

SEGURIDAD EN SISTEMAS OPERATIVOS

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

Curso 2018-19

Práctica 1. Administración de la seguridad en Linux

Sesión 1. Seguridad básica en Linux: privilegios de usuario y permisos

Autor¹: Víctor García Carrera

Ejercicio 1.

Comenzamos la práctica estudiando el formato de diversos archivos de claves. En primer lugar accedemos desde la terminal de Linux al directorio raiz o root, desde donde accedemos al directorio etc/ donde se encuentran, entre numerosos archivos de sistema, los ficheros **passwd**, **group**, **shadow** y **gshadow**, que nos interesan para nuestro estudio.

```
File Edit View Search Terminal Help
root@victor-portatil /etc
debian_version      lvm          smartd.conf
default             machine-id   smartmontools
deluser.conf        magic        smi.conf
depmod.d            magic.mime   speech-dispatcher
dhcpc               mailcap     sshclients, estudaremos los aspectos de seguridad relacionados con los privilegios de
dictionaries-common mailcap.order ssl
dkms                manpath.config subgid
dm                  mdn         subgid=sa,
dnsmasq.d           menu-methods subuid
doc-base            mime_types  subuid-
dpkg               mke2fs.conf sudoers
drirc               modprobe.d  sudoers.d
eclipse.ini         modules     sysctl.conf
emacs              modules-load.d sysctl.d
environment        mono        systemd
esound              mtab       terminfo
ffserver.conf       mtools.conf  thermald
firefox             mysql       thunderbird
fonts               nanorc      network
fstab               netscsid.conf timezone
fuse.conf           network     tmpfiles.d
fwupd.conf          NetworkManager ucf.conf
gai.conf            networks    udev /etc/shadow y /etc/gshadow gestionan las claves de usuarios y grupos,
gconf               newt       udisks2
gdb                 nsswitch.conf ufw
ghostscript         ntp.conf    upstart
gimp               obex-data-server update-motd.conf
gnome              octave.conf UPower
gnome-app-install  ODBCDataSources upstart-xsessions
gnome-chess        odbc.ini   upstream-release la clave de grupo con:
gnome-vfs-2.0      odbcinst.ini usb_modeswitch.conf
groff              openal      usb_modeswitch.d
group              openvpn     vdpa_wrapper.cfg
group-             opt        vim
grub.d             os-release  vtrgb
gshadow             pam.conf   wgetrc
gshadow-            pam.d     wildmidi
gss                papersize wireshark
gtk-2.0            passwd    wodim.conf
gtk-3.0            passwd-w  wpa_supplicant
gufw               perl      X11
hdtemp.db          php       xdg
hparm.conf         phpmyadmin zsh_command_not_found

victor-portatil etc #
```

Estos archivos contienen una entrada por línea, y en toda entrada *cada campo se encuentra separado por el símbolo (:)*

Visualizamos con el comando **cat file** el contenido de **passwd** por la terminal. Este archivo es la base de datos de los usuarios donde se especifica información acerca de cada uno de ellos siguiendo el siguiente formato:

User:Password:UID:GID:Description:Home:Shell

¹ Como autor declaro que los contenidos del presente documento son originales y elaborados por mi. 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 ...”

User → Nombre del usuario

Password → Contraseña encriptada en aquellos sistemas que no usen el archivo shadow para ello. En este último caso (el de mi ordenador), simplemente contendrá una x

UID → Identificador numérico de usuario (UserID). En el caso del root es 0

GID → Identificador numérico de grupo (GroupID). En el caso del root es 0

Description → Descripción opcional del usuario, utilizado habitualmente para indicar el nombre real del mismo

Home → Directorio principal del usuario

Shell → Intérprete de comando por defecto

Aquí se encuentra una captura de la terminal donde se muestra el contenido del archivo **passwd** para todos los usuarios del sistema.

The screenshot shows a terminal window titled "root@victor-portatil /etc". The window displays the contents of the /etc/passwd file. The file lists various users with their corresponding UIDs, GIDs, home directories, and shells. Key entries include:

```
File Edit View Search Terminal Help
root@victor-portatil /etc
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin/nologin
bin:x:2:2:bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev/usr/sbin/nologin
sync:x:4:65534:sync:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/notif/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd/bin/false
gshadow:/:104:108::/home/syslog/bin/false
apt:x:105:65534:/:/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus/bin/false
messagebus:x:107:111::/run/uuidd/bin/false
ntp:x:108:114::/home/ntp/bin/false
avahi-autopid:x:109:117:Avahi Autopilot Daemon,,,:/var/lib/avahi-autoipd/bin/false
avahi:x:110:118:Avahi mDNS daemon,,,:/var/run/avahi-daemon/bin/false
dnsmasq:x:111:65534:dnsmasq,,,:/var/lib/misc/bin/false
colord:x:112:121:color colour management daemon,,,:/var/lib/colord/bin/false
speech-dispatcher:x:113:29:Speech Dispatcher,,,:/var/run/speech-dispatcher/bin/false
hplip:x:114:7:HPLIP system user,,,:/var/run/hplip/bin/false
kernoops:x:115:65534:Kernel Ooops Tracking Daemon,,,:/bin/false
pulse:x:116:122:PulseAudio daemon,,,:/var/run/pulse/bin/false
mdm:x:117:124:MDM Display Manager:/var/lib/mdm/bin/false
nm-openvpn:x:118:126:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot/bin/false
rtkit:x:119:127:RealtimeKit,,,:/proc/bin/false
saned:x:120:128::/var/lib/saned/bin/false
usbmux:x:121:46:usbmux daemon,,,:/var/lib/usbmux/bin/false
victor:x:1000:1000:victor,,,:/home/victor/bin/bash
mysql:x:122:131:MySQL Server,,,:/nonexistent/bin/false
sshd:x:123:65534:/:/var/run/sshd:/usr/sbin/nologin
victor-portatil etc #
```

Visualizamos de la misma manera que antes el archivo **group**. Este archivo contiene una lista de los grupos de usuarios existentes. Todo usuario del sistema pertenece a un grupo. El formato de cada entrada es el siguiente:

Name:Password:GID:Members

Name → Nombre del grupo

Password → Contraseña encriptada del grupo. Es opcional, en caso de no haberla implica que cualquier usuario puede formar parte del grupo sin necesidad de una password (habrá una x en este campo)

GID → Identificador numérico del grupo (GroupID)

Members → Lista de los nombres de usuario que forman parte del grupo, separados cada usuario por una coma

A continuación una captura del contenido de mi archivo **group** donde se puede observar el formato previamente mencionado

The screenshot shows a terminal window titled 'root@victor-portatil /etc'. The command 'cat group' is run, displaying the following content:

```
File Edit View Search Terminal Help
victor-portatil etc # cat group
root:x:0:
daemon:x:1: Google YouTube Recibidos - victor Universidad Autónoma de Madrid Correo Entrada GitHub PRADO - GRADO - I Universidad de Granada Webmail UGR - Entrada
bin:x:2:
sys:x:3:
adm:x:4:syslog,victor
tty:x:5:
disk:x:6:victor
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:victor
floppy:x:25:
tape:x:26:
sudo:x:27:victor
audio:x:29:pulse
dip:x:30:victor
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:
sasl:x:45:
plugdev:x:46:victor
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
systemd-journal:x:101:
systemd-timesync:x:102:
systemd-network:x:103:
systemd-resolve:x:104:
systemd-bus-proxy:x:105:
```

Below the terminal window, a web browser tab is visible with the URL 'http://localhost/~victor/Practica_1/Practica_1.html'. The page content discusses user groups and includes a section on keys (Claves) with the following text:

apartados siguientes, estudiaremos los aspectos de seguridad relacionados con los privilegios de usuario y sus permisos. Abordaremos también la configuración de la autenticación y el registro de eventos del sistema.

2. Archivos de claves

La información de usuario se almacena en los archivos de claves. En los sistemas actuales, en el archivo `/etc/passwd` se guardan las credenciales UID y GID que son las que determinan los objetos a los que tiene acceso un usuario.

Los archivos `/etc/shadow` y `/etc/gshadow` gestionan las claves de usuarios y grupos, respectivamente. Recordad que se desgajan del primero por que los permisos de lectura son diferentes. Estos archivos necesitan para su manejo privilegios de root.

