

SEGURIDAD EN SISTEMAS OPERATIVOS

4º Grado en Informática – Complementos de Ing. del Software

Curso 2017-18

Práctica [1]

Sesión [1]

Autor¹: Iván Rodríguez Millán.

Ejercicio 1.

/etc/passwd:

<nombre usuario>:<contraseña>Normalmente sale una x:<UID>Identificador del usuario:<GID>Identificador del grupo principal al que pertenece el usuario:<Información Adicional>:<carpeta personal> Se usa como carpeta de inicio del usuario:<Shell>.

Por ejemplo:

```
root@ubuntu:/etc# cat passwd | grep ivancin:x
ivancin:x:1000:1000:ivan rodriguez,,,:/home/ivancin:/bin/bash
```

/etc/shadow:

<nombre de login>:<contraseña encriptada>:<fecha del último cambio de contraseña>:<mínimo de tiempo (en días) de espera para nuevo cambio de contraseña>:<máximo número de días de validez de la cuenta>:<Número máximo de días para que expire la cuenta>:<Número de días para que caduque una contraseña>:<fecha de expiración de una cuenta desde el 1-Enero-1970>.

/etc/group:

<nombre del grupo>:<contraseña del grupo>:<GID>:<lista de usuarios miembros>.

/etc/gshadow:

<nombre del grupo>:<contraseña encriptada>:<administradores, para cambiar contraseñas por ejemplo>:<lista de usuarios miembros>.

¹ Como autor declaro que los contenidos del presente documento son originales y elaborados por mí. De no cumplir con este compromiso, soy consciente de que, de acuerdo con la “Normativa de evaluación y de calificaciones de los estudiantes de la Universidad de Granada” esto “conllevará la calificación numérica de cero ... independientemente del resto de calificaciones que el estudiante hubiera obtenido ...”

Ejercicio 2.

En primer lugar accedemos al fichero login.defs con el comando **nano** y modificamos los 60 segundos que vienen por defecto por 10 segundos.

```
GNU nano 2.2.6      File: login.defs

#
# Max number of login retries if password is bad. This will most likely be
# overridden by PAM, since the default pam_unix module has it's own built
# in of 3 retries. However, this is a safe fallback in case you are using
# an authentication module that does not enforce PAM_MAXTRIES.
#
LOGIN_RETRIES      5
█
#
# Max time in seconds for login
#
LOGIN_TIMEOUT      10

#
# Which fields may be changed by regular users using chfn - use
# any combination of letters "frwh" (full name, room number, work
# phone, home phone).  If not defined, no changes are allowed.
# For backward compatibility, "yes" = "rwh" and "no" = "frwh".

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text ^T To Spell
```

Una vez hecha la modificación creamos un nuevo usuario para comprobar que la modificación se ha hecho correctamente:

```
sudo useradd -d /home/pruebasso -s /bin/bash pruebasso
```

```
sudo passwd pruebasso
```

Una vez creado el usuario probamos la directiva saliendo del entorno gráfico y entrando en el modo texto. Esto es **control+alt+f1**. Una vez en el modo texto nos debe salir la siguiente pantalla:

```
Ubuntu 14.04.5 LTS ubuntu tty1
ubuntu login:
```

Para comprobar el correcto funcionamiento de la directiva introducimos el usuario y nos pedirá la contraseña, es en este momento en donde si no introducimos nada durante 10 segundos, volverá a pedirnos el usuario.

Una vez visto que funciona correctamente, salimos de este entorno con **control+alt+f7**.

Ejercicio 3.

```
root@ubuntu:/home/ivancin# ls -lai | grep text.txt
2626007 -rw-rw-r--+ 1 root    root      30 oct  4 16:55 text.txt
root@ubuntu:/home/ivancin# setfacl -m u:pruebasso:rw text.txt
root@ubuntu:/home/ivancin# getfacl text.txt
# file: text.txt
# owner: root
# group: root
user::rw-
user:pruebasso:rw-
group::r--
mask::rw-
other::r--
```

En primer lugar creamos un fichero llamado text.txt y vemos los permisos. Ahora nuestro objetivo es modificar el ACL o crear uno nuevo para que **pruebasso** tenga permisos tanto de escritura como de lectura. Para ello hacemos uso del comando:

setfacl -m u:nombre de usuario:permisos a dar fichero en cuestión

Para ver que se ha modificado correctamente usamos el siguiente comando:

```
getfacl text.tx
```

Y vemos como el usuario **pruebasso** tiene permisos tanto de lectura como de escritura, al igual que el **user**.

