

Access.conf

13/02/2024

Guillermo Bellettini

Seguridad

Creado por: Nicolas Pavel Ballesteros Barrado



Contenido

Access.conf	1
Vemos la ruta donde estamos.....	3
Editamos el fichero common-password	4
Nos movemos de carpeta.....	5
Editamos el fichero	6
Añadimos estas líneas.....	6
Intentamos entrar con usuario.....	7
Entramos con root	8
Pero si podemos entrar con usuario desde la tty3.....	9
Bloqueamos al usuario el acceso desde cualquier lugar	9
Conectarse por IP.....	11
Permitimos que solo miembros del grupo sudo puedan conectarse.....	13

Vemos la ruta donde estamos

```
root@ubuntu:~# cd /etc/pam.d/  
root@ubuntu:/etc/pam.d# pwd  
/etc/pam.d  
root@ubuntu:/etc/pam.d# |
```

Vemos los ficheros

```
root@ubuntu:/etc/pam.d# ls -l  
total 104  
-rw-r--r-- 1 root root 384 ene 25 2018 chfn  
-rw-r--r-- 1 root root 92 ene 25 2018 chpasswd  
-rw-r--r-- 1 root root 581 ene 25 2018 chsh  
-rw-r--r-- 1 root root 1208 nov 30 16:20 common-account  
-rw-r--r-- 1 root root 1249 nov 30 16:20 common-auth  
-rw-r--r-- 1 root root 1440 nov 30 16:20 common-password  
-rw-r--r-- 1 root root 1470 nov 30 16:20 common-session  
-rw-r--r-- 1 root root 1435 nov 30 16:20 common-session-noninteractive  
-rw-r--r-- 1 root root 606 nov 16 2017 cron  
-rw-r--r-- 1 root root 884 mar 22 2018 lightdm  
-rw-r--r-- 1 root root 551 mar 22 2018 lightdm-autologin  
-rw-r--r-- 1 root root 727 mar 22 2018 lightdm-greeter  
-rw-r--r-- 1 root root 4945 ene 25 2018 login  
-rw-r--r-- 1 root root 92 ene 25 2018 newusers  
-rw-r--r-- 1 root root 520 abr 4 2018 other  
-rw-r--r-- 1 root root 92 ene 25 2018 passwd  
-rw-r--r-- 1 root root 270 mar 27 2018 polkit-1  
-rw-r--r-- 1 root root 168 feb 26 2018 ppp  
-rw-r--r-- 1 root root 143 feb 14 2018 runuser  
-rw-r--r-- 1 root root 138 feb 14 2018 runuser-l  
-rw-r--r-- 1 root root 2133 mar 30 2022 sshd  
-rw-r--r-- 1 root root 2257 ene 25 2018 su  
-rw-r--r-- 1 root root 239 ene 18 2018 sudo  
-rw-r--r-- 1 root root 317 abr 20 2018 systemd-user  
-rw-r--r-- 1 root root 319 may 7 2014 vsftpd  
root@ubuntu:/etc/pam.d#
```

Nos fijamos en common-password

Editamos el fichero common-password

```
# 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)
# end of pam-auth-update config
account [REDACTED] requisite                                pam_acces.so
```

(**CORREGIDO EL FALLO DE PAM_ACCESS.CONF**)

Añadimos la ultima línea

Verificamos que se ha guardado

```
root@ubuntu:/etc/pam.d# cat 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:
#
# 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      [success=1 default=ignore]                pam_unix.so obscure 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;
# 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)
# end of pam-auth-update config
account       requisite                                pam_acces.so
root@ubuntu:/etc/pam.d#
```

Nos movemos de carpeta

```
root@ubuntu:/etc/pam.d# cd /etc/security/  
root@ubuntu:/etc/security# |
```

