两种路径名：绝对路径和相对路径。

绝对路径：从根目录开始到达相应文件的所有目录名连接而成，各目录名之间以“/”隔开。

相对路径：是相对于当前工作路径指定一个文件。当访问当前工作目录或其子目录中的文件时，可以使用相对路径。

①显示目录内容：ls 命令

-a 列出指定目录下所有子目录和文件，包括以“.”开头的隐藏文件。

-t 按照文件最后修改时间的新旧顺序，最新的文件列在前面。

-F 显示当前目录下的文件及其类型。在列出的文件名后面加上不同的符号，以区分不同类型的文件，可以附加的符号有：“/”表示目录，“*”表示可执行文件。

-R 递归地列出该目录及其子目录下的文件信息。

-l 显示目录下所有文件类型·权限·链接数·文件主·文件组·文件大小·最近修改时间·文件名。

实验内容如图 1-1、图 1-2 所示。

②创建目录：mkdir 命令

格式：mkdir【选项】dirname

常用选项：

-p 可在指定目录下逐级创建目录。

-m 创建指定目录的同时设置该目录存取权限，权限用数字表示。

实验内容如图 1-3 所示。

③删除目录：rmdir 命令

格式：rmdir【选项】dirname

常用选项：

-p 递归删除指定目录下的所有空目录，如果有非空目录，则该目录保留下来。

实验内容如图 1-4 所示。


图 1-1　ls 命令

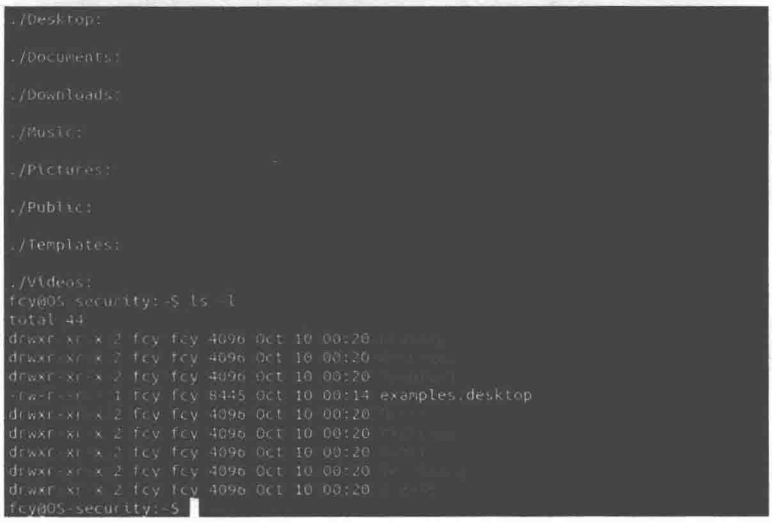



图 1-2　ls 命令

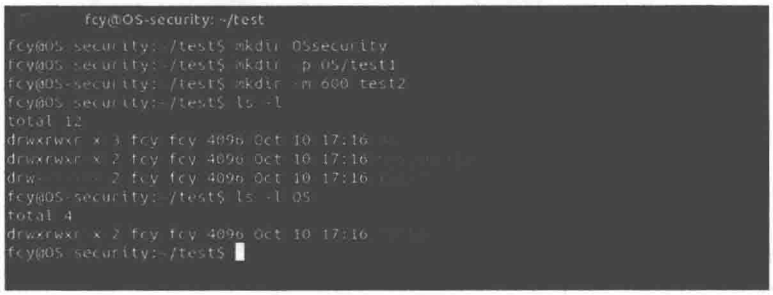



图 1-3　mkdir 命令


图 1-4　rmdir 命令

④改变工作目录：cd 命令

格式：cd【dirname】

Dirname 表示目标目录的绝对路径或相对路径。

cd . . 改变目录位置，至当前目录的上层目录。

cd -　回到进入当前目录前的上一个目录。

实验内容如图 1-5 所示。


图 1-5　cd 命令

⑤显示当前工作目录的绝对路径：pwd 命令

实验内容如图 1-6 所示。


图 1-6　pwd 命令

(4)文件操作命令

①查看文件内容：cat 命令

格式：cat【选项】filename

-b 从 1 开始对所有非空输出进行编号。

-n 从 1 开始对所有输出进行编号。

-s 将多个相邻的空行进行合并成一个空行。

实验内容如图 1-7、图 1-8 所示。

②删除文件：rm 命令

格式：rm【选项】filename

-f 忽略不存在的文件，并且不给提示。

-r 递归删除指定目录及其下属的各级子目录和文件。

-i 交互式删除文件，系统提示是否删除文件，输入 y 确定。

```
fcy@OS-security:~$ cat test.c
#include <stdio.h>


int main(void)
{
    printf("Hello, world!\n");
}
fcy@OS-security:~$ cat -b test.c
     1  #include <stdio.h>


     2  int main(void)
     3  {
     4      printf("Hello, world!\n");
     5  }
```

