网络安全技术基础实验报告

年 月 日

实验名称： 实验5 Linux安全策略设置

姓名： 徐彬涵 学号： 32001272 班级： 软件工程2003

指导教师评定：

**一、实验目的和要求**

1. 了解操作系统安全的概念。
2. 熟悉Linux安全策略设置的工具和方法。
3. 了解Apache服务器和Ftp服务器安全配置。

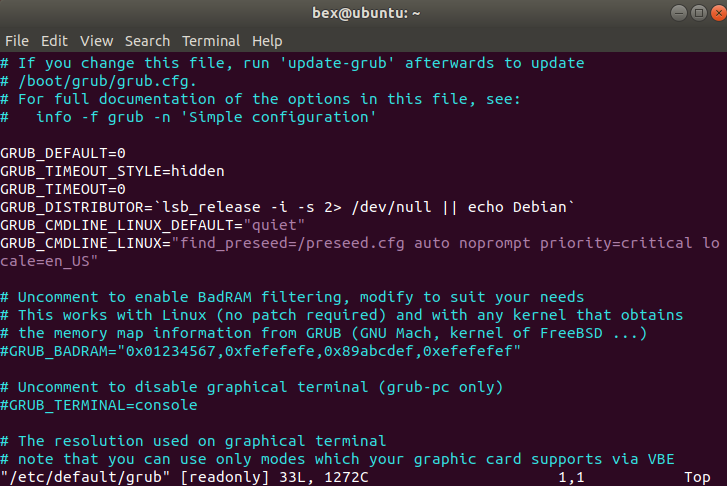
**二、实验内容**

1. 查看并修改Linux相关配置文件，提高系统的安全性，并验证配置效果。
2. 查看并修改Apache服务器配置文件相关配置项，提高服务器的安全性，并验证配置效果。
3. 查看并修改Ftp服务器配置文件相关配置项，创建虚拟用户，提高服务器的安全性，并验证配置效果。

