五、控制文本和目录权限

Linux黑客基础–39–文件和目录权限的控制

Permissions 权限

linux中常见权限

r Permission to read. This grants permission only to open and view a file.（允许读和查看）

w Permission to write. This allows users to view and edit a file.（允许读和写）

x Permission to execute. This allows users to execute a file (but not necessarily view or edit it)（允许用户执行权限）如：脚本、二进制文件

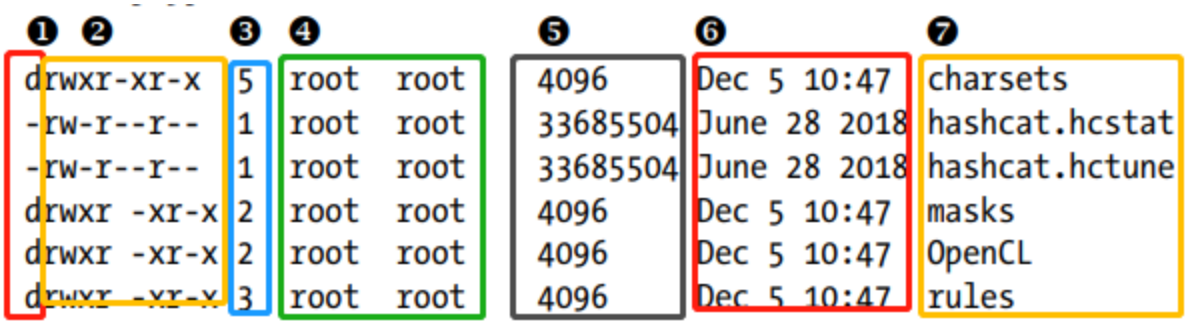
Checking Permissions 检查权限

ls –ld script查看目录权限

drwxr–xr–x 2 root root 4096 3月30日 12:06 script

ls –l archive–key.asc查看文件的权限

–rw–r––r–– 1 root root 3155 2022年 1月27日 archive–key.asc



1-----文件的类型　　2-----文件的权限（rw-r--r--：属主、属组、其他人）　　3----链接的数目

4----属主　　5----属组　　6----文件大小　　7-----文件的时间　　8-----文件名字

Changing Permissions 更改用户的权限

chmod

(1) Changing Permissions with UGO 、、通过表达式更改权限

– Removes a permission

+ Adds a permission

= Sets a permission

chmod u+x f1　　添加执行权限

chmod u-x f1　　去除执行权限

chmod u=x f1　　赋予执行权限（属主只有执行权限）

chmod +w /exam/f1　　只是给属主添加写权限

chmod +x /exam/f1　　给所有用户添加执行权限

chmod u=rwx /exam/f1　　赋予多种权限

chmod u-rwx /exam/f1　　去除多种权限

chmod u=rwx,o=rwx /exam/f1

（2） Changing Permissions with Decimal Notation //通过10进制计数法更改权限

r Permission to read. This grants permission only to open and view a file.（允许读和查看）4

w Permission to write. This allows users to view and edit a file.（允许读和写）2

x Permission to execute. This allows users to execute a file (but not necessarily view or edit it)（允许用户执行权限）如：脚本、二进制文件 1

Binary	Octal	rwx
000	0	---
001	1	--x
010	2	-w-
011	3	-wx
100	4	r--
101	5	r-x
110	6	rw-
111	7	rwx

