



Curso de Especialización de Ciberseguridad en Entornos de Tecnología de la Información (CETI)



Bastionado de redes y sistemas

UD08. Configuración de dispositivos para
la instalación de sistemas informáticos.
Tarea Online.

JUAN ANTONIO GARCIA MUELAS

INDICE

	Pag
1. Descripción de la tarea	2
2. Directorios con permisos de escritura	2
3. Directorios con permisos de ejecución	2
4. Ficheros con SUID o GUID activado	3
5. Ficheros de la variable PATH	6
6. Carpetas compartidas mal configuradas	6
7. Particiones con permisos	7
8. Borrado seguro	7
9. Webgrafía	8

1.- Descripción de la tarea.

¿Qué te pedimos que hagas?

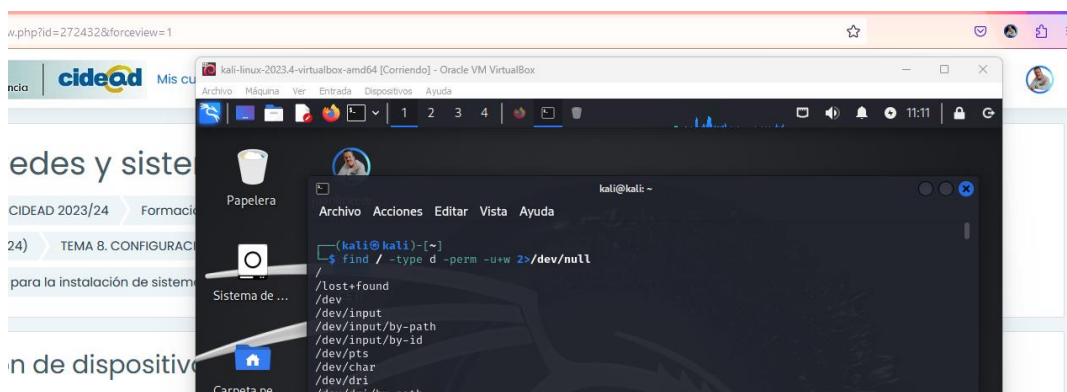
El departamento de I+D tiene unos resultados extraordinarios por los logros conseguidos en el descubrimiento de un nuevo sistema de propulsión eléctrica en los coches fabricados por la compañía. Existen intereses económicos de empresas de la competencia y actores externos por hacerse con esta información para poder aplicarla a sus modelos.

El CISO de la compañía quiere que se investigue si el sistema donde se guarda la información sensible y crítica es segura. Por lo que ha pedido que se revisen las medidas de seguridad relativas a estos sistemas. Buscando:

- ✓ Los directorios que tienen permisos de escritura.

Utilizaré **find** como comando de búsqueda. Buscamos desde el directorio raíz y filtramos por los directorios cuyos usuarios tengan permisos de escritura. Finalmente, redirigimos los errores a la papelera.

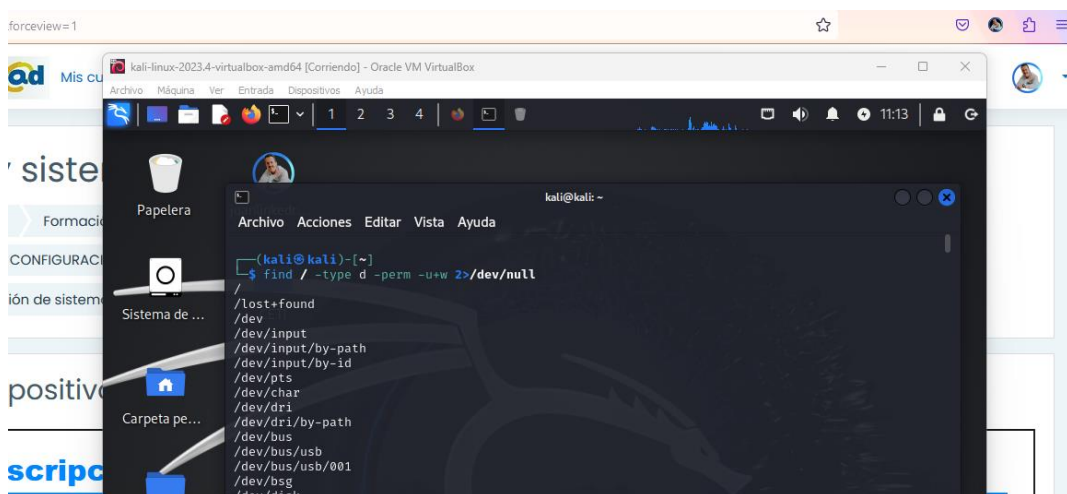
```
find / -type d -perm -u+w 2>/dev/null
```



