《Linux操作系统与Shell编程实验》

期末考查

2021-2022学年第1学期

1. 程序设计题（每小题20分，共4小题）

1. 新建文件data1，输入以下几行：

www.taobao.com

www.sdyu.edu.cn

www.baidu.com

www.sdyu.edu.cn/111222error.html

www.baidu.com/11111error.html

[www.bilibili.com](http://www.bilibili.com)

写一段代码，使用wget命令逐一测试文件data1中的链接是否有效，将有效链接写入文件goodlink，并显示输出文件goodlink内容。

答：（粘贴代码、代码执行截图）

1.新建脚本：gedit testweb.sh

2.编辑脚本

3.赋予权限：chmod +x testweb.sh

4.执行脚本：./testweb.sh

5.输入测试网址，由脚本自动保存网址到data文件，并开始测试链接，测试完毕，输出goodlink中测试有效的链接

6.查看data/goodlink内容：cat data/goodlink

脚本：

#!/bin/bash

echo "请输入您要测试的web链接用空格隔开！"

read input

input\_array=(${input})

len=${#input\_array[@]}

echo > data

echo > goodlink

if [[ "${len}" -gt "0" ]]; then

for (( index = 0; index < len; ++index )); do

echo ${input\_array[index]} >> data

resp\_status=$(wget --save-headers -q -O - ${input\_array[index]} | grep -o '200 OK')

