权限

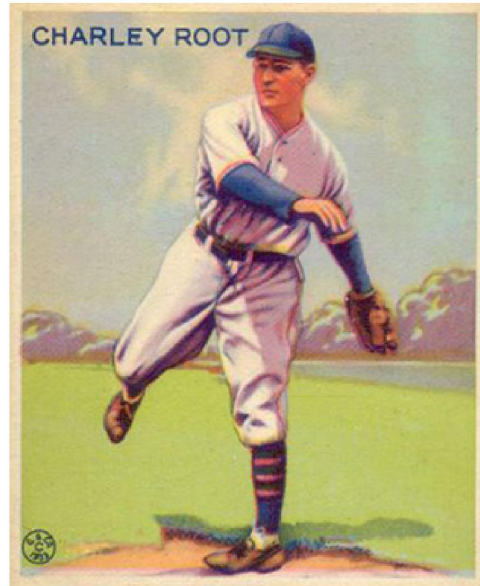
约瑟夫·哈利特

2023 年 1 月 12 日

一开始有根...

这很好。

root用户拥有一切权力。 ▶超级用户▶系统管理员▶ UID 0



所以 root 会产生 init,从而产生登录……

于是其他用户也纷纷效仿▶每一个都比原来的 root 更弱

对于密码文件内部...

在计算机内部的配置目录/etc/中：

$ grep -Ev ^_ /etc/passwd | $ grep -Ev ^_ /etc/passwd |列-ts：

用户名 root 守	密码	UID	GID GECOS	主目录 /root /root /	壳
护进程	*	0	0 查理 & 1		/bin/ksh
操作员 bin	*		恶魔本人		/sbin/nologin
build sshd	*	1	5 系统&	operator / /	/sbin/nologin
www	*	2	7 二进制命令和源 21 base 和 xenocara build 27 sshd		/sbin/nologin
	*	3	privsep	var/empty /	/bin/ksh
	*	21		var/empty /	/sbin/nologin
	*	27 67	67 HTTP 服务器	var/www /	/sbin/nologin
没有人	*	32767 32767	非特权用户	nonexistent /	/sbin/nologin
约瑟夫	*	1000 1000	约瑟夫 哈利特,,,	home/joseph	/usr/local/bin/bash

请参阅 man 5 passwd 或操作系统的手册页。

（有人能看出我用的是什么操作系统吗？）

在组文件里面……

$ grep -Ev ^_ /etc/group | $ grep -Ev ^_ /etc/group |列-ts：

组名轮守护	密码	GID成员	
进程	*	0	根,约瑟夫
kmem	*	1 守护进程	
	*	2根	
	*	3根	
sys	*	4根	
tty	*	5根	
操作员 bin	*	7	
	*	9 约瑟夫	
WSRC	*	10	
用户	*	11	
授权	*	13	
游戏工作人	*	20	根,约瑟夫
员 wobj	*	21	约瑟夫
sshd 访	*	27	
客 utmp	*	31	根
crontab	*	45	
www 网	*	66	
络 authpf 拨号	*	67	
器	*	69	
nogroup 无人	*	72	
joseph	*	117	
	*	32766	
	*	32767	
	*	1000	

