SISTEMAS OPERATIVOS II

Tercer curso Ingeniería Informática. Curso 2004-2005

Práctica 3: Procesos en UNIX. Credenciales

Añadir al shell de la práctica anterior las siguientes funciones de manejo de las credenciales. (Nótese que deben seguir siendo operativos los comandos de las prácticas anteriores)

getuid Indica las credenciales de usuario del proceso. Indica tanto la real como la efectiva. Tanto para la real como la efectiva debe indicar el valor numérico y el login asociado.

```
#getuid
Credencial Real      15466 ->infaaa00
Credencial Efectiva      0 ->root
#
```

getgid Indica las credenciales de grupo del proceso. Indica tanto la real como la efectiva. Tanto para la real como la efectiva debe indicar el valor numérico y el nombre del grupo.

```
#getgid
Credencial Real Grupo       200 ->users
Credencial Efectiva Grupo     0 ->wheel
#
```

setuid uid Establece la credencial efectiva del proceso a *uid*. *uid* es un entero. En caso de no poder cambiar la credencial, indicará el motivo.

setuidl user Establece la credencial efectica del proceso a la del usuario *user*. *user* es el login de un usuario. En caso de no poder cambiar la credencial, indicará el motivo.

setgid group Establece la credencial efectiva de grupo del proceso a *gid*. *gid* es un entero. En caso de no poder cambiar la credencial, indicará el motivo.

setgidl user Establece la credencial efectica de grupo del proceso a la del grupo *group*. *grupo* es el nombre de un grupo. En caso de no poder cambiar la credencial, indicará el motivo.

info gid Muentra la información del usuario con número de identificación *uid*.

infol user Muentra la información del usuario de nombre *user*. Análogo al comando finger del sistema.

Información detallada de las llamadas al sistema y las funciones de la librería debe obternerse con man (setuid, getuid, getpwent, wait...).

Para que un proceso de un usuario distinto del root pueda ejecutar con éxito la llamada setuid es necesario que ejecute un fichero propiedad de otro usuario que tenga activado el bit *setuid*, lo cual se consigue poniéndole a dicho fichero los permisos 04755. Criterios de seguridad aconsejan que no puedan crearse ficheros *setuid* en sistemas de ficheros exportados por NFS, de ahi que no pueden crearse ficheros *setuid* en los directorios HOME de los usuarios. Hay que crearlos en un directorio local de la máquina donde se trabaja. El único directorio local de las maquinas castro donde los usuarios normales tienen permiso de escritura es /tmp. Por tanto para poder comprobar el uso de dichos comandos del shell es necesario algo como lo mostrado a continuación (suponiendo que el usuario es infaaa00)

```
%gcc p3.c
%mkdir /tmp/infaaa00
%cp a.out /tmp/infaaa00
%chmod 755 /tmp/infaaa00
%chmod 4755 /tmp/infaaa00/a.out
```

Ahora el compañero de prácticas de infaaa00 entraría en la máquina (por ejemplo usando telnet) y haciendo

```
cd /tmp/inaaa00
./a.out
```

podría comprobar como funciona el cambio de credenciales.

Conviene borrar el fichero a.out al terminar las pruebas (y/o usar alguna protección adicional) pues ese shell DA ACCESO a nuestra cuenta

FORMA DE ENTREGA Igual que en prácticas anteriores

FECHA DE ENTREGA JUEVES 5 MAYO 2005