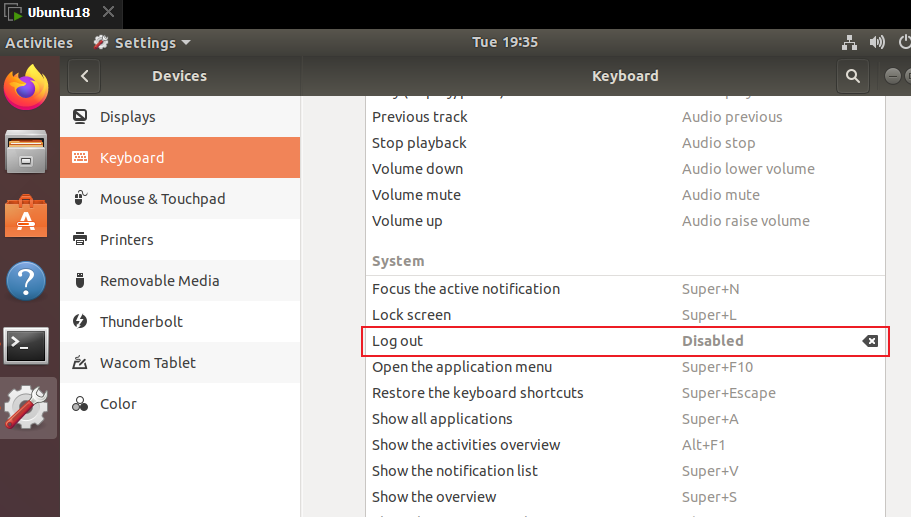
**三、实验步骤：**

1. 查看并修改Linux配置文件，提高系统的安全性：
   1. Linux引导程序安全设置：grub.conf；



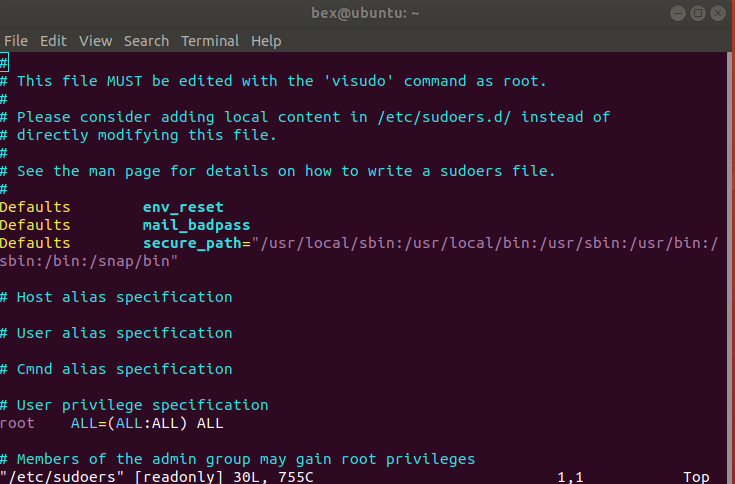


* 1. 防止使用组合键重启系统：/etc/inittab；

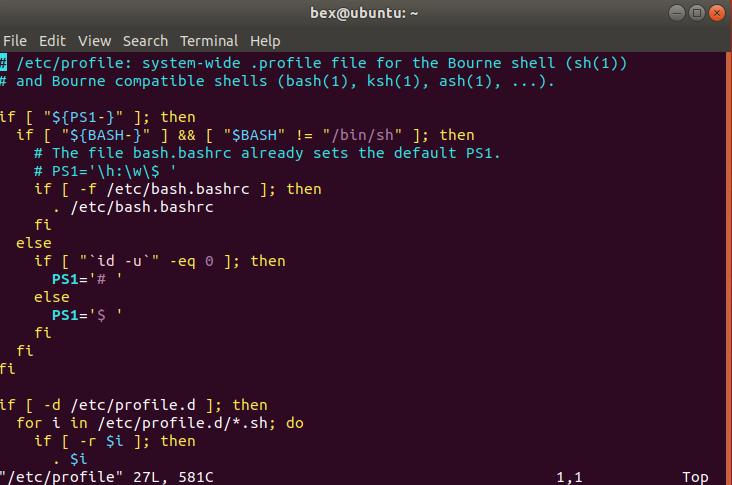


* 1. 安全登录、注销：/etc/sudoers /etc/profile；



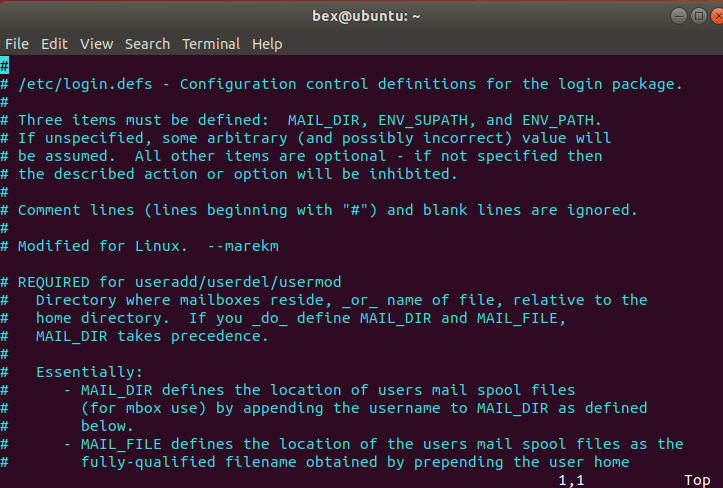






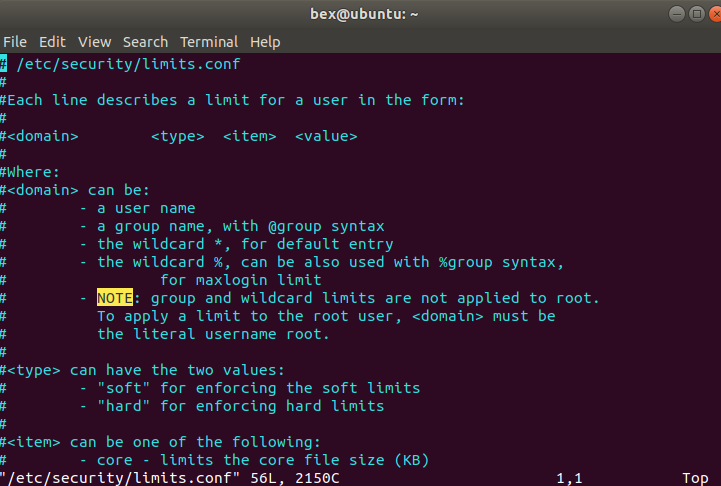
* 1. 用户账号安全管理：/etc/login.defs；



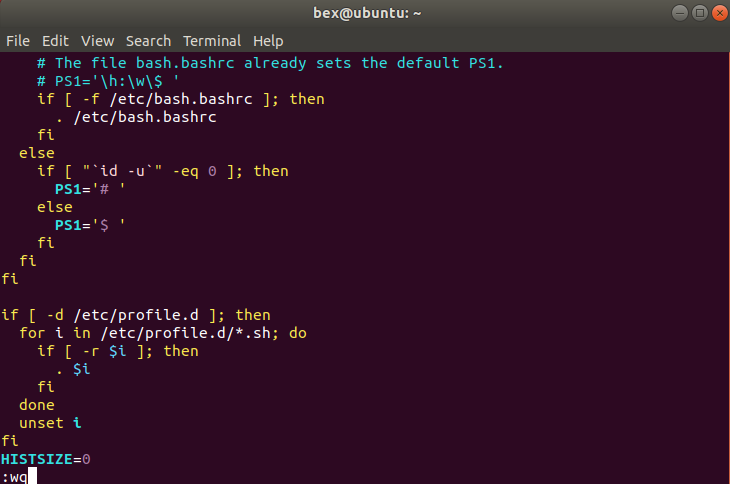


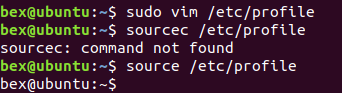