La diferencia entre ambos radica en que las claves `/etc/gshadow` se configuran con mucha menor asiduidad. Podemos cambiar la clave de grupo con:

```
$ gpasswd proyecto
```

Ejercicio 1: Indicar los formatos de los archivos `/etc/passwd`, `/etc/group`, `/etc/shadow` y `/etc/gshadow`.

El siguiente archivo a analizar es **shadow**. Este fichero contiene información acerca de las contraseñas de los usuarios del sistema junto con algo de información adicional acerca de los mismos. Por motivos de seguridad, este archivo no debería ser legible para usuarios normales. Podemos traducir los campos de cada entrada con el comando `chage -l username`. Cada entrada contiene 9 campos separados, como se especificó al inicio del ejercicio, por el símbolo (:), en el siguiente orden:

- Nombre de usuario
- Contraseña cifrada, si no está definida se indica con (!)
- Último cambio de contraseña: días desde el 1 de enero de 1970 hasta el último cambio de contraseña
- Número mínimo de días para efectuar un cambio de contraseña
- Número máximo de días para mantener la misma contraseña
- Número de días para avisar con antelación al usuario de la expiración de la contraseña
- Número de días después de que caduque la contraseña antes de que se inhabilite la cuenta (campo 3 + campo 5)
- Número de días desde el 1 de enero de 1970 para la inhabilitación de la cuenta
- Campo reservado

A continuación, el volcado del contenido del archivo **shadow**

```

File Edit View Search Terminal Help
root@victor-portatil etc # cat shadow
root:$6$4LUBca05$gJGj.yobdyNjgZdGF/dQfySie7iQg3m4QPQoLptmlu5XR1nMy8l7HmaxFKuuXcpM/79U7SXMrkGzEFooL20d0:17200:0:99999:7:::
daemon:*:17149:0:99999:7:::
bin:*:17149:0:99999:7:::
sys:*:17149:0:99999:7:::
sync:*:17149:0:99999:7:::
games:*:17149:0:99999:7:::
man:*:17149:0:99999:7:::
lp:*:17149:0:99999:7:::
mail:*:17149:0:99999:7:::
news:*:17149:0:99999:7:::
uucp:*:17149:0:99999:7:::
proxy:*:17149:0:99999:7:::
www-data:*:17149:0:99999:7:::
backup:*:17149:0:99999:7:::
list:*:17149:0:99999:7:::
irc:*:17149:0:99999:7:::
gnats:*:17149:0:99999:7:::
nobody:*:17149:0:99999:7:::
systemd-timesync:*:17149:0:99999:7:::
systemd-network:*:17149:0:99999:7:::
systemd-resolve:*:17149:0:99999:7:::
systemd-bus-proxy:*:17149:0:99999:7:::
syslog:*:17149:0:99999:7:::
apt:*:17149:0:99999:7:::
messagebus:*:17149:0:99999:7:::
uuid:*:17149:0:99999:7:::
ntp:*:17149:0:99999:7:::
avahi-autoipd:*:17149:0:99999:7:::
avahi:*:17149:0:99999:7:::
dnsmasq:*:17149:0:99999:7:::
colorld:*:17149:0:99999:7:::
speech-dispatcher:*:17149:0:99999:7:::
hplip:*:17149:0:99999:7:::
kernoops:*:17149:0:99999:7:::
pulse:*:17149:0:99999:7:::
mdm:*:17149:0:99999:7:::
nm-openvpn:*:17149:0:99999:7:::
rtkit:*:17149:0:99999:7:::
saned:*:17149:0:99999:7:::
usbmux:*:17149:0:99999:7:::
victor:$6$nbhd8ksGzP2pu4ltlK1cJI80IHxhAz0pWqATGHbpdfPD5JUIsU7..gJz0FernY6p0PyCz/ED1z0L3As0cGAoJFRn1c70:17200:0:99999:7:::
mysqld:*:17201:0:99999:7:::
sshd:*:17201:0:99999:7:::
sshd:root@victor-portatil etc #

```

Finalmente, el archivo **gshadow** es un fichero que sólo es legible por el usuario root y contiene una entrada por cada grupo. El formato del mismo es el siguiente:

- Nombre del grupo
- Contraseña encriptada. Si el grupo carece de ella aparecerá el símbolo (!)
- Administradores del grupo, en forma de lista separada por comas
- Miembros del grupo, en forma de lista separada por comas

```

File Edit View Search Terminal Help
root@victor-portatil etc # cat gshadow
root:::
daemon:::
bin:::
sys:::
adm:::syslog,victor
tty:::
disk:::victor
lp:::
mail:::
news:::
uucp:::
man:::
proxy:::
kmem:::
dialout:::
fax:::
voice:::
cdrom:::victor
floppy:::
tape:::
sudo:::victor
audio:::pulse
dip:::victor
www-data:::
backup:::
operator:::
list:::
irc:::
src:::
gnats:::
shadow:::
utmp:::
video:::
sasl:::
plugdev:::victor
staff:::
games:::
users:::
nogroup:::
systemd-journal:::
systemd-timesync:::
systemd-network:::
systemd-resolve:::
systemd-bus-proxy:::

```

Ejercicio 2.

Trabajamos con el archivo `/etc/login.defs`. Al analizar su contenido comprobamos que la directiva `LOGIN_TIMEOUT` tiene un valor de 60 segundos.

victor@victor-portatil /etc

```
File Edit View Search Terminal Help
GID_MAX          60000
# System accounts          128
#SYS_GID_MIN        100
#SYS_GID_MAX        999
LOG_OK_LOGINS
#
# Max number of login retries if password is bad. This will most likely be
# overridden by PAM, since the default pam_unix module has its 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. » ENAB
#
LOGIN_RETRIES      5
SULOG_FILE
#
# Max time in seconds for login
#
LOGIN_TIMEOUT      60
#
# Which fields may be changed by regular users using chfn - use
# any combination of letters "rwh" (full name, room number, work
# phone, home phone). If not defined, no changes are allowed.
# For backward compatibility, "yes" = "rwh" and "no" = "frwh".
#
CHFN_RESTRICT      rwh
#
# Should login be allowed if we can't cd to the home directory?
# Default is no.
#
DEFAULT_HOME       yes
#
# 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
#
# Enable setting of the umask group bits to be the same as owner bits
# (examples: 022 -> 002, 077 -> 007) for non-root users, if the uid is
# the same as gid, and username is the same as the primary group name.
#
# If set to yes, userdel will remove the user's group if it contains no
#
# Los logins con éxito se registran en el archivo /var/log/syslog.conf
# Se registran los usos de la orden su.
# Se registran los usos de la orden sg.
# Si se define, registra toda la actividad de su.
#
# Mínimo número de días que se puede reservar la carpeta.
#
# Tiempo máximo de un login de consola.
#
# Recordad las órdenes para la gestión de usuario y grupos vistas en Sistemas Operativos: useradd,
# usermod, userdel, groupadd, groupmod, groupdel, groups, y chage.
#
Ejercicio 2.- Modificar el archivo /etc/login.defs para que los usuarios creados a partir de ese
momento tengan un valor asignado para las directiva LOGIN_TIMEOUT. Crear un usuario y comprobar
que efecto tiene la citada directiva.
```

