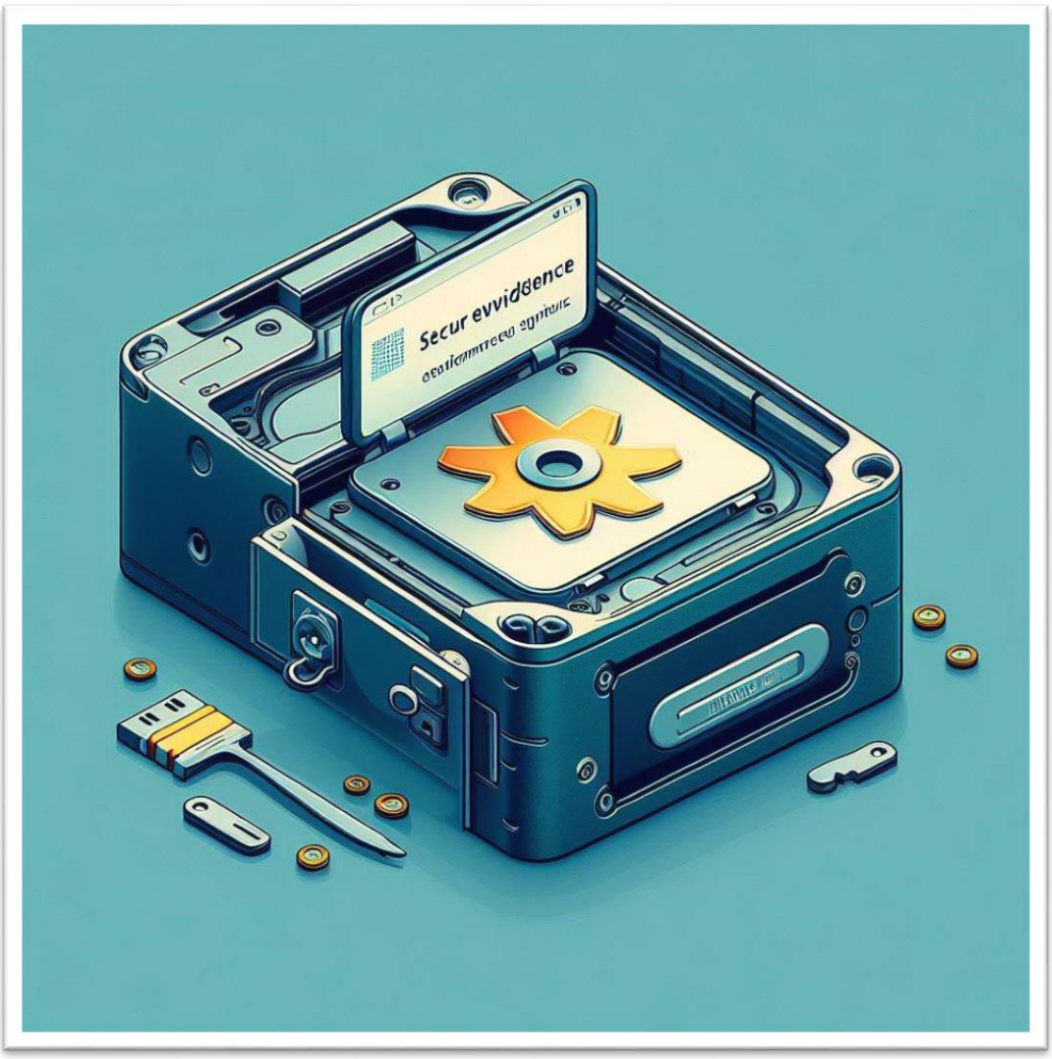
ERIC SERRANO MARÍN



PRÁCTICA 4.1 ALMACENAMIENTO SEGURO DE EVIDENCIAS

INCIDENTES DE CIBERSEGURIDAD

ERIC SERRANO MARÍN

CETI

Contenido

Contenido 1

1. Investiga cómo se utiliza la herramienta *dd* de Linux para hacer copias de unidades, ficheros…. 2

Sintaxis básica 2

Copia de unidades 2

Copia de archivos 2

Opciones adicionales 3

2. Usando la herramienta *dd* de Linux diseña un script que realice el borrado seguro de un pendrive o unidad 3 veces. 3

3. Después usando esta misma herramienta haz una copia de una unidad o varios ficheros en ese pendrive usando las opciones notrunc, noerror, count, sync y status=progress. Explica para que se utilizan las opciones utilizadas de la herramienta dd en cada caso. 5

