课件名称

目录与文件管理：目录、文件权限概念与管理

题目内容

1. 文件/examdata/training/wenjian.sh当前权限属性为-rw-r--r--，请修改其权限属性为-rwxrwxr--。

评分因素和命令

1）/examdata/training/wenjian.sh的最终权限为774，注意：原题目为754，需修改题目，普通用户加入该组能对其做写入操作，其他用户只有读权限，root可强制写入

2）该脚本的组为root，所以需要将普通用户加入root组：

3）以t1用户为例（没有的则需先创建该用户）：

usermod -G root t1

4）使用root对脚本写入数据，使用vi,或使用cat结合EOF方式：

cat > /examdata/training/wenjian.sh <<EOF

#!/bin/bash

echo “hello world”

EOF

5）使用t1用户执行脚本： /examdata/training/wenjian.sh查看输出是否为脚本的内容 这一步检查了属组用户具有执行脚本能力,

6）使用t1 用户对该脚本进行写入操作：

比如 echo “ls /tmp” >> /examdata/training/wenjian.sh,正常能写入，否则报错

7）使用其他用户t2（没有的则需先创建该用户），对脚本进行写操作，正常为写入报错，但能执行该脚本

8）由于root是超级用户，即使没有按题目改成有x(执行权限）也能执行该脚本，所以这里可酌情测试，意义不大

1. 查看/目录inode使用率，并将结果输出到/examdata/result/inode.txt。

评分因素和命令

1. 检查根目录的inode，与/examdata/result/inode.txt作对比，相差无几则为正常（因为考生可能考试时有在根目录创建过文件，所以得出的数字不需严格一致，相差不大就行，该题目主要考检查inode的方法
2. 检查inode数量：df -i /|awk 'NR>1 {print $2}'，单单df -i / 也可以，只是该命令应该比较方便写评分脚本，可按自己的来，不强求
3. 比较与2）的输出是否和/examdata/result/inode.txt 的输出相近
4. 将/examdata/training/sam.txt 移动到/examdata/result/下，并重命名为jack.txt

评分因素和命令

1. 检查/examdata/training/是否存在sam.txt

ls /examdata/training/sam.txt,正常为报错

1. 检查/examdata/result/下是否存在jack.txt文件

ls /examdata/result/jack.txt，正常不报错

1. 显示/目录下的所有文件，要求结果包含在不限于：隐藏文件、能看到文件属性、所有者、组，把结果存放到/examdata/result/list\_file。

评分因素和命令

1. 执行 ls -a / >/a.txt或 ll -a / >/a.txt

2）使用命令： diff /a.txt /examdata/result/list\_file，对比两个文内容是否一致，相同的话没有输出

1. 在/examdata/result/下新建一个目录dir\_right，使其owner为root,group为 user20

评分因素和命令

1. 执行命令：/examdata/result/dir\_right |awk '{print $3,$4}'，检查其用户和组，正常输出为root user20，对比是否一致，不一致为错误
2. 假设有个目录的权限如下所示： drwxr--r-- 3 root root 4096 Nov 19 08:35 .ssh 请修改这条示例，使user20可以对该文件有修改权限，把结果存放到/examdata/result/user20\_can\_write

评分因素和命令

1. 要使user20对文件有写权限，题目只是要求修改示例（即类似某益智游戏里面的题目：改改某个地方，性质就不一样），我们可以设置other用户有w（写权限）：
2. 结果为drwxr--rw- 3 root root 4096 Nov 19 08:35 .ssh
3. cat .ssh检查输出是否与2）的一致
4. /examdata/result下新建一个文件file\_right，使该文件，只能由其创建的所有者才能删除

评分因素和命令

1. 该题目使用到sbit(t权限位）的知识
2. 执行命令：chmod 1777 /examdata/result
3. touch /examdata/result/file\_right
4. 使用其他普通用户尝试该文件，正常会报错，不能删除
5. 在/examdata/result下新建一个group\_exam目录： 1）使其下所有"文件和子目录"的所属组都会继承该目录"所属组" 2）创建的"子目录"将会继承具父目录的组属性

评分因素和命令

1)此题用到SGID的知识,使用过滤方法检查组权限是否含有s权限标志即可，使用简单的grep就行，比如：

2） ll -d /examdata/result/group\_exam|grep “drwxr-s”

drwxr-sr-x. 2 root root 4096 Nov 19 14:13 /examdata/result/group\_exam

1. 修改/etc/passwd权限，使user20可以修改该文件内容，并把权限信息重定向到 /examdata/result/passwd\_right\_change