Vemos lo que hay dentro de la carpeta

```
root@ubuntu:/etc/security# ls -lh  
total 56K  
-rw-r--r-- 1 root root 4,6K abr  5 2018 access.conf  
-rw-r--r-- 1 root root 1,8K ene  6 2014 capability.conf  
-rw-r--r-- 1 root root 2,2K feb  2 2023 faillock.conf  
-rw-r--r-- 1 root root 3,6K abr  5 2018 group.conf  
-rw-r--r-- 1 root root 2,1K abr  5 2018 limits.conf  
drwxr-xr-x 2 root root 4,0K abr  5 2018 limits.d  
-rw-r--r-- 1 root root 1,5K abr  5 2018 namespace.conf  
drwxr-xr-x 2 root root 4,0K abr  5 2018 namespace.d  
-rwxr-xr-x 1 root root 1016 abr  5 2018 namespace.init  
-rw----- 1 root root  0 sep 28 2020 opasswd  
-rw-r--r-- 1 root root 3,0K abr  5 2018 pam_env.conf  
-rw-r--r-- 1 root root 2,2K dic 20 2017 pwquality.conf  
-rw-r--r-- 1 root root 419 abr  5 2018 sepermit.conf  
-rw-r--r-- 1 root root 2,2K abr  5 2018 time.conf  
root@ubuntu:/etc/security# |
```

Nos fijamos en el Access.conf

Editamos el fichero

```
GNU nano 2.9.3 access.conf

# Login access control table.
#
# Comment line must start with "#", no space at front.
# Order of lines is important.
#
# When someone logs in, the table is scanned for the first entry that
# matches the (user, host) combination, or, in case of non-networked
# logins, the first entry that matches the (user, tty) combination. The
# permissions field of that table entry determines whether the login will
# be accepted or refused.
#
# Format of the login access control table is three fields separated by a
# ":" character:
#
# [Note, if you supply a 'fieldsep=|' argument to the pam_access.so
# module, you can change the field separation character to be
# '|'. This is useful for configurations where you are trying to use
# pam_access with X applications that provide PAM_TTY values that are
# the display variable like "host:0".]
#
# permission : users : origins
#
# The first field should be a "+" (access granted) or "-" (access denied)
# character.
#
# The second field should be a list of one or more login names, group
# names, or ALL (always matches). A pattern of the form user@host is
# matched when the login name matches the "user" part, and when the
# "host" part matches the local machine name.
#
# The third field should be a list of one or more tty names (for
# non-networked logins), host names, domain names (begin with "."), host
# addresses, internet network numbers (end with "."), ALL (always
# matches), NONE (matches no tty on non-networked logins) or
# LOCAL (matches any string that does not contain a "." character).
#
# You can use @netgroupname in host or user patterns; this even works
# for @usergroup@@hostgroup patterns.
#
# The EXCEPT operator makes it possible to write very compact rules.
#
[ 122 líneas leídas ]
^G Ver ayuda  ^O Guardar   ^W Buscar    ^K Cortar Texto ^J Justificar  ^C Posición
^X Salir      ^R Leer fich. ^\ Reemplazar ^U Pegar txt    ^T Ortografía ^_ Ir a línea
```

Añadimos estas líneas

```
#
#      1. Deniega a todos la conexion en la tty1 (LOCAL)excepto a "root":
-:ALL EXCEPT root:tty1
```

Intentamos entrar con usuario

```
Ubuntu 18.04.5 LTS ubuntu tty1
ubuntu login: usuario
Password: _
```

No nos deja

```
Ubuntu 18.04.5 LTS ubuntu tty1
ubuntu login: _
```

Entramos con root

```
Ubuntu 18.04.5 LTS ubuntu tty1
ubuntu login: root
Password:
Last login: Tue Feb 13 22:08:30 CET 2024 on tty1
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-20-generic x86_64)

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

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

Pueden actualizarse 400 paquetes.
326 actualizaciones son de seguridad.

root@ubuntu:~# _
```


Pero si podemos entrar con usuario desde la tty3

```
Ubuntu 18.04.5 LTS ubuntu tty3
ubuntu login: usuario
Password:
Last login: Tue Feb 13 22:07:21 CET 2024 on tty1
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-20-generic x86_64)

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

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

Pueden actualizarse 400 paquetes.
326 actualizaciones son de seguridad.

usuario@ubuntu:~$ _
```