* 1. 资源使用的限制：/etc/security/limits.conf；





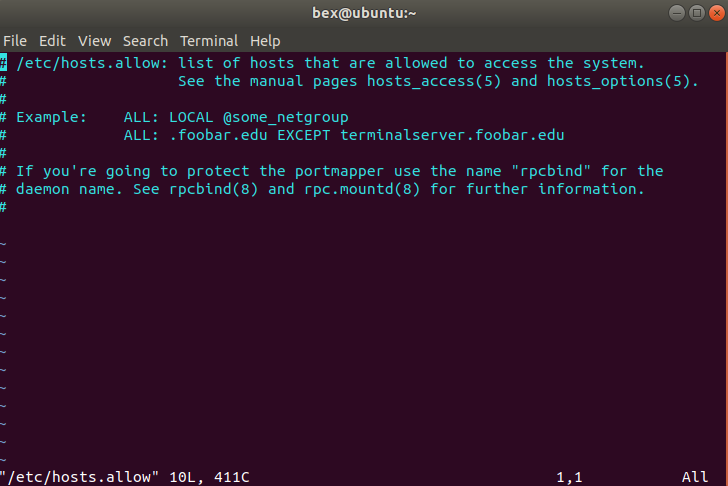
* 1. 清除历史记录：/etc/profile histsize；



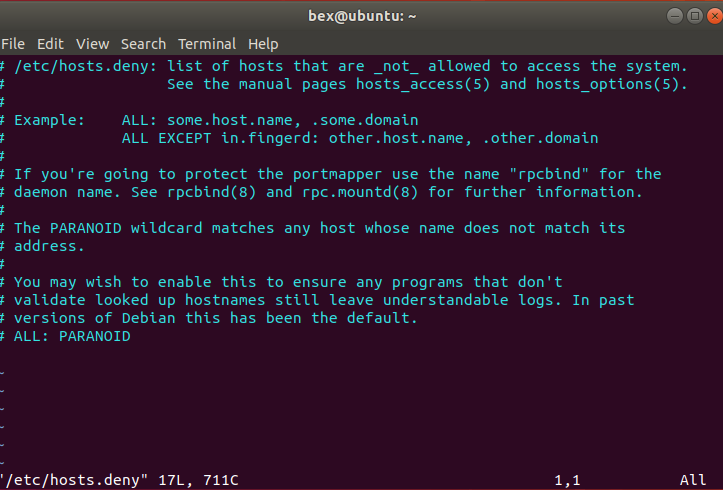


* 1. 系统服务的访问控制：hosts.allow hosts.deny；

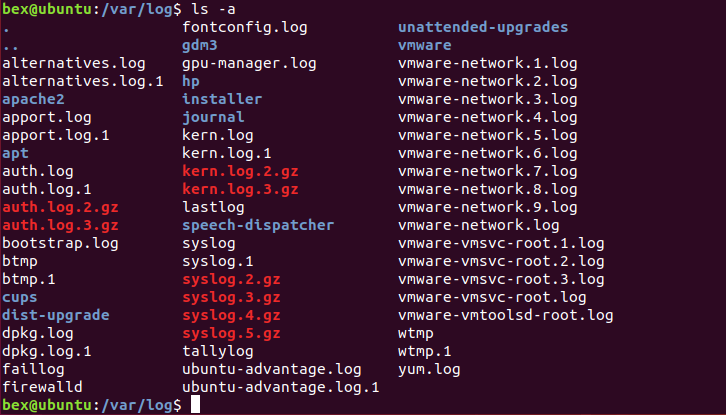






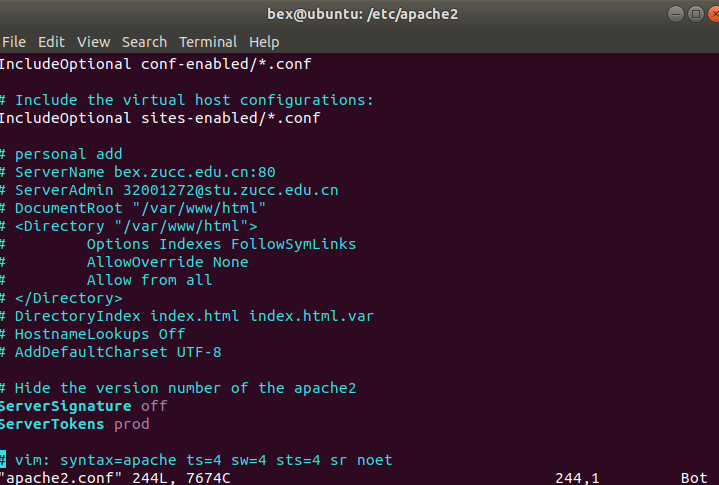


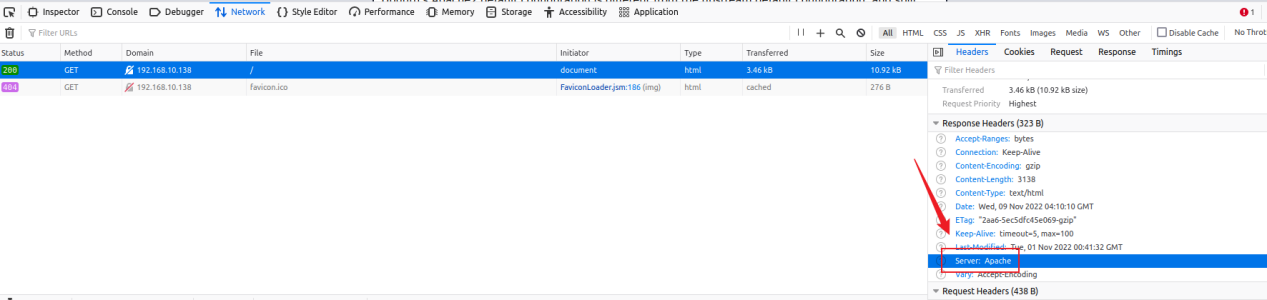
* 1. 系统日志安全： syslog日志服务 /var/log。



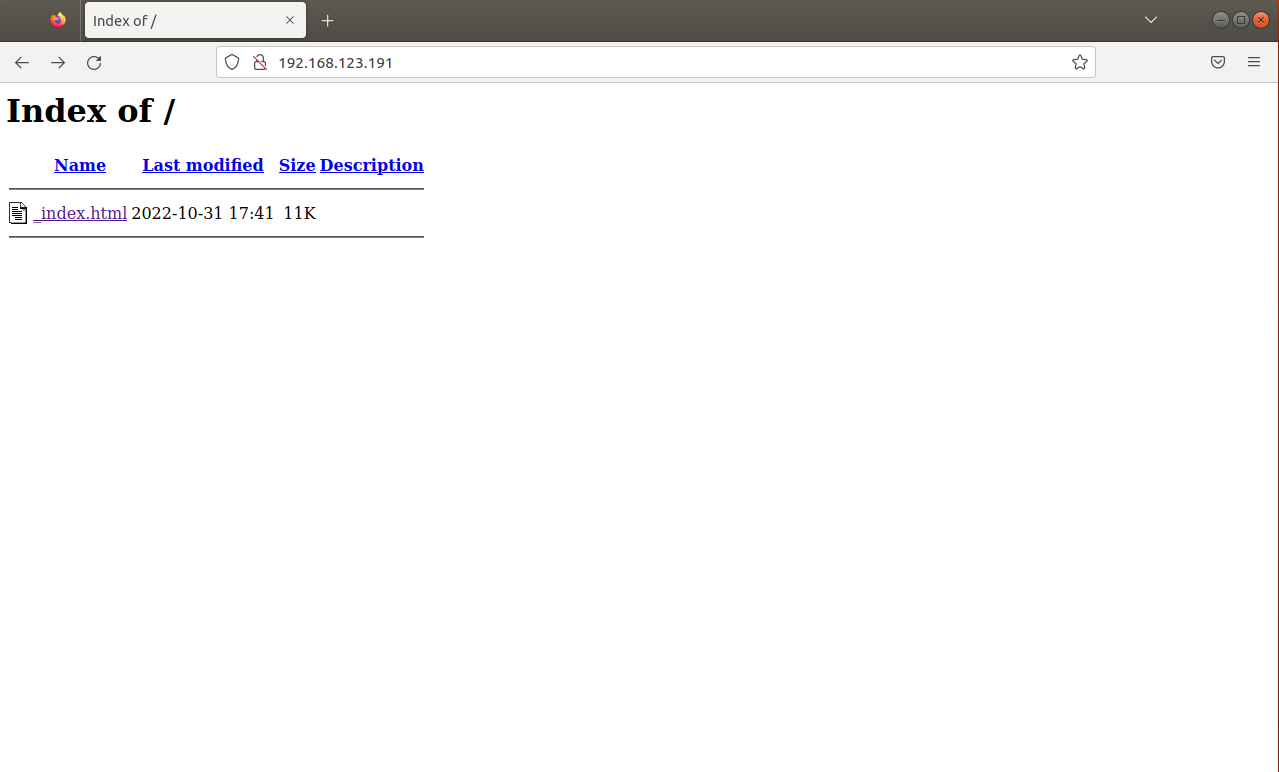
1. 查看并修改Apache服务器配置文件相关配置项，提高服务器的安全性，并验证配置效果。
   1. 隐藏或伪装Apache版本号；