4. Para finalizar comprueba que las copias son identicas al original haciendo una comprobación *hash*. usando los comandos *md5sum* y *sha1sum*. 6

1. Investiga cómo se utiliza la herramienta *dd* de Linux para hacer copias de unidades, ficheros…

Sintaxis básica

- **dd if=origen of of=destino [opciones]**

- **if=origen**: Entrada de los datos que se van acopiar, puede ser un dispositivo (como /dev/sda para una unidad de disco) o para un archivo regular.
- **of=destino**: Especifica la salida o el destino donde se copiarán los datos.
- **[opciones]** = Hay varias opciones que se pueden utilizar para ajustar el comportamiento de dd, como el tamaño del bloque de datos, el número de bloques, etc.

Copia de unidades

Una de las aplicaciones más comunes de 'dd' es la copia de unidades de disco. Para hacer una copia de una unidad de disco '/dev/sda' en otra unidad '/dev/sdb' podemos usar:

- **dd if=/dev/sda of=/dev/sdb**

Esto copiará todos los datos de la unidad /dev/sda a la unidad /dev/sdb.

Copia de archivos

También se puede usar dd para copiar archivos específicos. Por ejemplo, para copiar un archivo llamado archivo1 en otro llamado archivo2, podemos usar:

- **dd if=archivo1 of=archivo2**

Hay que tener en cuenta que copiará exactamente como está, incluyendo cualquiera metadato o espacio no utilizado.

Opciones adicionales

Algunas opciones útiles incluyen bs para especificar el tamaño del bloque, count para el número de bloques a copiar y status para ver el progreso de la operación.

Por ejemplo, para copiar solo los primeros 1 MB de un archivo, puedes usar:

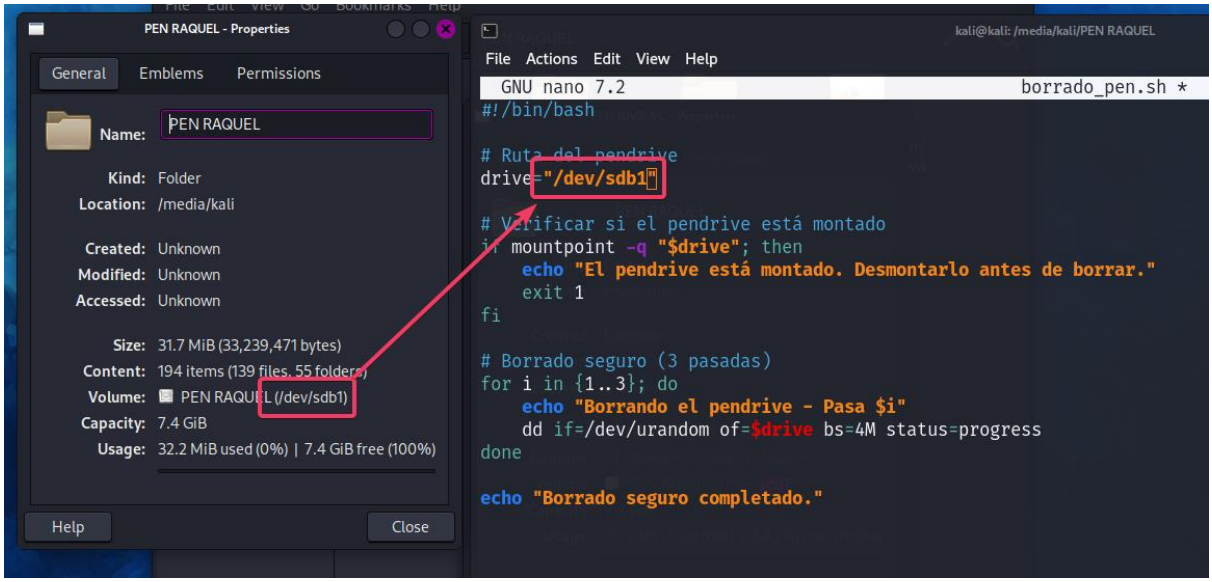
- **dd if=archivo1 of=archivo2 bs=1M count=1**

Esto copiará solo el primer megabyte del archivo archivo1 en archivo2.