if [[ "$resp\_status" != "" ]]; then

echo ${input\_array[index]} >> goodlink

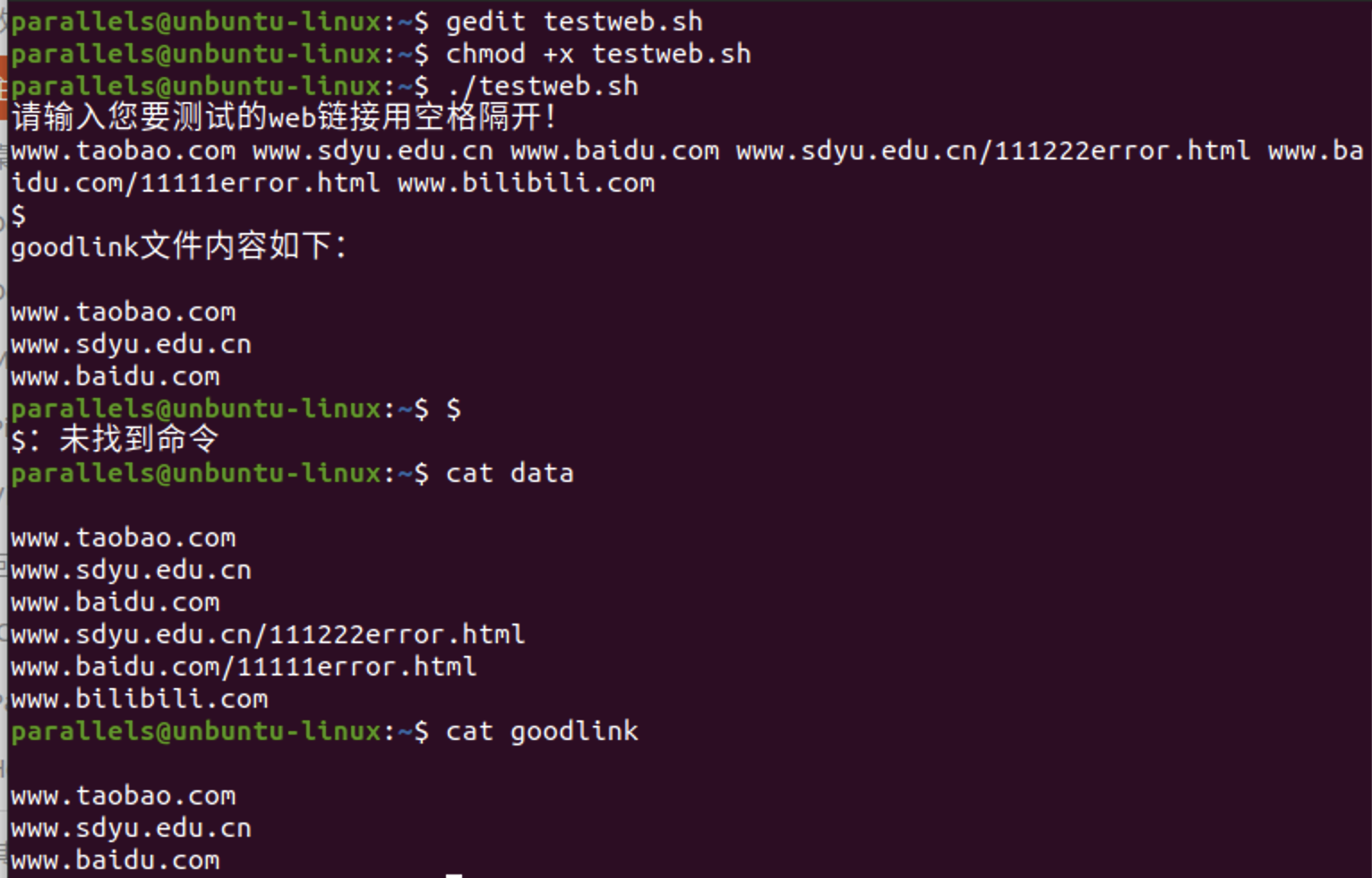
fi

done

echo "goodlink文件内容如下："