- ✓ Los directorios que tienen permisos de ejecución.

Similar al caso anterior, pero modificando el filtro a ejecución.

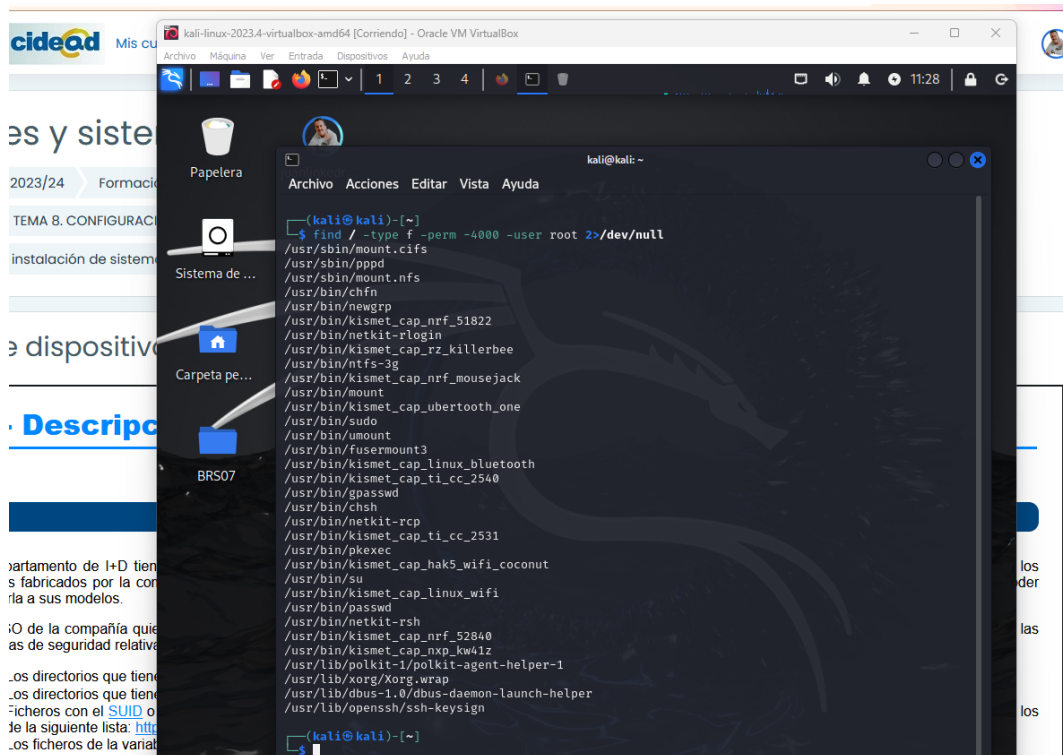
```
find / -type d -perm -u+x 2>/dev/null
```



- ✓ Ficheros con el SUID o SGID activado, que permitan ejecutar los ficheros con permisos de root, incluyendo si existe algún fichero con permisos de root entre los de la siguiente lista: <https://gtfobins.github.io>