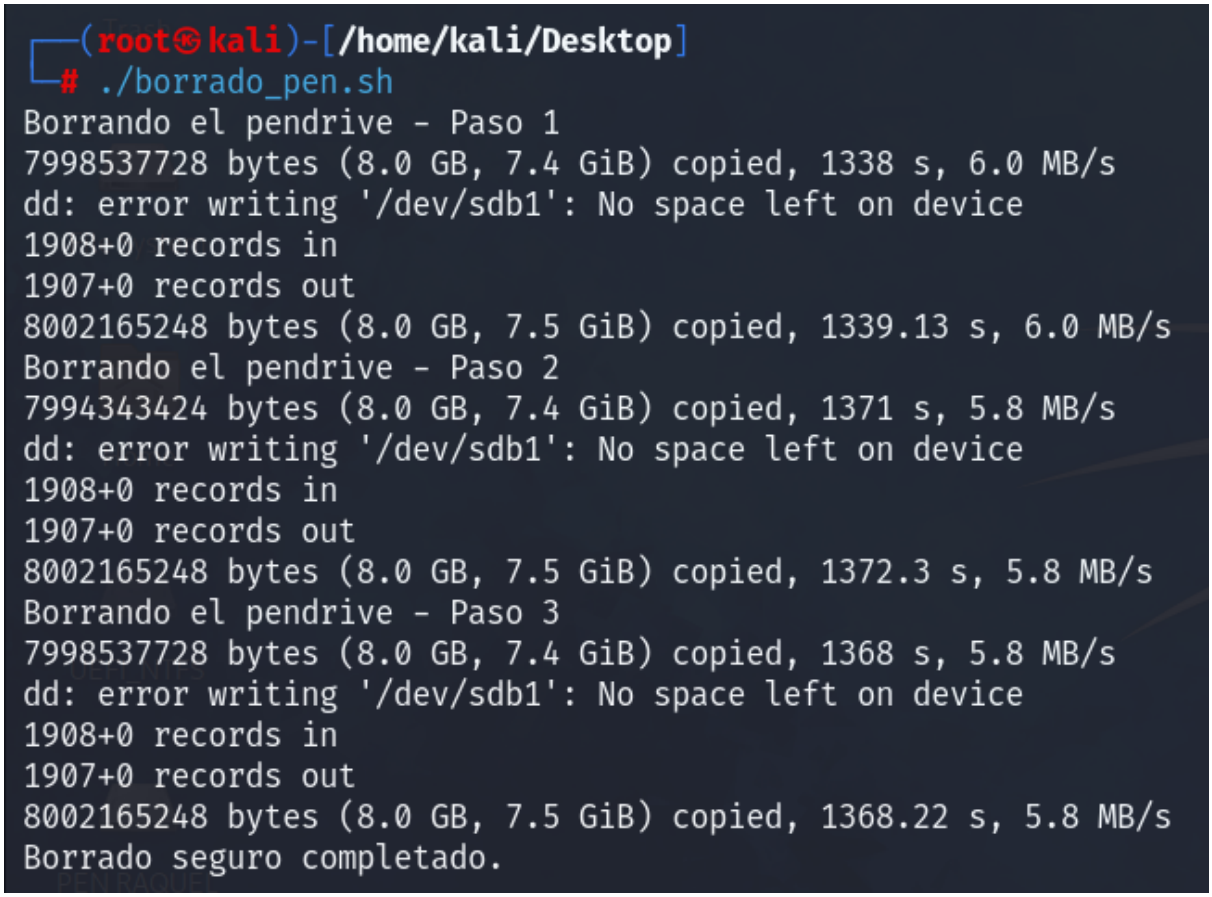
Tenemos que tener en cuenta que hay que tener precaución a la hora de utilizar 'dd', ya que puede sobrescribir datos de forma irreversible si se usa incorrectamente.

