Seguridad Limits Conf

17/10/2023

Guillermo Bellettini
Seguridad
Creado por: Nicolas Pavel Ballesteros Barrado

Contenido

Hacemos hostnamectl

```
root@ubuntu:~# hostnamectl
   Static hostname: ubuntu
         Icon name: computer-vm
           Chassis: vm
        Machine ID: e2336474fc3c4d10984fcf44ab3484f1
           Boot ID: 6734f8b789c44baeaa680c409f5facd2
    Virtualization: oracle
  Operating System: Ubuntu 18.04.6 LTS
            Kernel: Linux 4.15.0-213-generic
      Architecture: x86-64
root@ubuntu:~#
```

Nos metemos en el fichero /etc/security/limits.conf

```
 GNU nano 2.9.3                          /etc/security/limits.conf

# /etc/security/limits.conf
#
#Each line describes a limit for a user in the form:
#
#<domain>        <type>  <item>  <value>
#
#Where:
#<domain> can be:
#        - a user name
#        - a group name, with @group syntax
#        - the wildcard *, for default entry
#        - the wildcard %, can be also used with %group syntax,
#                 for maxlogin limit
#        - NOTE: group and wildcard limits are not applied to root.
#          To apply a limit to the root user, <domain> must be
#          the literal username root.
#
#<type> can have the two values:
#        - "soft" for enforcing the soft limits
#        - "hard" for enforcing hard limits
#
#<item> can be one of the following:
#        - core - limits the core file size (KB)
#        - data - max data size (KB)
                                [ 56 líneas leídas ]
^G Ver ayuda    ^O Guardar      ^W Buscar       ^K Cortar Texto ^J Justificar   ^C Posición     M-U Deshacer    M-A Marcar texto
^X Salir        ^R Leer fich.   ^\ Reemplazar   ^U Pegar txt    ^T Ortografía   ^_ Ir a línea   M-E Rehacer     M-6 Copiar txt
```

Vemos el tipo de restricción que puede ser soft o hard

```
#<type> can have the two values:
#         - "soft" for enforcing the soft limits
#         - "hard" for enforcing hard limits
#
```

Vemos la configuración de las restriciones

```
#<domain>      <type>  <item>          <value>
#

#*               soft    core            0
#root            hard    core            100000
#*               hard    rss             10000
#@student        hard    nproc           20
#@faculty        soft    nproc           20
#@faculty        hard    nproc           50
#ftp             hard    nproc           0
#ftp             -       chroot          /ftp
#@student        -       maxlogins       4

# End of file
```

Añadimos los grupos y el usuario usuario en el fichero de las restricciones, en esta lista vemos grupos, usuarios y vemos el * que significa todos los usuario y grupos

```
#<domain>      <type>  <item>          <value>
#

#*               soft    core            0
#root            hard    core            100000
#*               hard    rss             10000
#@student        hard    nproc           20
#@faculty        soft    nproc           20
#@faculty        hard    nproc           50
#ftp             hard    nproc           0
#ftp             -       chroot          /ftp
#@student        -       maxlogins       4
@admin          hard    maxlogins       2
usuario         hard    maxlogins       2
*               hard    maxsyslogins    2
*               hard    maxlogins       2
```

Guardamos cambios y salimos

Comando W

Vemos la cantidad de usuarios

```
root@ubuntu:~# w
 18:37:37 up 30 min,  1 user,  load average: 0,00, 0,00, 0,00
USUARIO  TTY      DE               LOGIN@   IDLE   JCPU   PCPU WHAT
usuario  tty7     :0               18:07   30:33   3.65s  0.06s /usr/bin/lxsession -s Lubuntu -e LXDE
root@ubuntu:~#
```

Vemos que el usuario usuario tiene una sesion abierta

Creamos otro usuario y dejamos la sesión abierta

```
root@ubuntu:~# useradd -m -s /bin/bash admin
root@ubuntu:~# passwd admin
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
passwd: contraseña actualizada correctamente
root@ubuntu:~#
```

Le ponemos una contraseña al usuario admin

```
root@ubuntu:~# passwd admin
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
passwd: contraseña actualizada correctamente
root@ubuntu:~#
```

Nos conectamos al usuario admin

```
Contraseña:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-213-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

El mantenimiento de seguridad expandido para Infrastructure está desactivado

Se pueden aplicar 0 actualizaciones de forma inmediata.

Active ESM Infra para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»

New release '20.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

admin@ubuntu:~$
```

Hacemos otra vez el comando W

```
admin@ubuntu:~$ w
 19:02:03 up 55 min,  2 users,  load average: 0,00, 0,01, 0,00
USUARIO  TTY      DE               LOGIN@   IDLE   JCPU   PCPU WHAT
usuario  tty7     :0               18:07   54:59  11.29s  0.09s /usr/bin/lxsession -s Lubuntu -e LXDE
admin    pts/0    -                19:00    0.00s  0.10s  0.00s w
admin@ubuntu:~$
```