Linux黑客基础–40–文件和目录权限的控制–umask

Setting More Secure Default Permissions with Masks 赋予默认的安全级别权限

通过umask设置文件（目录）默认权限

linux系统默认为文件分配的权限如下：

usually（文件） 666 rw-rw-rw-　　files（目录） 777　rwxrwxrwx

可以通过umask把相应的权限从linux基本权限中掩去

对于个人用户来讲也可以定义自己的umask值，建议写在用户家目录中的.profile中

Linux黑客基础-41-更改文件的属主和属组

Granting Ownership to an Individual User　更改文件的属主和属组

useradd lsj　添加用户

-b, --base-dir BASE_DIR　新账户的主目录的基目录

--btrfs-subvolume-home　use BTRFS subvolume for home directory

-c, --comment COMMENT　新账户的 GECOS 字段

-d, --home-dir HOME_DIR　新账户的主目录

-D, --defaults　显示或更改默认的 useradd 配置

-e, --expiredate EXPIRE_DATE　新账户的过期日期

-f, --inactive INACTIVE　新账户的密码不活动期

-F, --add-subids-for-system　add entries to sub[ud]id even when adding a system user

-g, --gid GROUP　新账户主组的名称或 ID

-G, --groups GROUPS　新账户的附加组列表

-h, --help　显示此帮助信息并退出

-k, --skel SKEL_DIR　使用此目录作为骨架目录

-K, --key KEY=VALUE 不使用 /etc/login.defs 中的默认值

-l, --no-log-init 不要将此用户添加到最近登录和登录失败数据库

-m, --create-home 创建用户的主目录

-M, --no-create-home 不创建用户的主目录

-N, --no-user-group 不创建同名的组

-o, --non-unique 允许使用重复的 UID 创建用户

-p, --password PASSWORD 加密后的新账户密码

-r, --system 创建一个系统账户

-R, --root CHROOT_DIR chroot 到的目录

-P, --prefix PREFIX_DIR prefix directory where are located the /etc/* files

-s, --shell SHELL 新账户的登录 shell

-u, --uid UID 新账户的用户 ID

-U, --user-group 创建与用户同名的组

-Z, --selinux-user SEUSER 为 SELinux 用户映射使用指定 SEUSER

groupadd hh 添加组

-f, --force 如果组已经存在则成功退出

并且如果 GID 已被使用则取消 -g

-g, --gid GID 为新组使用 GID

-h, --help 显示此帮助信息并退出

-K, --key KEY=VALUE 不使用 /etc/login.defs 中的默认值

-o, --non-unique 允许创建有重复 GID 的组

-p, --password PASSWORD 为新组使用此加密过的密码

-r, --system 创建一个系统账户

-R, --root CHROOT_DIR chroot 到的目录

把用户加入组 Granting Ownership to a Group

方法一、gpasswd

```
┌──(root💀kali)-[/home/hy]
└─# gpasswd -a hy lsj
正在将用户“hy”加入到“lsj”组中
```

```
┌──(root💀kali)-[/home/hy]
└─# gpasswd -d hy lsj
正在将用户“hy”从“lsj”组中删除
```

-a, --add USER 向组 GROUP 中添加用户 USER

-d, --delete USER 从组 GROUP 中添加或删除用户

-h, --help 显示此帮助信息并退出

-Q, --root CHROOT_DIR 要 chroot 进的目录

-r, --remove-password 移除组 GROUP 的密码

-R, --restrict 向其成员限制访问组 GROUP

-M, --members USER,... 设置组 GROUP 的成员列表

-A, --administrators ADMIN,... 设置组的管理员列表

方法二、usermod

```
┌──(root💀kali)-[/home/hy]
└─# usermod -G lsj hy
```

-a, --append GROUP 将用户追加至上边 -G 中提到的附加组中，并不从其它组中删除此用户

-b, --badname allow bad names

-c, --comment COMMENT GECOS 字段的新值

-d, --home HOME_DIR 用户的新主目录

-e, --expiredate EXPIRE_DATE 设定帐户过期的日期为 EXPIRE_DATE

-f, --inactive INACTIVE 过期 INACTIVE 天数后，设定密码为失效状态

-g, --gid GROUP 强制使用 GROUP 为新主组

-G, --groups GROUPS 新的附加组列表 GROUPS

-h, --help 显示此帮助信息并退出

-l, --login NEW_LOGIN 新的登录名称

-L, --lock 锁定用户帐号

-m, --move-home 将家目录内容移至新位置 (仅于 -d 一起使用)

