网络攻防实战

第2周

陈健

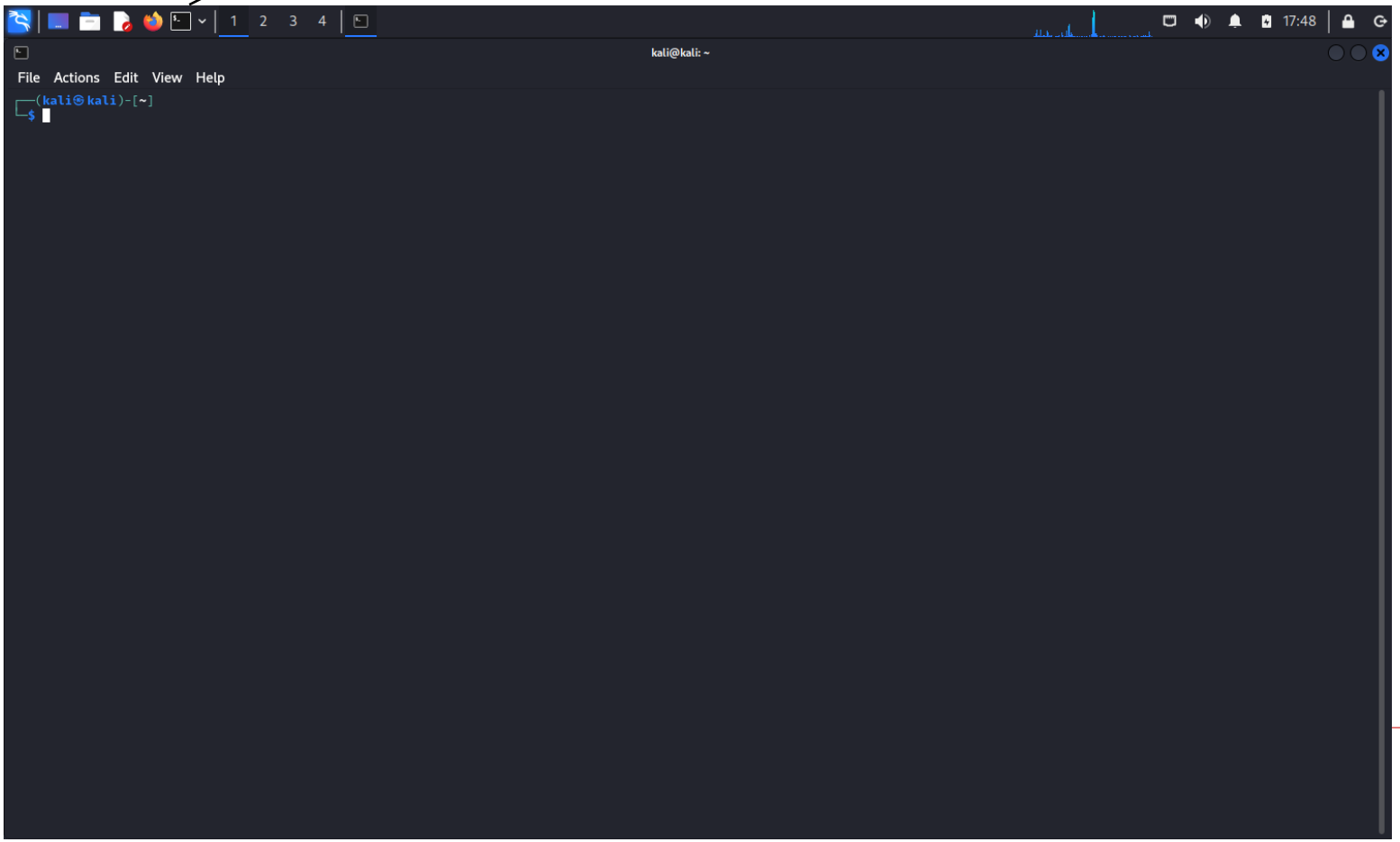
chenj@nju.edu.cn

Virtualbox中虚拟机的远程访问

- 添加端口转发
  - 管理->工具->网络管理器->NAT网络->端口转发->添加转发规则
    - 将虚拟机的端口号22映射到本机回路地址的未使用端口
- 虚拟机启用SSH服务
  - sudo systemctl start ssh

