LINUX – SETUID

Impersonificazione

(Fischetti P.)

Login:

```
sysadmin@localhost:~$
```

Aggiungo un utente di prova ‘uprova’:

```
sysadmin@localhost:~$ cat u.sh
useradd uprova ; passwd -d uprova ; echo "uprova:prova" | chpasswd ; usermod -a  -G users uprova;

sysadmin@localhost:~$ ls -l u.sh
-rwxrw-r-- 1 sysadmin sysadmin 98 May 17 09:41 u.sh

sysadmin@localhost:~$ sudo ./u.sh
```

Creo un semplice programma in C che scrive un messaggio e aspetta input da tastiera;

```
sysadmin@localhost:/tmp$ cat h.c
#include <stdio.h>
void main(){
  int d;
  printf("hello\n");
  scanf("%d",&d);
}
```

Compilo:

```
sysadmin@localhost:/tmp$ gcc h.c -oh
```

controllo i permessi:

```
sysadmin@localhost:/tmp$ ls -l h
-rwxrwxr-x 1 sysadmin sysadmin 8400 May 17 10:54 h
```

Avvio il programma in background (nel caso di un solo terminale, altrimenti usare un secondo terminale) per poter interagire con la shell:

```
sysadmin@localhost:/tmp$ ./h &
[1] 332
sysadmin@localhost:/tmp$ hello

[1]+  Stopped                 ./h
sysadmin@localhost:/tmp$ ps -aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0   4384    64 pts/0    Ss   09:38   0:00 /sbin/init
root         8  0.0  0.0  78640  1808 pts/0    S    09:38   0:00 /bin/login -f
syslog      11  0.0  0.0 191332  1284 ?        Ssl  09:38   0:00 /usr/sbin/rsysl
root        15  0.0  0.0  28364  1396 ?        Ss   09:38   0:00 /usr/sbin/cron
root        17  0.0  0.0  72308  1296 ?        Ss   09:38   0:00 /usr/sbin/sshd
bind        27  0.0  0.0 217056 13696 ?       Ssl  09:38   0:00 /usr/sbin/named
sysadmin    48  0.0  0.0  19352  3728 pts/0    S    09:38   0:00 -bash
sysadmin   332  0.0  0.0   4516   784 pts/0    T    10:55   0:00 ./h
sysadmin   333  0.0  0.0  36708  3100 pts/0    R+   10:55   0:00 ps -aux
```

Si puo' notare che il processo h 'gira' ovviamente come sysadmin
Forzo la terminazione del processo:

```
sysadmin@localhost:/tmp$ kill -9 332
```

Cambio utente:

```
sysadmin@localhost:/tmp$ su uprova
Password:
uprova@localhost:/tmp$
```

controllo:

```
uprova@localhost:/tmp$ whoami
uprova
```

avvio lo stesso programma h:

```
uprova@localhost:/tmp$ ./h &
[1] 339
uprova@localhost:/tmp$ hello



[1]+  Stopped                 ./h
uprova@localhost:/tmp$ ps -aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0   4384    64 pts/0    Ss   09:38   0:00 /sbin/init
root         8  0.0  0.0  78640  1808 pts/0    S    09:38   0:00 /bin/login -f
syslog      11  0.0  0.0 191332  1284 ?        Ssl  09:38   0:00 /usr/sbin/rsysl
root        15  0.0  0.0  28364  1396 ?        Ss   09:38   0:00 /usr/sbin/cron
root        17  0.0  0.0  72308  1296 ?        Ss   09:38   0:00 /usr/sbin/sshd
bind        27  0.0  0.0 217056 13696 ?       Ssl  09:38   0:00 /usr/sbin/named
sysadmin    48  0.0  0.0  19352  3728 pts/0    S    09:38   0:00 -bash
root       334  0.0  0.0  60088  3308 pts/0    S    10:56   0:00 su uprova
uprova     335  0.0  0.0  18516  3308 pts/0    S    10:56   0:00 bash
uprova     339  0.0  0.0   4516   760 pts/0    T    10:57   0:00 ./h
uprova     340  0.0  0.0  36708  3044 pts/0    R+   10:57   0:00 ps -aux
```

Notare che il processo 339 gira ovviamente come uprova.
Lo termino

```
uprova@localhost:/tmp$ kill -9 339
```

torno al precedante utente (sysadmin)

```
uprova@localhost:/tmp$ exit
exit
[1]+  Killed                  ./h
sysadmin@localhost:/tmp$
```

imposto il bit s per il file h:

```
sysadmin@localhost:/tmp$ chmod u+s h
```

controllo il bit s impostato:

```
sysadmin@localhost:/tmp$ ls -l h
-rwsrwxr-x 1 sysadmin sysadmin 8400 May 17 10:54 h
```

Cambio utente:

```
sysadmin@localhost:/tmp$ su uprova
Password:
uprova@localhost:/tmp$
```

controllo:

```
uprova@localhost:/tmp$ id
uid=1002(uprova) gid=1002(uprova) groups=1002(uprova),100(users)
```

lancio il processo h:

```
uprova@localhost:/tmp$ ./h &
[1] 349
uprova@localhost:/tmp$ hello

[1]+  Stopped                 ./h
uprova@localhost:/tmp$ ps -aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0   4384    64 pts/0    Ss   09:38   0:00 /sbin/init
root         8  0.0  0.0  78640  1808 pts/0    S    09:38   0:00 /bin/login -f
syslog      11  0.0  0.0 191332  1284 ?        Ssl  09:38   0:00 /usr/sbin/rsysl
root        15  0.0  0.0  28364  1396 ?        Ss   09:38   0:00 /usr/sbin/cron
root        17  0.0  0.0  72308  1296 ?        Ss   09:38   0:00 /usr/sbin/sshd
bind        27  0.0  0.0 217056 13696 ?        Ssl  09:38   0:00 /usr/sbin/named
sysadmin    48  0.0  0.0  19352  3728 pts/0    S    09:38   0:00 -bash
root       344  0.0  0.0  60088  3372 pts/0    S    11:00   0:00 su uprova
uprova     345  0.0  0.0  18516  3464 pts/0    S    11:00   0:00 bash
sysadmin   349  0.0  0.0   4516   740 pts/0    T    11:01   0:00 ./h
uprova     350  0.0  0.0  36708  3072 pts/0    R+   11:01   0:00 ps -aux
```

Ecco, notiamo che l'utete uprova lancia il file h che ha il bit s impostato e gira come sysadmin!
Comunque ricordiamo che e' stato sysadmin in precedenza a concedere questa oppurtinita' agli altri utenti, tramite il comando chmod u+s .