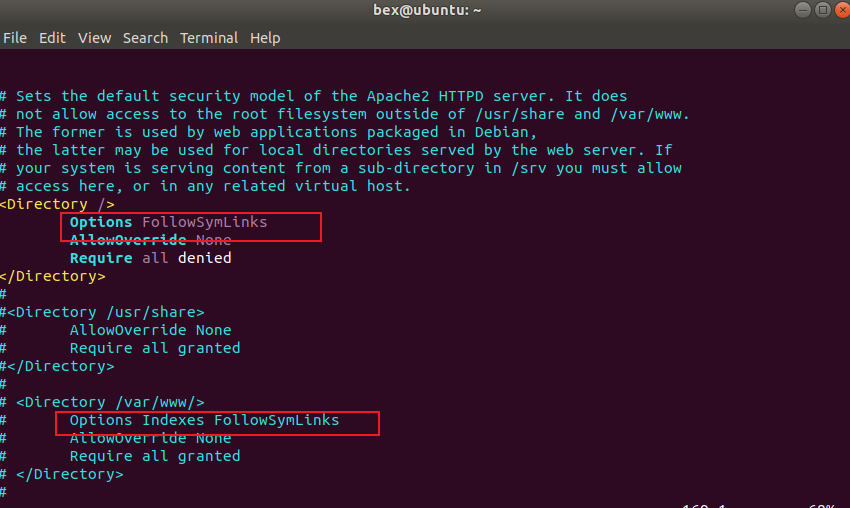
<https://wker.com/hide-apache-info/>

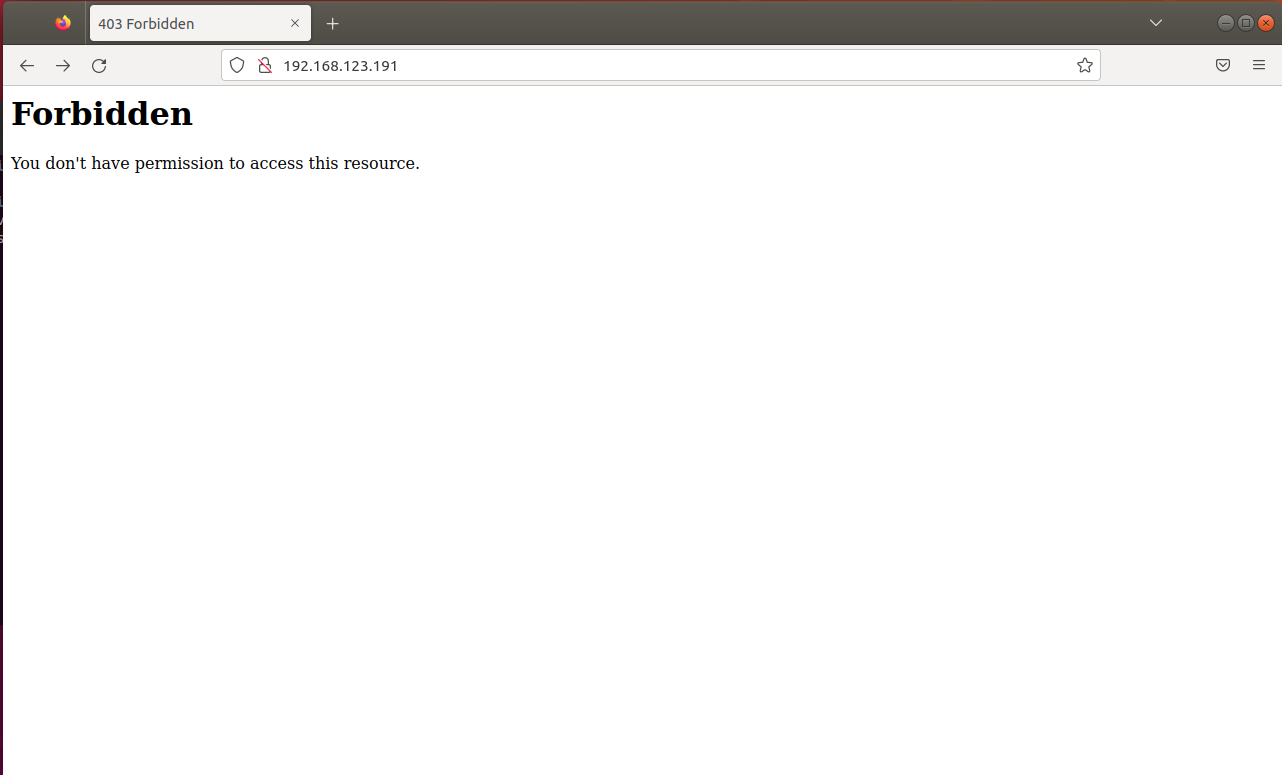




* 1. 禁止使用目录索引；







* 1. 配置web目录的访问策略；

禁止使用目录索引：

Options FollowSymLinks

Options指令通知apache禁止使用目录索引，FollowSymLinks表示不允许使用符号连接。

禁止默认访问：

要的安全策略必须要禁止默认访问的存在，只对指定的目录开放权限，如果允许访问/var/www/html目录，使用如下设定

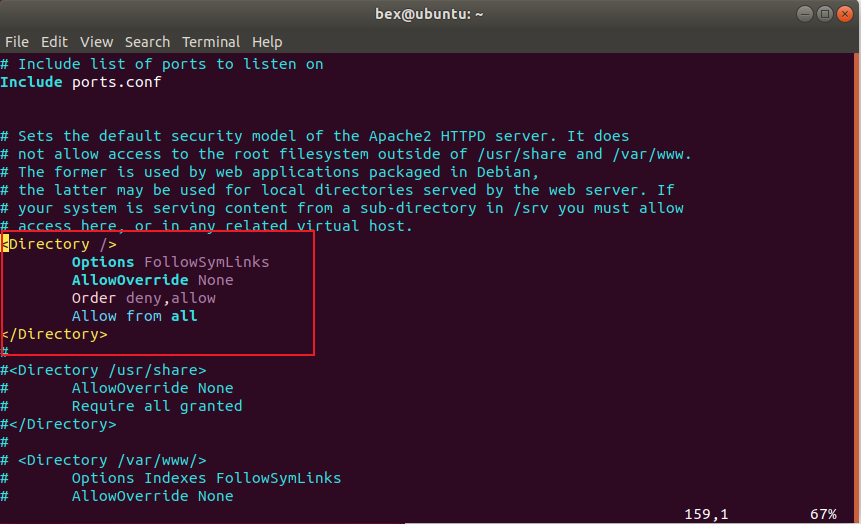
Order deny,allow

Allow from all

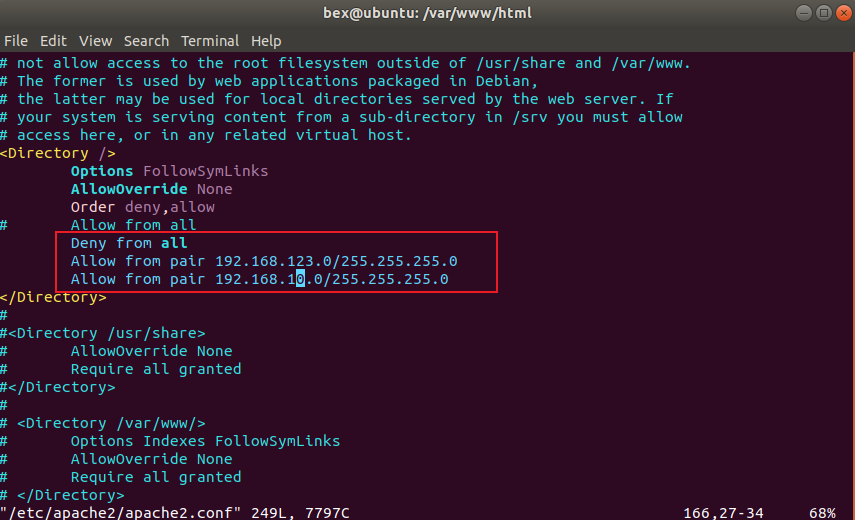
禁止用户重载：

为了禁止用户对目录配置文件（htaccess）进行重载（修改），可以这样设定

AllowOverride None



* 1. Apache服务器的访问控制；

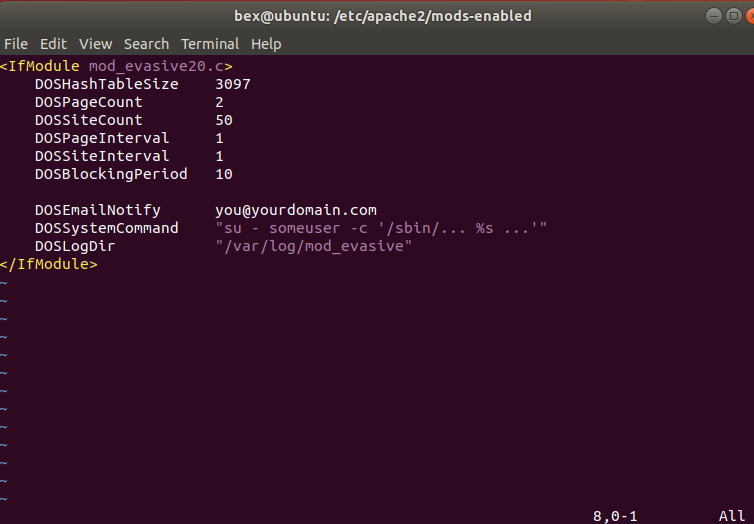


* 1. 使用mod\_evasive来反驳DoS攻击；

安装



打开/etc/apache2/mods-enabled并去除所有注释



创建日志



* 1. 建立安全的目录结构。

ServerRoot #保存配置文件，二进制文件与其他服务器配置文件

DocumentRoot #保存web站点内容，包括HTML文件和图片等

ScripAlias #保存CGI脚本

Customlog 和 Errorlog #保存日志和错误日志

建议的目录结构为，以上四种目录相互独立并且不存在父子逻辑关系

注：

ServerRoot目录只能为root用户访问

DocumentRoot目录应该能够被管理web站点内容的用户访问和使用apache服务器的apache用户与组访问

ScripAlias目录应该只能被CGI开发人员和apache用户访问

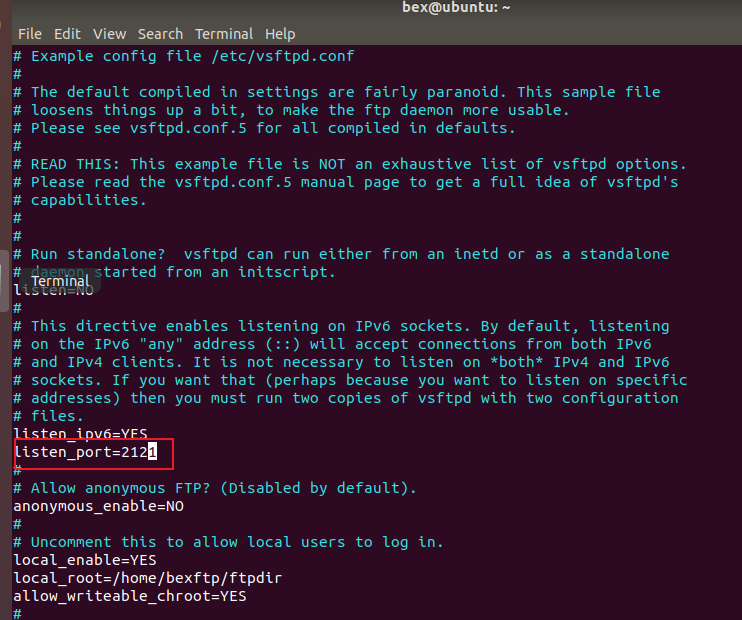
1. 查看并修改Ftp服务器配置文件相关配置项，创建虚拟用户，提高服务器的安全性，并验证配置效果。

