1. 什么是SUID

SUID 是 Set User ID的意思

文件的权限显示：

11 10 9 8 7 6 5 4 3 2 1 0   
S G T r w x r w x r w x

第8-6位、5-3位、2-0位分别表示文件所有者的权限，同组用户的权限，其他用户的权限，其形式为rwx：

r表示可读，可以读出文件的内容

w表示可写，可以修改文件的内容

x表示可执行，可运行这个程序

如果一个文件被设置了SUID位，会分别表现在所有者或同组用户的权限的可执行位上。例如：

1、rwsr-xr-x 表示SUID和所有者权限中可执行位被设置

2、rwSr--r-- 表示SUID被设置，但所有者权限中可执行位没有被设置

给文件加SUID和SUID的命令如下：

chmod u+s filename 设置SUID位

chmod u-s filename 去掉SUID设置

1. SUID的作用

由于SUID是在执行程序（程序的可执行位被设置）时起作用，而可执行位只对普通文件和目录文件有意义，所以设置其他种类文件的SUID位是没有多大意义的。

我们知道内核主要是根据euid来确定进程对资源的访问权限。一个进程如果没有SUID位，则euid=uid分别是运行这个程序的用户的uid。例如kevin用户的uid为204，foo用户的uid 200，kevin运行foo用户的my.exe（假定kevin也有x权限）程序形成的进程的euid=uid=204内核根据这些值来判断进程对资源访问的限制，其实就是kevin用户对资源访问的权限，和foo没关系。

如果一个程序设置了SUID，则euid变成被运行的程序的所有者的uid，例如kevin用户运行myfile，euid=200，uid=204，则这个进程具有它的属主foo的资源访问权限。

SUID的作用就是这样：让本来没有相应权限的用户运行这个程序时，可以访问他没有权限访问的资源，获得程序属主的资源访问权限。

1. SUID的例子

$ sudo > my.txt //创建root用户的my.txt文件

$ sudo chmod 600 my.txt //只允许root用户读写该文件

$ vi setuid.c

int main()

{

int ret, fd;

char buf[10];

if (geteuid())

{

fprintf(stderr, "The sandbox is not seteuid root, aborting\n");

return EXIT\_FAILURE;

}

if (!getuid())

{

fprintf(stderr, "The sandbox is not designed to be run by root, aborting\n");

return EXIT\_FAILURE;

}

fd = open("myt.txt", O\_RDWR);

assert(fd > 0);

printf("open ok\n");

ret = read(fd, buf, 9);

buf[9] = 0;

printf("read ok:%s!\n", buf);

close(fd);

return 0;

}

$sudo gcc –o setuid setuid.c //setuid程序俗语root所有

$sudo chmod 4555 setuid //设置setuid程序SUID位

$./setuid //用普通用户访问my.txt文件成功