非常相似的东西

- 每个群组可以有多个成员
- 从未实际列出过密码
  - （它们在/etc/shadow中）

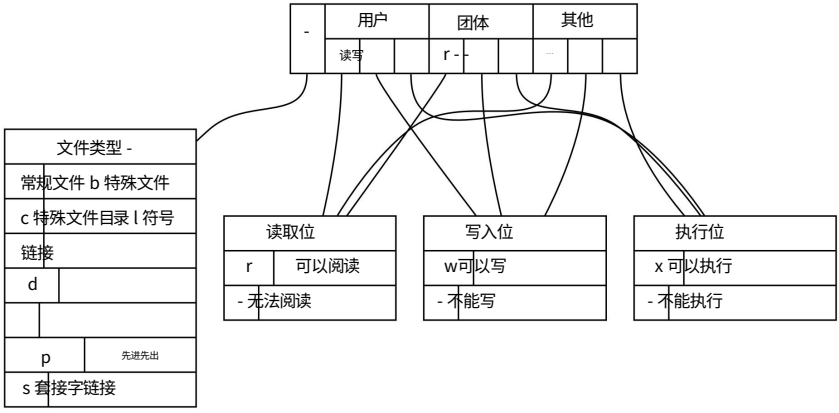
对于所有文件都由用户和组拥有……

ls -loh /etc/

权限 drwxr-xr-x		UID	GID	文件标志	尺寸	文件名
drwxr-xr-x drwxr-	5	根根	轮轮轮	-	512B	2022 年 5 月 20 日
xr-x -rw-r r	2	根根	轮轮轮	-	512B	11 月 25 日 13:25 ImageMagick
drwx------ -rw-	7	根根	轮轮轮	-	512B	11 月 16 日 20:19 X11
r r drwxr-	1	根根	轮轮轮	-	20.5K	11 月 6 日 12:41 abcde.conf
xr-x -rw-r	2	根根		-	512B	11 月 16 日 19:39 极致
r drwxr-	1	根根		-	1.7K	9 月 22 日 7:03 PM adduser.conf
xr-x-rw-r r	2	根		-	512B	11 月 16 日 19:39
	1			-	271B	10 月 30 日 19:14 anthy-conf
	3			-	512B	11 月 25 日 13:27 阿帕奇2
	1			-	1.8K	11 月 14 日 10:34 身份验证milter.json

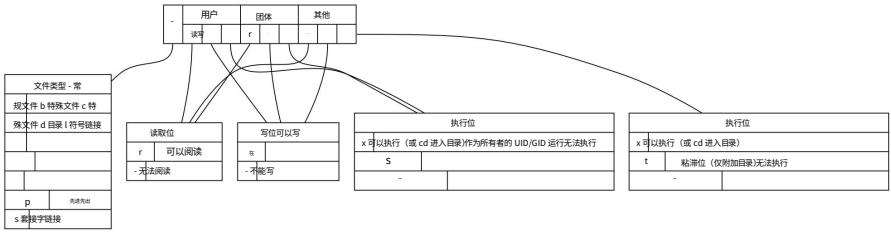
UNIX 自主访问控制

并且每个文件的所有者可以设置每个文件的权限



实际上它有点复杂

并且每个文件的所有者可以设置每个文件的权限



而且，老实说，在某些系统/文件系统上它变得更加复杂

- 但这是你见过或使用过的 99.99% 的东西

那么那些奇怪的额外位有什么用呢？

粘性位t 主要用于日志目录和临时目录▶您应该能够附加到日志文件，但不能删除它们

setuid/setgid 位用于权限分离。

例如，您如何更新密码？

密码通常安全地存储在影子文件 /etc/shadow 或等效文件中

▶但我使用 OpenBSD...

ls -l /etc/spwd.db

-rw-r – 1 root _shadow 40960 12 月 22 日 15:03 /etc/spwd.db

更改密码

passwd 程序更改您的密码： ls -l $(command -v passwd)

-r-sr-xr-x 1 root bin 21208 Jan 12 03:08 /usr/bin/passwd

其他有用的 setuid 程序

su使用密码切换到用户（默认为 root） sudo如果系统管理员允许您使用密码doas ,则切换到用户doas现代重写 sudo,减少 bug 和蜘蛛侠参考 请参阅 man su 或 man sudo 或 man doas...

▶或者Michael W. Lucas出色的Sudo 掌握▶ （你可以用 sudo 做很多事情...）

一般来说,setuid 程序是危险的,您要非常小心地使用它们!

系统管理

如何更改文件的所有者？

ls -l 考试

-rw-r r 1 joseph joseph 0 Jan 12 11:49 考试

chown joseph:staff exam # 或者...
chown :staff exam ls -l exam

-rw-r r 1位约瑟夫职员 0 Jan 12 11:49 考试
（参见 man 1 chown）

如何更改文件的权限

chmod go-wx exam ls -l
exam

-rw-r r 1位约瑟夫职员 0 Jan 12 11:49 考试

脚注有些人喜欢用八
进制（以8为底)来表达权限,其中r=4,w=2,x=1……

他们不会说 go-wx 从组中删除 w 和 x 位以及其他权限,而是说： chmod 744 exam

我建议你对这些人敬而远之。▶（但你应该知道怎么做）

回顾

系统有用户！

- UNIX DAC 允许您设置文件权限！
- setuid 和 setgid 程序存在！
- Root 的名字是Charlie！

chmod更改权限chown更改文件所有者

还有一件事…

传统上root 用户可以做任何事情……
在大多数现代操作系统中,这已被进一步分割

▶例如,Linux 使用功能来设置任何用户可以执行的操作▶ …以及命名空间以

允许多个 root 用户具有不同的功能

如果您想了解更多,请查看 man 7 功能▶ …但大

多数时候您不需要了解它们… ▶除非您使用 Docker…

这是一个谎言,您确实应该了解它们……但是除非您经常养成编写系统管理工具或特权程序的习惯,否则您通常不需要接触它们。嘿,我是一名安全研究员,我认为这些东西很有趣,但其他人不这么认为。不要自己理解:它并不那么复杂,但是嘿嘿。我试过。