Práctica 1

Sistemas Operativos

Escuela Técnica Superior de Ingeniería Informática de Granada (ETSIIT)

José Antonio Córdoba Gómez
2º Ingeniería Informática (1º Cuatrimestre)
Granada - 16 de septiembre de 2018

Índice general

Índice de figuras

Capítulo 1

Herramientas de administración básicas

1.1. Introducción

1.1.1. Repaso de scripts de bash

Crea un script de bash que automatiza todos los pasos vistos en este punto y que guardarás preferiblemente en tu directorio home. Al entrar de nuevo en el sistema sólo tendrás que ejecutar el script para empezar a trabajar en modo root

```
#!/bin/bash
read -p 'Estás en clase o en casa {clase, casa}: ' ubicacion
if [ $ubicacion == 'clase' ]; then
    cp /fenix/depar/lsi/UML/*.gz /tmp
    cd /tmp
    gunzip *.gz
    ./kernel32-3.0.4 ubda=./Fedora14-x86-root_fs mem=1024m
elif [ $ubicacion == 'casa' ]; then
    ./kernel32-3.0.4 ubda=./Fedora14-x86-root_fs mem=1024m
else
    echo "No se donde te ubicas, luego no sé que hacer"
fi
```

Figura 1.1: Solución ejercicio 1

1.2. Administración de usuarios

1.2.1. Valores por omisión para nuevas cuentas

Visualiza el contenido de los archivos /etc/default/useradd y /etc/login.defs y comprueba cuáles son las opciones por defecto que tendría un usuario que se creara en nuestro sistema. A continuación, crea una cuenta de usuario y visualiza el contenido de los archivos /etc/passwd y /etc/group

```
[root@localhost ~] $ cat /etc/default/useradd
    # useradd defaults file
    GROUP=100                # Max pertence a 100 grupos
    HOME=/home               # Su home cuelga de /home
    INACTIVE=-1              # No está inactivo = activo
    EXPIRE=                  # No expira su cuenta
    SHELL=/bin/bash          # Su shell es bash
    SKEL=/etc/skel           # El directorio donde configurar bashrc
    CREATE_MAIL_SPOOL=yes    # Crea directorio de mail

[root@localhost ~] $ cat /etc/login.defs
# *REQUIRED*
#   Directory where mailboxes reside, _or_ name of file,
#   relative to the
#   home directory.  If you _do_ define both,
#   MAIL_DIR takes precedence.
#   QMAIL_DIR is for Qmail
#
#QMAIL_DIR        Maildir
MAIL_DIR        /var/spool/mail
#MAIL_FILE        .mail

# Password aging controls:
#
#        PASS_MAX_DAYS        Maximum number of days a
#   password may be used.
#        PASS_MIN_DAYS        Minimum number of days
#   allowed between password changes.
#        PASS_MIN_LEN        Minimum acceptable password length.
#        PASS_WARN_AGE        Number of days warning given before
#   a password expires.
```

```
#
PASS_MAX_DAYS        99999
PASS_MIN_DAYS        0
PASS_MIN_LEN        5
PASS_WARN_AGE        7

#
# Min/max values for automatic uid selection in useradd
#
UID_MIN                          500
UID_MAX                        60000

#
# Min/max values for automatic gid selection in groupadd
#
GID_MIN                          500
GID_MAX                        60000

#
# If defined, this command is run when removing a user.
# It should remove any at/cron/print jobs etc. owned by
# the user to be removed (passed as the first argument).
#
#USERDEL_CMD        /usr/sbin/userdel_local

#
# If useradd should create home directories for users by default
# On RH systems, we do. This option is overridden with
# the -m flag on useradd command line.
#
CREATE_HOME        yes

# The permission mask is initialized to this value. If not
# specified, the permission mask will be initialized to 022.
UMASK           077

# This enables userdel to remove user groups if no members exist.
#
USERGROUPS_ENAB yes
```

```
# Use SHA512 to encrypt password.
ENCRYPT_METHOD SHA512

[root@localhost ~]# cat /etc/login.defs
# *REQUIRED*
#   Directory where mailboxes reside, _or_ name of file, relative to the
#   home directory.  If you _do_ define both, MAIL_DIR takes precedence.
#   QMAIL_DIR is for Qmail
#
#QMAIL_DIR        Maildir
MAIL_DIR        /var/spool/mail
#MAIL_FILE        .mail

# Password aging controls:
#
#        PASS_MAX_DAYS        Maximum number of days a password may be used.
#        PASS_MIN_DAYS        Minimum number of days allowed between
#   password changes.
#        PASS_MIN_LEN        Minimum acceptable password length.
#        PASS_WARN_AGE        Number of days warning given before a
#   password expires.
#
PASS_MAX_DAYS        99999
PASS_MIN_DAYS        0
PASS_MIN_LEN        5
PASS_WARN_AGE        7

#
# Min/max values for automatic uid selection in useradd
#
UID_MIN                         500
UID_MAX                       60000

#
# Min/max values for automatic gid selection in groupadd
#
GID_MIN                         500
GID_MAX                       60000

#
```

```
# If defined, this command is run when removing a user.
# It should remove any at/cron/print jobs etc. owned by
# the user to be removed (passed as the first argument).
#
#USERDEL_CMD        /usr/sbin/userdel_local

#
# If useradd should create home directories for users
# by default On RH systems, we do. This option is
# overridden with the -m flag on useradd command line.
#
CREATE_HOME        yes

# The permission mask is initialized to this value.
# If not specified, the permission mask
# will be initialized to 022.
UMASK           077

# This enables userdel to remove user groups if no members exist.
#
USERGROUPS_ENAB yes

# Use SHA512 to encrypt password.
ENCRYPT_METHOD SHA512
```

