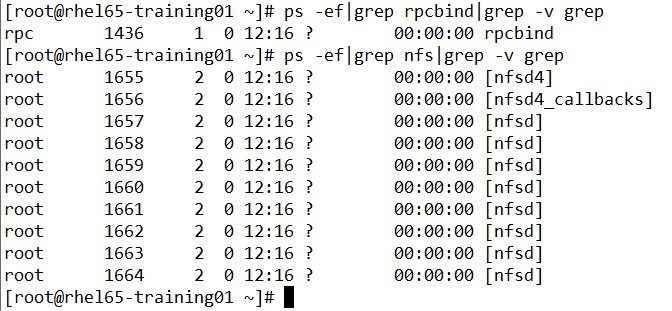
1. 安装nfs、ftp，安装完成后，启动服务并设置开机启动

评分因素和命令

1. ps -ef|grep rpcbind|grep -v grep ,能grep到则正确
2. ps -ef|grep nfs|grep -v grep
3. 上面两个命令输出的截图如下:

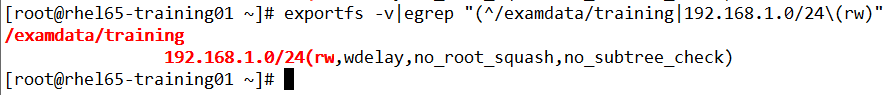


1. 将NFS Server的/examdata/training 共享给192.168.1.0/24网段，权限要求可读写 。

评分因素和命令

1）exportfs -v|egrep "(^/examdata/training|192.168.1.0/24\(rw)"

下面为截图



1. 建一个共享目录，使只有172.25.0.0/24的用户的访问，要求可读写，限制root权限

这题改为：

建共享目录/test1，使只有172.25.0.0/24的用户的访问，要求可读写，限制root权限

评分因素和命令

1）exportfs -v|egrep "(^/test1\s+172.25.0.0/24|,root\_squash)",能grep到则正确，下面是截图



1. 设置 ftp不允许匿名登陆

评分因素和命令

1. cat /etc/vsftpd/vsftpd.conf |grep "anonymous\_enable=no"
2. 或cat /etc/vsftpd/vsftpd.conf |grep "anonymous\_enable=NO"
3. 以上两个命令其中一个能grep到，则正确
4. 查询 nfs 、ftp 在系统开启了哪些端口，将结果保存到/examdata/result/port\_used

评分因素和命令

1）执行命令netstat -tulnp|grep vsftpd ，与cat /examdata/result/port\_used的输出对比是否一致

2）执行命令rpcinfo -p 与cat /examdata/result/port\_used 的输出对比是否一致

1. 新建一个用户test,修改其默认的登录目录为/var/ftp/pub/test，使用该帐号登录ftp，测试是否正常

评分因素和命令

1)grep "/var/ftp/pub/test" /etc/passwd,能grep到则为正确

1. 限制 test用户只能在默认登录目录内活动，不能切换到其他系统目录，比如：/etc、 /tmp等

评分因素和命令

1）grep "^chroot\_local\_user=YES" /etc/vsftpd/vsftpd.conf

1. 添加samba用户user05,已知samba包没安装 1) 共享 /examdata/result/samba\_05 目录， 2) 只有 172.25.0.0/24的客户端可以访问 samba\_05共享 3) 用户 floyd 必须能够读取共享中的内容

评分因素和命令

1. 执行命令 rpm -qa samba samba-common samba-client|wc -l，结果为3则这一步正确
2. grep "/examdata/result/samba\_05" /etc/samba/smb.conf，能grep到则这一步正确

3）egrep -i "^Hosts allow\s+=\s+172.25.0.0/255.255.255.0" /etc/samba/smb.conf 或

egrep -i "^Hosts allow\s+=\s+172.25.0.0/24" /etc/samba/smb.conf，能grep出来则这一步正确

4）grep -E "^valid users\s+=\s+floyd" /etc/samba/smb.conf ，能grep出来则这一步正确

1. 建立ftp虚拟用户user111(到实训云上修改题目），使这用户不影响其他系统用户的登陆，即虚拟用户和系统用户均可以登陆,user111使用9999端口登陆，密码为123123，家目录为/home/vftp/user111, vftp用户(系统真实用户）使用21端口登陆，密码为123123。

评分因素和命令

1. netstat -tulnp|grep vsftpd|grep '21'
2. netstat -tulnp|grep vsftpd|grep '9999'
3. 1和2两条命令都能过滤到则正确，只有一条过滤到则全错
4. 添加iptables规则，以允许 FTP被客户端访问

评分因素和命令

1. 检查防火墙是否在运行中：service iptables status|grep "Firewall is not running" ,不能grep到则正确
2. 检查放行20端口：iptables -L -n --line|egrep 'dports\s+20'|awk -F " " '{print $2}'，过滤出ACCEPT则这一步正确
3. 检查放行21端口：iptables -L -n --line|egrep 'dports\s+21'|awk -F " " '{print $2}'，过滤出ACCEPT则这一步正确

4）或使用以下命令检查20和21端口，如果3）不能过滤则使用这一条，能过滤出ACCEPT则正确：

iptables -L -n --line|egrep 'multiport\s+dports\s+20,21'|awk -F " " '{print $2}'

1. 将NFS以下端口值改为如下所示，并在防火墙开放以下端口，然后重启nfs服务、重启防火墙： RQUOTAD\_PORT=30001 LOCKD\_TCPPORT=30002 LOCKD\_UDPPORT=30002 MOUNTD\_PORT=30003 STATD\_PORT=30004

评分因素和命令

1. 检查nfs是否已使用更改后的端口：

rpcinfo -p|grep '30001'，能过滤出30001，则这一步正确

rpcinfo -p|grep '30002'，能过滤出30002，则这一步正确

rpcinfo -p|grep '30003'，能过滤出30003，则这一步正确

cat /etc/sysconfig/nfs |grep "^STATD\_PORT=30004"，能过滤出30004，则这一步正确

2）检查放行111端口：iptables -L -n --line|egrep 'dports\s+111'|awk -F " " '{print $2}'，过滤出ACCEPT则这一步正确

3）检查放行2049端口：iptables -L -n --line|egrep 'dports\s+2049'|awk -F " " '{print $2}'，过滤出ACCEPT则这一步正确

1. 检查放行30001端口：iptables -L -n --line|egrep 'dports\s+30001'|awk -F " " '{print $2}'，过滤出ACCEPT则这一步正确
2. 检查放行30002端口：iptables -L -n --line|egrep 'dports\s+30002'|awk -F " " '{print $2}'，过滤出ACCEPT则这一步正确
3. 检查放行30003端口：iptables -L -n --line|egrep 'dports\s+30003'|awk -F " " '{print $2}'，过滤出ACCEPT则这一步正确
4. 检查放行30004端口：iptables -L -n --line|egrep 'dports\s+30004'|awk -F " " '{print $2}'，过滤出ACCEPT则这一步正确