**http://vsftpd.beasts.org/vsftpd\_conf.html**

* 1. 修改配置文件，将ftp服务预设端口改为2121；

编辑/etc/vsftpd.conf配置文件添加

Listen\_port=2121



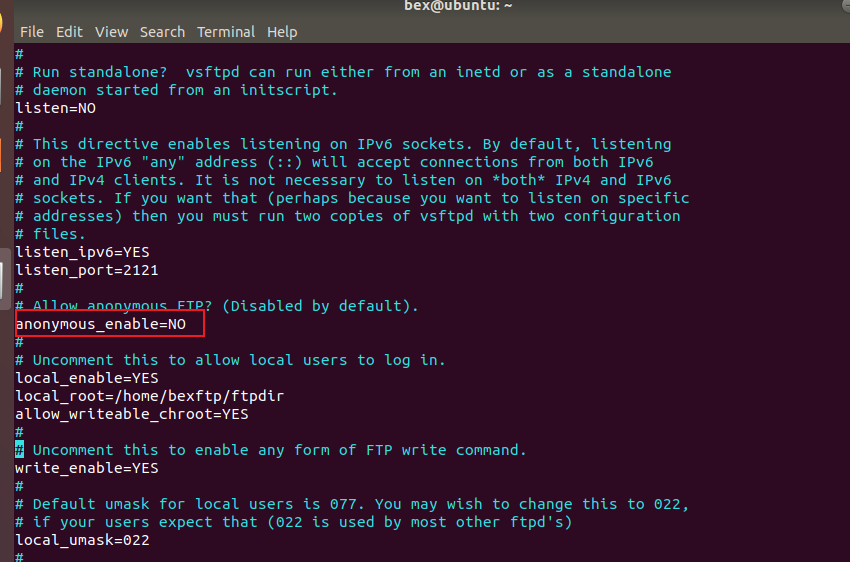
重启服务





* 1. 禁止匿名用户登录；

编辑/etc/vsftpd.conf配置文件修改

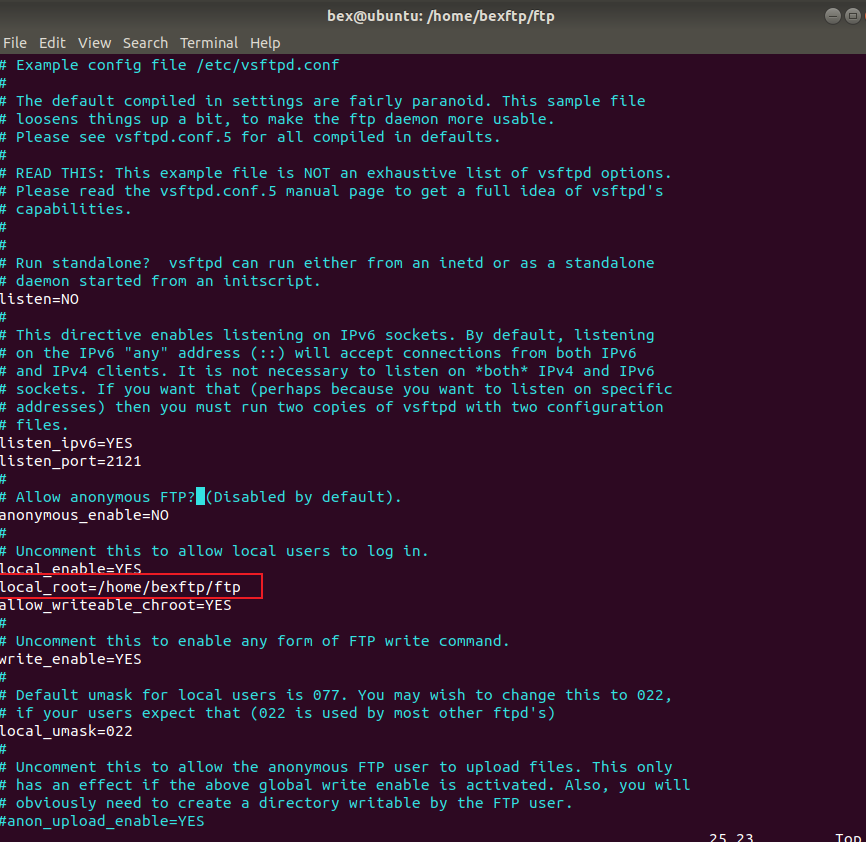


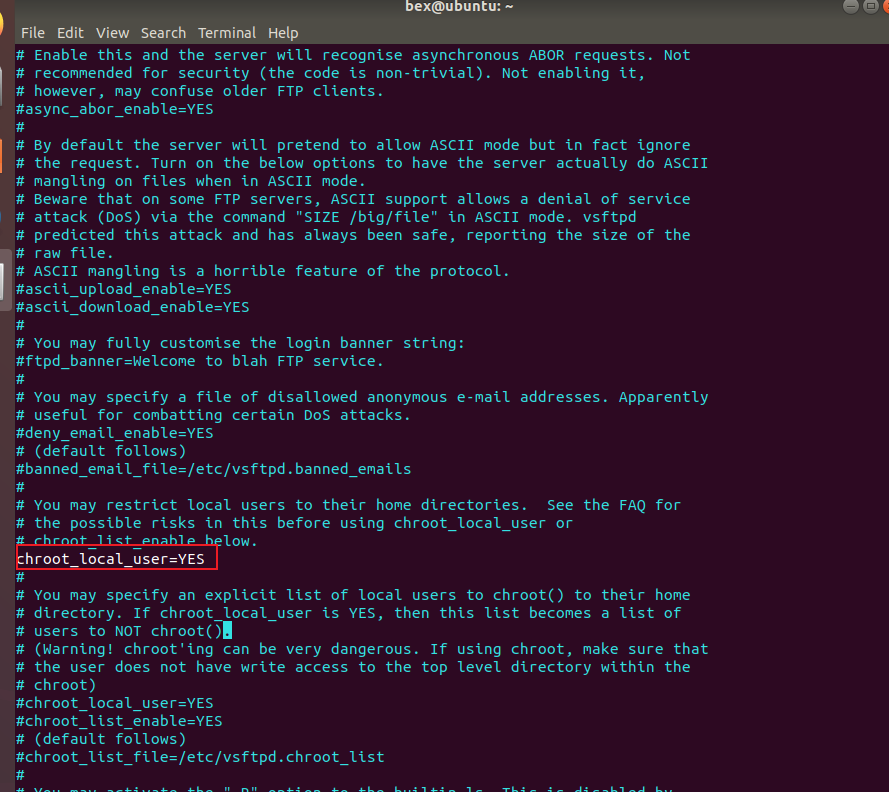
* 1. 修改ftp默认主目录为/ftp文件夹，并将用户锁定在主目录内；

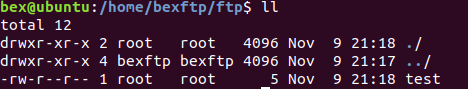