Listing 1: Solución ejercicio 2

1.2.2. Creación de usuarios

1. Utiliza el manual en línea para leer la sintaxis completa de la utilidad para creación de cuentas y crea dos o tres usuarios en tu sistema cambiando alguno de los valores por defecto.

2. Elimina alguno de ellos y comprueba que rastro ha dejado la cuenta recién eliminada en el sistema.

3. Entra (orden **su**) en el sistema como uno de estos usuarios que has creado y mira qué archivos tiene en su directorio home. La orden **sudo** permite cambiar el modo de trabajo a modo root específicamente para ejecutar una orden con privilegios de supervisor y tras su ejecución continuar con los privilegios del usuario que abrió la sesión.

```
#!/bin/bash
[root@localhost ~] $ adduser paquita
[root@localhost ~] $ adduser ola --disabled-login
[root@localhost ~] $ adduser --gid 500 alejandro
[root@localhost ~] $ adduser --no-create-home --uid 510 personaje
[root@localhost ~] $ adduser --shell /sbin/nologin noo

# El usuario ola desaparece de /etc/{shadow, passwd, groups}
# pero deja /home/alejandro
[root@localhost ~] $ userdel alejandro

# Una vez iniciado sesion con paquita, ella puede ver sus
# archivos de home
[root@localhost ~] $ su paquita
[paquita@localhost root] $ls -l
    dr-xr-x---  2 root root 4096 Sep 15 13:04 .
    dr-xr-xr-x 22 root root 4096 Sep 16 12:50 ..
    -rw-------  1 root root 3584 Sep 16 12:42 .bash_history
    -rw-r--r--  1 root root   18 Mar 30  2009 .bash_logout
    -rw-r--r--  1 root root  176 Mar 30  2009 .bash_profile
    -rw-r--r--  1 root root  176 Sep 22  2004 .bashrc
    -rw-r--r--  1 root root  100 Sep 22  2004 .cshrc
    -rw-r--r--  1 root root  129 Dec  3  2004 .tcshrc
```

Figura 1.2: Solución ejercicio 3

1.2.3. Archivo /etc/passwd

Visualiza el archivo /etc/passwd e indica cual es el formato de cada línea de dicho archivo. Para ello también puedes consultar el man o info de Linux. ¿Quién es el propietario de este archivo y cuáles son sus permisos?

```
#!/bin/bash
[root@localhost ~] $ cat /etc/passwd
    root::0:0:root:/root:/bin/bash
    bin:x:1:1:bin:/bin:/sbin/nologin
    daemon:x:2:2:daemon:/sbin:/sbin/nologin
    adm:x:3:4:adm:/var/adm:/sbin/nologin
    lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
    sync:x:5:0:sync:/sbin:/bin/sync
    shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
    halt:x:7:0:halt:/sbin:/sbin/halt
    mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
    uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
    operator:x:11:0:operator:/root:/sbin/nologin
    games:x:12:100:games:/usr/games:/sbin/nologin
    gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
    ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
    nobody:x:99:99:Nobody:/:/sbin/nologin
    saslauth:x:499:499:"Saslauthd user":/var/empty/saslauth:/sbin/nologin
    sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
    mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
    smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
    paquita:x:500:500::/home/paquita:/bin/bash
    paquito:x:501:500:paquito:/home/paquito:/bin/bash
    elena:x:502:500:elena:/home/elena:/bin/bash
    miguel:x:503:500:miguel:/home/miguel:/bin/bash
    ola:x:504:504::/home/ola:/bin/bash
    personaje:x:510:510::/home/personaje:/bin/bash
    no:x:511:511::/home/no:/bin/nologin
    noo:x:512:512::/home/noo:/sbin/nologin

El formato es:
<usuario>:<claveEncriptada>:<uid>:<gid>:<directorioTrabajo>:<terminal>
```