图 1-7　cat 命令

```
fcy@OS-security:~$ cat -n test.c
     1  #include <stdio.h>
     2
     3
     4  int main(void)
     5  {
     6      printf("Hello, world!\n");
     7  }
fcy@OS-security:~$ cat -s test.c
#include <stdio.h>

int main(void)
{
    printf("Hello, world!\n");
}
fcy@OS-security:~$
```

图 1-8　cat 命令

实验内容如图 1-9 所示。

```
fcy@OS-security:~
fcy@OS-security:~$ ls
                                                    test.c
examples.desktop
fcy@OS-security:~$ rm -i test.c
rm: remove regular empty file 'test.c'? y
fcy@OS-security:~$ rm file1
rm: cannot remove 'file1': No such file or directory
fcy@OS-security:~$ rm -f file1
fcy@OS-security:~$ rm -r testdir
fcy@OS-security:~$ ls
examples.desktop
fcy@OS-security:~$
```

图 1-9　rm 命令

③复制文件或目录：cp 命令

格式：cp【选项】source target

-i 交互式复制，覆盖已存在的目标文件之前给出提示信息。

-p 除复制源文件的内容外，还将其修改时间和存取权限也复制到新文件中。

-r 把源目录下的所有文件及其各级子目录都复制到目标位置。

-l 不复制文件，而是创建指向源文件的链接文件，链接文件名由目标文件给出。

实验内容如图 1-10 所示。


图 1-10　cp 命令

④移动或更改文件、目录名称：mv 命令

格式：mv【选项】source target

实验内容如图 1-11 所示。


图 1-11　mv 命令

(5)系统询问与权限命令

①查看系统中的使用者：who 命令

格式：who【选项】【am i】

-q 仅显示用户名及用户总数。

-H 显示信息时间时显示各列的标题。

am i 是该命令的一种常用方式，显示本用户终端的相关信息。

实验内容如图 1-12 所示。

②改变自己的 username 的账号与口令：su 命令

实验内容如图 1-13 所示。

③改变文件或目录的权限：chmod 命令

格式：chmod【选项】【who】【操作符号】【mode】name

-R 递归处理

who 可以是 u，g，o，a

操作符号可以是：“+”添加权限，“-”取消权限，“=”赋予给定权限并取消其他

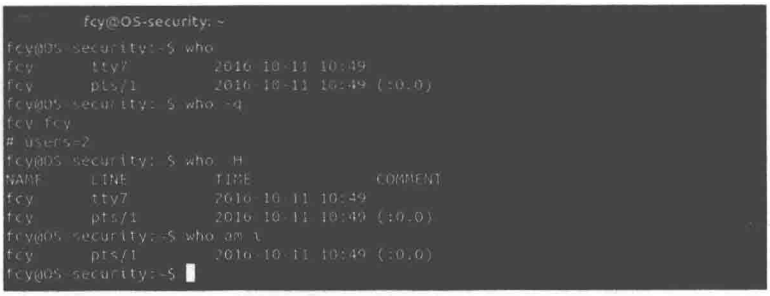



图 1-12　who 命令


图 1-13　su 命令

权限。

r 表示 read，数字代号“4”；w 表示 write，数字代号“2”，x 表示 execute，数字代号“1”。

实验内容如图 1-14 所示。

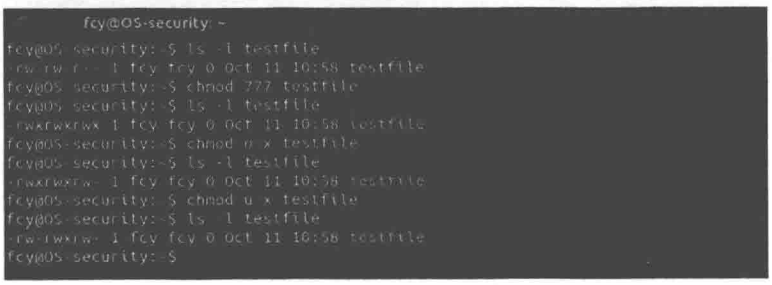



图 1-14　chmod 命令

④改变文件或目录的所有权：chown 命令

格式：chown【选项】username name

说明：该命令时用来改变指定文件所属的用户组。

-R 递归改变指定目录及其下面所有子目录和文件用户组。

实验内容如图 1-15 所示。

⑤检查用户所在组名称：groups 命令

实验内容如图 1-16 所示。

⑥改变文件或目录的最后修改时间：touch 命令