**电子科技大学信息与软件工程学院**

**标准实验报告**

**（实验）课程名称信息安全导论**

**电子科技大学教务处制表**

电子科技大学

**实 验 报 告**

**学生姓名： 贾怀宇 学 号： 2020090916007 指导教师：赵洋**

**实验地点：信软楼400 实验时间：2022年10月31日**

1. **实验室名称：**

**信软楼400**

**二、实验项目名称：Linux系统安全配置**

**三、实验学时： 4 学时**

**（一）实验目的**

Linux操作系统是信息安全领域最常见的一种操作系统。它操作简单又具有可扩展性，既可以作为主机服务器，又可以作为网络攻防中常见的靶机。本次实验希望通过安装linux和最基本的linux操作来初步体验Linux操作系统。

**（二）实验内容**

安装linux操作系统

更改用户登陆密码

添加用户，用户组

创建新文件修改文件权限

使用ssh实现远程登陆

**四、实验原理**

Linux安全体制包括硬件/软件选型、操作系统安全、文件系统、应用程序、网络结构等等，而操作系统安全是其中的一个重要组成部分。Linux系统安全配置可以由很多方面构成：稳定的内核、图形化界面、系统启动安全、防火墙、用户名密码、远程登录ssh、权限控制等等，这些系统安全配置共同保证了系统的安全性。本次实验主要从用户名密码、权限控制、防火墙和远程登录这四个角度出发，进行linux系统安全的配置

1. 用户名密码

用户在登录linux系统时，会对比password与之前保存在“/etc/shadow”、“/etc/gshadow”文件中的密码是否一致。linux的密码加密方式使用单向加密算法，并且添加随机数（salt）计算得出的。通过密码管理命令，可以修改用户密码、设置密码长度及有效时间等

1. 权限控制

**用户组：**linux把用户分为三个基本组：user，group，other来分配基本的权限。用户通过/etc/passwd用过用户名来获取用户的uid，通过/etc/group来获取用户所属组的gid。linux的文件管理权限分为读（r）、写(w)和执行(x)。Linux的文件权限用 3组 每组3位 共9位 字符表示，可以通过终端输入命令ls -al查看当前目录下的所有文件的权限。例如drwx------，会显示10个字符，其中第1位表示文件的类型: d表示文件夹, l表示链接文件, -表示文件；剩余9位分为3组，每组3位，分别表示: 文件所有者、同组用户、其他用户 对该文件的权限；每组的3位字母分别表示对该文件的读(r)、写(w)、执行(x)权限，显示字母表示有该权限，显示-表示没有该权限。

**权限管理：**每组权限可分别由3位二进制数分别表示 r、w、x 的权限开关，1表示有该权限，0表示没有该权限，3位二进制数转换为十进制的一个整数即可用于表示读、写、执行三个权限的开关。使用chmod即可修改文件/目录的 权限；使用chown即可修改文件/目录的 所有者；使用chgrp可修改文件/目录的 所属组

1. 防火墙

防火墙是在被保护网络和因特网之间，或者在其他网络之间限制访问的一种部件或一系列部件。Linux防火墙系统提供了如下功能：访问控制、审计、抗攻击和其他附属功能。Linux防火墙又分为iptables和firewall。防火墙中关键要素有：源IP、目的IP、协议、源端口、目的端口、网卡，通过对这几个要素的配置，能有效控制来自外部的攻击及内部的资料泄漏

1. ssh远程登录

（1）修改ssh端口：默认情况下，SSH监听连接端口22，攻击者使用端口扫描软件就可以看到主机是否运行有SSH服务，将SSH端口修改为大于1024的端口是一个明智的选择，因为大多数端口扫描软件（包括nmap）默认情况都不扫描高位端口

（2）ssh密钥认证：可有效抵御字典功击

（3）禁止root用户登录：如果一个攻击者获得root权限登陆到你的系统，相对他获得一个普通用户权限能造成更大的破坏，配置SSH服务器不允许root用户通过SSH登陆