评分因素和命令

本题目主要考acl知识点，题目没有说改属组等其他东西，所以只能用acl

1）getfacl /etc/passwd|grep "user:user20:rwx" ,有正常结果返回，则为正确

1. 在/examdata/result/下建一个五层目录，目录前缀为dir\_level

评分因素和命令

1. 将题目改为在/examdata/result/下建五个目录，要求目录前缀为dir\_level，不能一个一个的建立，将命令重定向到/examdata/result/fast\_create\_dir.txt
2. echo “mkdir /examdata/result/dir\_level{1..5}” >>/examdata/result/fast\_create\_dir.txt

3)ls -F /examdata/result/|grep ^dir\_level.\*/$|wc -l 如果输出为5，则为正确

1. 复制/var/log/messages 文件到/examdata/result/new\_messages目录下的，改名为empty1文件，保留该文件的所有属性； 4) 软链接该文件到/tmp目录下的new\_dir

评分因素和命令

1. 使用diff检查/examdata/result/new\_messagese/mpty1内容是否一致
2. 文件组主和属组都 为root，读写权限为600（即rw-------，只有属主root有读写权限，组和其他用户没有任何权限)
3. 可以先过滤有没有x权限位，ll -d /examdata/result/new\_messagese/mpty1|grep “x”
4. 再另外使用普通用户，比如 user20对其进行读写测试，正常会报错(-bash: /var/log/messages: Permission denied)
5. cat /examdata/result/new\_messagese/mpty1
6. echo “user20” >> /examdata/result/new\_messagese/mpty1
7. 将/etc/passwd的内容追加到文件aaa中，并保存到/examdata/result/new\_passwd下

评分因素和命令

1. 推荐答案为：cat /etc/passwd |tee /examdata/result/new\_passwd>> aaa
2. 题目提到追加，即使用重定向，使用的是 >> 符号
3. 注意写成cat /etc/passwd >> aaa |tee /examdata/result/new\_passwd是错误的，因为数据全都写进aaa里去了，这时new\_passwd是空白的
4. 统计/etc/passwd文件的字节数和行数,保存结果到/examdata/result/count\_pwd

评分因素和命令

1. 解题方法为：cat /etc/passwd |wc -cl,假设输出 为 “20 881”
2. cat /examdata/result/count\_pwd |grep “20”|grep “881” 与1）相比，正确为一致
3. 新建一个用户well，要求uid和gid均为502； 1）将用户well添加到组engineer； 2）在/examdata/training下创建目录technology; 3）修改其属性为well:engineer，目录权限为drwxr-xr-x。

评分因素和命令

1. cat /etc/passwd|grep well|awk -F ":" '{print $3,$4}',如果输出为两个502，则为正确
2. cat /etc/group|grep engineer|awk -F ":" '{print $4}'，如果输出为well则为正确
3. ls /examdata/training/technology,存在该目录的，则不报错
4. ll -d /examdata/training/technology|egrep "(well\sengineer)"ll -d /examdata/training/technology|grep “drwxr-xr-x”
5. 创建一个用户hill，要求该用户不能登录系统。

评分因素和命令

1)cat /etc/passwd|grep hill|grep nologin,返回正常则为正确

1. 创建一个用户tom，要求下次登录系统时，必须修改其密码。

评分因素和命令

1. 执行cat /etc/shadow|grep t1|awk -F ":" '{print $3}'，输出数据为0则为正确
2. 创建/examdata/result/dir目录，并修改目录的权限，要求： user01为该目录的所有者，admin是该目录的所属组 除该目录所有者和所属组成员以外的其它所有人对该目录没有任何权限，但user02用户可以在/testdata1/dir目录下创建和删除文件

评分因素和命令

1)ls /examdata/result/dir,没报错则代表有创建dir目录

2)ll -d /examdata/result/dir|egrep “(user01\sadmin),没报错则为属主属组设置正确

3) 使用用其他用户执行ls /examdata/result/dir 该目录或在该目录下建文件/目录

报错则为设置正确

4)使用user02在 /examdata/result/dir目录下创建/删除文件或目录，没报错为正确,之前提交的解题答案中，使用setfacl -m u:user02:rw /examdata/result/dir来操作，权限写少了x,需要修改一下答案，变成setfacl -m u:user02:rwx /examdata/result/dir