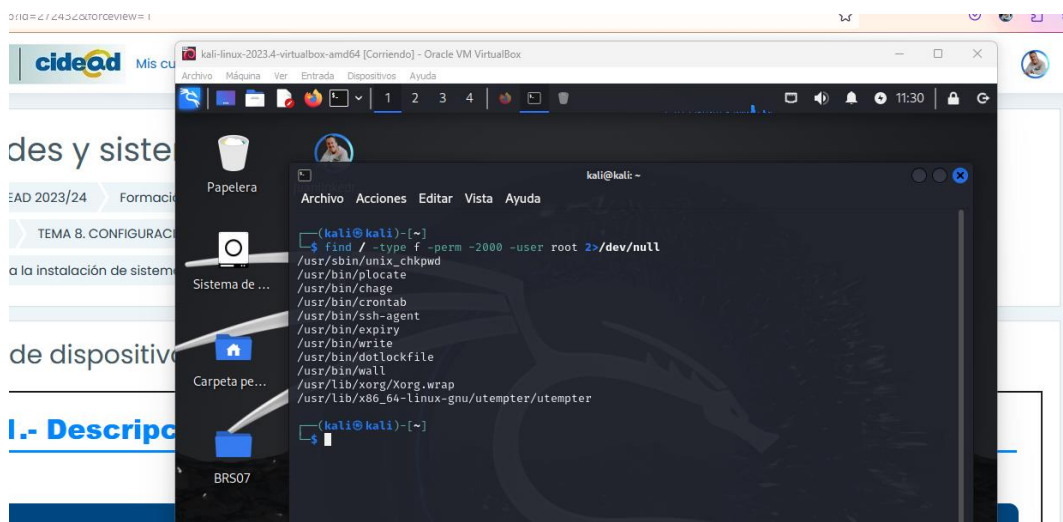
Filtramos por ficheros y por propiedad mediante **-perm**, buscando los que tengan los **SUID** o **SGID** activados.

```
find / -type f -perm -4000 -user root 2>/dev/null
```



The screenshot shows a Kali Linux terminal window with the command `find / -type f -perm -4000 -user root 2>/dev/null` executed. The output lists various system binaries and libraries with SUID or SGID bits set, including `/usr/sbin/mount.cifs`, `/usr/sbin/pppd`, `/usr/sbin/mount.nfs`, `/usr/bin/chfn`, `/usr/bin/newgrp`, `/usr/bin/kismet_cap_nrf_51822`, `/usr/bin/netkit-rlogin`, `/usr/bin/kismet_cap_rz_killerbee`, `/usr/bin/ntfs-3g`, `/usr/bin/kismet_cap_nrf_mousejack`, `/usr/bin/mount`, `/usr/bin/kismet_cap_ubertooth_one`, `/usr/bin/sudo`, `/usr/bin/umount`, `/usr/bin/fusermount3`, `/usr/bin/kismet_cap_linux_bluetooth`, `/usr/bin/kismet_cap_ti_cc_2540`, `/usr/bin/gpasswd`, `/usr/bin/chsh`, `/usr/bin/netkit-rpc`, `/usr/bin/kismet_cap_ti_cc_2531`, `/usr/bin/pkexec`, `/usr/bin/kismet_cap_hak5_wifi-coconut`, `/usr/bin/su`, `/usr/bin/kismet_cap_linux_wifi`, `/usr/bin/passwd`, `/usr/bin/netkit-rsh`, `/usr/bin/kismet_cap_nrf_52840`, `/usr/bin/kismet_cap_nxp_kw41z`, `/usr/lib/polkit-1/polkit-agent-helper-1`, `/usr/lib/xorg/Xorg.wrap`, `/usr/lib/dbus-1.0/dbus-daemon-launch-helper`, and `/usr/lib/openssh/ssh-keysign`.

