Pràctica 4: Gestió d'usuaris

Objectius de la pràctica

Gestionar els usuaris del sistema: realitzar l'alta i baixa d'usuaris i modificar les propietats dels comptes d'usuari.

Abans de començar

Per aquesta sessió hauríeu de ser capaços de contestar les següents preguntes abans de començar:

- A quin fitxer està definida, i quina estructura té la base de dades d'usuaris, la taula de passwords (shadow), i la base de dades de grups?
- Com es poden assignar els UID per als usuaris nous?
- Quines comandes es poden utilitzar per canviar els propietaris i els permisos d'un fitxer? I de tots el fitxers d'un directori?

Introducció

Al sistema cada usuari té un compte associat. Un compte són tots els fitxers, recursos i informació que pertanyen a cada usuari. Els comptes d'usuari permeten al sistema diferenciar les dades i processos de cada usuari i permeten als usuaris protegir la seva informació.

Per al kernel els usuaris s'identifiquen amb un nombre enter conegut com l'identificador d'usuari (*user identifier o UID*). A més hi ha una base de dades que associa el UID amb un nom textual: el *username.* Aquest *username és* l'utilitzat per l'usuari per fer *login*. La base de dades d'usuaris inclou altra informació relativa a l 'usuari com la ruta del directori *home,* el nom complet de l'usuari i l'interpret de comandes (shell).

La creació de un nou usuari inclou l'assignació d'un UID i la modificació de la base de dades d'usuaris per assignar els paràmetres propis de l'usuari. A més és necessari associar almenys un grup a l'usuari i finalment copiar els fitxers de configuració y personalització al directori *home* de cada usuari.

Opcionalment es pot assignar l'usuari a més d'un grup, la qual cosa permet a l'administrador del sistema dividir els usuaris en grups amb diferents permisos i privilegis. D'aquesta manera podem mantenir un millor control sobre què poden fer el usuaris.

Profile i entorn d'usuari

Quant s'inicia un *login* interactiu, el *shell* automàticament executa un o més fitxers predefinits. Cada *shell* executa fitxers diferents. El shell **bash** executa el fitxer /etc/profile i a més a més executa el fitxer .profile o .bash_profile del *home* de cada usuari. El fitxer /etc/profile permet a l'administrador del sistema definir un entorn comú per a tots els usuaris, especialment definint la variable PATH. Per altra banda .bash_profile permet a cada usuari definir el seu propi entorn adequant el *PATH*, el *prompt*, etc.

Quan es crea el directori home d'un usuari s'han de copiar els fitxers del directori /etc/skel. L'administrador del sistema pot posar fitxers a /etc/skel que donin un entorn inicial pels usuaris. Per exemple, com administradors creeu un fitxer /etc/skel/.bash_profile amb unes definicions bàsiques que després l'usuari podria canviar.

Comproveu que al PATH de tots els usuaris hi sigui el directori /usr/local/bin i feu que el .bash_profile modifiqui el PATH per incloure un directori bin situat en el directori *home* de cada usuari (*$HOME/bin*). També volem que el *prompt* sigui el *username* seguit de la data actual i finalment "> " (per exemple, el de l'usuari xavim seria "xavim (Tue April 10) >")

Quina variable d'entorn té la definició del prompt?

Creació manual d'usuaris

Ara volem donar d'alta un compte d'usuari per a cada membre del grup de laboratori. Abans de començar trieu els paràmetres de cada usuari. Els usuaris han de formar part del grup *admin*.

paràmetres /Usuari	Usuari 1	Usuari 2
UID		
Username		
Directori home		
Shell		
Grups		

Editeu la base de dades d'usuaris per afegir els nous usuaris. Utilitzeu la comanda **vipw** per editar aquest fitxer.

Quina és la diferencia en usar **vipw** o editar directament el fitxer de passwd amb vi? (pista: obriu dos vipw en sessions diferents)

De la mateixa manera, utilitzeu la comanda **vigr** per crear un grup per a cada usuari i definir els altres grups que siguin necessaris.

