206 - Permisos avançats fitxers

Curs 2020 - 2021

ASIX M01-ISO UF1-A01-03 Permisos avançats: SetUID / SetGID

Permisos

Descripció

Conceptes clau:

- ❏ Permisos avançats de fitxers
- ❏ SetUID
- ❏ SetGID

Ordres a treballar:

- ❏ chmod

Permisos avançats: fitxers

Consulteu el document *204 -Permisos Avançats* per saber l'establiment dels permisos avançats en format octal i simbòlic.

SetUID

El permís SetUID aplicat a fitxers executables provoca que el fitxer s'executi amb els permisos del propietari del fitxer i no amb els permisos de l'usuari que l'està executant.

Aquest permís només es pot aplicar a ordres executables (no scripts) i cal que el permís x d'execució al propietari estigui concedit.

Per defecte les ordres s'executen amb els permisos de l'usuari que està executant l'ordre, així quan l'usuari ecanet executa una ordre aquesta té permís de fer tot allò que l'usuari ecanet pot. Si és l'usuari guest qui executa una ordre, l'ordre pot fer tot allò que pot fer l'usuari guest. Fixem-nos que si l'ordre l'executa root llavors pot fer tot el que pot fer root, és a dir, tot!. Per això és important no treballar mai com a root i només executar com a tal les ordres que sigui imprescindible que executi root.

```
[guest@a36 dades]$ head -n3 /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin

[guest@a36 dades]$ head -n3 /etc/shadow
head: cannot open '/etc/shadow' for reading: Permission denied

[guest@a36 dades]$ useradd newuser
useradd: Permission denied.
useradd: cannot lock /etc/passwd; try again later.
```

```
[root@a36 ~]# head -n3 /etc/shadow
root:$6$4p8fBxdn0mlCDngGt367WQ3.:18164:0:99999:7:::
daemon:*:17416:0:99999:7:::
adm:*:17416:0:99999:7:::
```

- l'usuari guest pot llistar el fitxer /etc/password però no el fitxer /etc/shadow. Tampoc pot executar l'ordre useradd.
- l'usuari root si pot mostrar (i editar) el fitxer /etc/shadow que conté els passwords del sistema. També pot crear nous usuaris.

Fixem-nos que l'usuari guest pot canviar-se el password tot i que acabem de veure que no té permisos per accedir al fitxer /etc/shadow que és el que conté els passwords. Com és possible? Doncs perquè la ordre password que li permet canviar-se el pasword no s'executa en nom seu sinó en nom de root perquè té el SetUID activat.

```
$ which passwd
/usr/bin/passwd

$ ls -l /usr/bin/passwd
-rwsr-xr-x. 1 root root 27872 12 abr  2018 /usr/bin/passwd
```

- podem observar que els permisos per al propietari root són rws, això significa que sigui quin sigui l'usuari que executi aquesta ordre la ordre automàticament es converteix als drets de root i pot fer tot allò que pot fer root.
- és per això que l'ordre password pot modificar el fitxer /etc/shadow.

Atenció

generar ordres propietat de root amb el permís SetUID activat és un mecanisme tradicional de Linux per generar cavalls de troya, generar ordres aparentment inofensives que quan l'usuari les executa es converteixen en root i poden fer el que

volen. Usualment fan el que sembla que han de fer per dissimular i a més fan altres 'maldats'.

Per això els administradors del sistema han de portar un control rigorós de quines són les ordres amb SetUID i SetGID activats i disparar alarmes si apareixen en el sistema nous executables amb aquests permisos activats.

Anem a veure a mode d'exemple que si l'ordre passwd no té el permís setUID activat llavors els usuaris ja no es poden canviar el password. Feu *atenció* de tornar a deixar els permisos de l'ordre bé en acabar l'exemple.

```
[root@a36 ~]# chmod u-s /usr/bin/passwd

[root@a36 ~]# ls -l /usr/bin/passwd
-rwxr-xr-x. 1 root root 27872 Apr 12  2018 /usr/bin/passwd
```

- Com a root hem eliminat el SetUID de l'ordre i ara és una ordre executable normal. Quan un usuari l'executa té els permisos de l'usuari.

```
[guest@a36 dades]$ passwd
Changing password for user guest.
Current password:
New password: f3d0ra32
Retype new password: f3d0ra32
passwd: Authentication token manipulation error
```

- si l'usuari guest intenta canviar-se el password en finalitzar es mostra el missatge d'error que en realitat significa que no pot modificar el fitxer /etc/shadow.
- és possible que tingueu problemes per posar un password que compleixi els requeriments del sistema. En l'exemple es suggereix un password que segurament si compleix els requeriments.

Anem ara a comprovar que si qui estableix el password és root el canvi de password funciona tot i que l'ordre no té el SetUID activat. Funciona perquè l'ordre obté els permisos de l'usuari que l'executa i en aquest cas ja són els permisos de root.

```
[root@a36 ~]# passwd guest
Changing password for user guest.
New password: guest
BAD PASSWORD: The password is shorter than 8 characters
Retype new password: guest
passwd: all authentication tokens updated successfully.
```

- root ha pogut establir un password a guest i a més a més es pot saltar les regles que han de complir els passwords per ser vàlids. Tampoc ha d'indicar quin era el password anterior, directament indica el nou password.