Vamos a cambiarlo a 5. Para ello primero vamos a cambiar de usuario a root para poder tener permisos para modificar este archivo de configuración. Una vez seamos root, abrimos con cualquier visualizador de archivos (en este caso gedit, comando `gedit /etc/login.defs`) y cambiamos su valor a 5.

```
root@victor-portatil /etc
File Edit View Search Terminal Help
# Max number of login retries if password is bad. This will most likely be
# overridden by PAM, since the default pam_unix module has its 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_defs will change the LOGIN_MAXRETRIES value.
LOGIN_RETRIES      true - How can I get /bin/login to not timeout      5 respuestas   26 ene. 2017
#           password - Is there a tool that edits /etc/login.defs for...      3 respuestas   3 mar. 2016
# Max time in seconds for login
#
LOGIN_TIMEOUT      5

#
# Which fields may be changed by regular users using chfn - use -options
# any combination of letters "frwh" (full name, room number, work
# phone, home phone). If not defined, no changes are allowed.
#           increase... ▾ Traducir esta página
# For backward compatibility, "yes" = "rwh" and "no" = "frwh".
#           The problem is that in these cases the login timed out, so.... I suggest looking at /etc/login.defs (and
CHFN_RESTRICT      It's rwhys good to first make a backup.      Problem with changing /etc/login.defs      4 publicaciones   9 may. 2015
#           Default in no.      28 oct. 2012
# Should login be allowed if we can't cd to the home directory?
#           logon...      20 may. 2011
#           how to change telnet login timeout of 60 secs      4 publicaciones   19 mar. 2006
DEFAULT_HOME      yes      Mas resultados de www.linuxquestions.org

#
# If defined, this command is run when removing a user.
#           Super User      It should remove any at/cron/print jobs etc. owned by
#           the user to be removed (passed as the first argument).
#           timeout-on-linux ▾ Traducir esta página
#
#USERDEL_CMD      /usr/sbin/userdel_local      ... .DELLAY line in /etc/login.defs . That should affect both login and su. But
#           why would you want to do that?
#
# Enable setting of the umask group bits to be the same as owner bits
# (examples: 022 -> 002, 677 -> 007) for non-root users, if the uid is
# the same as gid, and username is the same as the primary group name.
#           Stack Overflow      ... ▾ Traducir esta página
#
# If set to yes, userdel will remove the user's group if it contains no
# more members, and useradd will create by default a group with the name
# of the user.      To another value.
#
USERGROUPS_ENAB yes

login.defs(5) — login — Debian unstable — Debian Manpages
```

Finalmente, dado que los cambios en este fichero no afectan automáticamente a la configuración de los usuarios ya existentes, creamos un nuevo usuario para probar si nuestro cambio está activo con el comando `useradd pruebalogin`.

Una vez creado este usuario, utilizamos el comando `login` para tratar de logear y aparece a los 5 segundos el timeout.

The screenshot shows a terminal window titled "root@victor-portatil /etc". The terminal content includes configuration snippets from /etc/pam.d/common-account and /etc/pam.d/common-password, and a command-line session where "pruebalogin" is created and then immediately logged in, failing due to a timeout.

```
#DIALUPS CHECK_ENAB
#LASTLOG_EMAB
#MAIL_CHECK_ENAB
#OBSCURE_CHECKS_ENAB
#PORTTIME_CHECKS_ENAB
#SU_WHEEL_ONLY
#CRACKLIB_DICTPATH
#PASS_CHANGE_TRIES
#PASS_ALWAYS_WARN
#ENVIRON_FILE
#NOLOGINS_FILE
#ISSUE_FILE
#PASS_MIN_LEN
#PASS_MAX_LEN
#ULIMIT
#ENV_HZ
#CHFN_AUTH
#CNSH_AUTH
#FAIL_DELAY

#####
##### OBSOLETE #####
#
# These options are no more handled by shadow.
#
# Shadow utilities will display a warning if they
# still appear.
#
# This entry only appears if password is set.

#####
##### successfully.

# CLOSE_SESSIONS
# LOGIN_STRING
# NO_PASSWORD_CONSOLE
# QMAIL_DIR

victor-portatil etc # useradd pruebalogin
victor-portatil etc # passwd pruebalogin
Enter new UNIX password: 504 tecmint:/home/victor/.bash
Retype new UNIX password:
passwd: password updated successfully
victor-portatil etc # login
victor-portatil login: pruebalogin
Login timed out after 5 seconds.
victor-portatil etc #
```

Ejercicio 3.

Trabajamos con un nuevo usuario creado llamado `pruebauser` y con el archivo `pruebaACL` creado por el usuario `victor`. Inicialmente comprobamos que sólo `victor` tiene permisos para modificar dicho archivo con el comando `getfacl pruebaACL`.

Para permitir al usuario `pruebauser` tener permisos de lectura y escritura en este archivo, vamos a modificar el ACL dándole estos permisos con el comando `setfacl`.

```
setfacl -m u:pruebauser:rw pruebaACL
```

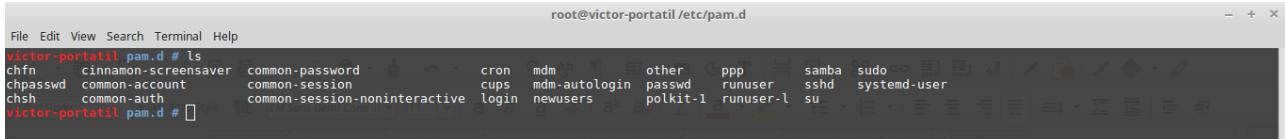
Después, podemos comprobar de nuevo con el comando `getfacl` que los permisos se han modificado como deseábamos.

The screenshot shows a terminal window titled "victor@victor-portatil ~". It displays the process of modifying the ACL of "pruebaACL" to include "pruebauser" with read/write permissions, and then verifying the changes with "getfacl". A note in the terminal states: "Trabajamos con un nuevo usuario creado llamado pruebauser. Vamos a trabajar con el archivo pruebaACL creado por el usuario victor. Inicialmente comprobamos que sólo".

```
victor@victor-portatil ~ $ getfacl pruebaACL
# file: pruebaACL
# owner: victor
# group: victor
user:::rw-
group:::r-
other:::r-
victor@victor-portatil ~ $ setfacl -m u:pruebauser:rw pruebaACL
victor@victor-portatil ~ $ getfacl pruebaACL
# file: pruebaACL
# owner: victor
# group: victor
user:::rw-
user:pruebauser:rw-
group:::r-
mask:::rw-
other:::r-
victor@victor-portatil ~ $
```

Ejercicio 4.

La siguiente imagen muestra los archivos de configuración existentes en el directorio pam.d



```
root@victor-portatil /etc/pam.d
File Edit View Search Terminal Help
victor-portatil pam.d # ls
chfn  cinnamon-screensaver  common-password  cron  mdm  other  ppp  samba  sudo
chpasswd  common-account    common-session   cups  mdm-autologin  passwd  runuser  sshd  systemd-user
chsh  common-auth         common-session-noninteractive  login  newusers  polkit-1  runuser-l  su
victor-portatil pam.d #
```

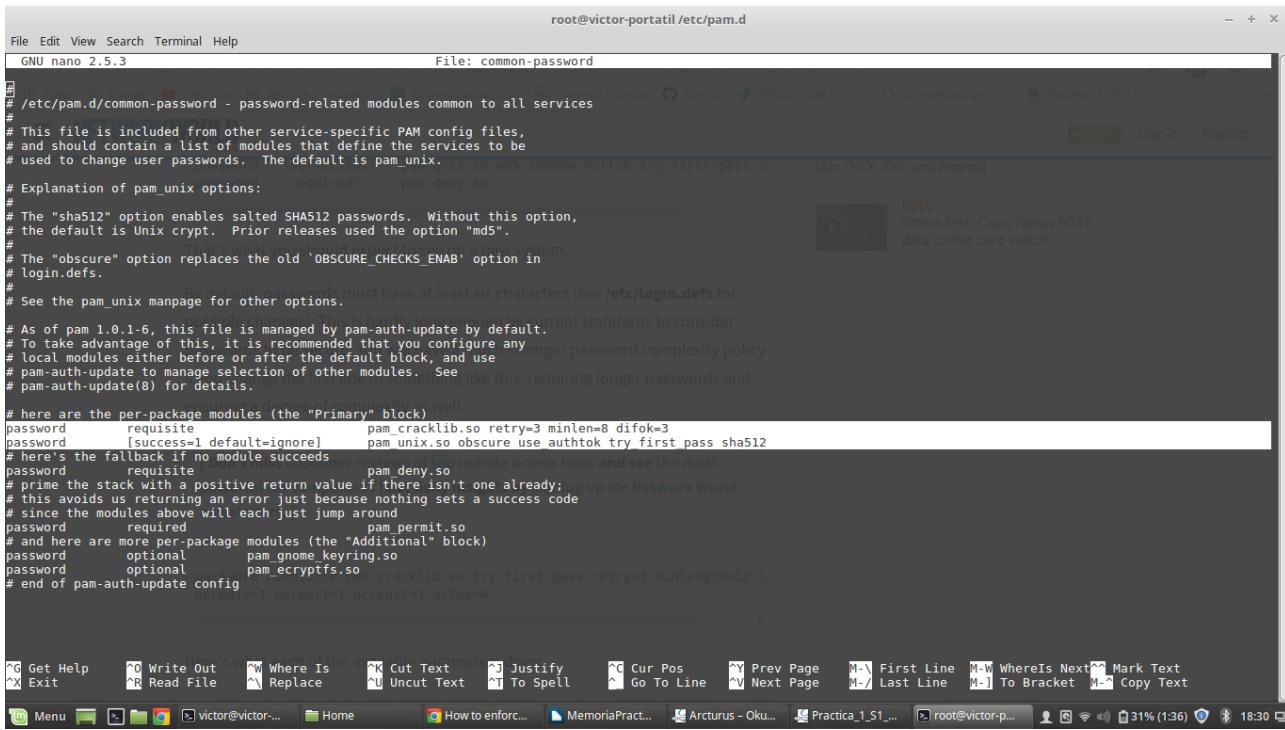
Cada fichero ejemplifica un servicio que proporciona el módulo PAM. Algunos son los siguientes:

common-account: Este módulo permite administrar las cuentas que no están basadas en autenticación. Es utilizado de manera usual para controlar el acceso a un servicio en función de parámetros como la ubicación del usuario, la hora del día...