Ejercicio 4.

```
-cat /etc/pam.d/login
```

Este es el archivo de configuración PAM para el servicio del login.

Algunos de los comportamientos programados que tiene son:

1. Hacer cumplir un retardo en caso de fallo (Microsegundos).

```
auth optional pam_faildelay.so delay=3000000
```

2. Sacar información de los últimos login que han entrado con éxito.

```
session optional pam_lastlog.so
```

3. Poner restricciones de tiempo en los logins.

```
account requisite pam_time.so
```

4. Poner restricciones a los usuarios según /etc/security/limits.conf

```
session required pam_limits.so
```

```
-cat /etc/pam.d/cron
```

Este es el archivo de configuración PAM para el demonio cron.

Algunos de los comportamientos programados que tiene son:

5. Leer información local del sistema.

```
session required pam_env.so envfile=/etc/default/locale
```

6. Leer variables de entorno desde los archivos pam_env.

```
session required pam_env.so
```

7. Poner límites a los usuarios definido por tareas cron.

```
session required pam_limits.so
```

Ejercicio 5.

a)

Para el caso de modificar el tamaño mínimo de contraseña necesario, solamente tenemos que introducir:

```
password requisite pam_cracklib.so retry=3 minlen=10
```

Con la opción minlen=10 estamos diciendo que como mínimo la contraseña debe ser de 10 caracteres.

b)

En este segundo ejemplo vamos de nuevo a coger el fichero common-password, pero esta vez vamos a hacer como en algunas páginas webs, y vamos a pedir que el usuario como mínimo introduzca un carácter en mayúscula.

Esto se hace introduciendo el siguiente comando:

```
password requisite pam_cracklib.so retry=3 minlen=10 difok=3  
ucredit=-1
```

Con el comando ucredit=-1, se pide que como mínimo el usuario introduzca un carácter en mayúscula.

Ejercicio 6.

Para verificar los cambios en un archivo log con respecto a la creación de un nuevo usuario y su cambio de contraseña utilizaremos el archivo /var/log/auth.log.

```
less /var/log/auth.log
```

Y nos encontramos con los siguientes datos relacionados con la creación de un nuevo usuario llamado pruebaaso:

```
Oct 8 11:13:21 ubuntu sudo: root : TTY=pts/7 ; PWD=/etc/pam.d ; USER=root ; COMMAND=/usr/sbin/useradd -d /home/pruebasso -s /bin/bash pruebasso
Oct 8 11:13:21 ubuntu sudo: pam_unix(sudo:session): session opened for user root by ivanovic(uid=0)
Oct 8 11:13:21 ubuntu useradd[11005]: new group: name=pruebasso, GID=1001
Oct 8 11:13:21 ubuntu useradd[11005]: new user: name=pruebasso, UID=1001, GID=1001, home=/home/pruebasso, shell=/bin/bash
Oct 8 11:13:21 ubuntu sudo: pam_unix(sudo:session): session closed for user root
Oct 8 11:13:33 ubuntu sudo: root : TTY=pts/7 ; PWD=/etc/pam.d ; USER=root ; COMMAND=/usr/bin/passwd pruebasso
Oct 8 11:13:33 ubuntu sudo: pam_unix(sudo:session): session opened for user root by ivanovic(uid=0)
Oct 8 11:13:44 ubuntu passwd[11048]: pam_cracklib(passwd:chauthtok): pam_get_authtok_verify returned error: Failed preliminary check by password service
Oct 8 11:13:56 ubuntu passwd[11048]: pam_unix(passwd:chauthtok): password changed for pruebasso
Oct 8 11:13:56 ubuntu passwd[11048]: gkr-pam: couldn't update the login keyring password: no old password was entered
Oct 8 11:13:56 ubuntu sudo: pam_unix(sudo:session): session closed for user root
Oct 8 11:17:01 ubuntu CRON[11698]: pam_unix(cron:session): session opened for user root by (uid=0)
Oct 8 11:17:01 ubuntu CRON[11698]: pam_unix(cron:session): session closed for user root
(END)
```

La primera línea de todas viene referida a la propia creación del usuario.