Figura 1.3: Solución ejercicio 4

1.2.4. Archivo /etc/shadow

Visualiza el archivo /etc/shadow desde un usuario distinto al root. ¿Te da algún problema? ¿Sabes por qué? Intenta averiguarlo.

```
Si intentamos ver /etc/shadow desde un usuario distinto al root nos
devuelve que no tenemos permiso de lectura sobre el archivo. Dicho archivo
pertenece al root, y aunque ni siquiera root tenga permiso de r,w,x, sabemos
que por defecto, la politica de control de accesos, hace que el root pueda
consultar cualquier archivo dentro del sistema ya que es el administrador.
Si quisieramos evitarlo podemos cambiar las propiedades del archivo mediante:

#!/bin/bash
[root@localhost ~] $ chattr +i <archivo>

De esta forma, root no podría ver el contenido del archivo, solo el propietario.
```

Figura 1.4: Solución ejercicio 5

1.2.5. Creación de grupos

1. Crea un par de grupos y asígnaselos a algunos de los usuarios de tu sistema.
2. ¿Qué información devuelve la orden *id* si estás conectado como root?

```
#!/bin/bash
[root@localhost ~] $ groupadd super
[root@localhost ~] $ groupadd nuevo
[root@localhost ~] $ groupadd pencos


[root@localhost ~] $ gpass -a paquita super
[root@localhost ~] $ gpass -a ola pencos
[root@localhost ~] $ gpass -a no pencos
[root@localhost ~] $ gpass -a root super


[root@localhost ~] $ id
uid=0(root) gid=0(root)
groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
```

Figura 1.5: Solución ejercicio 6

1.3. Información del Sistema de Archivos

1.3.1. Archivos del kernel de Linux

Utilizando la orden *find* que ya conoces para la búsqueda de archivos en el sistema de archivos, anota el nombre absoluto del archivo del kernel de Linux que se ha cargado en el sistema oeprativo que estás usando en el laboratorio de prácticas para acceso en modo root.

```
#!/bin/bash
[root@localhost ~] $ find / -name "vmlinu*"
    /boot/vmlinuz-4.15.0_34_generic
```

Figura 1.6: Solución ejercicio 7

1.3.2. Organización de SA

Un programa que se ejecuta en modo root, ¿dónde podría guardar la información temporal de forma que ésta se mantuviese entre arranques del sistema?

```
Un lugar donde pueda tener información temporal podría ser
/tmp pero se perdería en cada reinicio. Como queremos que
contenga programas una opción sería sobre /var.
/var/tmp podría ser buena opción
```

Figura 1.7: Solución ejercicio 8

1.3.3. Información de los SAs

Los archivos */etc/fstab* y */etc/mtab* muestran información sobre los sistemas de archivos que se encuentran montados en el sistema. ¿Cuál es la diferencia entre la información que muestra cada uno de ellos?

```
fstab indica los discos y las particiones junto a la información
necesaria de configuración. (lista disponibles)
mtab indica los sistemas de archivos montados actualmente.
(lista montados)
```