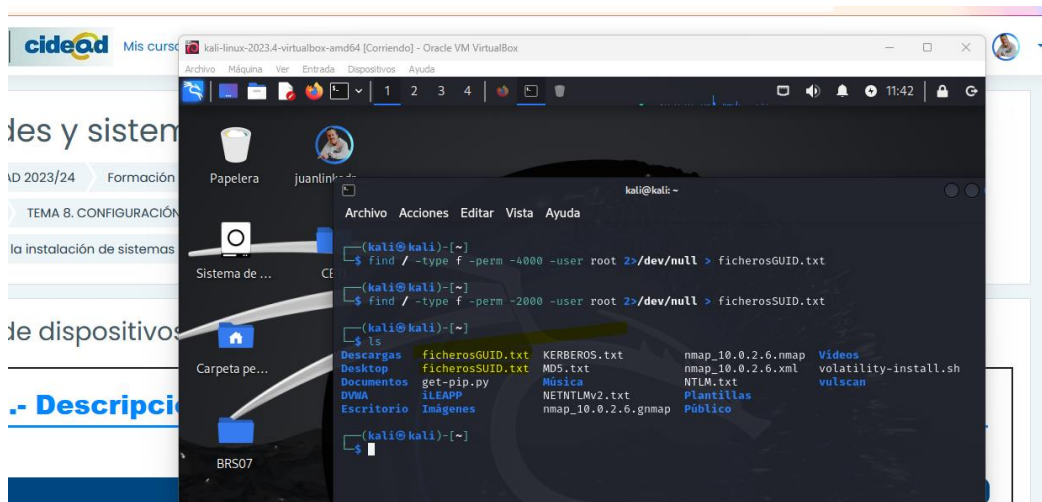
```
find / -type f -perm -2000 -user root 2>/dev/null
```



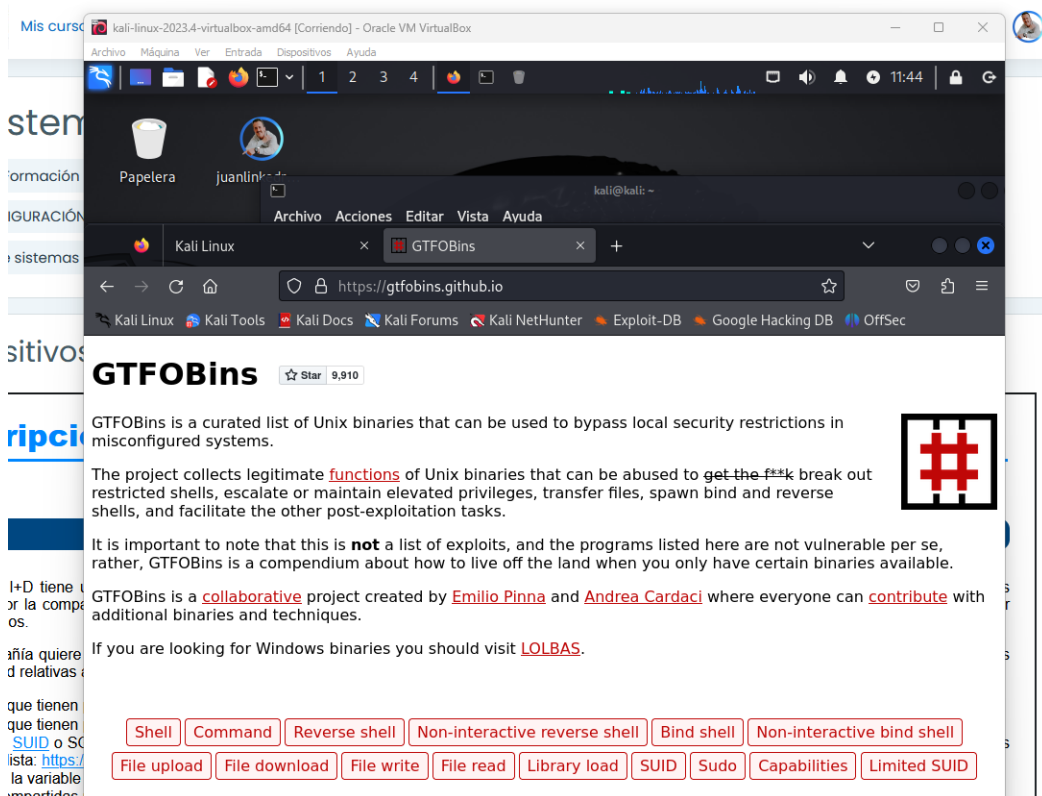
The screenshot shows a Kali Linux terminal window with the command `find / -type f -perm -2000 -user root 2>/dev/null` executed. The output lists various system binaries and libraries with SGID bits set, including `/usr/sbin/unix_chkpwd`, `/usr/bin/plocate`, `/usr/bin/chage`, `/usr/bin/crontab`, `/usr/bin/ssh-agent`, `/usr/bin/expiry`, `/usr/bin/write`, `/usr/bin/dotlockfile`, `/usr/bin/wall`, `/usr/lib/xorg/Xorg.wrap`, and `/usr/lib/x86_64-linux-gnu/utempter/utempter`.

