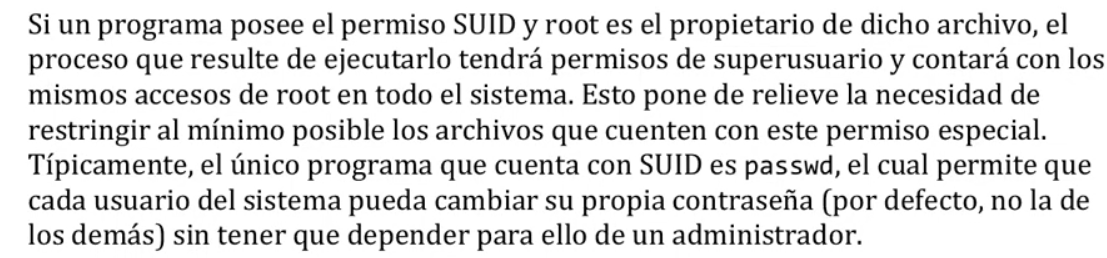
Clase 12

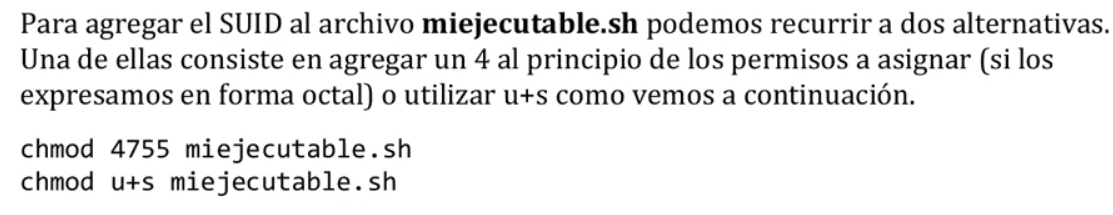
Continuamos con los permisos especiales

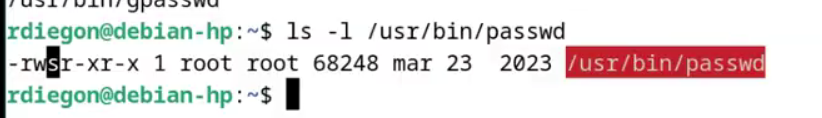
# SUID y SGID

Set User ID y Set Group ID



Si un programa tiene un permiso SUID y root es owner, el programa tiene permisos de root.

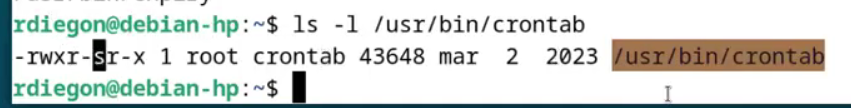




Con la S se sabe que tiene permisos de SUID

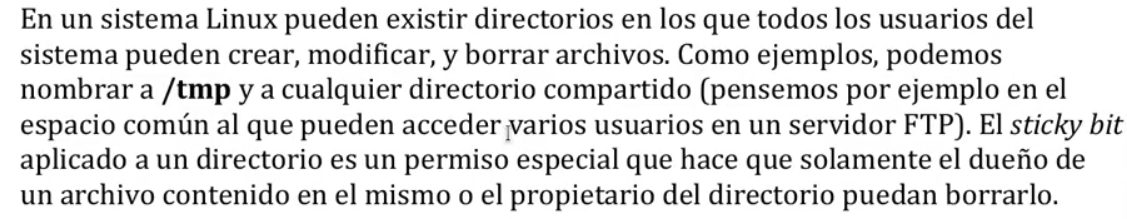
Podemos usar el permiso find <path> -type f -perm -u+s  
Y busca en el path, con el tipo file y los permisos u+s que son los permisos de SUID

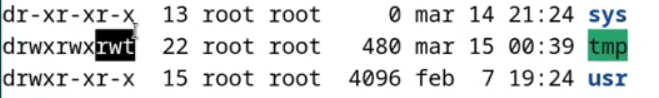
En los grupos es g+s para el GUID o en **2**755 haciendo referencia al ejemplo de usuario arriba



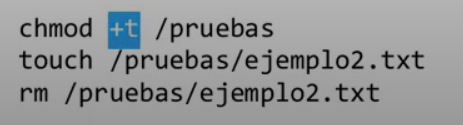
Cualquier usuario puede ejecutar crontab mientras permanezcan en el grupo crontab

# Sticky Bit



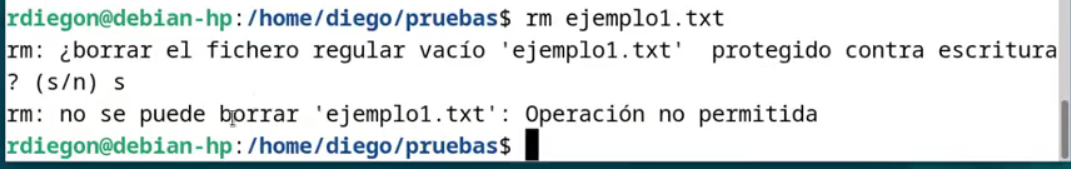


La t al final, indica que es sticky bit

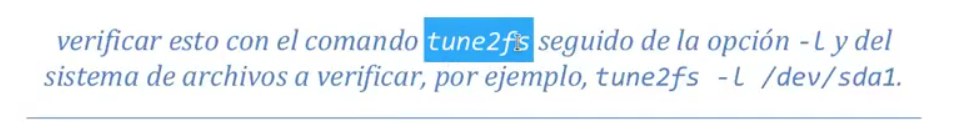
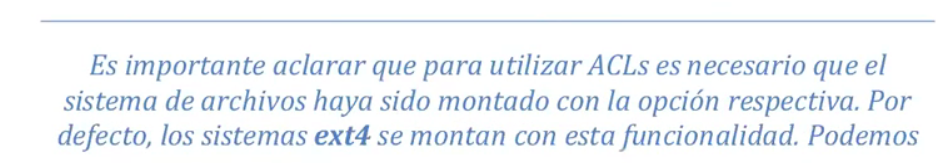


