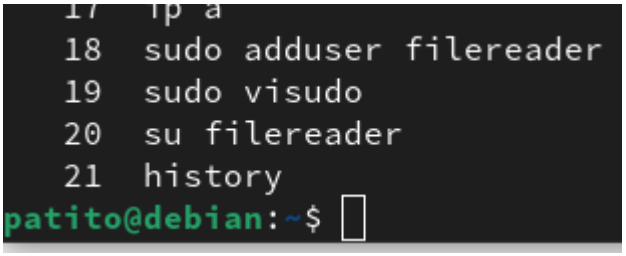
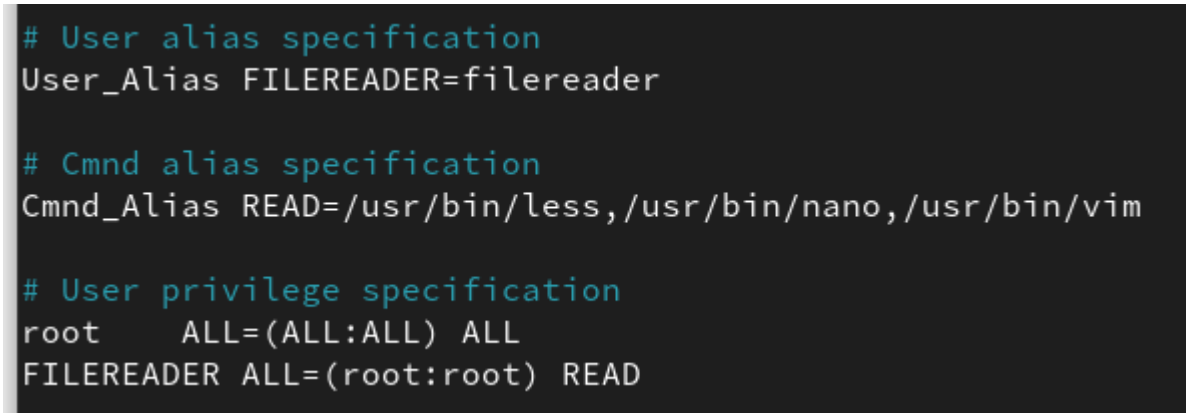
Actividad 20-03-25
José Camilo García Ponce

Primero creamos el usuario nuevo con “sudo adduser filereader”

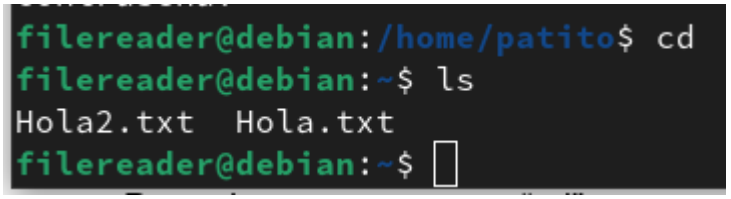


Luego modificamos /etc/sudoers usando “sudo visudo” para darle privilegios al nuevo usuario



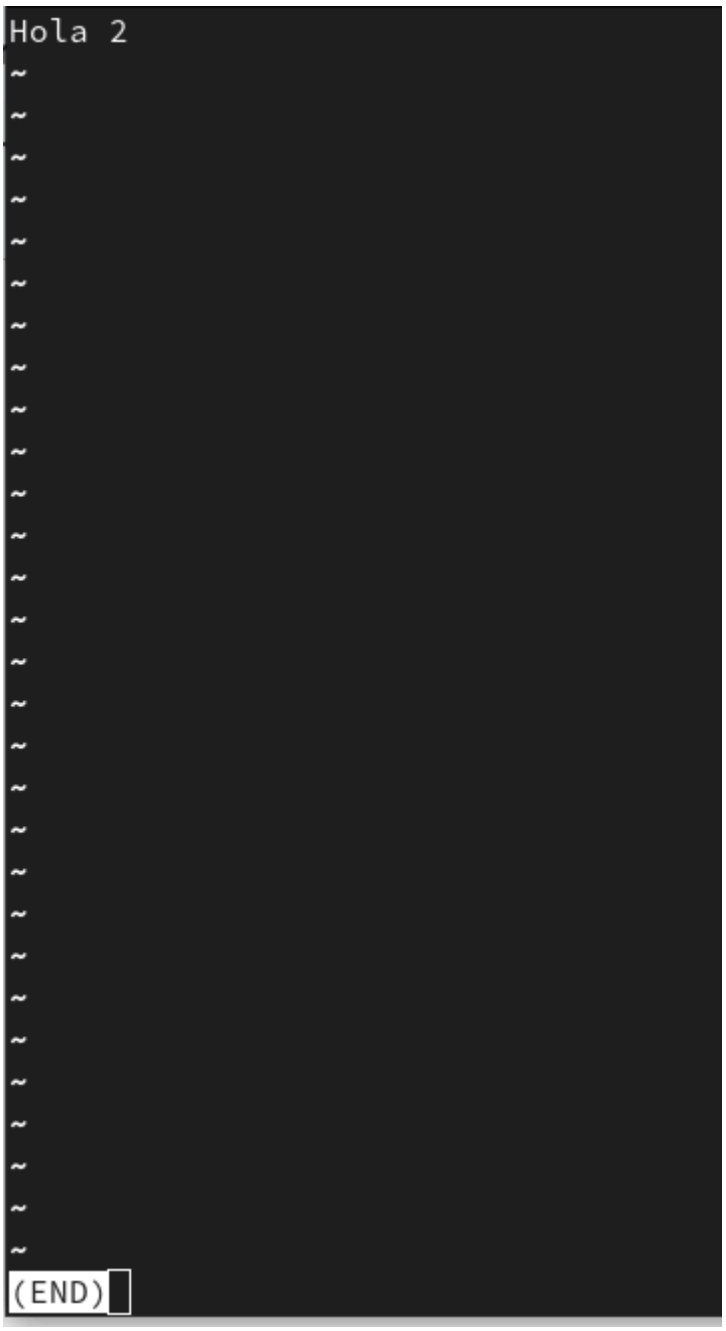
Después usamos el usuario nuevo con “su filereader”