common-auth: Este módulo proporciona dos aspectos de autenticación del usuario, por un lado solicita al usuario una contraseña u otro medio de identificación para asegurar que se trata de quien dice ser, y por otro otorga permisos y privilegios de grupo a éste usuario.

Ejercicio 5.

Comenzamos instalando el modulo *libpam-cracklib*. Vamos a modificar el archivo */etc/pam.d/common-password*



```
root@victor-portatil /etc/pam.d
File Edit View Search Terminal Help
GNU nano 2.5.3          File: common-password
# /etc/pam.d/common-password - password-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords. The default is pam_unix.
#
# Explanation of pam_unix options: required pam_deny.so
#
# The "sha512" option enables salted SHA512 passwords. Without this option,
# the default is Unix crypt. Prior releases used the option "md5".
#
# The "obscure" option replaces the old 'OBSCURE_CHECKS_ENAB' option in
# login.defs.
#
# See the pam_unix manpage for other options.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.
#
# here are the per-package modules (the "Primary" block).
password  requisite      pam_cracklib.so retry=3 minlen=8 difok=3
password  [success=1 default=ignore]  pam_unix.so obscure use authtok try first pass sha512
# here's the fallback if no module succeeds
password  requisite      pam_deny.so
# prime the stack with a positive return value if there isn't one already; hangs up for Network World
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password  required      pam_permit.so
# and here are more per-package modules (the "Additional" block)
password  optional     pam_gnome_keyring.so
password  optional     pam_encryptfs.so
# end of pam-auth-update config
#
```

En primera instancia ya podemos observar la siguiente linea donde ya existe una configuración de las contraseñas:

password requisite pam_cracklib.so retry=3 minlen=8 difok=3

El campo *retry* hace referencia al numero de intentos para escoger una buena contraseña antes de que el programa *passwd* aborte.

El campo *difok* representa el número mínimo de caracteres que han de ser diferentes en la nueva contraseña respecto a la anterior.

El campo *minlen* establece el número mínimo de caracteres que ha de tener la contraseña. Es algo más que eso, pues realmente se trata de una medida de la complejidad mínima de la contraseña. El cálculo del nivel de complejidad de la contraseña se realiza de la siguiente manera:

- Cada carácter en la contraseña suma 1 punto, sea del tipo que sea.
- Cada minuscula suma 1 punto hasta el valor definido en *lcredit*
- Cada mayúscula suma 1 punto hasta el valor definido en *ucredit*
- Cada dígito suma 1 punto hasta el valor definido en *dcredit*
- Cada carácter especial suma 1 punto hasta el valor definido en *ocredit*

Definimos los parámetros mencionados:

lcredit = establece el número mínimo de minúsculas requeridas

ucredit = establece el número mínimo de mayúsculas requeridas

dcredit = establece el número mínimo de dígitos requeridos

ocredit = establece el número mínimo de caracteres especiales requeridos

Podemos modificar los valores de estos parámetros para imponer ciertas condiciones a los caracteres que conforman las contraseñas (por ejemplo establecer que como mínimo tengan 1 mayúscula y 2 dígitos, *ucredit*=1 *dcredit*=2). Si todos esos parámetros están a 0, *minlen* representa directamente el número mínimo de caracteres que ha de tener la contraseña. En cambio, supongamos que *minlen*=8, si estos 4 parámetros valen 1, podríamos tener una contraseña con 4 caracteres formada por una minúsculas, una mayúscula, un dígito y un carácter especial.

En la siguiente imagen se ejemplifican varios aspectos de seguridad que han actuado a la hora de cambiar la contraseña. En primer lugar, tras 3 intentos fallidos, el programa *passwd* finaliza, el intento de cambio de contraseña acaba (*retry*=3). Además, se ha probado tanto con contraseñas de menos de 8 caracteres (*minlen*=8) como con alguna de 8 pero construida a partir de la ya existente (*difok*=3), impidiéndonos el cambio. Después de este último caso, ponemos una contraseña que cumpla con los requisitos establecidos

```
victor-portatil ~ # login pruebouser
Password:
Last login: Thu Oct 11 20:06:01 CEST 2018 on pts/0
Welcome to Linux Mint 18.1 Serena (GNU/Linux 4.4.0-53-generic x86_64)

* Documentation: https://www.linuxmint.com
No directory, logging in with HOME=/
$ passwd pruebouser
Changing password for pruebouser. g. password for vivek
(current) UNIX password: (current) UNIX password:
New password:          Enter new UNIX password
BAD PASSWORD: it is based on a (reversed) dictionary word
New password:          Enter new UNIX password
BAD PASSWORD: it is based on a dictionary word
Retype new password:   Re-enter new UNIX password
passwd: password updated successfully
New password:
BAD PASSWORD: it is too short
passwd: Have exhausted maximum number of retries for service
passwd: password unchanged
$ passwd pruebouser
Changing password for pruebouser.
The user is first prompted for his/her old password, if one is present. This password is
(current) UNIX password:      encrypted and compared against the stored password. The user has only one
New password:          Enter new UNIX password
BAD PASSWORD: is too similar to the old one
Retype new password:   Re-enter new UNIX password
passwd: password updated successfully
$ exit
logout
A new password is tested for complexity. As a general guideline, passwords should
consist of 6-to-8 characters including one or more from each of following sets.

Top 20 Nginx WebServer Best Security Practices
20 Examples: Make Sure Unix/Linux Configuration Files Are Free From Syntax Errors
15 Greatest Open Source Terminal Applications Of 2012
My 10 UNIX Command Line Mistakes
Top 10 Open Source Web-Based Project Management Software
Top 5 Email Client For Linux, Mac OS X, and Windows Users
The Novice Guide To Buying A Linux Laptop
```

Para exemplificar aún más el apartado b) de este ejercicio, impongo mediante la directiva *dcredit* que la contraseña tenga 2 dígitos como mínimo. De nuevo comprobamos como hicimos anteriormente que esta condición se impone a la hora de definir una nueva contraseña.

```

root@victor-portatil /etc/pam.d
GNU nano 2.5.3
File Edit View Search Terminal Help
File: common-password
Modified

# /etc/pam.d/common-password - password-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords. The default is pam_unix.

# Explanation of pam_unix options: nocracit = establece el número mínimo de caracteres especiales requeridos
# The "sha512" option enables salted SHA512 passwords. Without this option,
# the default is Unix crypt. Prior releases used the option "md5".
# The "obscure" option replaces the old 'OBSCURE_CHECKS_ENAB' option in
# login.defs. minlen=8 establece el número mínimo de caracteres para imponer ciertas condiciones a
# los usuarios que tienen 1 mayúscula y 2 dígitos, ucredit=1 dcredit=2. Si todos esos
# caracteres que ha de tener la contraseña. En cambio, supongamos que minlen=8, si
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use . Una mayúscula, un dígito y un carácter especial.
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

# here are the per package modules (the "Primary" block)
password requisite pam_cracklib.so try_first_pass sha512 difok=3 ucredit=-2 dcredit=2
password [success=1 default=ignore] pam_unix.so obscure use_authtok try_first_pass sha512 try=3
# here's the fallback if no module succeeds
password requisite pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password required pam_permit.so
# and here are more per-package modules (the "Additional" block)
password optional pam_gnome_keyring.so
password optional pam_encryptfs.so
# end of pam-auth-update config

```

Ejercicio 6.

