
网络攻防实战

第三周

陈健

chenj@nju.edu.cn

在程序之间建立连接

——重定向

☐ 输入流

- 默认键盘

☐ 输出流

- 默认屏幕

☐ 重定向流到文件

- **> file**

- ☐ `echo hello > hello.txt`
- ☐ `cat hello.txt`

- **< file**

- ☐ `cat < hello.txt`
- ☐ `cat < hello.txt > hello2.txt`

- **>> file**

- ☐ `cat < hello.txt >> hello2.txt`

在程序之间建立连接

——管道

- 管道“|”将一个程序的输出和另一个程序的输入连接起来
 - `ls -l /usr/bin | less`
 - `ls -l /usr/bin | tail -n1`

在程序之间建立连接

——管道

□ ls | rm

- 这个命令能删除当前目录下的所有文件吗？如果不行，为什么？
- 如果一定要通过管道实现这个功能，应该怎么做？

Linux系统基本命令

☐ 创建文件

■ cat

- ☐ cat > test.txt

- ☐ cat >> test.txt

■ touch

- ☐ touch newfile

☐ 创建目录

■ mkdir

- ☐ mkdir newdirectory

Linux系统基本命令

□ 删除目录

■ rmdir

- rmdir directory
- 只能删除空目录

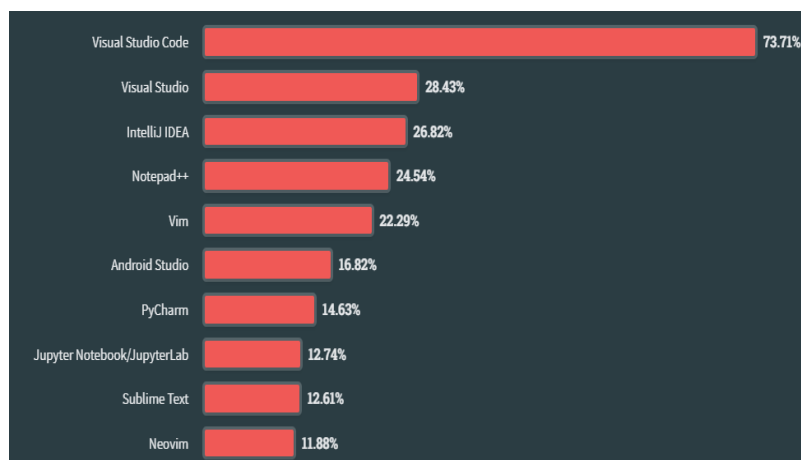
■ rm

- 删除目录及其中所有文件
 - rm -r directory

Shell的通配

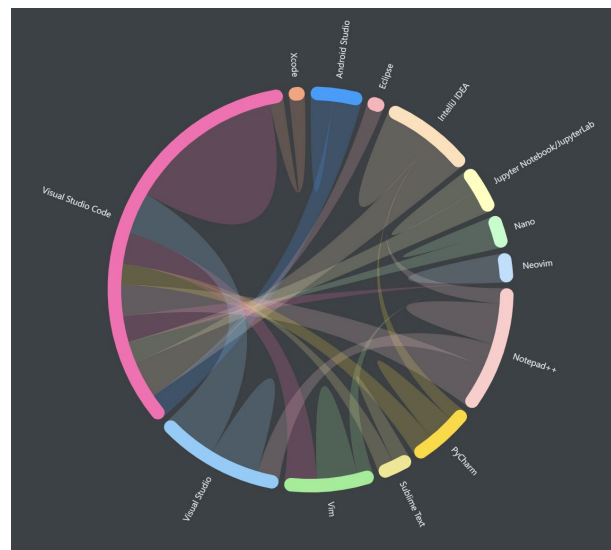
- 通配符*、?
 - `rm foo?`
 - `rm foo*`
- 方括号[]
 - `ls test[123]`
 - `ls test[1-3]`
 - `ls test[a-z]`
- 花括号{}
 - `cp /project/{foo,bar,baz}.sh /newproject`
 - 展开为 `cp /project/foo.sh /project/bar.sh /project/baz.sh /newproject`
 - `mv *{.py,.sh} folder`
 - 会移动所有*.py和*.sh文件
 - `touch {foo,bar}/{a..h}`

该学哪个代码编辑器



stack overflow 2023年调查

<https://survey.stackoverflow.co/2023/#worked-with-vs-want-to-work-with-new-collab-tools-worked-want>



stack overflow 2024年调查

<https://survey.stackoverflow.co/2024/technology#worked-with-vs-want-to-work-with>

vim历史

- ❑ 1976年, Bill Joy发布vi
- ❑ 1991年, Bram Moolenaar发布vim
- ❑ 有“模式”的编辑器



Ken Thompson



Bill Joy



Bram Moolenaar

Linux系统基本命令

☐ 查找二进制程序

- whereis

- which

- ☐ 在PATH环境变量中查找

☐ 查找文件

- find

- ☐ find directory options expression

- find / -type f -name apache2

- ☐ 通配符的使用*、?、[]

- find / -type f -name apache2.*

- locate

- ☐ locate test

- ☐ updatedb负责更新后台数据库

find命令练习

- ❑ 查找当前目录及其子目录下所有名为src的目录
 - `find . -name src -type d`
- ❑ 查找当前目录及其子目录下名为test的目录下的所有py文件
 - `find . -path '**/test/*.py' -type f`
- ❑ 查找当前目录下前一天修改的所有文件
 - `find . -mtime -1`
- ❑ 查找当前目录下所有大小在100k至1M的后缀为.tar.gz的文件
 - `find . -size +100k -size -1M -name '*.tar.gz'`
- ❑ 删除当前目录下后缀为.tmp的所有文件
 - `find . -name '*.tmp' -exec rm {} \;`
 - `find . -type f -exec rm -- {} +`
 - `find . -type f -exec rm {} \;`

Linux系统基本命令

□ 查找文件内容

■ grep

- grep text file
- 递归搜索目录
 - grep -R text .
- 获取匹配文本的上下文
 - grep -C 2 text *
- 输出不匹配的结果
 - grep -v text file
- 利用管道实现关键字搜索
 - ps aux | grep cron

课堂练习-1

请利用前面学到的命令来显示文件`/etc/passwd`中包含字符串**kali**的一行之前五行的内容。

注：如果你想到用某个命令来完成这个任务，但遇到困难，可以查看该命令的帮助信息，了解是否有某个选项支持你的想法。

作业1提交方法和截止时间

- 实验报告的文件名命名统一为：
 - 学号_lab01.pdf
- 提交截止时间：2025年9月16日零点
- 实验报告通过电子邮件发送给
chenj@nju.edu.cn