打开终端

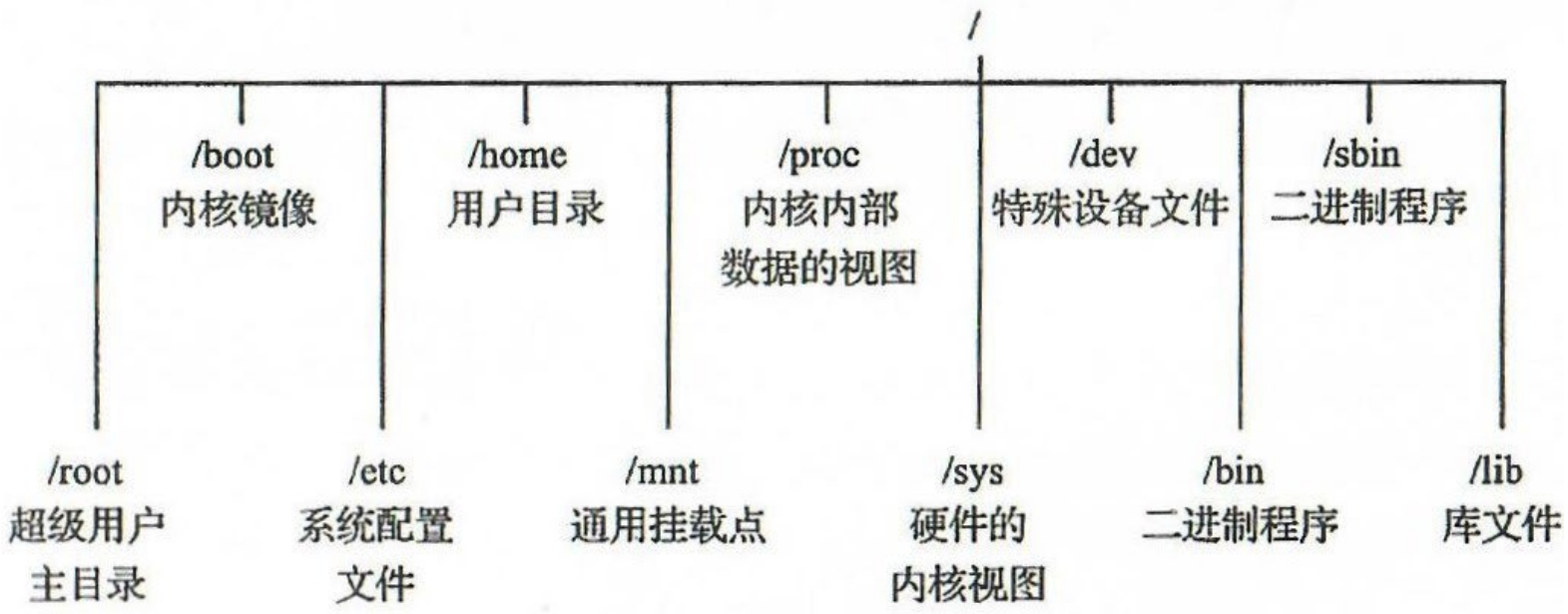
点击该图标或按下ctrl-alt-t组合键打开终端



修改密码

$ passwd

Linux文件系统


/
/boot
内核镜像
/home
用户目录
/proc
内核内部
数据的视图
/dev
特殊设备文件
/sbin
二进制程序
/root
超级用户
主目录
/etc
系统配置
文件
/mnt
通用挂载点
/sys
硬件的
内核视图
/bin
二进制程序
/lib
库文件

Linux系统基本命令

- 查看当前位置
  - pwd
- 查看当前登录用户
  - whoami
- 切换目录
  - cd 路径
  - 绝对路径
    - 以/开头的路径
  - 相对路径
    - 相对于当前工作目录的路径
  - 在路径中，.表示当前目录，..表示上级目录

路径练习

```
$ pwd
$ cd /home
$ pwd
$ cd ..
$ pwd
$ cd ./home
$ pwd
$ cd kali
$ pwd
$ ../../bin/echo hello
```

下面两个命令的作用是什么？

```
$ cd ~
$ cd -
```

Linux系统基本命令

- 列举目录内容
  - ls
  - 查看文件和目录的更详细信息
    - ls -l
  - 显示隐藏文件信息
    - ls -la
- 获取帮助
  - command –h | command --help
    - ls --help
  - man command
    - man ls

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 {} \;