cat goodlink

fi



2. 新建文件data2，输入以下几行数据，注意不要忘记输入英文逗号：

huawei, 1000

iphone, 3500

vivo , 1600

Lenovo , 2000

Samsung, 4000

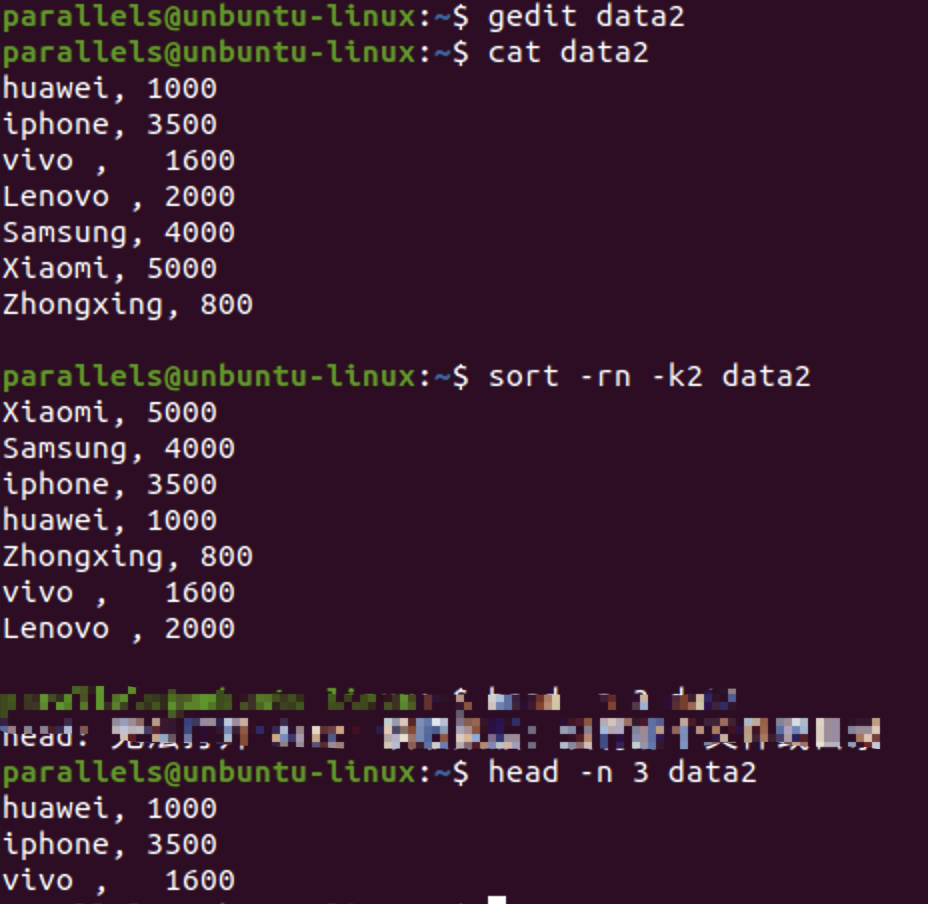
Xiaomi, 5000

Zhongxing, 800

第一列数据是手机品牌，第二列是某月销量。使用命令或脚本，取销量前三名的品牌及其销量。

答：（粘贴命令、执行截图）

1. gedit data2
2. cat data2
3. head -n 3 data2



3. root用户启动vim， 其他用户如何查看root用户正在运行vim程序？ 用户Alice能否停止用户Bob的进程？ 为什么？

答：

1. 使用ps -e|grep root 命令查看root用户的全部运行进程

2.可以。因为Linux的进程管理手段非常丰富，可以采取多种方法杀掉进程。通过ps查找到进程的PID，直接用kill -9 [PID]命令强迫停止指定进程。

4. 写一段代码，循环测试root账号是否登录，如果root账户登录后，打印一段提示信息：root checked in，并测试你的代码

答：（粘贴命令或代码、执行截图）

1.gedit testUser.sh

2.chmod +x testUser.sh

3../testUser.sh

testUser.sh脚本：

#/bin/bash

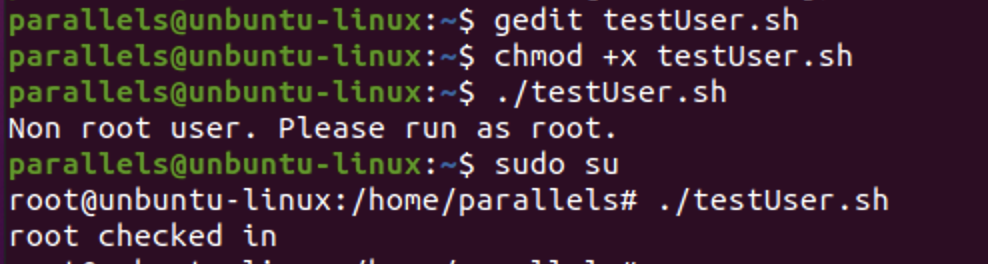
until who | grep "root" &> /dev/null;