Quin grups heu creat i quin usuaris pertanyen a aquests grups?

Per raons de seguretat és millor desactivar el compte de l'usuari fins que tot el procés d'alta no hagi finalitzat.

Com es pot desactivar un compte de forma que l'usuari no pugui fer *login?*

Desactiveu els comptes nous fins que no hagi finalitzat de donar d'alta els usuaris.

Creeu el directori *home* de cada usuari, copieu els fitxers que estiguin a /etc/skel i assigneu el propietari i permisos adequats per al directori *home* i per a tots el fitxers que estiguin dintre del directori.

Quines comandes i amb quins paràmetres heu utilitzat per canviar el propietari?

I per canviar els permisos dels fitxers?

Ara assigneu una clau (password) per a cada usuari nou.

Per raons de seguretat la clau no es posa directament al fitxer /etc/passwd. Per això hi ha un altre fitxer anomenat /etc/shadow que només té permisos de lectura per al superusuari. En aquest fitxer el posa la clau xifrada i altres paràmetres associats a la vigència de la clau.

Amb quina comanda es pot editar de manera segura el fitxer de *shadow?*

Quin es el significat dels altres paràmetres que es poden definir al fitxer de *shadow?*

Amb quina comanda es poden modificar aquests paràmetres?

Per editar altres paràmetres del compte d'usuari es poden utilitzar les comandes: **chfn** i **chsh.** Utilitzeu aquestes comandes per assignar valors adequats als comptes creats.

Creació automàtica d'usuaris

La majoria de les distribucions de Linux inclouen programes per automatitzar les tasques de creació i modificació de dades d'usuaris. Unes d'aquestes aplicacions son **useradd i adduser,** que permeten crear usuaris i assignar els diferents paràmetres necessaris per donar d'alta cada compte.

Utilitzeu aquestes comandes per donar d'alta els usuaris següents:

- Professors: profe1, profe2, profe3
- Becari: becari
- Resta d'usuaris: quatre comptes per a quatre grups de pràctiques diferents del vostre. El nom d'usuari del compte serà: asoXX, on XX és el número de dos dígits del grup de pràctiques en qüestió.

Trieu i justifiqueu el lloc més adequat per als home de tots els usuaris. Penseu que alguns usuaris especials poden requerir home directoris també especials.

Per definir els següents permisos ho heu de fer sense modificar les proteccions dels directoris ni dels fitxers.

Els permisos de cadascun d'aquests grups d'usuaris (professors, becaris, administradors, i la resta de grups que considereu necessaris) venen definits de la següent forma:

• Els professors tindran control d'accés a nivell de grup a tots els fitxers de tots els usuaris definits. És a dir: l'accés dels professors a fitxers i directoris dels altres usuaris vindrà determinat pels permisos de grup d'aquests fitxers i directoris.

• Els becaris tindran control d'accés, a nivell de grup, a tots els fitxers de tots els usuaris, exceptuant els dels usuaris professors.

• Els administradors han de poder accedir, a nivell de grup, als fitxers dels seus companys de grup, i a cap altre més.

• Els usuaris que representen la resta de grup de pràctiques NO tindran accés, a nivell de grup, als fitxers dels professors, ni dels becaris, ni dels administradors, ni dels altres grups de pràctiques.

Tingueu en compte que les condicions anteriors estan especificant els nivells d'accés. El nivell d'accés només indica a quin nivell es miren els privilegis sobre un fitxer o directori determinat (user, group, other).

Com es poden definir aquests nivells d'accés sense modificar els permisos dels directoris de home cada usuari?

Eliminació i desactivació d'usuaris

Per donar de baixa un usuari és necessari eliminar tots els seus fitxers, les bústies de correu, treballs d'impressió, treballs **cron** i **at** i totes les referències a l'usuari. Després d'això es poden esborrar les línies associades a l'usuari al fitxer de passwd i de grups. Com un usuari pot tenir fitxers fora del seu directori home es necessari buscar per tot l'arbre de directoris el fitxers que pertanyen l'usuari i esborrar-los

Amb quina comanda es poden buscar tots els fitxers d'un usuari i esborrar-los?