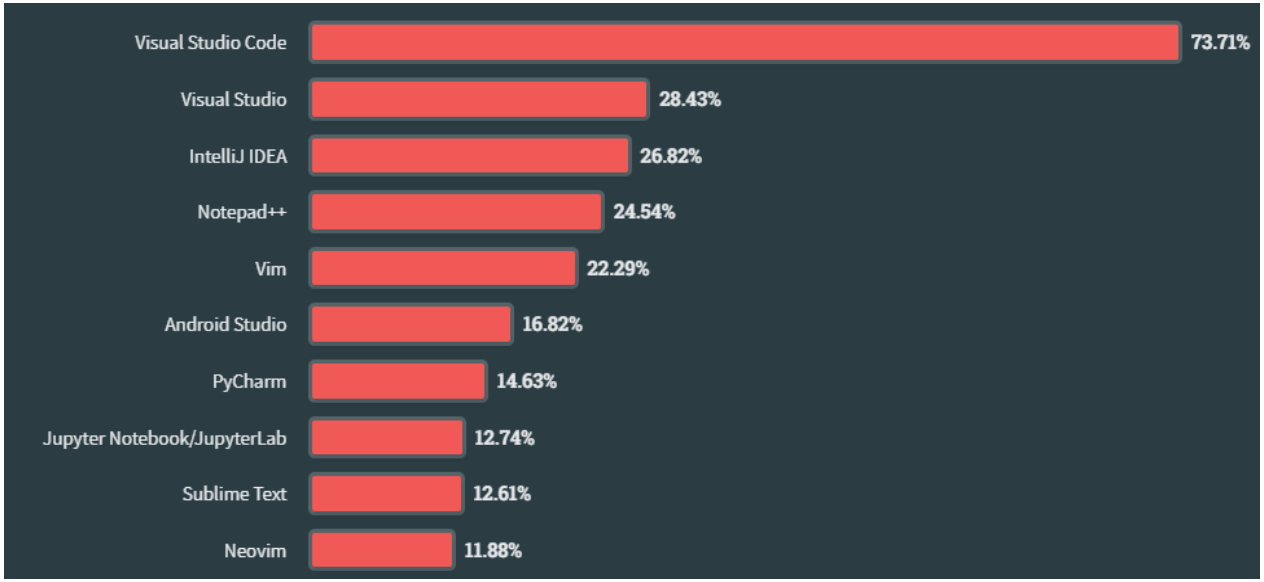
Linux系统基本命令

- 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

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

该学哪个代码编辑器

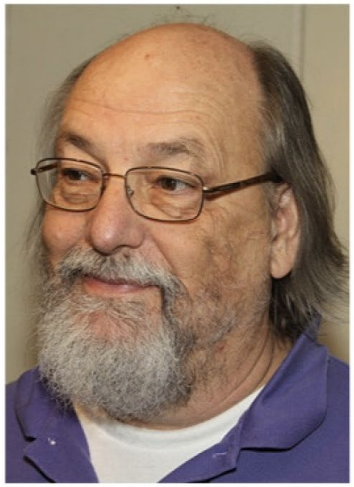


stack overflow 2023调查

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

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

- 复制文件
  - cp
    - cp a.txt b.txt
    - cp a.txt ../
- 重命名文件
  - mv
    - mv a.txt b.txt
    - mv directory-1 directory-2
    - mv a.txt /home/kali
- 删除文件
  - rm
    - rm a.txt

Linux系统基本命令

- 删除目录
  - rmdir
    - rmdir directory
    - 只能删除空目录
  - rm
    - rm –r directory
    - 删除目录及其中所有文件

Linux系统基本命令

- 查看文件
  - more
    - more /etc/passwd
      - 输入q提前退出
  - less
    - less /etc/passwd
      - 输入q退出
      - 支持上下翻页
      - 支持输入“/”进行关键字搜索

Linux系统基本命令

- 查看文件
  - 获取文件头部内容
    - head
      - head /etc/passwd
      - head -20 /etc/passwd
  - 获取文件尾部信息
    - tail
      - tail /etc/passwd
      - tail -20 /etc/passwd
  - 标注行号
    - nl
      - nl /etc/passwd

课堂练习

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。

KALI修改时区

```
$ echo “zone=Asia/Shanghai” | sudo tee -a /usr/share/zoneinfo/Asia/Shanghai

$ sudo rm /etc/localtime

$ sudo ln -s /usr/share/zoneinfo/Asia/Shanghai /etc/localtime
```

KALI设置软件源

- 编辑文件/etc/apt/sources.list
  - $ sudo mousepad /etc/apt/sources.list

```
deb http://mirror.nju.edu.cn/kali kali-rolling main contrib non-free non-free-firmware
```

KALI软件更新

- 更新本地软件包索引
  - sudo apt update
- 升级所有已安装软件包到新版本
  - sudo apt upgrade
- KALI大版本升级
  - sudo apt-get dist-upgrade

谨慎使用

KALI软件包管理

- 搜索软件包
  - apt-cache –n search 软件包名
- 安装软件包
  - apt install 软件包名
- 卸载软件包
  - apt remove 软件包名
  - apt purge 软件包名
    - 删除软件包括其配置文件

KALI软件包管理

- 查看软件包是否已安装
  - apt list --installed | grep 软件包名
  - dpkg –l 软件包名
- 查看已安装软件包中包含的文件
  - dpkg –L 软件包名
- 查看某个命令是由哪个软件包提供
  - dpkg –S command

KALI设置中文环境

- sudo dpkg-reconfigure locales
  - 选择字符编码： en_US.UTF-8、zh_CN.GBK、zh_CN.UTF-8
  - 选择zh_CN.UTF-8 后回车确认
- 安装字体
  - sudo apt install ttf-wqy-microhei ttf-wqy-zenhei xfonts-wqy
- 重启

作业1提交方法和截止期限

- 实验报告的文件名命名统一为：学号_lab01.pdf
- 提交截止期限：2024年9月17日零点
- 实验报告通过电子邮件发送给chenj@nju.edu.cn