编辑/etc/vsftpd.conf配置文件添加和修改

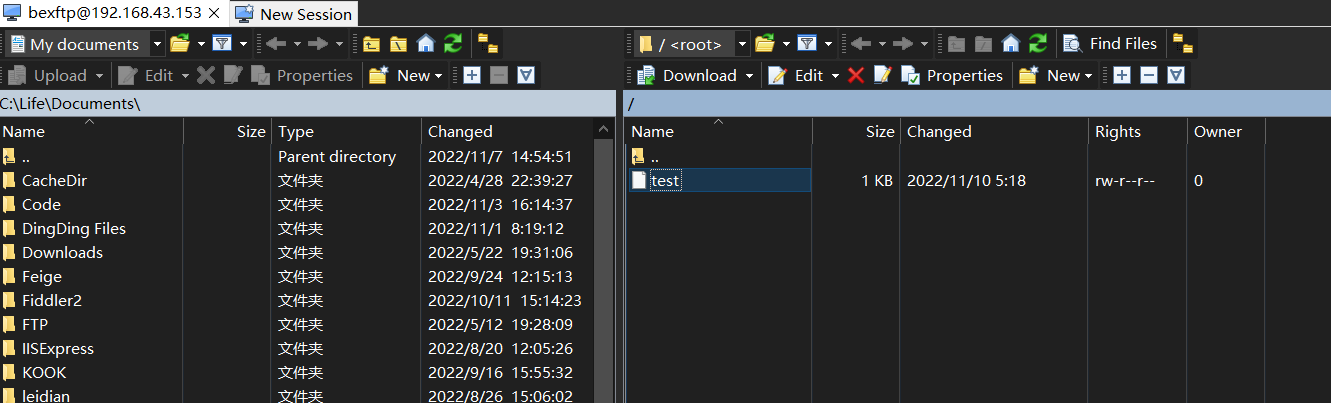
local\_root=/home/$USER/ftp

chroot\_local\_user=YES





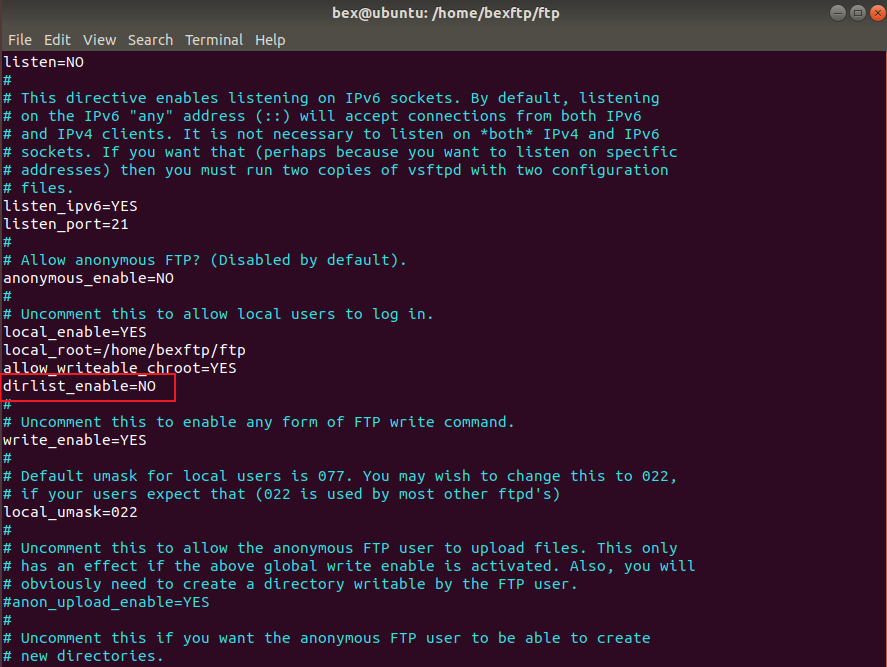


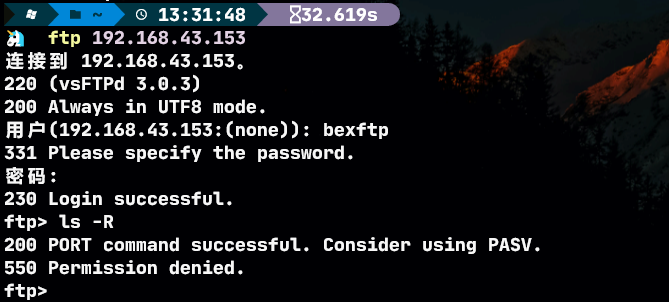


* 1. 关闭ls -R命令，防止服务器被DoS攻击；

编辑/etc/vsftpd.conf配置文件添加

dirlist\_enable=NO



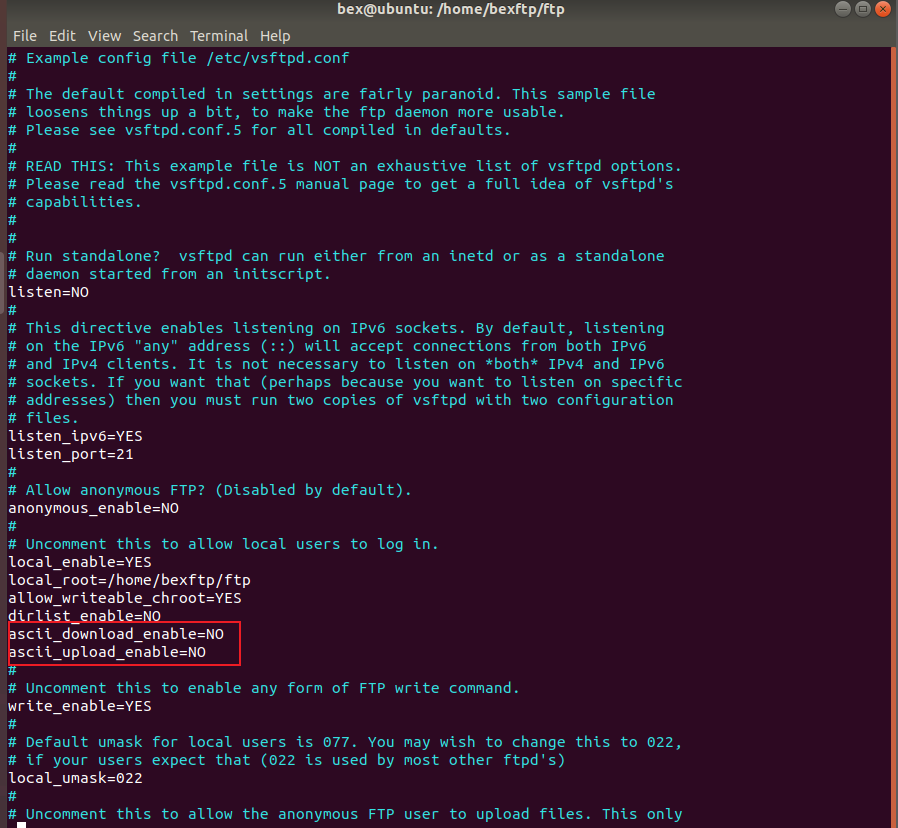