Posteriormente usamos “cd” y creamos dos archivos

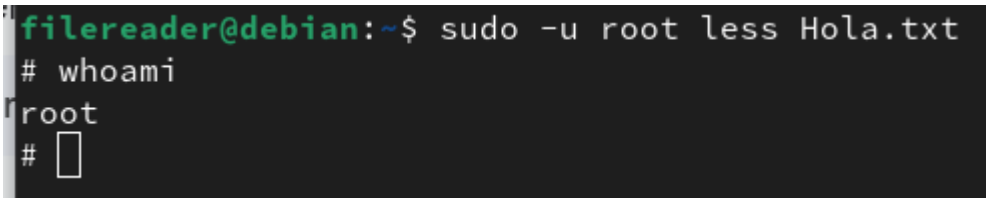


Luego usamos el comando “sudo -l”

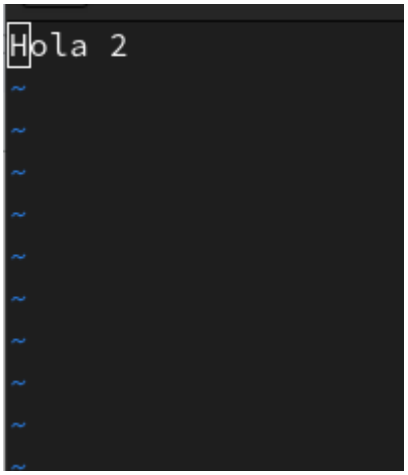
Después usamos “sudo -u root less Hola.txt”



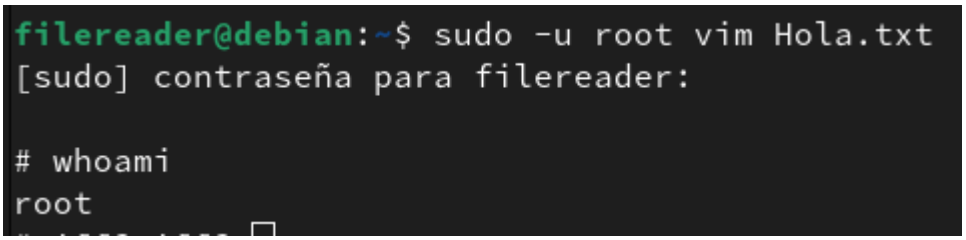
Posteriormente dentro de less escribimos “!sh”



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



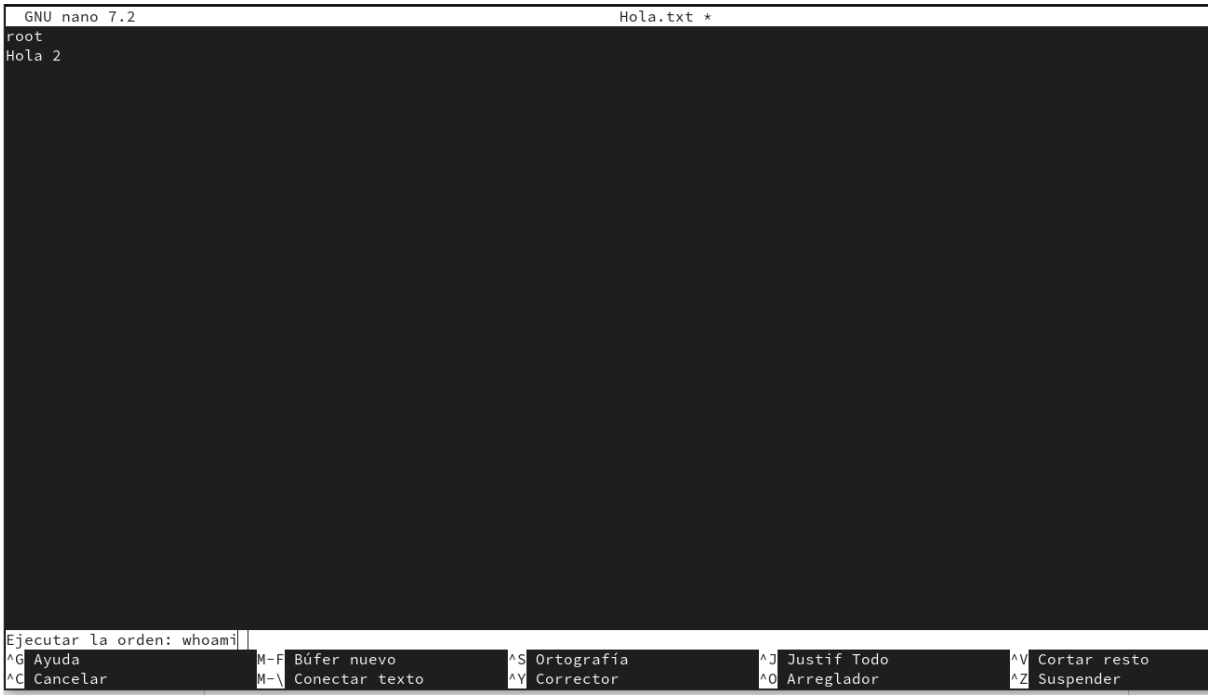
Después dentro de vim escribimos “:!sh”



Y con eso pudimos obtener una shell de root

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

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



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