（4）ssh白名单：仅允许指定用户可登录、指定IP可访问服务器

（5）重试次数：一段时间内，超过登录失败重试次数后，不允许登录

（6）连接超时：超过特定时间后，断开空闲的ssh连接

（7）极端安全措施：ssh审计、端口敲门、动态端口

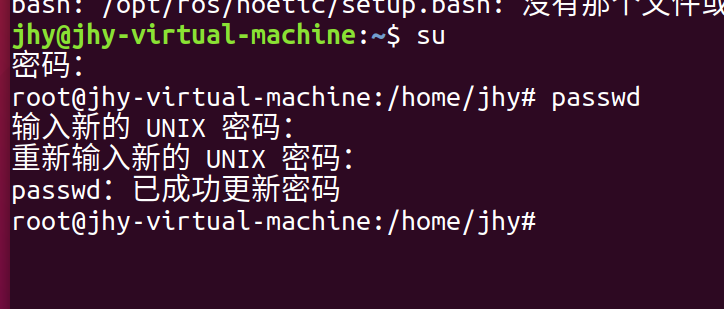
**五、实验器材（设备、元器件）**

（一）学生每人一台PC，安装WindowsXP/2000以上操作系统。

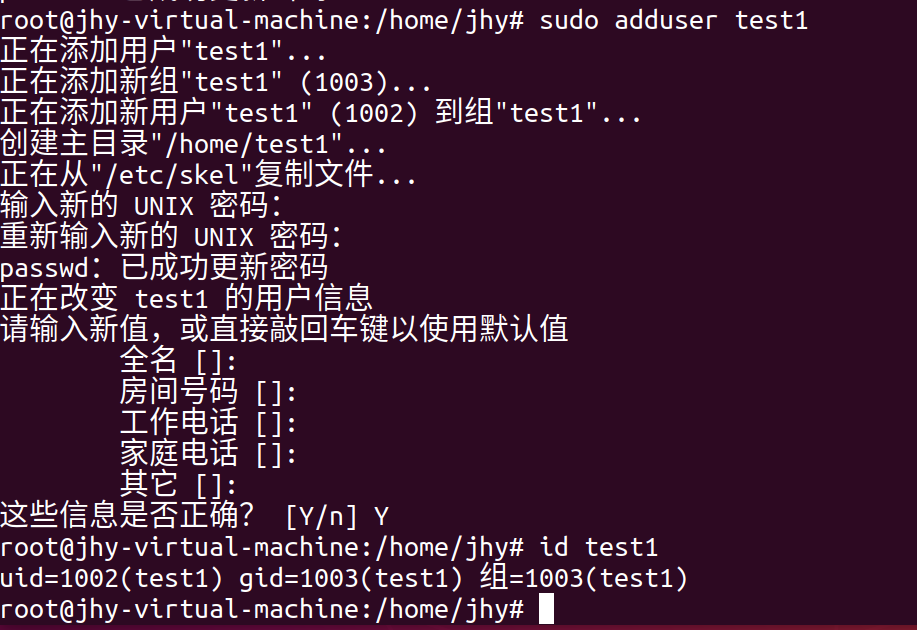
（二）PC机除了最基本的Windows操作系统，还应安装linux操作系统

**六、实验步骤**

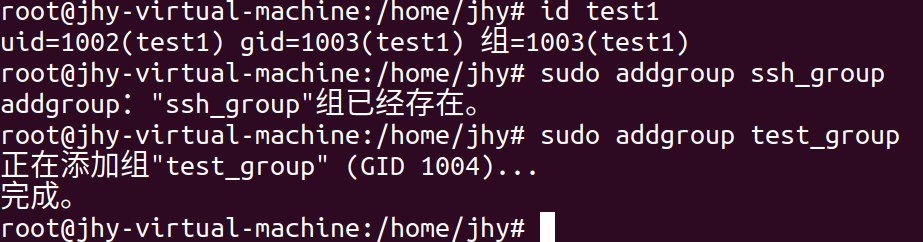
1、先使用su登录root账户，然后使用passwd进行密码修改