1. 请写出命令：限制 user08用户只能使用 cat 、lsblk、ping、vi 命令，命令写到/examdata/result/目录下，并生成文件user08.sh

评分因素和命令

##题目要修改，要将源题目中的vi字眼删除，即只能使用 cat lsblk ping三个命令

1. /examdata/result/user08.sh里的内容应该为:

cp /bin/bash /bin/rbash

usermod -s /bin/rbash user08

mkdir /home/user08/bin

PATH=$HOME/bin

export PATH

ln -s /bin/cat /home/user08/bin/cat 或ln -s /bin/cat ~user08/bin/cat

ln -s /bin/lsblk /home/user08/bin/lsblk 或ln -s /bin/cat ~user08/bin/lsblk

ln -s /bin/ping /home/user08/bin/ping 或ln -s /bin/cat ~user08/bin/ping

1. 只题只是让考生写出命令
2. 批量创建10个用户stu01-stu10，并且设置随机8位密码，要求不能用shell的循环（例如：for,while等），只能用linux命令及管道实现。

答:评分因素和命令

1. 这道题没有统一的答案，当初不知道要评分所以出了这道题，检查一下是否有这几个用户被创建
2. 我给的答案：

echo stu{01..10}|tr " " "\n"|sed -r 's#(.\*)#useradd \1 ; pass=$((RANDOM+10000000)); echo "$pass"|passwd --stdin \1; echo -e "\1 \t `echo "$pass"`">>/tmp/exam\_51.log#g'|bash

解释: 1)echo stu{01..10}|tr " " "\n" echo 出来的stu开头的用户名之间是以空格相间的,tr是把这些空格替换成换行,也就是说这些用户名最终以列显示出来,大家可以拆分这个答案就知道这个命令是什么意思

2)sed使用了后向引用, (.\*)里面的就列出的用户名 ,然后useradd按顺序创建这些用户

3) $RANDOM为内部系统变量,加号后面的8位数字可以随意写

4)echo "$pass"|passwd --stdin \1; 也是用了后向引用, echo 密码|passwd --stdin 用户名 是常见的免交互式设置密码的方法,适合批量建用户的时候使用.

5) echo -e "\1 \t `echo "$pass"`">>/tmp/oldboy.log 是把用户名和密码重定向到/tmp/oldboy.log

1. 统计系统上允许登陆的有多少个用户，请列出并统计，把结果保存到/examdata/result/num\_users

评分因素和命令

1. 检查命令：

grep -v "nologin" /etc/passwd|awk -F ":" '{print $1}'

1. cat /examdata/result/num\_users 对比一下与1）的输出是否一致，一致为正确
2. 将/etc/fstab复制到/examdata/result/fstab.bak，设置harry可以读写，natasha不能做任何操作，其他用户可读，设置manager组为fstab的所属组(题目中提到的用户和组可能要自己创建，请先检查再操作)

评分因素和命令

1. 这题主要考查acl命令的使用
2. 先检查这两个文件内容是否一致：diff /etc/fstab /examdata/result/fstab.bak
3. ll /examdata/result/fstab.bak|awk -F “ “ ‘{print $4}’，输出为manager则表示正确
4. 检查harry natasha及其他用户的权限设置

getfacl /examdata/result/fstab.bak|egrep ‘(harry|natasha|other)’

输入应该为：

user:harry: rw-

user:natasha: ---

other:: r--

如果一致的为正确

1. 在/examdata/result/ 下创建一个目录，名为admins，要求所属组为manager组，组成员可以读写，其他用户没有任何权限，同组成员在目录下创建的文件的所属组也为manager组

评分因素和命令

1）本题考查设置sgid权限，属组设置

2)ls /examdata/result/admins ，如果没报错，则为有创建该目录，正确

3）ll -d /examdata/result/admins|awk -F “ “ ‘{print $4}’，输出为manager则表示正确

4）ll -d /examdata/result/admins|grep “drwxrwsr--” 如果输出没报错，则满足条件：

“组成员可以读写，其他用户没有任何权限，同组成员在目录下创建的文件的所属组也为manager组”

5）注意第4）点，sgid在组权限位置里有字母 s标志，所以上面是没有写错的