Para la realización de este ejercicio, primero borramos y creamos de nuevo un usuario *pruebauser*, le asignamos como root una contraseña, logeamos como *pruebauser* y probamos a cambiar la contraseña. Fallamos algunos intentos apostando finalmente cambiamos la contraseña. Además de que, obviamente, se habrán actualizado los ficheros de *passwd* y *shadow*, podemos ver en el log del sistema que se ha realizado este cambio. Al tratarse de la distribución de Linux Mint, no contamos con el log *messages*, pero sí con el log *auth.log*, donde como se muestra en la siguiente imagen aparece este cambio de contraseña.

```

root@victor-portatil /var/log
File Edit View Search Terminal Help
Oct 11 20:27:13 victor-portatil sudo:  victor : TTY=pts/0 ; PWD=/etc/pam.d ; USER=root ; COMMAND=/bin/bash
Oct 11 20:27:13 victor-portatil pam_unix(sudo:session): session opened for user root by pruebauser(uid=0)
Oct 11 20:39:01 victor-portatil CRON[29946]: pam_unix(cron:session): session opened for user root by (uid=0)
Oct 11 20:55:36 victor-portatil login[31174]: pam security(login:auth): access denied: tty '/dev/pts/0' is not secure !
Oct 11 20:55:37 victor-portatil login[31174]: pam unix(login:auth): check pass; user unknown
Oct 11 20:55:37 victor-portatil login[31174]: pam unix(login:auth): authentication failure; logname=pruebauser uid=0 euid=0 tty '/dev/pts/0' rhost=
Oct 11 20:55:41 victor-portatil login[31174]: FAILED LOGIN (1) on '/dev/pts/0' FOR 'UNKNOWN', User not known to the underlying authentication module
Oct 11 20:55:47 victor-portatil login[31174]: pam security(login:auth): access denied: tty '/dev/pts/0' is not secure !
Oct 11 20:55:50 victor-portatil login[31174]: pam unix(login:auth): check pass; user unknown
Oct 11 20:55:53 victor-portatil login[31174]: FAILED LOGIN (2) on '/dev/pts/0' FOR 'UNKNOWN', User not known to the underlying authentication module
Oct 11 20:58:08 victor-portatil sudo:  victor : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/bin/bash
Oct 11 20:59:58 victor-portatil sudo:  victor : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/bin/bash
Oct 11 21:00:05 victor-portatil useradd[31674]: new group: name=pruebauser, GID=1001
Oct 11 21:00:15 victor-portatil passwd[31687]: pam_unix(passwd:chauthtok): password changed for pruebauser
Oct 11 21:00:27 victor-portatil passwd[31687]: pam_unix(passwd:chauthtok): password changed for pruebauser
Oct 11 21:00:27 victor-portatil passwd[31687]: gkr-pam: couldn't update the login keyring password: no old password was entered
Oct 11 21:00:27 victor-portatil passwd[31687]: pam_encryptfs: Passphrase file wrapped
Oct 11 21:00:27 victor-portatil passwd[31687]: pam_encryptfs: PAM passphrase change module retrieved at least one NULL passphrase; nothing to do
Oct 11 21:00:56 victor-portatil login[31799]: pam_unix(login:auth): authentication failure; logname=pruebauser uid=0 euid=0 tty '/dev/pts/0' rhost= user=pruebauser
Oct 11 21:01:00 victor-portatil login[31799]: FAILED LOGIN (1) on '/dev/pts/0' FOR 'pruebauser', Authentication failure ->, que comprueba que el
Oct 11 21:01:09 victor-portatil login[31799]: FAILED LOGIN (2) on '/dev/pts/0' FOR 'pruebauser', Authentication failure ->, que comprueba que el
Oct 11 21:01:23 victor-portatil userdel[31763]: delete user 'pruebauser'
Oct 11 21:01:23 victor-portatil userdel[31763]: removed group 'pruebauser' owned by 'pruebauser'
Oct 11 21:01:23 victor-portatil userdel[31763]: removed shadow group 'pruebauser' owned by 'pruebauser'
Oct 11 21:01:50 victor-portatil useradd[31798]: new group: name=pruebauser, GID=1001
Oct 11 21:01:57 victor-portatil passwd[31807]: pam_unix(passwd:chauthtok): password changed for pruebauser
Oct 11 21:02:09 victor-portatil passwd[31807]: pam_unix(passwd:chauthtok): password changed for pruebauser
Oct 11 21:02:09 victor-portatil passwd[31807]: gkr-pam: couldn't update the login keyring password: no old password was entered
Oct 11 21:02:09 victor-portatil passwd[31807]: pam_encryptfs: Passphrase file wrapped
Oct 11 21:02:09 victor-portatil passwd[31807]: pam_encryptfs: PAM passphrase change module retrieved at least one NULL passphrase; nothing to do
Oct 11 21:02:17 victor-portatil login[31810]: pam_unix(login:session): session opened for user pruebauser by pruebauser(uid=0)
Oct 11 21:02:17 victor-portatil login[31810]: pam_systemd(login:session): Cannot create session: Already running in a session
Oct 11 21:02:50 victor-portatil passwd[31848]: pam_unix(passwd:chauthtok): password changed for pruebauser
Oct 11 21:02:50 victor-portatil gnome-keyring-daemon[31865]: couldn't create socket directory: /home/pruebauser/.cache/keyring-I6LMQZ: No such file or directory
Oct 11 21:02:50 victor-portatil gnome-keyring-daemon[31865]: couldn't bind to control socket: /home/pruebauser/.cache/keyring-I6LMQZ/control: No such file or directory
Oct 11 21:02:50 victor-portatil passwd[31848]: pam_encryptfs: Passphrase file wrapped
Oct 11 21:02:50 victor-portatil passwd[31866]: Failed to detect wrapped passphrase version: No such file or directory
Oct 11 21:02:50 victor-portatil passwd[31866]: pam_encryptfs: Error attempting to unwrap passphrase; rc = [-2]
Oct 11 21:02:54 victor-portatil login[31810]: pam_unix(login:session): session closed for user pruebauser

```

Ejercicio 7.

Aprovechando el usuario *pruebauser*, primero logeamos y comprobamos mediante la instrucción *sudo -i* si es posible tener acceso a las ordenes de root, y vemos que por el momento no es posible.

```
File Edit View Search Terminal Help
root@victor-portatil ~
victor-portatil ~ # login pruebauer
Password:
Last login: Thu Oct 11 21:34:42 CEST 2018 on pts/1
Welcome to Linux Mint 18.1 Serena (GNU/Linux 4.4.0-53-generic x86_64)

* Documentation: https://www.linuxmint.com command as root
No directory, logging in with HOME=/
$ sudo -i
[sudo] password for pruebauer:
Sorry, user pruebauer is not allowed to execute '/bin/bash' as root on victor-portatil.
$ 
```

Para cambiar esto, accedemos como root al archivo `/etc/sudoers` donde, a través del comando `visudo` (como se establece por motivos de seguridad e integridad del sistema, no a través de cualquier otro editor), modificamos este archivo para añadir a `pruebauser` como un usuario con todos los privilegios de root. La entrada añadida es la siguiente: `pruebauser ALL=(ALL:ALL) ALL`

File Edit View Search Terminal Help

GNU nano 2.5.3 File: /etc/sudoers.tmp Modified

```
# 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.
# env_reset Esta directiva AAA se utiliza como comodín para cualquier campo del archivo sudoers.
Defaults Defaults mail_badpass
Defaults secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/bin:/snap/bin"
# Host alias specification
# User alias specification
# Cmnd alias specification
# User privilege specification
root    ALL=(ALL:ALL) ALL
# Members of the admin group may gain root privileges
%admin  ALL=(ALL:ALL) ALL
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
pruebaser ALL=(ALL:ALL) ALL
# See sudoers(5) for more information on "#include" directives:
#includeadir /etc/sudoers.d
```

IMPORTANTE: Si utilizamos sudo para ceder acceso de root a un usuario para ejecutar ciertas órdenes, debemos asegurarnos de que estas órdenes no permitan "escapar" a un shell. Si eso ocurriese, el usuario en cuestión tendría acceso limitado como root a cualquier orden a través de ese shell. Por ejemplo, el editor vi permite ejecutar este shell a través de su función de escape.