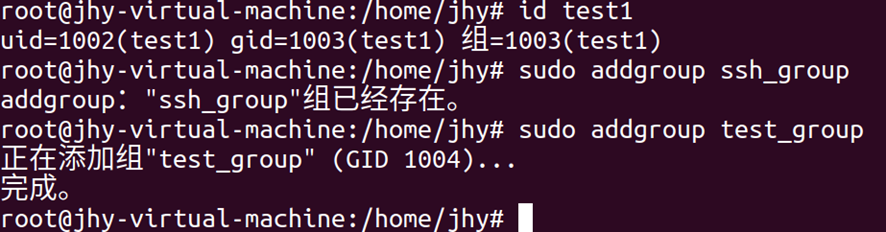
2、使用sudo adduser XXX新建用户，输入密码



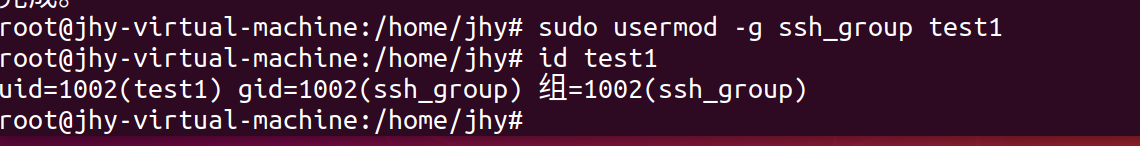
使用id xxx查看用户信息



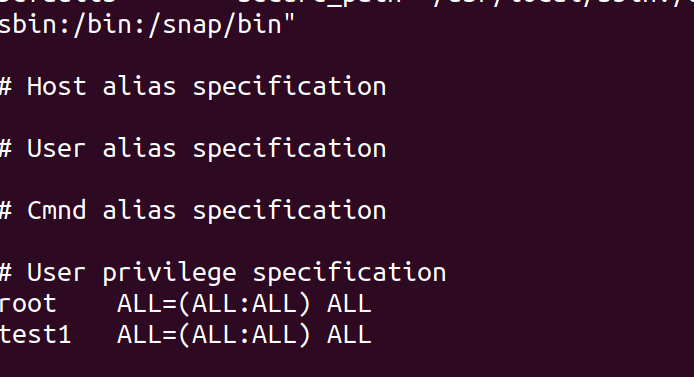
使用groupadd xxx新建用户组



将用户退出原来的默认组并添加到一个已有用户组



赋予用户root权限 vim /etc/sudoers，找到# User privilege specification，在root下面添加用户

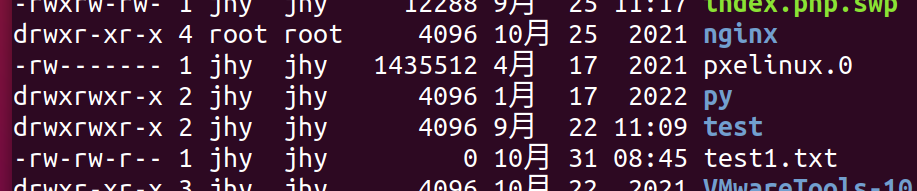


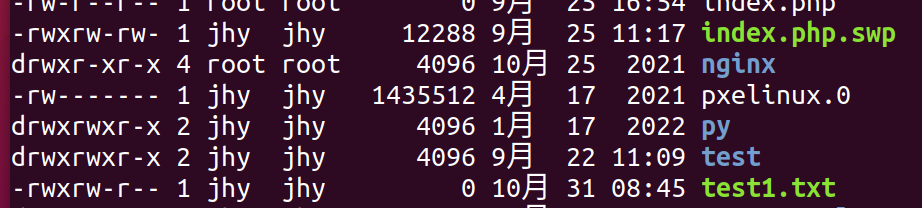
（vim操作：i进入insert模式；esc退出insert模式；:wq!保存并退出）