* 1. 关闭ascii模式下载，防止被用于DoS攻击；

编辑/etc/vsftpd.conf配置文件添加

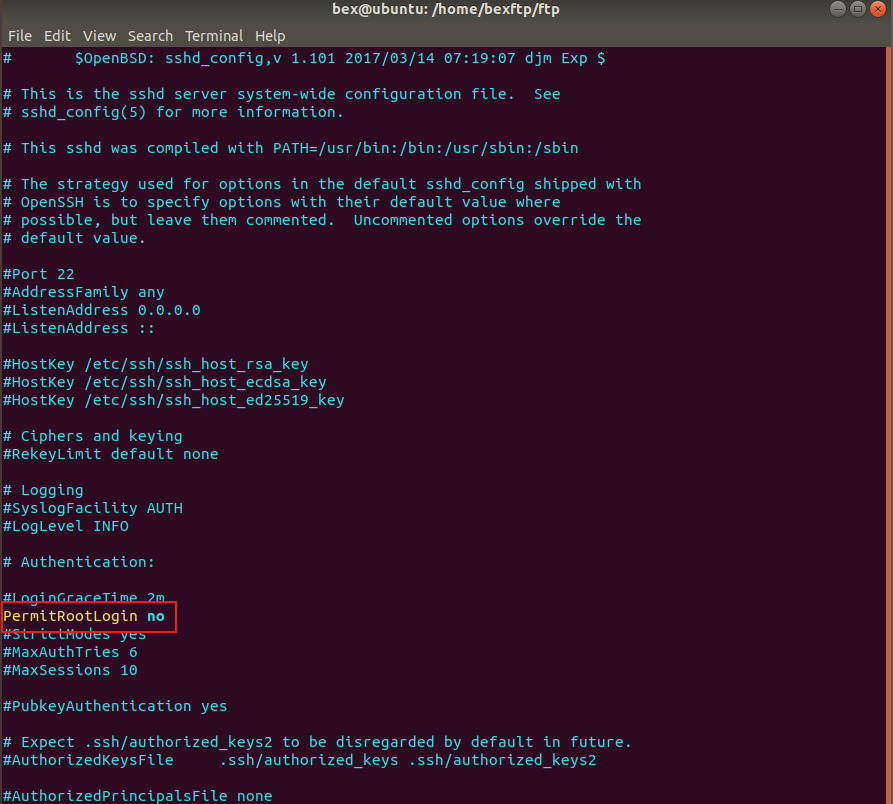
ascii\_download\_enable=NO

ascii\_upload\_enable=NO



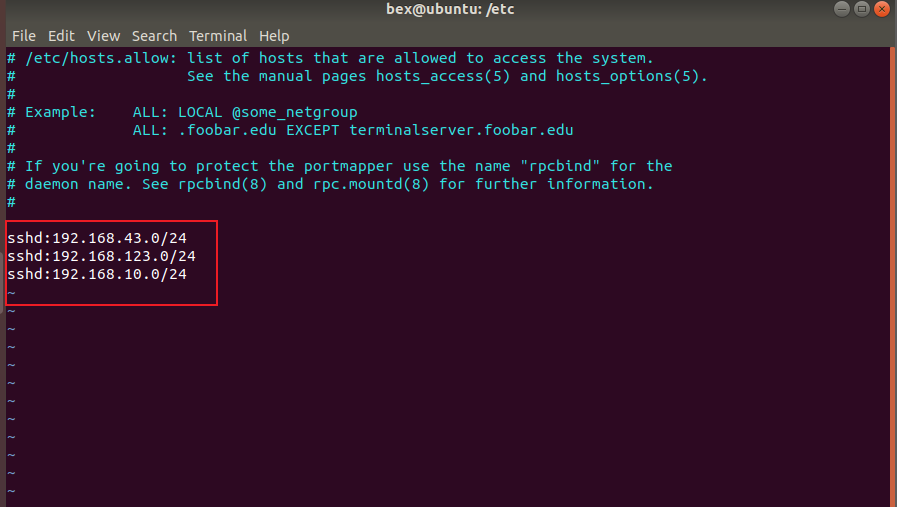
* 1. 修改ssh配置文件，禁止root用户通过ssh登录；

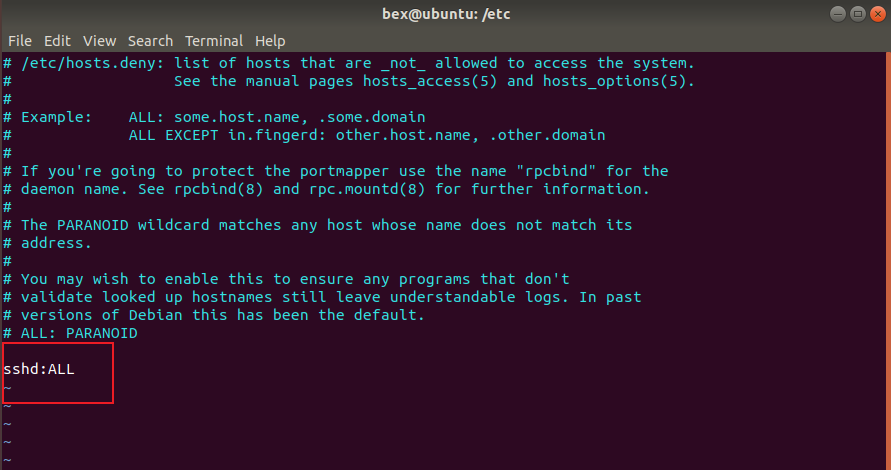
编辑/etc/ssh/sshd\_config文件



* 1. 配置TCP Wrappers ，对远程主机进行访问控制，仅允许特定网段使用ssh进行登录；

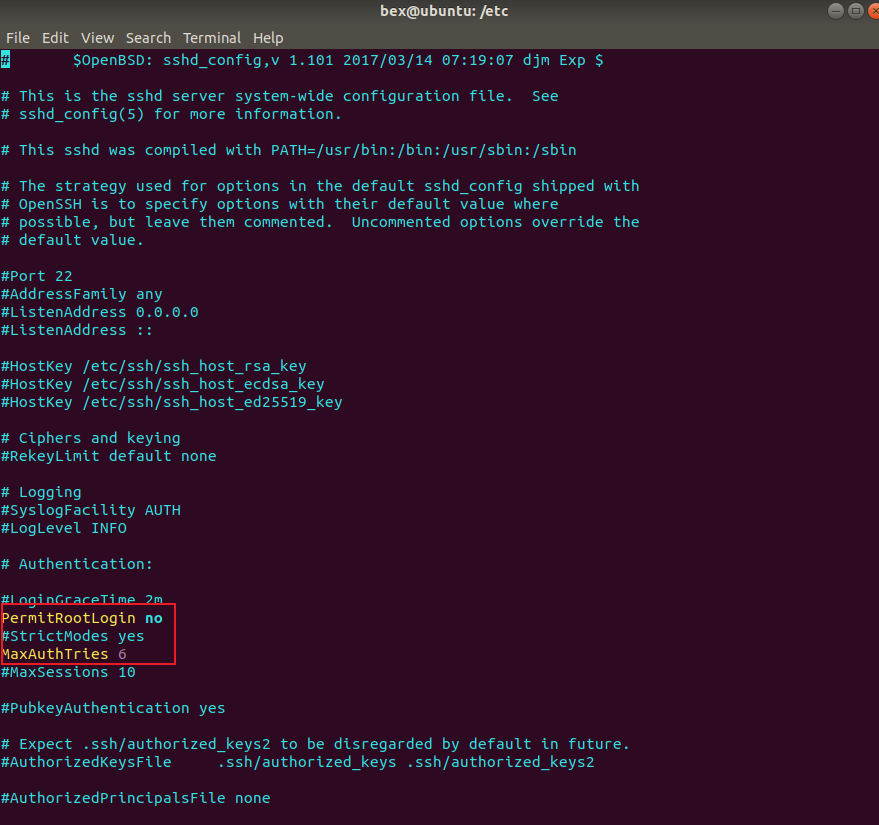