En principio y como medida de seguridad, solo se debe poder acceder a la cuenta root desde la consola. Como ya se ha comentado, si se necesita hacer un acceso remoto a la cuenta root, entrar quedan registrados en el archivo de logs /var/log/messages. De esta forma un posible atacante tendría que conocer el nombre de un usuario del sistema, conocer su clave y también conocer la clave del root, y añadiría dificultades para obtener privilegios remotos en el sistema.

No utilizar las ordenes xlogin/rsh/rcp como root. Pueden ser objeto de diversos tipos de ataques y es peligroso ejecutarlas como root. No crear nunca un archivo .hosts para root.

En el archivo /etc/security se especifican aquellas terminales (ttyn | vcn) desde las que se puede conectar el root como tal. Se puede limitar la conexión de root, como tal, desde las

Para finalizar, volvemos a logear con *pruebauser* y probamos de nuevo el comando *sudo -i*, que ahora funciona correctamente y nos permite ejecutar las ordenes reservadas al root.

```
root@victor-portatil ~
File Edit View Search Terminal Help
victor-portatil ~ # login pruebauer
Password:
Last login: Thu Oct 11 21:34:42 CEST 2018 on pts/1
Welcome to Linux Mint 18.1 Serena (GNU/Linux 4.4.0-53-generic x86_64)

 * Documentation: https://www.linuxmint.com
No directory, logging in with HOME=/
$ sudo -i
[sudo] password for pruebauer: 
Sorry, user pruebauer is not allowed to execute '/bin/bash' as root on victor-portatil.
$ exit
/etc/sudoers.d/01_unchanged
logout
victor-portatil ~ # login pruebauer
Password:
Last login: Thu Oct 11 21:35:25 CEST 2018 on pts/1 id as root
Welcome to Linux Mint 18.1 Serena (GNU/Linux 4.4.0-53-generic x86_64)

 * Documentation: https://www.linuxmint.com
No directory, logging in with HOME=/
$ sudo -i
in page for details on how to write a sudoers file.
[sudo] password for pruebauer:
victor-portatil ~ # 
```

Ejercicio 8.

En este ejercicio trabajamos con los logs del sistema. Podemos encontrarlos en la ruta `/var/log` y a continuación se muestra aquellos presentes en mi sistema:

```
victor@victor-portatil ~
victor@victor-portatil ~ % cd var/log
victor@victor-portatil /var/log $ ls
alternatives.log          auth.log.4.gz      dmesg        dpkg.log.6.gz      kern.log       mysql        syslog.5.gz      Xorg.20.log.old
alternatives.log.1         apt.log          dpdk.log     dpkg.log.7.gz      kern.log.1     ntpstats     syslog.6.gz      Xorg.20.log.old
alternatives.log.2         aptitude        bootstrap.log dpkg.log.1     kern.log.2.gz    samba        syslog.7.gz
alternatives.log.3         aptitude.1.gz   btmp        dpkg.log.10.gz    kern.log.3.gz   speech-dispatcher upstart
alternatives.log.4         aptitude.4.gz   btmp        dpkg.log.11.gz    kern.log.4.gz   syslog       wtmp
alternatives.log.5         auth.log        chrootkit   dpkg.log.2.gz    faillog      lastlog     syslog.1        wtmp.1
alternatives.log.6         auth.log.1      Consolekit  dpkg.log.3.gz    fskck       mdm        syslog.2.gz      Xorg.0.log
alternatives.log.7         auth.log.2      cups        dpkg.log.4.gz    hp          mintsystem.log  syslog.3.gz      Xorg.0.log.old
alternatives.log.8         auth.log.3      dbusconfig-common dpkg.log.5.gz    installer   mintsystem.timestamps  syslog.4.gz      Xorg.20.log
victor@victor-portatil /var/log $ []
```

De los logs mencionados en la práctica, los que están presentes en mi sistema (con software Linux Mint) son los de *lastlog*, *wtmp*, *utmp*, *btmp* y *syslog*. No están el de *sudo* ni el de *messages*, aunque por ejemplo existe *auth.log* que mantiene un registro de diversas actividades y comandos ejecutados por los usuarios. A continuación se muestran los contenidos de estos logs del sistema (en el mismo orden que antes), corroborando que los eventos que registran son los descritos en el guión de la práctica:

```
victor@victor-portatil ~ $ lastlog
Username      Port   From
victor          19
daemon
bin
sys
sync
games
man
lp
mail
news
ucp
proxy
www-data
backup
list
irc
gnats
nobody
systemd-timesync
systemd-network
systemd-resolve
systemd-bus-proxy
syslog
apt
messagebus
uuid
ntp
avahi-autoipd
avahi
dnsmasq
colord
speech-dispatcher
hplico
kernoops
pulse
mdm
nscd
openvpn
atkis
saned
usbmix
victor
mysql
sshd
pruebauer      pts/0
victor@victor-portatil ~ $ 
victor@victor-portatil ~ $ lastlog
Latest
***Never logged in**
Thu Oct 11 22:09:34 +0200 2018
***Never logged in**
***Never logged in**
Thu Oct 11 21:37:40 +0200 2018

victor@victor-portatil ~ $ 

Ivo domine las órdenes «logging» con la orden root. Pueden ser objetos de diversos tipos un ataques y es peligroso ejecutarlas como root. No crear nunca un archivo .rhosts para root.

En el archivo /etc/security se especifican aquellas terminales (ttyn | ve/n) desde las que se puede conectar el root como tal. Se puede limitar la conexión de root, como tal, desde las terminales que se deseen. Si el root debe conectarse desde un lugar diferente de la consola y esta limitado desde /etc/security, deberá conectarse como usuario y luego ejecutar la orden su.

También, deberemos limitar el acceso al root a través de montajes NFS (Network File System). En este caso debemos prestar especial atención al archivo /etc/export donde se declaran los sistemas de archivos locales que se exportan vía NFS. Por defecto, el servidor NFS mapea el ID 0 (root) sobre un usuario no privilegiado, como nobody. Este comportamiento puede corregirse evitando a toda costa el uso de la opción no_root_squash del servidor NFS en el archivo /etc/export.

5. Log del sistema.

Un registro (logging) es cualquier procedimiento por el que un sistema operativo o aplicación graba eventos mientras ocurren y los guarda para su estudio posterior. Los archivos de log de un servidor deben ser propiedad del usuario y grupo root y no tener ningún permiso para otros. Además, por seguridad, se les debería poner el flag de solo añadir:
```