Finalment anem a restaura el SetUID a l'ordre passwd i observar que ara si l'usuari guest es pot canviar el password. Tot i que ell no té permisos per modificar el fitxer /etc/shadow l'ordre password no s'executa amb els seus permisos sinó amb els del propietari del fitxer, que és root.

```
[root@a36 ~]# chmod u+s /usr/bin/passwd
[root@a36 ~]# ls -l /usr/bin/passwd
-rwsr-xr-x. 1 root root 27872 Apr 12  2018 /usr/bin/passwd
```

```
[guest@a36 dades]$ passwd
Changing password for user guest.
Current password: guest
New password: f3d0ra32
Retype new password: f3d0ra32
passwd: all authentication tokens updated successfully.
```

SetGID

El funcionament del permís avançat ***SetGID*** és anàleg al del SetUID però amb el grup de l'ordre en lloc del propietari. Una ordre executable s'executarà amb el permís del grup propietari de l'ordre en lloc del permís de l'usuari que executa l'ordre. Aquest permís va al bloc de permisos del grup i requereix tenir concedir també el permís x.

Mirem per exemple l'ordre *write* que permet enviar missatges de consola a altres usuariss (el funcionament és més fàcil si es fa a les consoles de text). Aquesta ordre pertany al grup tty i té activat el permís de SetGID. Quan l'ordre s'executa pot escriure al terminal dels altres usuaris perquè s'executa en nom de tty. recordeu que els terminals són dispositius /dev/tty que pertanyen al grup tty.

```
$ ls -l /usr/bin/write
-rwxr-sr-x. 1 root tty 19584 27 mar  2018 /usr/bin/write

$ ls -l /dev/tty
crw-rw-rw- 1 root tty 5, 0 20 des 15:49 /dev/tty
```

- observar que l'ordre write té activat el SetGID i pertany al grup tty. Això fa que quan s'executa ho fa en nom de tty i pot fer tot allò que tty pot fer.
- observem també que els terminals, les consoles, són de root però pertanyen al grup tty i els permisos per al grup són rw. Això significa que qui sigui del grup tty pot escriure en els terminals dels altres usuaris.

```
$ write guest
hola que tal
adeu
```

```
a36 login: guest
Password:
Last login: Sun Dec 20 21:30:19 on pts/1
[guest@a36 ~]$ ~
Message from ecanet@a36.informatica.escoladeltreball.org on pts/0 at 21:30 ...
hola que tal
adeu
EOF
```

- l'usuari ecanet escriu un missatge a l'usuari guest que ha iniciat una sessió de consola de text.
- es pot observar que en la consola de text apareix el missatge de l'usuari ecanet.

```
[root@a36 ~]# chmod g-s /usr/bin/write
[root@a36 ~]# ls -l /usr/bin/write
-rwxr-xr-x. 1 root tty 19584 Mar 27  2018 /usr/bin/write
```

- l'usuari root elimina el SetGID de l'ordre write. Ara quan s'executi ho farà amb els permisos efectiu de l'usuari que l'està executant.

```
$ write guest
write: effective gid does not match group of /dev/pts/0
```

- ara quan l'usuari ecanet intenta escriure un nou missatge no pot perquè no té els permisos per escriure en un tty d'un altre usuari.

```
[root@a36 ~]# chmod g+s /usr/bin/write
[root@a36 ~]# ls -l /usr/bin/write
-rwxr-sr-x. 1 root tty 19584 Mar 27  2018 /usr/bin/write
```

- finalment root restaura els permisos de l'ordre write activant de nou el SetGID.

Exercicis d'exemple

1. Elimina el SetUID de l'ordre paasword i verifica que els usuaris no es poden modificar el password. Torna a establir el SetUID a l'ordre password.

   ```
   <seguir els passos de l'exemple en l'apartat SetUID>
   ```

2. Llistar els fitxers del directori /usr/bin que tenen el setUID activat.

   ```
   [guest@a36 dades]$ ll /usr/bin/ | grep "rws"
   -rwsr-xr-x.  1 root  root       52984 Aug  2  2017 at
   -rwsr-xr-x.  1 root  root       73864 Aug 14  2017 chage
   -rws--x--x.  1 root  root       27992 Mar 27  2018 chfn
   -rws--x--x.  1 root  root       23736 Mar 27  2018 chsh
   -rwsr-xr-x.  1 root  root       57608 Aug  2  2017 crontab
   -rwsr-xr-x.  1 root  root       32040 Aug  7  2017 fusermount
   -rwsr-xr-x.  1 root  root       31992 Oct 14  2018 fusermount-glusterfs
   -rwsr-xr-x.  1 root  root       78432 Aug 14  2017 gpasswd
   -rwsr-xr-x   1 root  root       61336 Apr 23  2018 ksu
   -rwsr-xr-x.  1 root  root       36064 Mar 27  2018 mount
   -rwsr-xr-x.  1 root  root       39000 Aug 14  2017 newgidmap
   -rwsr-xr-x.  1 root  root       41920 Aug 14  2017 newgrp
   -rwsr-xr-x.  1 root  root       39000 Aug 14  2017 newuidmap
   -rwsr-xr-x.  1 root  root       27872 Apr 12  2018 passwd
   -rwsr-xr-x.  1 root  root       27688 Jul 11  2018 pkexec
   -rwsr-xr-x.  1 root  root       32136 Mar 27  2018 su
   -rwsr-xr-x.  1 root  root       27880 Mar 27  2018 umount
   ```