Vamos ahora a comprobar si alguno de ellos está en el listado de **gtfobins**.

Primero, para realizar la búsqueda de forma más sencilla, pasamos los resultados anteriores a ficheros de texto.

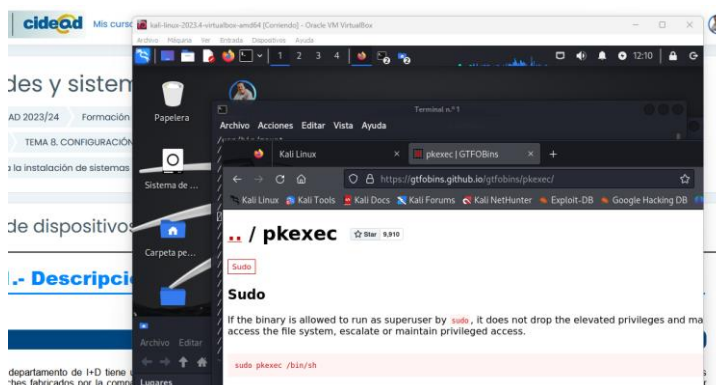
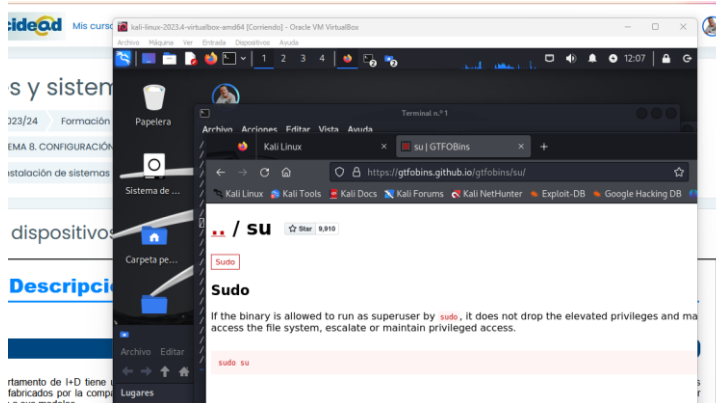
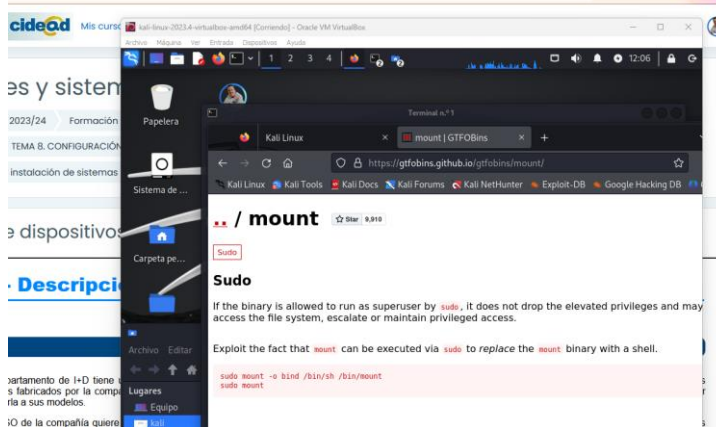
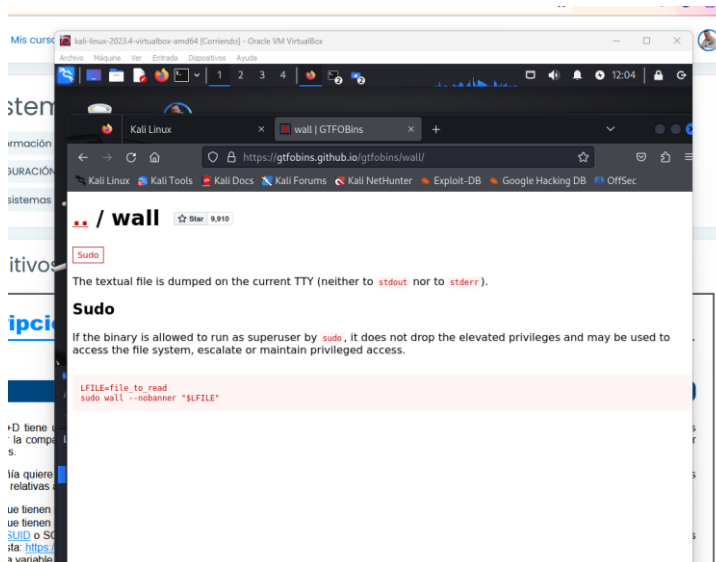