Y si bajamos más abajo concretamente a la hora: 11:13:56 vemos como se ha realizado el cambio de contraseña al usuario pruebasso.

(PD: Lamento la mala calidad de la imagen).

Ejercicio 7.

```
root@ubuntu:/etc/pam.d# cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
pruebasso    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin   ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#include_dir /etc/sudoers.d
root@ubuntu:/etc/pam.d# █
```

Para esto introducimos la siguiente línea en user privilege specification:

pruebasso ALL=(ALL:ALL) ALL

Ejercicio 8.

Comando last:

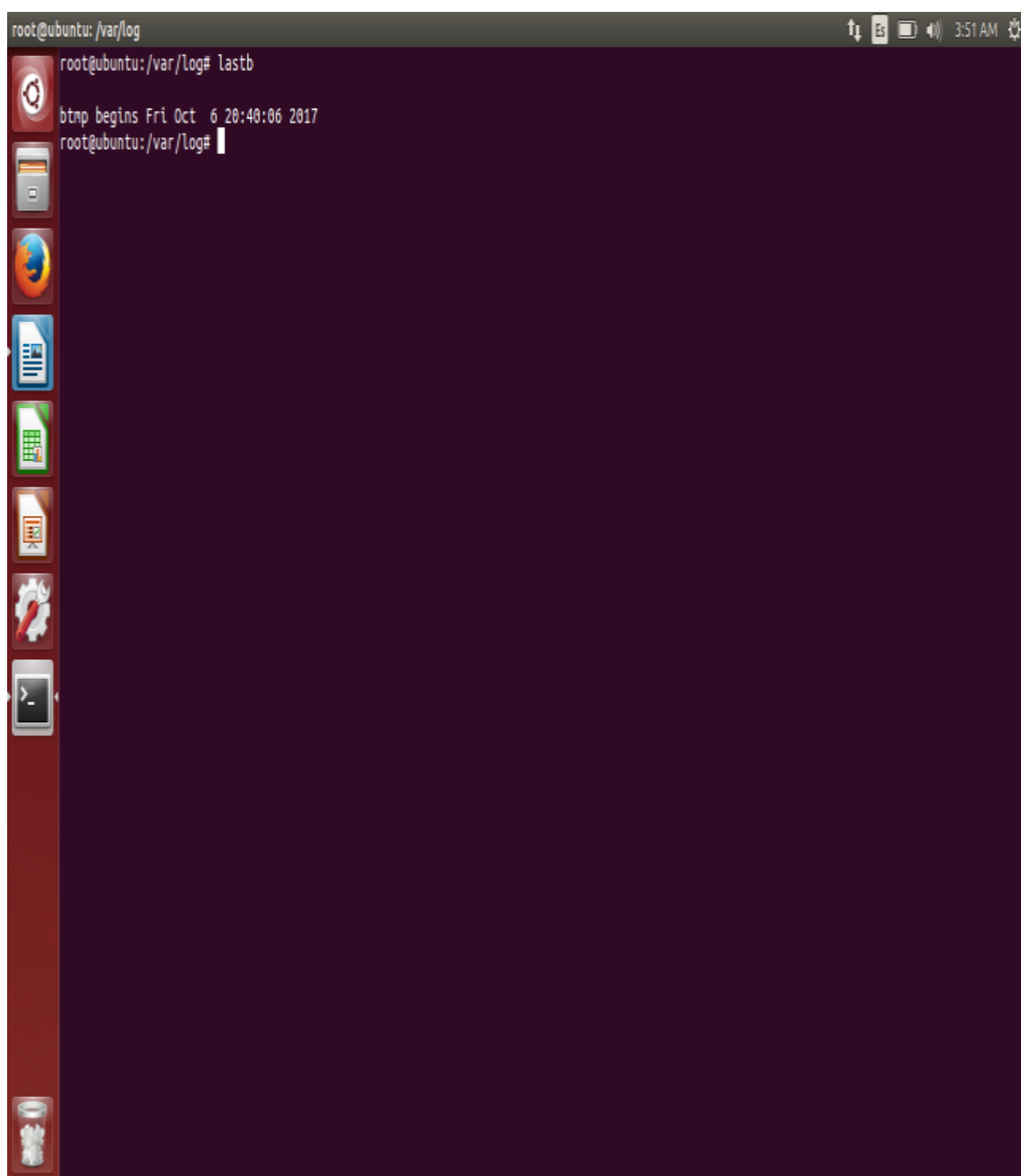
```
root@ubuntu: /var/log
root@ubuntu:/var/log# last
ivanovic pts/1      :0                Sun Oct 8 12:25    still logged in
ivanovic pts/1      :0                Sun Oct 8 11:34 - 11:43    (00:09)
ivanovic pts/7      :0                Sun Oct 8 09:50 - 11:44    (01:54)
ivanovic :0          :0                Sun Oct 8 09:50    still logged in
reboot  system boot  3.16.0-30-generi Sun Oct 8 09:49 - 12:52    (03:02)
ivanovic :0          :0                Fri Oct 6 20:43 - down    (00:03)
reboot  system boot  3.16.0-30-generi Fri Oct 6 20:43 - 20:46    (00:03)
reboot  system boot  3.16.0-30-generi Fri Oct 6 20:42 - 20:43    (00:00)

wtmp begins Fri Oct 6 20:42:48 2017
root@ubuntu:/var/log#
```