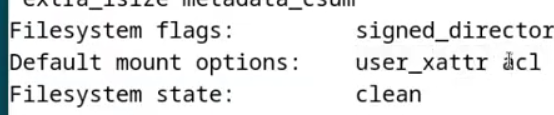
Se puede agregar con +t

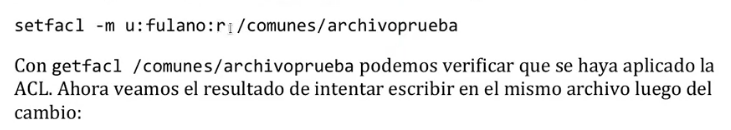
Si no soy el ownr del directorio me dice esto



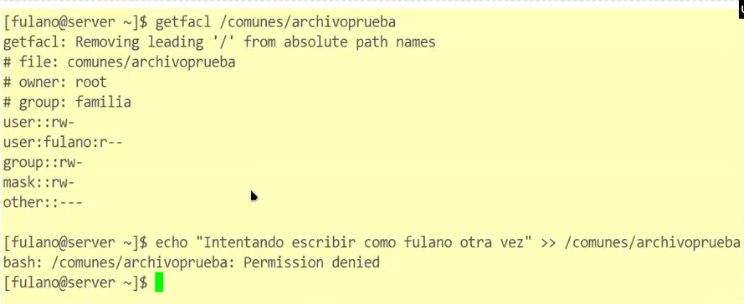
# ACL (Access Control List)

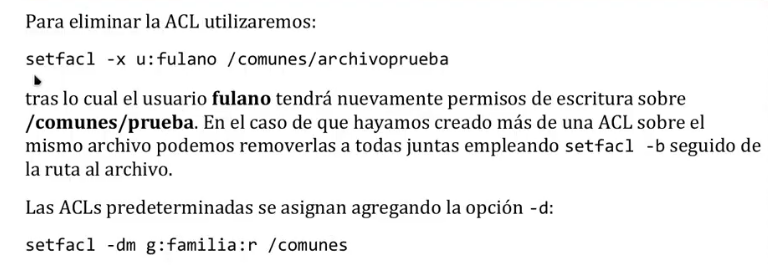


  
Si sale la línea de user\_xattr acl, es que se puede usar ACL

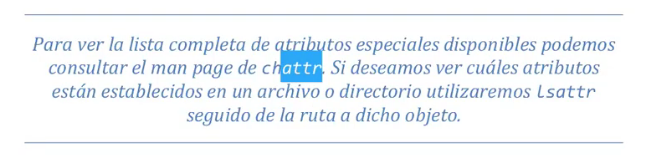


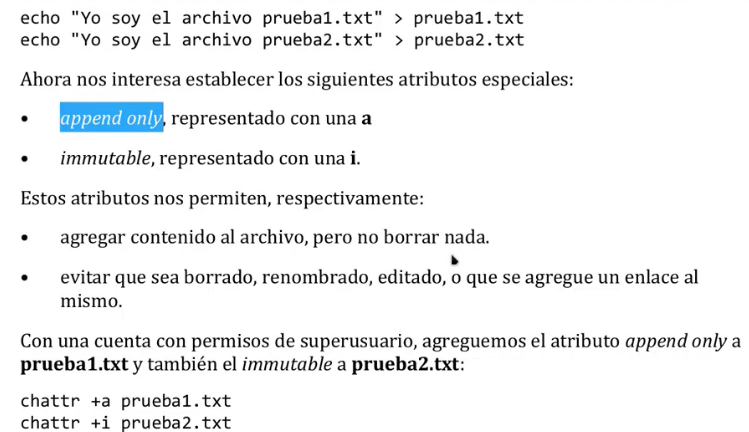
Con setfacl -m u:fulano:r /comunes/archivoprueba hace que fulano se le modifiquen los permisos, haciendo que ahora no tenga permisos de LECTURA ósea r  
setfacl -m u:<user>:<permiso> <path>

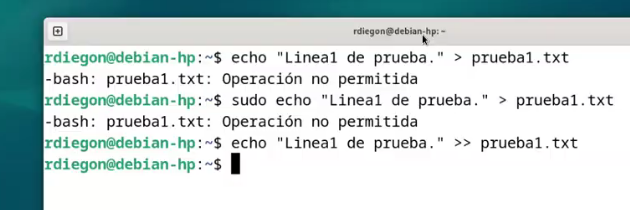




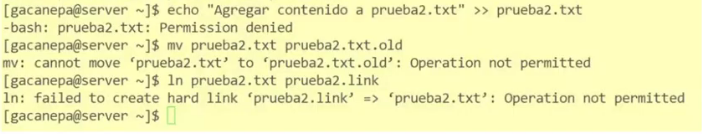
# Atributos especiales







No pudo editarlo ni con nano ni con echo, solo pudo editarlo de manera que lo AGREGO con los “>>” porque estaba con el atributo +a de APPEND ONLY



Con el inmutable, no podes hacer nada

# Administracion de Procesos