Accedemos desde el navegador al **gtfobins**.



Comprobamos ahora y vemos estas coincidencias:

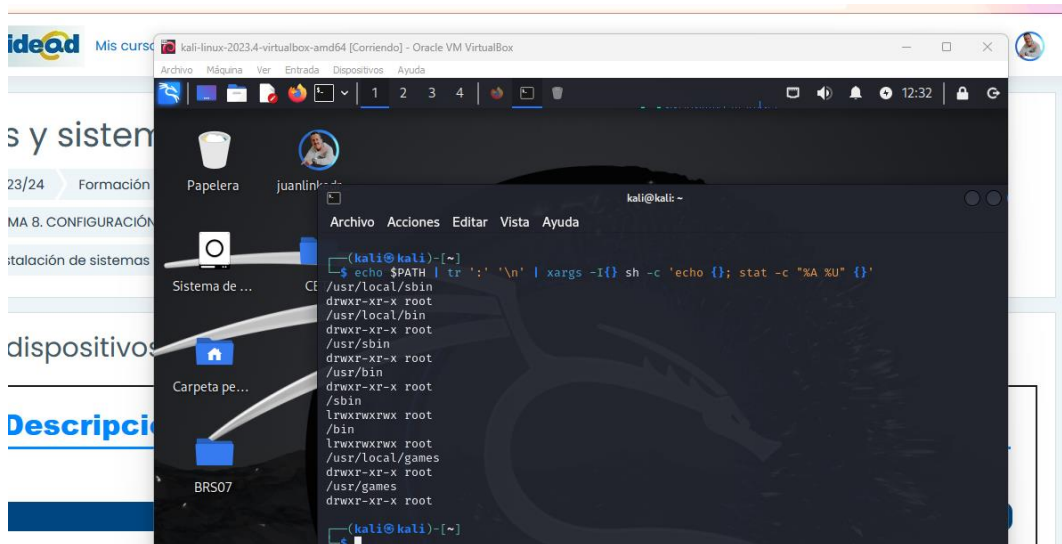
wall
mount
sudo
su
pkexec



- ✓ Los ficheros de la variable **PATH**, comprobando qué usuarios tienen acceso de escritura en esos directorios.