-o, --non-unique 允许使用重复的(非唯一的) UID

-p, --password PASSWORD 将加密过的密码 (PASSWORD) 设为新密码

-P, --prefix PREFIX_DIR prefix directory where are located the /etc/* files

-r, --remove remove the user from only the supplemental GROUPS

mentioned by the -G option without removing

the user from other groups

-R, --root CHROOT_DIR chroot 到的目录

-s, --shell SHELL 该用户帐号的新登录 shell

-u, --uid UID 用户帐号的新 UID

-U, --unlock 解锁用户帐号

-v, --add-subuids FIRST-LAST 添加子 UID 范围

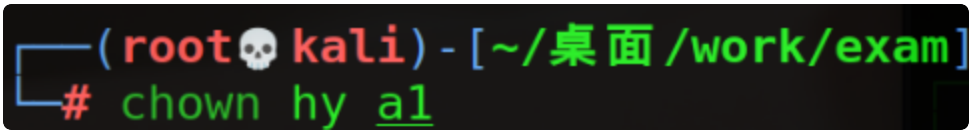
-V, --del-subuids FIRST-LAST 移除子 UID 范围

-w, --add-subgids FIRST-LAST 添加子 GID 范围

-W, --del-subgids FIRST-LAST 移除子 GID 范围

-Z, --selinux-user SEUSER 用户的新的 SELinux 用户映射

更改文件的属主 chown



-c, --changes 类似 verbose 选项，但仅在做出修改时进行报告

-f, --silent, --quiet 不显示大多数错误消息

-v, --verbose 为每个处理的文件输出一条诊断信息

--dereference 影响每个符号链接指向的文件（这是默认行为），而非符号链接本身

-h, --no-dereference 影响符号链接，而非其指向的文件（仅当系统支持更改符号链接的所有权时，该选项才有用）

--from=当前所有者:当前组

仅在文件的当前所有者和/或组和这里指定的一致时，才更改所有者和/或组。其中一个可以省略，表示不对被省略的属性作出要求

--no-preserve-root 不特殊对待 "/"（默认行为）

--preserve-root 不允许在 "/" 上递归操作

--reference=参考文件 使用指定 <参考文件> 的所有者和组信息，而非手工指定 <所有者:组> 的值

-R, --recursive 递归操作文件和目录

指定了 -R 选项时，以下选项设置如何遍历目录层次。

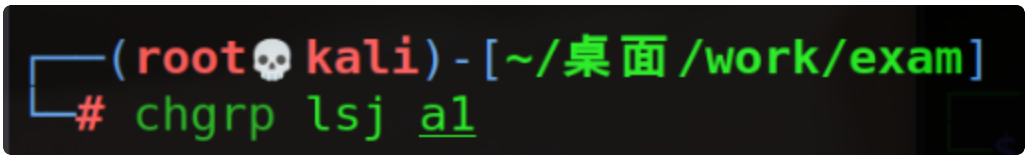
如果您指定了多于一个选项，那么只有最后一个会生效。

-H	如果命令行参数是一个指向目录的符号链接，则对其进行遍历
-L	遍历每一个遇到的指向目录的符号链接
-P	不遍历任何符号链接（默认）

--help	显示此帮助信息并退出
--version	显示版本信息并退出

更改文件的属组

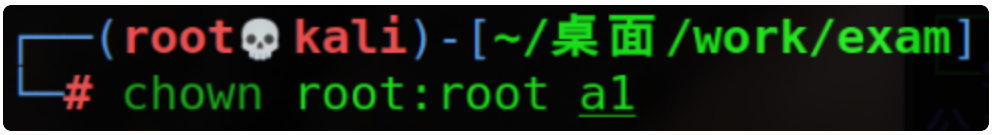
方式一、chgrp



方式二、chown

chown 属主:属组 文件

chown ： 属组 文件



Linux黑客基础-42-特殊的权限位-SUID位

Granting Temporary Root Permissions with SUID　　使用 SUID 授予临时 root 权限

通过SUID位给用户临时root权限

当执行设置了SUID位的程序时，是以该程序的属主身份执行，而不是当前用户

```
┌──(root💀kali)-[~/桌面/work/exam]
└─# ls -l /etc/shadow
-rw-r----- 1 root shadow 1976  4月  3日 22:22 /etc/shadow
```

```
┌──(root💀kali)-[~/桌面/work/exam]