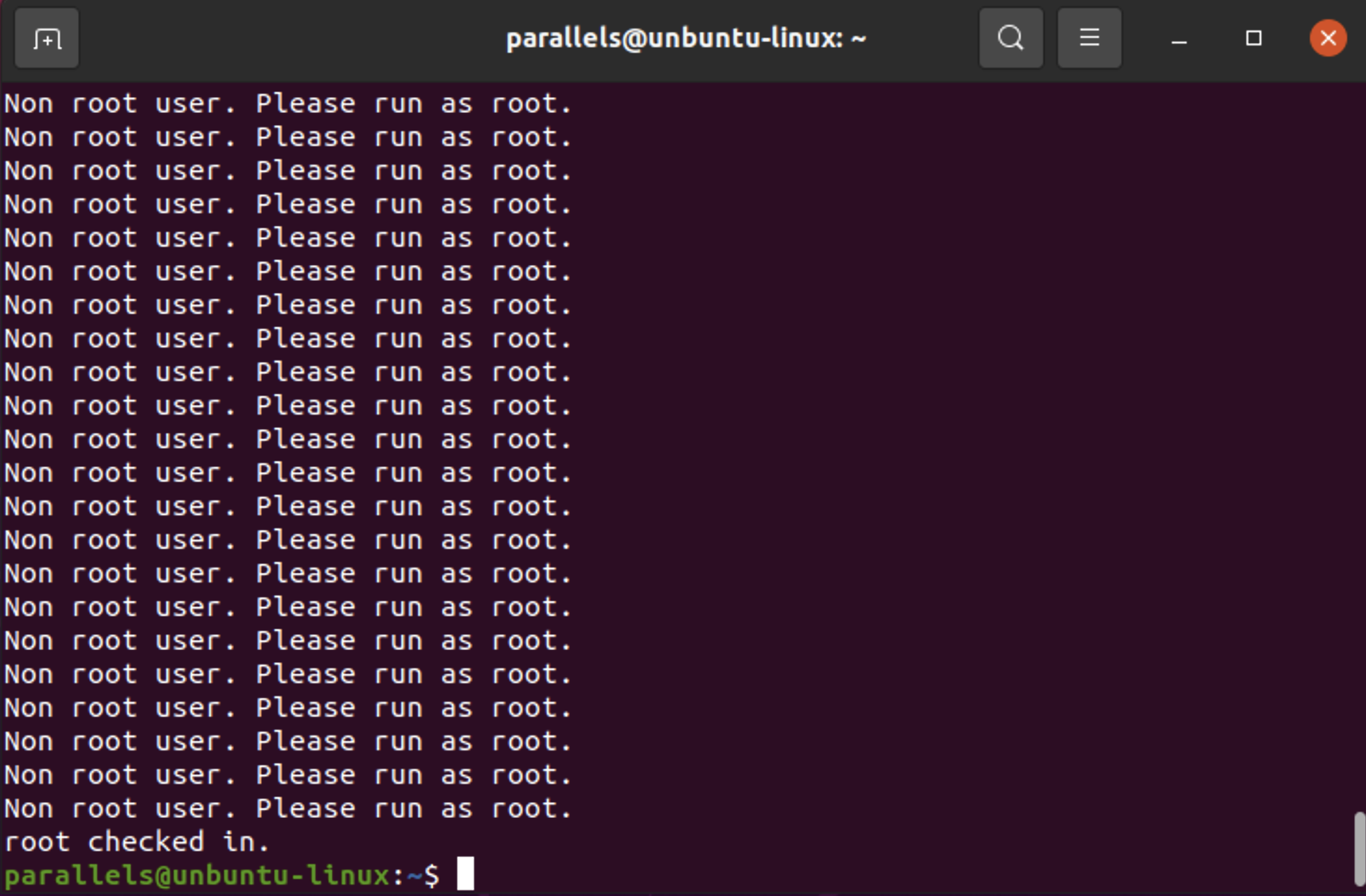
do

echo "Non root user. Please run as root. "

done

echo "root checked in."





二、论述题（20分）

5. Windows系统经常遭受软件病毒的侵害，比如熊猫烧香、勒索病毒等，Linux系统较少受到这种病毒攻击，为什么？

答：

1. 对一个二进制的 Linux 病毒，要感染可执行文件，这些可执行文件对启动这个病毒的用户一定要是可写的。而实际情况通常是，程序被 root 拥有，用户通过无特权的帐号运行。而且，越是没有经验的普通用户，他拥有可执行文件的可能性就越小。因此，不适合病毒繁殖。
2. Linux的应用软件和系统软件几乎都是开源的。这对病毒有两方面的影响。首先，病毒很难藏身于开源的代码中间。其次，对仅有二进制的病毒，一次新的编译安装就截断了病毒一个主要的传播途径。虽然 Linux 发行商也提供大量的二进制软件包，但是用户大都是从发行商提供的可靠的软件仓库中下载这些软件包，大都具有 md5 验证机制，安全性极高。
3. Linux桌面的用户人数相对较少，病毒攻击无利可图，攻陷Linux系统的难度又极高。