3、ls –l 查看文件列表

touch test.txt创建文件

chmod 764 修改权限





4、$ apt-get install firewalld

安装防火墙





查看firewalld的帮助：

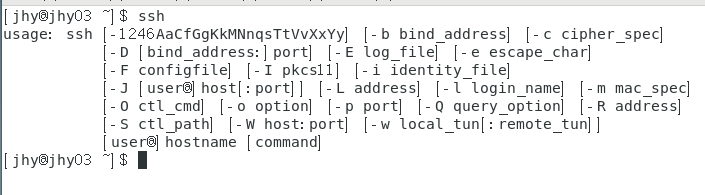
$ firewall-cmd --help

查看防火墙的状态：

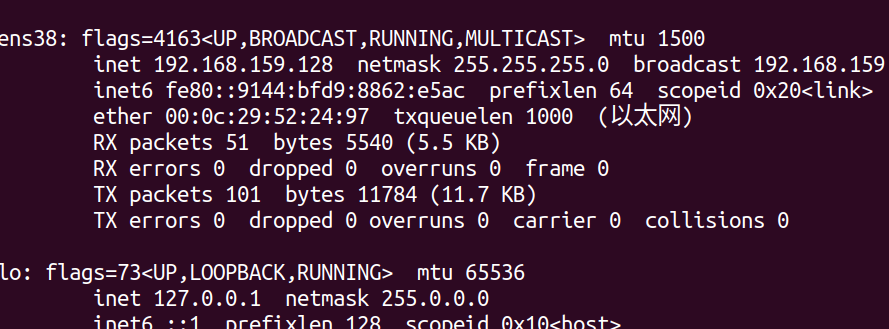
$ firewall-cmd --state

5、先安装ssh客户端

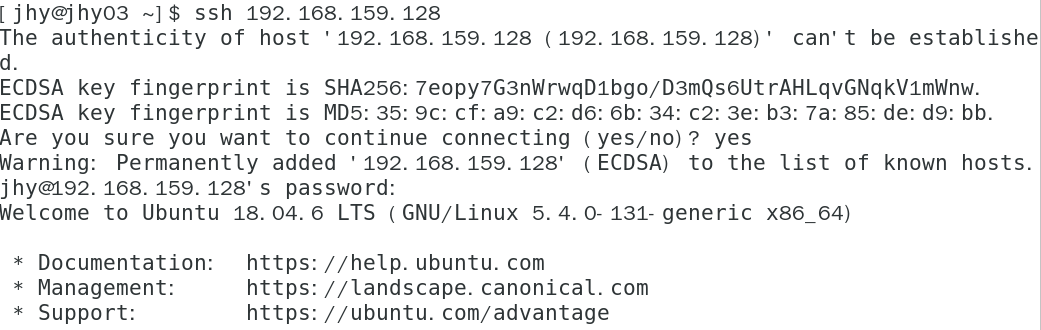
使用sudo apt-get install openssh-server安装ssh客户端



使用ifconfig查看另一台电脑的ip地址



使用ssh 192.168.159.128 (参考) ，输入服务器端登录密码



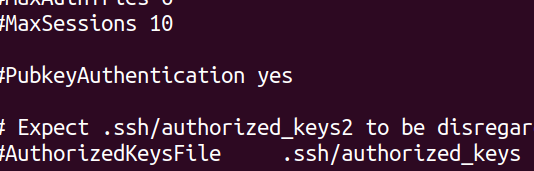
默认的ssh端口往往存在安全风险，修改默认的ssh端口为其他端口(例如33)，然后再使用另一台电脑进行ssh远程登录,在一台电脑(作为服务器端)，使用vim /etc/ssh/sshd\_config用vim编辑器打开ssh配置表，找到# Port 22所在的一行，去掉行首的#号，修改默认端口号为2222；保存文件，重启ssh服务：$ service ssh restart