Comando lastlog:

```
root@ubuntu: /var/log
root@ubuntu: /var/log# lastlog
Username      Port      From      Latest
root          **Never logged in**
daemon        **Never logged in**
bin           **Never logged in**
sys           **Never logged in**
sync          **Never logged in**
games         **Never logged in**
man           **Never logged in**
lp            **Never logged in**
mail          **Never logged in**
news          **Never logged in**
uucp          **Never logged in**
proxy         **Never logged in**
www-data      **Never logged in**
backup        **Never logged in**
list          **Never logged in**
irc           **Never logged in**
gnats         **Never logged in**
nobody        **Never logged in**
libuuid       **Never logged in**
syslog        **Never logged in**
messagebus    **Never logged in**
usbmux        **Never logged in**
dnsmasq       **Never logged in**
avahi-autoipd **Never logged in**
kernoops      **Never logged in**
rtkit         **Never logged in**
saned         **Never logged in**
whoopsie      **Never logged in**
speech-dispatcher **Never logged in**
avahi         **Never logged in**
lightdm       **Never logged in**
colord        **Never logged in**
hplip         **Never logged in**
pulse         **Never logged in**
ivanovic      **Never logged in**
pruebasso     **Never logged in**
root@ubuntu: /var/log#
```

Comando lastb:



A terminal window titled 'root@ubuntu: /var/log' with a dark purple background. The window shows the command 'lastb' being executed. The output is 'btmp begins Fri Oct 6 20:40:06 2017'. The prompt 'root@ubuntu: /var/log#' is visible at the end of the line. On the left side of the terminal, there is a vertical dock with several application icons: a gear, a document, a globe, a file, a spreadsheet, a presentation, a settings gear, a terminal, and a trash can. The top right corner of the terminal window shows system icons for network, battery, and volume, along with the time '3:51 AM'.

```
root@ubuntu: /var/log# lastb
btmp begins Fri Oct 6 20:40:06 2017
root@ubuntu: /var/log#
```

Ejercicio 9.

Podemos ver con la imagen anterior extraida del comando lastlog, que no ha habido ninguna conexión ajena al sistema.