wtmp, utmp y btmp

```
root@victor-portatil ~
File Edit View Search Terminal Help
victor-portatil ~ # last
victor pts/0      :0          Thu Oct 11 22:09  still logged in com Selection ~
pruebaus pts/1    :0          Thu Oct 11 21:37 - 22:04 (00:27)
pruebaus pts/1    :0          Thu Oct 11 21:35 - 21:35 (00:00)
pruebaus pts/1    :0          Thu Oct 11 21:34 - 21:35 (00:00)
pruebaus pts/0    :0          Thu Oct 11 21:02 - 21:02 (00:00)
pruebaus pts/0    :0          Thu Oct 11 20:25 - 20:26 (00:01)
pruebaus pts/0    :0          Thu Oct 11 20:12 - 20:14 (00:02)
pruebaus pts/0    :0          Thu Oct 11 20:06 - 20:06 (00:00)
victor  tty8      :0          Thu Oct 11 12:37 gone - no logout
reboot system boot 4.4.0-53-generic Thu Oct 11 12:36 still running
reboot system boot 4.4.0-53-generic Wed Oct 10 22:21 - 22:23 (00:01)
victor  tty8      :0          Wed Oct 10 12:40 - 22:21 (09:40)
reboot system boot 4.4.0-53-generic Wed Oct 10 12:39 - 22:21 (09:42) creó el archivo. El comando last vuclla esta información. A last se le puede
victor  tty8      :0          Tue Oct  9 17:47 - 03:45 (09:57) la cuenta de usuario que se quiere controlar o la terminal tty.
wtmp begins Tue Oct  9 17:47:41 2018
victor-portatil ~ # who
victor  tty8      2018-10-11 12:37 (:0)
victor  pts/0      2018-10-11 22:09
victor-portatil ~ # lastb
pruebaus pts/1    :0          Thu Oct 11 21:34 - 21:34 (00:00)
pruebaus pts/1    :0          Thu Oct 11 21:33 - 21:33 (00:00) intento se visualiza con la orden lastb.
UNKNOWN pts/1     20
pruebaus pts/1    :0          Thu Oct 11 21:33 - 21:33 (00:00) /var/run/utmp: registra las entradas de los usuarios que todavía están conectados al sistema.
pruebaus pts/0    :0          Thu Oct 11 21:33 - 21:33 (00:00) Cada vez que un usuario se desconecta se borra la entrada correspondiente en utmp. El
pruebaus pts/0    :0          Thu Oct 11 21:01 - 21:01 (00:00) contenido de este archivo es utilizado por la orden who.
UNKNOWN pts/0     20
pruebaus pts/0    :0          Thu Oct 11 20:55 - 20:55 (00:00) /var/log/btmp: contiene todos los intentos fallidos de conexión de los usuarios del sistema.
UNKNOWN pts/0     20
pruebaus pts/0    :0          Thu Oct 11 20:55 - 20:55 (00:00) /var/log/utmp: registra toda la actividad de la orden sudo. El formato de sus entradas es
pruebaus pts/0    :0          Thu Oct 11 20:24 - 20:24 (00:00) user:HOSTNAME:TTY:terminal:PID:dir:USER:COMMAND:cmd
UNKNOWN pts/0     20
pruebaus pts/0    :0          Thu Oct 11 20:24 - 20:24 (00:00) /var/log/messages: almacena (en el orden en que se presentan) los mensajes del kernel y del
pruebaus pts/0    :0          Thu Oct 11 20:23 - 20:23 (00:00) sistema. Estos son manipulados por los demonios syslogd y klogd.
Thu Oct 11 20:23 - 20:23 (00:00) es el servicio de login para programas y aplicaciones (no para conexiones y
desconexiones de usuarios). Guarda el nombre del programa, el tipo de servicio, prioridad, etc. Su
archivo de configuración es /etc/syslog.conf. En él se establece qué eventos se van a registrar y en
victor-portatil ~ #
```

syslog

```
victor@victor-portatil ~
File Edit View Search Terminal Help
victor@victor-portatil ~ # cat syslog
Oct 11 20:01:27 victor-portatil anacron[25550]: Job `cron.daily' terminated
Oct 11 20:01:27 victor-portatil anacron[25550]: Normal exit (1 job run)
Oct 11 20:04:45 victor-portatil systemd[1]: Starting Daily apt download activities...
Oct 11 20:04:46 victor-portatil systemd[1]: Started Daily apt download activities.
Oct 11 20:06:06 victor-portatil console-kit-daemon[1829]: Glib-CRITICAL: Source ID 96 was not found when attempting to remove it
Oct 11 20:06:06 victor-portatil console-kit-daemon[1829]: Glib-CRITICAL: Source ID 96 was not found when attempting to remove it
Oct 11 20:09:01 victor-portatil CRON[27282]: (root) CMD ( [ -x /usr/lib/php/sessionclean ] && /usr/lib/php/sessionclean)
Oct 11 20:14:45 victor-portatil console-kit-daemon[1829]: Glib-CRITICAL: Source ID 112 was not found when attempting to remove it
Oct 11 20:14:45 victor-portatil dbus[966]: [system] Activating via systemd: service name='org.freedesktop.hostname1' unit='dbus-org.freedesktop.hostname1.service'
Oct 11 20:14:49 victor-portatil systemd[1]: Starting Hostname Service...
Oct 11 20:14:49 victor-portatil dbus[966]: [system] Successfully activated service 'org.freedesktop.hostname1'
Oct 11 20:14:49 victor-portatil systemd[1]: Started Hostname Service.
Oct 11 20:14:49 victor-portatil org.gtk.vfs.Daemon[1979]: ** (process:2230): WARNING **: send_infos_cb: No such interface 'org.gtk.vfs.Enumerator' on object at path /org/gtk/vfs/client/enumerator/2 (g-dbus-error-quark, 19)
Oct 11 20:14:49 victor-portatil org.gtk.vfs.Daemon[1979]: message repeated 15 times: [ ** (process:2230): WARNING **: send_infos_cb: No such interface 'org.gtk.vfs.Enumerator' on object at path /org/gtk/vfs/client/enumerator/2 (g-dbus-error-quark, 19)]
Oct 11 20:14:49 victor-portatil org.gtk.vfs.Daemon[1979]: ** (process:2230): WARNING **: send_done_cb: No such interface 'org.gtk.vfs.Enumerator' on object at path /org/gtk/vfs/client/enumerator/2 (g-dbus-error-quark, 19)
Oct 11 20:17:01 victor-portatil CRON[28079]: (root) CMD ( cd / & run-parts --report /etc/cron.hourly)
Oct 11 20:23:02 victor-portatil dbus[966]: [system] Activating via systemd: service name='org.freedesktop.hostname1' unit='dbus-org.freedesktop.hostname1.service'
Oct 11 20:23:02 victor-portatil systemd[1]: Starting Hostname Service...
Oct 11 20:23:02 victor-portatil org.gtk.vfs.Daemon[1979]: ** (process:2230): WARNING **: send_infos_cb: No such interface 'org.gtk.vfs.Enumerator' on object at path /org/gtk/vfs/client/enumerator/2 (g-dbus-error-quark, 19)
Oct 11 20:23:02 victor-portatil org.gtk.vfs.Daemon[1979]: message repeated 16 times: [ ** (process:2230): WARNING **: send_infos_cb: No such interface 'org.gtk.vfs.Enumerator' on object at path /org/gtk/vfs/client/enumerator/2 (g-dbus-error-quark, 19)]
Oct 11 20:23:02 victor-portatil org.gtk.vfs.Daemon[1979]: ** (process:2230): WARNING **: send_done_cb: No such interface 'org.gtk.vfs.Enumerator' on object at path /org/gtk/vfs/client/enumerator/2 (g-dbus-error-quark, 19)
Oct 11 20:23:02 victor-portatil dbus[966]: [system] Successfully activated service 'org.freedesktop.hostname1'
Oct 11 20:23:02 victor-portatil systemd[1]: Started Hostname Service.
Oct 11 20:26:52 victor-portatil console-kit-daemon[1829]: Glib-CRITICAL: Source ID 125 was not found when attempting to remove it
Oct 11 20:26:52 victor-portatil console-kit-daemon[1829]: Glib-CRITICAL: Source ID 125 was not found when attempting to remove it
Oct 11 20:30:07 victor-portatil dbus[966]: [system] Activating via systemd: service name='org.freedesktop.hostname1' unit='dbus-org.freedesktop.hostname1.service'
Oct 11 20:30:07 victor-portatil systemd[1]: Starting Hostname Service...
Oct 11 20:30:07 victor-portatil dbus[966]: [system] Successfully activated service 'org.freedesktop.hostname1'
Oct 11 20:30:07 victor-portatil systemd[1]: Started Hostname Service.
Oct 11 20:30:07 victor-portatil org.gtk.vfs.Daemon[1979]: ** (process:2230): WARNING **: send_infos_cb: No such interface 'org.gtk.vfs.Enumerator' on object at path /org/gtk/vfs/client/enumerator/2 (g-dbus-error-quark, 19)
Oct 11 20:30:07 victor-portatil org.gtk.vfs.Daemon[1979]: message repeated 14 times: [ ** (process:2230): WARNING **: send_infos_cb: No such interface 'org.gtk.vfs.Enumerator' on object at path /org/gtk/vfs/client/enumerator/2 (g-dbus-error-quark, 19)]
Oct 11 20:30:07 victor-portatil org.gtk.vfs.Daemon[1979]: ** (process:2230): WARNING **: send_done_cb: No such interface 'org.gtk.vfs.Enumerator' on object at path /org/gtk/vfs/client/enumerator/2 (g-dbus-error-quark, 19)
Oct 11 20:39:01 victor-portatil CRON[29941]: (root) CMD ( [ -x /usr/lib/php/sessionclean ] && /usr/lib/php/sessionclean)
victor@victor-portatil ~ #
```