在客户端，使用ssh 192.168.200.128 -p 2222 进行连接

1. 禁止root账户登录：

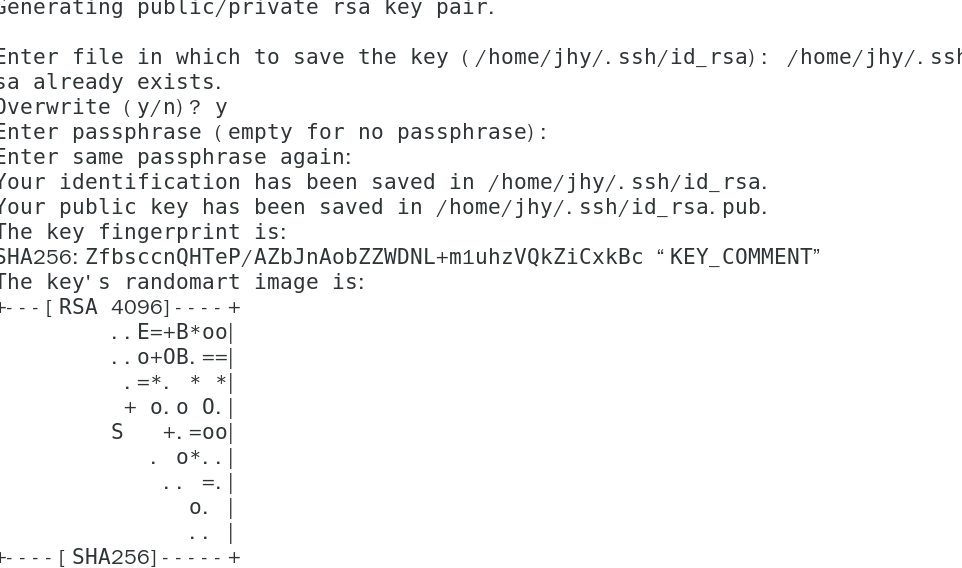
修改/etc/ssh/sshd\_config文件为PermitRootLogin no

在服务器中修改sshd服务的配置文件：打开/etc/ssh/sshd\_config，将Passwd Authentication改成no，将PubkeyAuthentication改成yes，然后保存配置文件



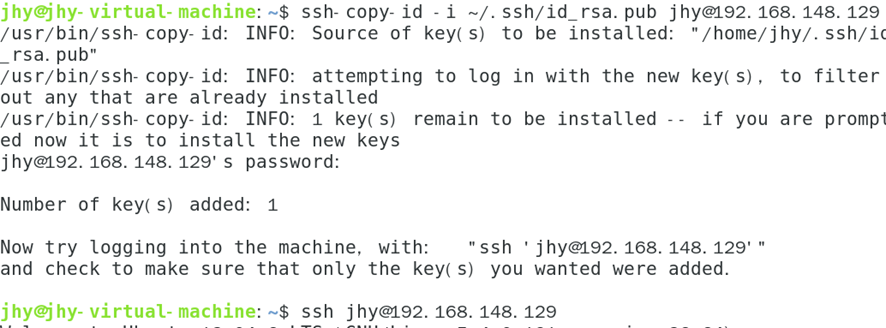
客户端生成密钥对：

ssh-keygen -t rsa -b 4096 -o -a 100 -C “KEY\_COMMENT”。 其中，-t设置密钥类型，-b设置密钥位数，-C设置注释，提示的passphrase就是为私钥设置的密码，不设置的话直接两次回车即可。默认情况下，生成的密钥保存在当前用户的.ssh文件夹下，id\_rsa是私钥，id\_rsa.pub是公钥