Mostramos la variable **PATH**. Por claridad, sustituyo los ':' por un salto de línea y mostrar aparte los permisos asignados a ese fichero y el propietario a través de **xargs**.

```
echo $PATH | tr ':' '\n' | xargs -I{} sh -c 'echo {}; stat -c "%A %U" {}'
```



- ✓ Las carpetas compartidas mal configuradas que permiten realizar acciones no controladas.

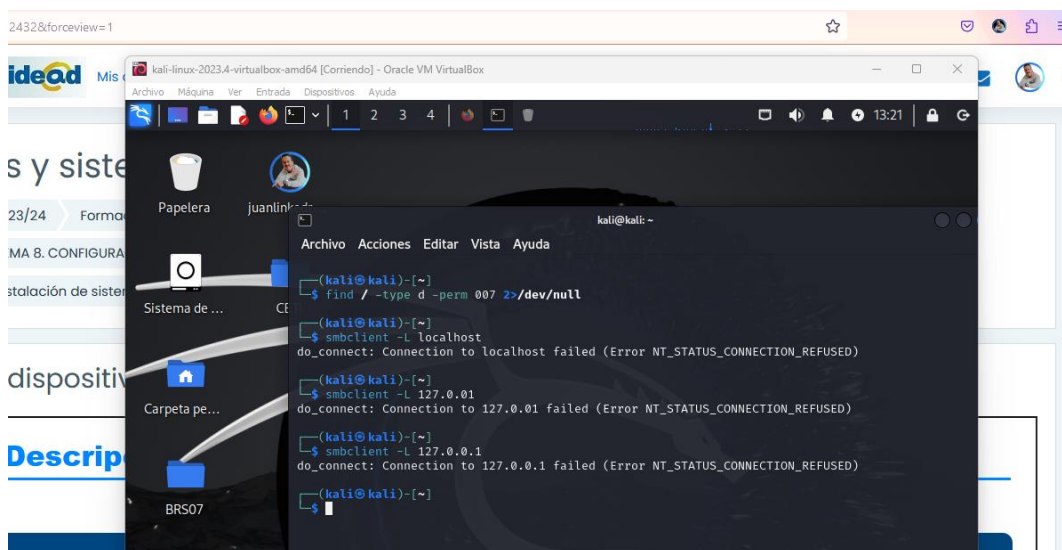
Podemos intentar comprobar si hay carpetas mal configuradas comprobando los permisos no asignados al grupo o a otros.

```
find / -type d -perm 007 2>/dev/null
```

Podemos hacer una búsqueda para listar los recursos compartidos disponibles.

```
smbclient -L localhost
```

```
smbclient -L 127.0.0.1
```



En este caso, no aparece ninguno.

Si se hubiera listado alguno, se podría comprobar la configuración mediante `ls -ld /rutaCompartida`

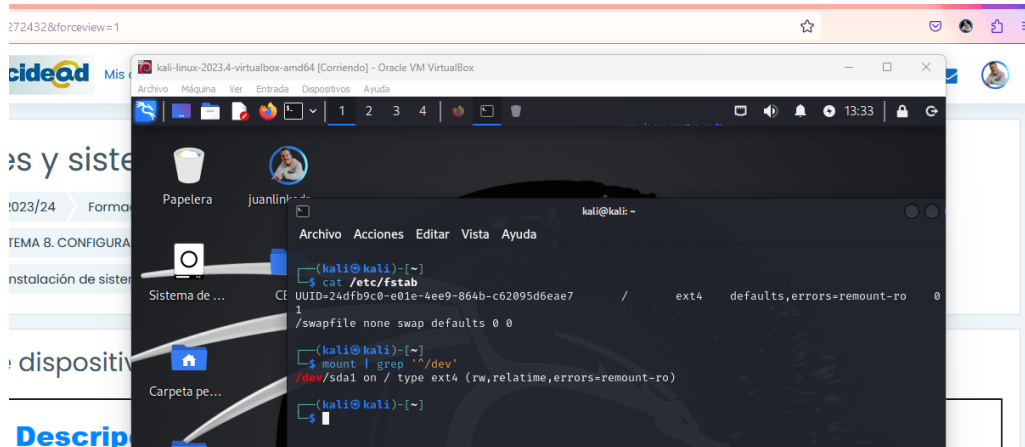
- ✓ Las particiones que tienen permisos para ejecutar ficheros y otras características que tienen impacto sobre la seguridad.