Ara volem fer un backup amb tots els fitxers de l'usuari? (tingueu en compte que potser una llista molt llarga de fitxers. Pista: feu servir **xargs**)

Quin problema hi ha amb els fitxers que tinguin espais al seu nom? Com es pot resoldre això? (veure les opcions de la comanda **xargs** o la opció -exec de **find**)

És una bona practica de seguretat primer desactivar el compte del usuari abans de començar el procés de donar-lo de baixa.

Una manera de desactivar un compte, a banda d'invalidar el password, consisteix en canviar el *shell* de l'usuari per un un programa senzill que només escriu a la pantalla un missatge i dóna informació a l'usuari de les raons per les quals el seu compte d'usuari ha estat desactivat. Per això es pot crear un 'tail script'. Per exemple:

```
#!/usr/bin/tail -n 2
This account has been closed due to a security problem. Please contact the system administrator.
```

Aquest script es pot posar com shell de l'usuari usant la comanda **chsh** i es pot guardar en un directori separat, per exemple */usr/local/lib/no-login.*

Utilitzeu la comanda **chsh** per posar un *tail script* per desactivar el compte d'un dels usuaris asoXX.

Com es pot comprovar que el compte ha quedat desactivat?

Ara creeu un script que donat el nom d'usuari, faci un backup del seu directori home, esborri tots el fitxers que l'usuari tingui al sistema i canviï el shell per un *tail script* que avisi a l'usuari que el seu compte ha estat esborrat.

Esborreu el compte d'un usuari asoXX fent ús d'aquest script.

Quin és el contingut d'aquest script?

Usuari especial asosh

A Unix hi ha comandes com el shutdown per apagar la màquina que només pot executar l'usuari root. En moltes ocasions pot ser interessant que algun altre usuari pugui apagar també la màquina però sense que tingui accés als privilegis de root. Per aconseguir-ho es demana que creeu un compte especial que serveixi per executar un shell simplificat que permetrà fer **shutdown** i altres tasques especials amb permisos de superusuari. L'username corresponent serà **asosh**, i el password serà **asoxx**, amb xx el vostre número de disc. Quan algú faci un login en aquest compte s'executarà l'script asosh que hauríeu de tenir instal·lat de la pràctica anterior d'aplicacions. Per raons de seguretat cal que us assegureu que quan s'entra amb aquest compte no s'executa cap shell script.

Quins permisos posaríeu a aquesta aplicació perquè no pugui ser executat per cap usuari directament?

Com queda finalment l'entrada de la base de dades d'usuaris per a l'usuari **asosh?**

Sudo i control d'execució d'aplicacions

Com el **`shutdown`** hi ha altres comandes d'administració que només poden ser executades per el superusuari. És una mala pràctica de seguretat utilitzar el compte del superusuari per executar aquestes comandes. Per resoldre això es pot utilitzar la comanda ***sudo***. *Sudo* permet executar una comanda a un usuari autoritzat com superusuari o un altre usuari. L'especificació de quines aplicacions pot executar un determinat usuari es defineix al fitxer /etc/sudoers. Aquest fitxer es pot editar de forma segura fent servir la comanda **visudo.**

Feu els canvis necessaris perquè els membres del *grup admin* puguin executar qualsevol comanda amb privilegis de superusuari.

També feu els canvis necessaris perquè els usuaris professors puguin executar l'script per esborrar els usuaris que heu creat abans i tots els binaris que siguin al directori /usr/local/professors/bin.

Comproveu que això funciona executant la comanda **vipw.**

Quins canvis heu fet al fitxer /etc/sudoers per activar els controls anteriors?

Finalment desactiveu el compte del root de tal forma no es pugui fer *login* com superusuari. Les comandes d'administració es podran fer només des dels comptes del grup admin o fent ús de l'usuari asosh. Assegureu-vos que podeu fer comandes des d'un usuari administrador abans de desactivar-ho.

Com es pot desactivar l'accés de login per a l'usuari root?