3. Amb l'usuari *guest* modificar el shell que té assignat usant l'ordre *chsh*. Establir el shell */bin/sh* (o qualsevol del fitxer */etc/shells* diferent de l'actual).
   Amb l'usuari *root* eliminar el permís *SetUID* de l'ordre chsh.
   Amb l'usuari *guest* intentar tornar a establir el seu shell a */bin/bash*, pot?
   Amb l'usuari *root* tornar a activar el SetUID a l'ordre *chsh*.
   Pot ara l'usuari *guest* assignar-se el shell */bin/bash*?

```
[guest@a36 dades]$ finger guest
Login: guest                            Name: guest
Directory: /home/guest                  Shell: /bin/bash
Last login Sun Dec 20 19:35 (CET) on pts/1
No mail.
No Plan.

[guest@a36 dades]$ chsh -s /bin/sh guest
Changing shell for guest.
Password:
Shell changed.
```

- l'usuari guest consulta amb l'ordre finger el seu shell i a continuació el modifica establint com a shell /bin/sh.

```
[root@a36 ~]# chmod u-s /usr/bin/chsh
[root@a36 ~]# ls -l /usr/bin/chsh
-rwx--x--x. 1 root root 23736 Mar 27  2018 /usr/bin/chsh
```

- l'usuari root elimina el SetUID de l'ordre chsh.

```
[guest@a36 dades]$ chsh -s /bin/bash guest
Changing shell for guest.
chsh: libuser initialization failed: not executing with superuser privileges.
```

- ara l'usuari guest no es pot modificar el shell. L'ordre chsh es queixa de que s'està executant sense els privilegis de super usuari root. Aquests privilegis els obtenia en ser propietat de root i tenir activat el SetUID.

```
[root@a36 ~]# chmod u+s /usr/bin/chsh
[root@a36 ~]# ls -l /usr/bin/chsh
-rws--x--x. 1 root root 23736 Mar 27  2018 /usr/bin/chsh
```

- root torna a activar el SetUID a l'ordre chsh. Ara s'executarà amb permisos de root sigui quin sigui l'usuari que l'executa.

```
[guest@a36 dades]$ chsh -s /bin/bash guest
Changing shell for guest.
Password:
Shell changed.
```

4. Anem a fer una maldat en el sistema. Convertim l'ordre tail en un cavall de troya que adquireix els permisos de root en executar-se.

```
$ ls -l /etc/shadow
```

```
---------- 1 root root 1858 20 des 21:09 /etc/shadow

$ tail -n3  /etc/shadow
tail: cannot open '/etc/shadow' for reading: Permission denied
```

- primerament conrastem que l'usuari guest no pot llistar les tres últimes línies del fitxer /etc/shadow (no en té permís).

```
[root@a36 ~]# chmod u+s /usr/bin/tail
[root@a36 ~]# ls -l /usr/bin/tail
-rwsr-xr-x. 1 root root 70200 Apr 20  2018 /usr/bin/tail
```

- amb l'usuari root activem el SetUID del fitxer tail. Ara quan s'executi ho farà amb els permisos de root.

```
$ tail -n3  /etc/shadow
new:$6$Uss1Fq60wleV5wUS$7tVB0ZsPs/TVP7s9JT.Pip.NPlrYdxwKUb4Gb0B.:18523:0:99999:7:::
ntop:!!:18568::::::
user01:$6$O.WSUfgsHY/WKd0N$QWsXXOPij2q6zvGYd1XI1J0xlK1RjcIsViy0r.:18614:0:99999:7:::
```

- ara l'usuari és capaç de llistar el contingut del fitxer /etc/shadow tot i que el fitxer té permisos --- --- --- (cool?).

```
[root@a36 ~]# chmod u-s /usr/bin/tail
[root@a36 ~]# ls -l /usr/bin/tail
-rwxr-xr-x. 1 root root 70200 Apr 20  2018 /usr/bin/tail
```

- finalment amb l'usuari root tornem a restablir els permisos apropiats eliminant el SetUid de l'ordre tail.

Ara ja podem demanar a l'anna que en python fem un programa que encripta el disc dur, l'anomenem tail, li activem el setuid, el passem a companys i coneguts dient que és una versió nova en colors super xula i finalment demanem un rescat per desencriptar el disc dur. Llavors amb el rescat ens fugem a Abu Dhabi.

5. Modifica els permisos de l'ordre write desactivant el setGID i verifica que quan el té actiu pot escriure missatges a la còsola d'altres usuaris i que quan no el té no pot.

```
< seguir les explicacions i exemple de l'apartat dels apunts SetGID >
```