auth.log

```
root@victor-portatil:~# tail -f /var/log/auth.log
Oct 11 21:33:49 victor-portatil login[2223]: pam_unix(login:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/pts/1 ruser= rhost=
Oct 11 21:33:52 victor-portatil login[2223]: FAILED LOGIN (2) on '/dev/pts/1' FOR 'UNKNOWN', User not known to the underlying authentication module
Oct 11 21:33:59 victor-portatil login[2223]: FAILED LOGIN (3) on '/dev/pts/1' FOR 'pruebauer', Authentication failure
Oct 11 21:34:05 victor-portatil userdel[2268]: delete user 'pruebauer'
Oct 11 21:34:05 victor-portatil userdel[2268]: removed group 'pruebauer' owned by 'pruebauer'
Oct 11 21:34:05 victor-portatil userdel[2268]: removed shadow group 'pruebauer' owned by 'pruebauer'
Oct 11 21:34:10 victor-portatil useradd[2292]: new group: name=pruebauer, GID=1001
Oct 11 21:34:16 victor-portatil login[2307]: pam_unix(login:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/pts/1 ruser= rhost= user=pruebauer
Oct 11 21:34:20 victor-portatil login[2307]: FAILED LOGIN (1) on '/dev/pts/1' FOR 'pruebauer', Authentication failure
Oct 11 21:34:28 victor-portatil passwd[2300]: pam cryptpfs: PAM passphrase change module retrieved a NULL passphrase; nothing to do
Oct 11 21:34:33 victor-portatil passwd[2300]: pam_unix(passwd:chauthtok): password changed for pruebauer
Oct 11 21:34:33 victor-portatil passwd[2300]: gkr-pam: couldn't update the login keyring password: no old password was entered
Oct 11 21:34:33 victor-portatil passwd[2300]: pam cryptpfs: Passphrase file wrapped
Oct 11 21:34:33 victor-portatil passwd[2300]: pam cryptpfs: PAM passphrase change module retrieved at least one NULL passphrase; nothing to do
Oct 11 21:34:42 victor-portatil login[2345]: pam_unix(login:session): session opened for user pruebauer by (uid=0)
Oct 11 21:34:42 victor-portatil login[2345]: pam_systemd(login:session): Cannot create session: Already running in a session
Oct 11 21:34:55 victor-portatil sudo: pruebauer : command not allowed ; TTY=pts/1 ; PWD=/ ; USER=root ; COMMAND=/bin/bash
Oct 11 21:35:16 victor-portatil login[2435]: pam_unix(login:session): session closed for user pruebauer
Oct 11 21:35:25 victor-portatil login[2435]: pam_unix(login:session): session opened for user pruebauer by pruebauer(uid=0)
Oct 11 21:35:25 victor-portatil login[2435]: pam_systemd(login:session): Cannot create session: Already running in a session
Oct 11 21:35:30 victor-portatil sudo: pruebauer : command not allowed ; TTY=pts/1 ; PWD=/ ; USER=root ; COMMAND=/bin/bash
Oct 11 21:35:44 victor-portatil login[2435]: pam_unix(login:session): session closed for user pruebauer
Oct 11 21:37:40 victor-portatil login[2665]: pam_unix(login:session): session opened for user pruebauer by pruebauer(uid=0)
Oct 11 21:37:40 victor-portatil login[2665]: pam_systemd(login:session): Cannot create session: Already running in a session
Oct 11 21:37:45 victor-portatil sudo: pruebauer : TTY=pts/1 ; PWD=/ ; USER=root ; COMMAND=/bin/bash
Oct 11 21:37:45 victor-portatil sudo: pam_unix(sudo:session): session opened for user root by pruebauer(uid=0)
Oct 11 21:39:01 victor-portatil CRON[2824]: pam_unix(cron:session): session opened for user root by (uid=0)
Oct 11 21:39:01 victor-portatil CRON[2824]: pam_unix(cron:session): session closed for user root
Oct 11 22:04:21 victor-portatil sudo: pam_unix(sudo:session): session closed for user root
Oct 11 22:04:44 victor-portatil sudo: pruebauer : command not allowed ; TTY=pts/1 ; PWD=/ ; USER=root ; COMMAND=/bin/bash
Oct 11 22:04:48 victor-portatil login[2665]: pam_unix(login:session): session closed for user pruebauer
Oct 11 22:04:48 victor-portatil sudo: pam_unix(sudo:session): session closed for user root
Oct 11 22:04:52 victor-portatil sudo: pam_unix(sudo:session): session closed for user root
Oct 11 22:09:01 victor-portatil CRON[4960]: pam_unix(cron:session): session opened for user root by (uid=0)
Oct 11 22:09:01 victor-portatil CRON[4960]: pam_unix(cron:session): session closed for user root
Oct 11 22:09:28 victor-portatil sudo: victor : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/bin/bash
Oct 11 22:09:28 victor-portatil sudo: pam_unix(sudo:session): session opened for user root by pruebauer(uid=0)
Oct 11 22:09:34 victor-portatil login[5057]: pam_unix(login:session): session opened for user victor by pruebauer(uid=0)
Oct 11 22:09:34 victor-portatil login[5057]: pam_systemd(login:session): Cannot create session: Already running in a session
Oct 11 22:13:24 victor-portatil sudo: victor : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/bin/bash
Oct 11 22:13:24 victor-portatil sudo: pam_unix(sudo:session): session opened for user root by victor(uid=0)
Oct 11 22:17:01 victor-portatil CRON[5549]: pam_unix(cron:session): session opened for user root by (uid=0)
Oct 11 22:17:01 victor-portatil CRON[5549]: pam_unix(cron:session): session closed for user root
victor-portatil log #
```

Ejercicio 9.

Finalmente, con la ayuda de los comandos *last*, *lastb* y especialmente *lastlog* comprobamos quienes han logeado en el sistema, qué intentos de login ha habido y si se ha dado algún intento de conexión de red. La salida es la siguiente, adelantando que en principio parece que no ha habido ninguna conexión ajena al equipo:

```
root@victor-portatil:~# lastlog
victor-portatil log # lastlog
File Edit View Search Terminal Help
Username      Port   From   Latest
root          pts/0   -      **Never logged in**
daemon        pts/0   -      **Never logged in**
bin           pts/0   -      **Never logged in**
sys           pts/0   -      **Never logged in**
sync          pts/0   -      **Never logged in**
games         pts/0   -      **Never logged in**
man           pts/0   -      **Never logged in**
lp            pts/0   -      **Never logged in**
mail          pts/0   -      **Never logged in**
news          pts/0   -      **Never logged in**
uucp          pts/0   -      **Never logged in**
proxy         pts/0   -      **Never logged in**
www-data      pts/0   -      **Never logged in**
backup        pts/0   -      **Never logged in**
list          pts/0   -      **Never logged in**
irc           pts/0   -      **Never logged in**
gnats         pts/0   -      **Never logged in**
nobody        pts/0   -      **Never logged in**
systemd-timesync pts/0   -      **Never logged in**
systemd-network  pts/0   -      **Never logged in**
systemd-resolve   pts/0   -      **Never logged in**
systemd-bus-proxy  pts/0   -      **Never logged in**
syslog         pts/0   -      **Never logged in**
apt           pts/0   -      **Never logged in**
messagebus     pts/0   -      **Never logged in**
uuid          pts/0   -      **Never logged in**
ntp            pts/0   -      **Never logged in**
avahi-autoipd   pts/0   -      **Never logged in**
avahi          pts/0   -      **Never logged in**
dnsmasq        pts/0   -      **Never logged in**
colord         pts/0   -      **Never logged in**
speech-dispatcher pts/0   -      **Never logged in**
hplip          pts/0   -      **Never logged in**
kernoops       pts/0   -      **Never logged in**
pulse          pts/0   -      **Never logged in**
mdm           pts/0   -      **Never logged in**
nm-openvpn     pts/0   -      **Never logged in**
rtkit          pts/0   -      **Never logged in**
saned          pts/0   -      **Never logged in**
usbmux         pts/0   -      **Never logged in**
victor         pts/0   Thu Oct 11 22:09:34 +0200 2018
mysql          pts/0   **Never logged in**
sshd          pts/0   **Never logged in**
```