编辑/etc/hosts.allow和/etc/hosts.deny配置





* 1. 修改ssh配置文件，禁止使用空密码进行登录，设置最大尝试次数以防密码爆破；

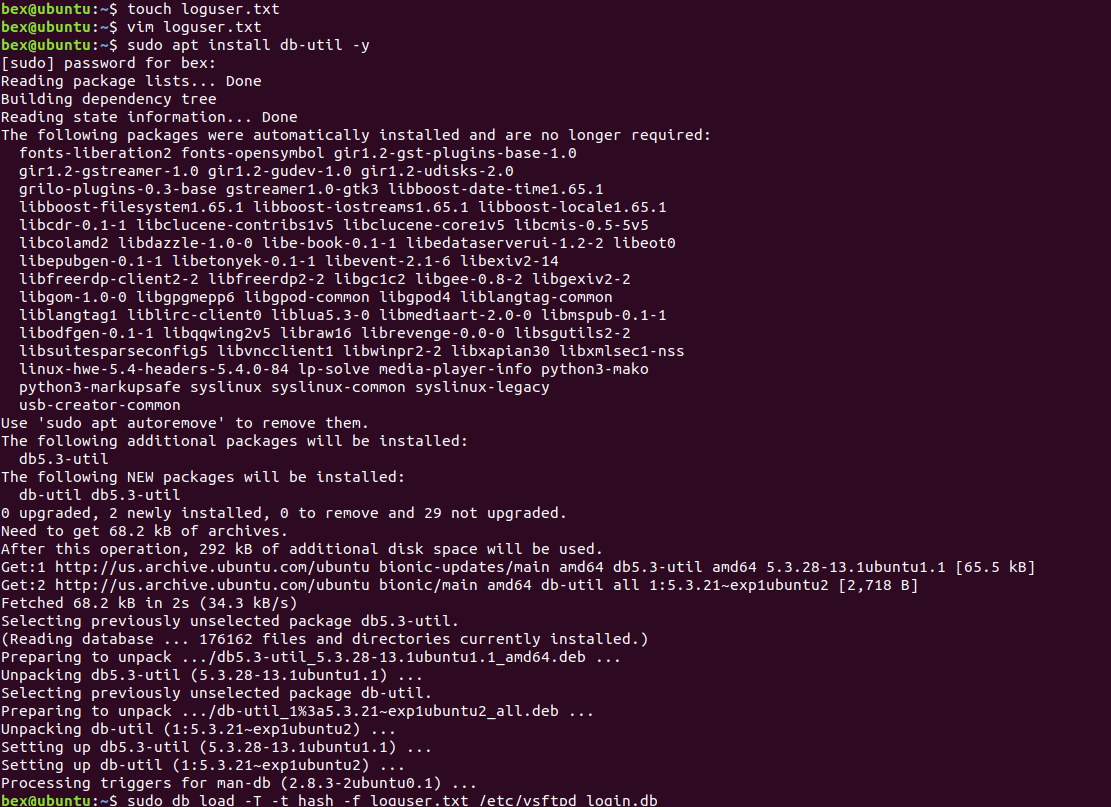
编辑/etc/ssh/sshd\_config文件

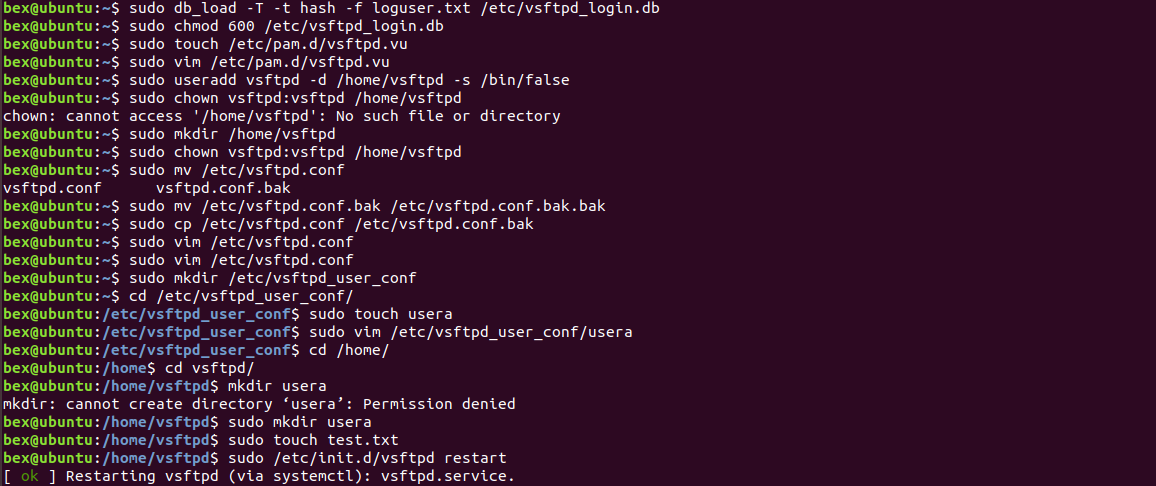


* 1. （选做）使用虚拟用户访问ftp 服务器。

创建了用户vsftpd作为宿主账户，并在此基础上创建虚拟账户usera

参考https://blog.csdn.net/u010257920/article/details/52435250





成功利用虚拟账号usera登录