Figura 1.8: Solución ejercicio 9

1.3.4. Información de los SAs

Edita el archivo */etc/fstab* del sistema de archivos que estás utilizando en modo root y anota y describe la información que tiene registrada. Sino conoces alguna opción puedes consultar el manual en línea: **man fstab**

```
Reune la información sobre los sistemas de archivos y es leído
por el demonio init para poder montarlos al bootear el SO.

Tiene varios campos:

Primero: en este campo se indica el dispositivo o la partición
donde se encuentra el filesystem.

Segundo: aquí va el punto de montaje para el dispositivo especificado.
Tercer: el tipo de sistema de archivos. Puede tomar varios valores,
entre los que se destacan: ext2, ext3, ext4, iso9660, nfs, ntfs,
reiserfs, smbfs, swap, vfat, xfs.

Cuarto: en esta columna van las opciones para el montaje del filesystem.
Son muchas y a continuación se mencionan las más comunes.
Para un listado más completo se pueden leer el manual del comando mount
y el del nfs (para los parámetros específicos de nfs).

    async:  las escrituras al filesystem se demoran,
            es decir que no se hacen en el momento sino
            que se hacen varias escrituras juntas.
            Esto da un mayor rendimiento, aunque si el sistema se cuelga,
            apaga o el filesystem se desmonta, los datos se pederán
            si aún no han sido escritos.
    auto:   el sistema de archivos será montado automáticamente al iniciar
            el sistema o al ejecutar el comando mount -a.
    noauto: debe ser montado explícitamente.
    defaults:   utiliza las opciones por defecto, que son rw, suid, dev,
                exec, auto, nouser, async.
    ro: monta el filesystem como de sólo lectura.
    rw: monta el filesystem como lectura/escritura.
    user: permite que cualquier usuario pueda montar el filesystem.
    nouser: especifica que el filesystem sólo puede ser montado por
            el usuario root y no por un usuario común.
    sync:   todas las escrituras al filesystem se hacen en el momento.
```

```
            Esto da mayor seguridad a los datos pero un menor rendimiento.

Quinto: esta columna indica a la utilidad dump si debe o no hacer backup
        del filesystem. Puede tomar dos valores: 0 y 1. Con 0 se indica
        que no se debe backupear, con 1 que sí se haga. Lógicamente,
        depende de que se tenga instalado y configurado dump, por lo que
        en la mayoría de los casos este campo es 0.

Sexto:  en este caso se trata de una indicación para el fsck (comando que
        chequea el filesystem) y nuevamente se define con un valor
        numérico. Las posibilidades son 0, 1 y 2. El 0 indica que el
        filesystem no debe ser chequeado, mientras que el 1 y el 2 le
        dicen a fsck que sí lo chequee. La diferencia es que el 1
        representa una prioridad mayor que el 2, por lo que debe
        utilizarse para el sistema raíz y el 2 para el resto de los
        sistemas de archivos.
```

Listing 2: Solución ejercicio 10

1.3.5. Archivos de información para los SAs

Compara la información que contienen los cuatro archivos de texto que se han presentado en este apartado (*/etc/fstab*, */etc/mtab*, */proc/filesystems*, */proc/mounts*). Describe en un párrafo para qué te sirve la información que proporcionan.

```
/etc/fstab: lista sistemas de archivos disponibles junto
            a las opciones de configuración.

/etc/mtab:  lista de sistemas de archivos montados actualmente.


/proc/filesystem: lista de sistemas de archivos soportados por el kernel.

/proc/mounts: sistemas de archivos en uso (más actual que mstab).
```

Figura 1.9: Solución ejercicio 11

Capítulo 2

Herramientas de administración del Sistema de Archivos

Capítulo 3

Monitorización del sistema

Capítulo 4

Automatización de tareas

Apéndice A

Información adicional

1. Para apagar el sistema: halt, poweroff o init 0.
2. date -d @numero convierte tiempo epoch a humano UTC.
3. LFS significa Linux from Scratch (desde 0).
4. Cuando se crea un usuario con useradd o adduser, el administrador es quien debe establecerle la contraseña. Sino, cuando el usuario inicie sesión deberá de ejecutar passwd para establecer una.
5. Para averiguar el propietario de un archivo, nos fijamos en la tercera columna de un ls -la.
6. Un enlace blando o simbólico se hace mediante ln -s origen destino
7. Un enlace duro se hace mediante ln origen destino
8. Los enlaces duros son copias fisicas y se destruyen si destruyes una de las copias.
9. Los enlaces blandos son copias simbolicas y se destruyen si destruyes el original.
10. Los enlaces blandos se ejecutan sobre directorios y archivos, mientras que los duros solo sobre archivos.
11. /usr/local está pensado para que el root construya los programas ahí (./configure, make, make install).
12. /opt está pensado para instalar las aplicaciones empaquetadas (por ejemplo sublime, spotify).

Apéndice B

Visto en clase de prácticas

Apéndice C

Dudas

1. En la ejecución con UML no aparece vmlinuz sobre boot. En el anfitrión sí ¿Por qué?

Bibliografía

[Referencia] `http://www.slack.com`