将客户端公钥id\_rsa.pub复制到服务端：

scp ~/.ssh/id\_rsa.pub [jhy@192.168.148.129:~](mailto:jhy@192.168.148.129:~)（自行修改用户名和ip）



传送结束后可以在服务端对应用户home目录下看到该文件

在服务端，切换要使用的ssh登录用户：

su username

服务端，切换到用户目录下，并新建.ssh文件夹：

使用ls –a 命令或者直接图形界面下ctrl+“H”可查看是否新建了.ssh隐藏文件夹

将上传到服务端的公钥添加到.ssh/authorzied\_keys之中

cat ~/id\_rsa.pub >> ~/.ssh/authorized\_keys

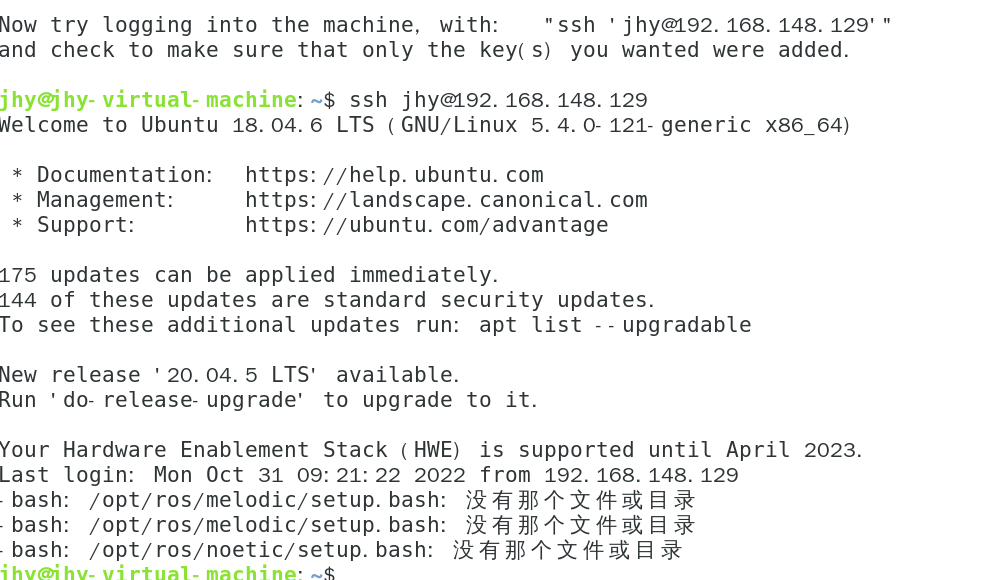
设置文件及文件夹权限：

sudo chmod 755 .ssh

sudo chmod 600 .ssh/authorized\_keys

在客户端使用ssh证书登录命令登录服务器（注意用户名是服务端保存密钥的用户）

ssh -p 2222 yourusername@yourserver



可以看到，无需通过用户名密码，使用本地密钥和服务端公钥配对，即可进行ssh登录

**八、实验结论、心得体会**

本次实验我们进行了linux的安装和基本使用，了解到了如何安装最基本的Linux操作系统（如Ubuntu），并且还尝试添加登录用户和修改密码，这是针对操作系统用户权限的实验。此外我们还使用ssh实现远程免密登录，初步体验了远程登陆的方便。掌握到即使没有电脑主机我们也可以通过ssh等方法实现远程控制。

**九、对本实验过程及方法、手段的改进建议**

1.本实验只是使用了Ubuntu虚拟机和centos虚拟机，可以尝试其他，如windows，或者kali，多次实验感受不同操作系统之间的差别和远程登陆

2.本次使用虚拟机直接操作，可以使用Xshell，finalshell等不需要虚拟机的远程登陆软件。

3.本次实验选择逐步输入指令，可以将ssh指令进行容器编写，达到一键集成部署多台服务器。

**报告评分：**

**指导教师签字：**