Vemos que tenemos dos sesiones abiertas, una el usuario y la otra admin

Vemos a que grupo pertenecen los usuarios admin y usuario

```
admin@ubuntu:~$ groups admin
admin : admin adm dialout fax cdrom floppy tape sudo audio dip video plugdev lpadmin scanner sambashare
admin@ubuntu:~$ groups usuario
usuario : usuario adm cdrom sudo dip plugdev lpadmin sambashare admin
admin@ubuntu:~$
```

Vemos que están los dos metidos en el grupo admin

Creamos otro usuario para meterlo en el grupo admin y ver si nos echa y no nos deja iniciar sesion

```
root@ubuntu:~# useradd -m -s /bin/bash AdminServer
root@ubuntu:~# passwd AdminServer
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
passwd: contraseña actualizada correctamente
root@ubuntu:~#
```

Nos deja iniciar sesión porque no esta en el grupo admin

```
usuario@ubuntu:~$ groups AdminServer
AdminServer : AdminServer adm dialout fax cdrom floppy tape sudo audio dip video plugdev lpadmin scanner sambashare
usuario@ubuntu:~$
```

Añadimos el usuario AdminServer al grupo admin

```
usuario@ubuntu:~$ sudo su
[sudo] contraseña para usuario:
root@ubuntu:/home/usuario# usermod -aG admin AdminServer
root@ubuntu:/home/usuario# groups AdminServer
AdminServer : AdminServer adm dialout fax cdrom floppy tape sudo audio dip video plugdev lpadmin scanner sambashare admin
root@ubuntu:/home/usuario#
```

Vemos que todos los usuarios están metidos en el grupo admin

```
root@ubuntu:~# groups usuario
usuario : usuario adm dialout fax cdrom floppy tape sudo audio dip video plugdev lpadmin scanner sambashare admin
root@ubuntu:~# groups admin
admin : admin adm dialout fax cdrom floppy tape sudo audio dip video plugdev lpadmin scanner sambashare
root@ubuntu:~# groups AdminServer
AdminServer : AdminServer adm dialout fax cdrom floppy tape sudo audio dip video plugdev lpadmin scanner sambashare admin
root@ubuntu:~#
```

Nos metemos en el fichero de restricciones

```
#<domain>      <type>  <item>         <value>
#

#*               soft    core            0
#root            hard    core            100000
#*               hard    rss             10000
#@student        hard    nproc           20
#@faculty        soft    nproc           20
#@faculty        hard    nproc           50
#ftp             hard    nproc           0
#ftp             -       chroot          /ftp
#@student        -       maxlogins       4
@admin          hard    maxlogins       2
usuario         hard    maxlogins       2
admin           hard    fsize           2048
*               hard    maxsyslogins    2
*               hard    maxlogins       2
```

Añadimos fsize al usuario admin, guardamos y cerramos

Nos metemos con admin

```
root@ubuntu:~# nano /etc/security/limits.conf
root@ubuntu:~# login admin
Contraseña:
```

Están los dos usuarios conectados

```
admin@ubuntu:~$ w
 19:42:26 up  1:35,  2 users,  load average: 0,70, 0,27, 0,15
USUARIO  TTY      DE               LOGIN@   IDLE   JCPU   PCPU WHAT
usuario  tty7     :0               19:35    1:35m  2.10s  0.03s /usr/bin/lxsession -s Lubuntu -e LXDE
admin    pts/0    -                19:40    2.00s  0.11s  0.00s w
admin@ubuntu:~$
```

Hacemos la prueba del fichero mas de dos megas

```
usuario@ubuntu:~/Descargas$ ls -l
total 1140
-rw-rw-r-- 1 usuario usuario   52001 oct  9  2020 169-1695145_linux.png
-rw-rw-r-- 1 usuario usuario 1112492 oct  9  2020 2886057.png
usuario@ubuntu:~/Descargas$
```

Vemos que tenemos dos fotos png

Este nos deja pasarlo porque pesa menos de dos megas

```
root@ubuntu:/home/usuario/Descargas# cp -v 2886057.png /home/admin/
'2886057.png' -> '/home/admin/2886057.png'
root@ubuntu:/home/usuario/Descargas#
```

Ahora haremos la prueba de pasar uno que sea mas grande

Pasamos el instalador de telegram al usuario admin

```
admin@ubuntu:/home/usuario/Descargas$ ls -lh
total 51M
-rw-rw-r-- 1 usuario usuario  51K oct  9  2020 169-1695145_linux.png
-rw-rw-r-- 1 usuario usuario 1,1M oct  9  2020 2886057.png
-rw-rw-r-- 1 usuario usuario  50M oct 17 19:51 tsetup.4.10.3.tar.xz
admin@ubuntu:/home/usuario/Descargas$ cp -v tsetup.4.10.3.tar.xz /home/admin
'tsetup.4.10.3.tar.xz' -> '/home/admin/tsetup.4.10.3.tar.xz'
cp: no se puede crear el fichero regular '/home/admin/tsetup.4.10.3.tar.xz': Permiso denegado
admin@ubuntu:/home/usuario/Descargas$
```

Y nos dice que no lo podemos copiar al usuario admin