Bloqueamos al usuario el acceso desde cualquier lugar

```
# 2.Deniega al user "usuario" el acceso desde cualquier lugar:
-:usuario:all
#
```

Probamos desde tty1

```
Ubuntu 18.04.5 LTS ubuntu tty1
ubuntu login: ^[[A^[[B^C
Ubuntu 18.04.5 LTS ubuntu tty1
ubuntu login: usuario
Password: _
```

Sin acceso

```
Ubuntu 18.04.5 LTS ubuntu tty1
ubuntu login: _
```

Probamos desde tty2

```
Ubuntu 18.04.5 LTS ubuntu tty2
ubuntu login: usuario
Password: _
```

Sin acceso

```
Ubuntu 18.04.5 LTS ubuntu tty2
ubuntu login: _
```

Conectarse por IP

Nos conectamos por telnet, ponemos la restricción

```
#
#      3.Las sig reglas permiten al user usuario acceso desde la ip ""
+:usuario:10.68.16.62
-:usuario:10.68.16.0/22
#
```

Nos conectamos con usuario desde telnet

Miramos la ip en el powershell

```
Se ha perdido la conexión con el host.
PS C:\> ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . : madrid.fusp.ceu
    Vínculo: dirección IPv6 local. . . : fe80::3dc9:e7e1:2fa7:f32a%3
    Dirección IPv4. . . . . : 10.68.16.62
    Máscara de subred . . . . . : 255.255.252.0
    Puerta de enlace predeterminada . . . . . : 10.68.16.1
PS C:\> █
```

Tenemos la 62

Debería dejarnos entrar

```
ubuntu 18.04.5 LTS
ubuntu login: usuario
Password:
Last login: Thu Feb 15 16:06:12 CET 2024 from 10.68.16.62 on pts/1
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-20-generic x86_64)

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

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

Pueden actualizarse 400 paquetes.
326 actualizaciones son de seguridad.

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

usuario@ubuntu:~$
```

Ahora cambiamos la ip de acceso

```
# All other users should be denied to get access from all sources
- : ALL : ALL

#
# 3.Las sig reglas permiten al user usuario acceso desde
:usuario:10.68.16.60
:usuario:10.68.16.0/22
#
```

Y ahora no nos dejaría entrar

```
Ubuntu 18.04.5 LTS
ubuntu login: usuario
Password:
```

```
Permission denied
```

```
Se ha perdido la conexión con el host.
```

```
PS C:\> █
```

Permitimos que solo miembros del grupo sudo puedan conectarse

```
#
#      4.Las 2 sig reglas permiten el acceso desde la red 192.168.1.0/22 a los
#      miembros del grupo "sudo"
+:sudo:10.68.16.0/22
-:ALL:10.68.16.0/22
#
```

```
root@ubuntu:/etc/security# groups prueba
prueba : prueba
root@ubuntu:/etc/security# groups usuario
usuario : usuario adm cdrom sudo dip plugdev lpadmin sambashare
root@ubuntu:/etc/security# |
```

Creamos el usuario prueba que no esta dentro del grupo sudo

```
root@ubuntu:/etc/security# nano access.conf
root@ubuntu:/etc/security# useradd -m -s /bin/bash prueba
root@ubuntu:/etc/security# passwd prueba
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
passwd: contraseña actualizada correctamente
root@ubuntu:/etc/security#
```

```
ubuntu login: prueba
Password:

Permission denied

Se ha perdido la conexión con el host.
PS C:\> █
```

No nos deja entrar

Probamos ahora con usuario si que esta dentro del grupo sudo

```
ubuntu login: usuario
Password:
Last login: Thu Feb 15 16:18:33 CET 2024 from 10.68.16.62 on pts/1
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-20-generic x86_64)

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

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

Pueden actualizarse 400 paquetes.
326 actualizaciones son de seguridad.

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

usuario@ubuntu:~$
```

Si nos deja entrar