└─# chmod u-s /usr/bin/passwd
```
去除SUID位

```
┌──(root💀kali)-[~/桌面/work/exam]
└─# chmod u+s /usr/bin/passwd
```
添加SUID位

SUID---冒险位-4-作用于属主

```
┌──(root💀kali)-[~/桌面/work/exam]
└─# chmod 4755 /usr/bin/passwd
```

如何在系统中查找那些文件设置了SUID位

```
┌──(root💀kali)-[~/桌面/work/exam]
└─# find / -perm -4000 -type f 2>/dev/null
```

```
┌──(root💀kali)-[~/桌面/work/exam]
└─# find / -perm -u=s -type f 2>/dev/null
```

高版本的linux中，如果启动bash的effective（有效的）UID与Real（真实的）UID不同，而且没有使用-p参数，则bash会将effective UID还原成Real UID，当find设置了SUID位之后，就会造成find提权，这将会对计算机造成漏洞并让黑客利用

find –name f1 –exec ls –l {} \;

find –name f1 –exec /bin/bash \;

find –name f1 –exec /bin/bash –p \;

Linux黑客基础–43–特殊的权限位–SGID位

SGID　2–––作用于属组

SGID针对命令程序的作用

1、只有可执行二进制的程序才能设置SGID权限

2、命令执行者要对该程序拥有执行权限

3、命令执行者在执行程序的时候，组身份升级为该可执行程序文件的属组

4、SGID权限只在该程序执行过程中有效，也就是组身份只在程序执行过程中发生改变，命令结束用户组身份恢复

SGID对目录的作用

1、普通用户必须对该目录有rx权限，才能进入此目录

2、普通用户在该目录中的有效组会变成该目录的属组

3、若普通用户对此目录拥有w（可创建文件）权限时，新创建的文件默认属组是这个目录的属组

groupadd lsj

chgrp lsj /exam/

chmod g+s /exam　　chmod 2755 /exam

ls –ld /exam

touch /exam/d9

ls –l /exam/d9

　　–rw–r––r–– 1 root lsj 0　4月 5日 21:59 /exam/d9

find / –perm –2000 –type d 2>/dev/null　　在系统中查找设置了SGID的目录

find / –perm –2000 –type f 2>/dev/null　　在系统中查找设置了SGID的文件

find / –perm –2000 –or –perm –4000 2>/dev/null　　在系统中查找设置了suid位或sgid位的文件?

find / –type f \(–perm –4000 –o –perm –2000 \)

–o (meaninglogical OR)（逻辑或）　　条件满足其中一个

–a (meaning logical AND).（逻辑与）　　默认

在系统中监视文件权限的变化，如发现系统中有无异常的suid位或sgid位的程序?

Linux黑客基础–44–特殊的权限位–stick位

The Outmoded Sticky Bit　（粘连位）

stick 粘连位 1 作用于其他人

chmod o+t dir

通常用于目录（公共），每个人只管理自己的文件，但root用户除外

```
┌──(root💀kali)-[~]
└─# find / -perm -1000 -type d 2>/dev/null
```

查看哪些文件用了stick

```
┌──(root💀kali)-[~]
└─# ls -ld /tmp
drwxrwxrwt 14 root root 4096  4月 5日 21:09 /tmp
```

查看目录权限