Buscamos las particiones existentes

```
cat /etc/fstab
```

Vemos ahora sus propiedades

```
mount | grep '^/dev'
```



Se encuentra con permisos de lectura y escritura. En caso de error, se montaría con permisos de lectura.

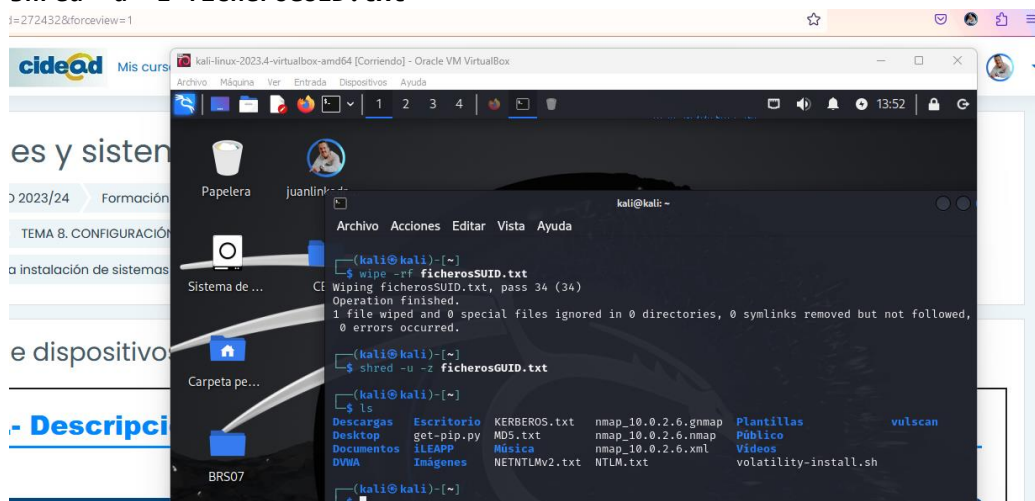
- ✓ Borrado seguro de archivos.

Vamos a realizar un borrado seguro con **wipe** forzando el borrado recursivo.

```
wipe -rf ficherosSUID.txt
```

Hacemos otra prueba con **shred** que sobrescribirá con ceros (**-z**) y borrará de forma segura (**-u**).

```
shred -u -z ficherosGUID.txt
```



El escenario se puede realizar con un sistema operativo Linux Ubuntu.

Webgrafía.

<https://www.mecd.es/cidead/aulavirtual/course/view.php?id=2368#section-7>

<https://gtfobins.github.io>

<https://payatu.com/blog/a-guide-to-linux-privilege-escalation>

<http://ntfs.com/ntfs-permissions.htm>

<https://proyectoa.com/borrado-seguro-de-ficheros-y-particiones-en-linux-con-shred/>

<https://www.hackingarticles.in/linux-privilege-escalation-using-path-variable/>

<https://medium.com/purplebox/linux-privilege-escalation-with-path-variable-suid-bit-6b9c492411de>

[Linux Privilege Escalation : PATH](#)

[Linux Privilege Escalation: SUID](#)

[Practicar Escalada de Privilegios en Linux](#)

<https://snapshooter.com/learn/linux/find>

<https://lagaialinux.es/buscar-archivos-comando-find/>

<https://recoverit.wondershare.es/computer-tips/secure-delete-linux.html>