2. Usando la herramienta *dd* de Linux diseña un script que realice el borrado seguro de un pendrive o unidad 3 veces.

El script realiza tres pasadas de borrado seguro en el pendrive, utilizando datos aleatorios para eliminar los datos existentes de manera segura. Finalmente, muestra un mensaje de completado.



Aquí vemos como está el script funcionando.

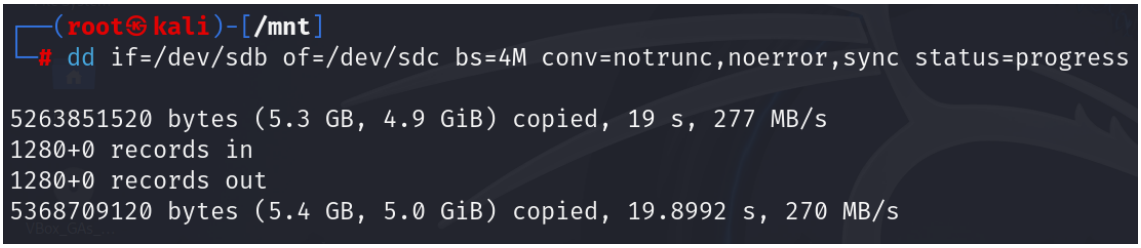


3. **Después usando esta misma herramienta haz una copia de una unidad o varios ficheros en ese pendrive usando las opciones notrunc, noerror, count, sync y status=progress. Explica para que se utilizan las opciones utilizadas de la herramienta dd en cada caso.**

   dd if=/dev/sdb of=/dev/sdc bs=4M,noerror,sync status=progress

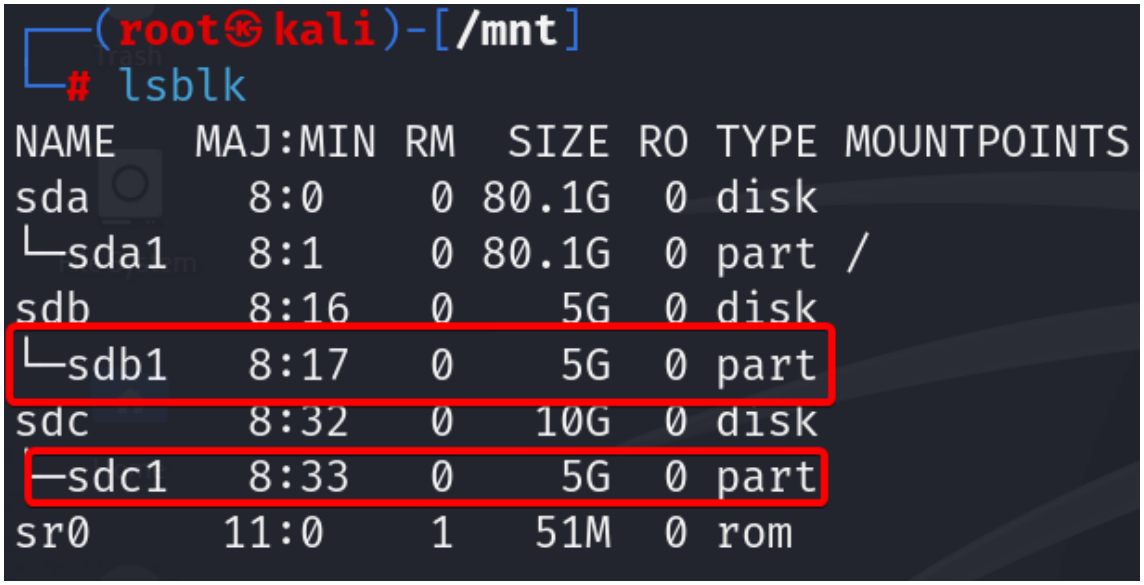
bs=4m	Establece el tamaño del bloque de lectura y escritura. En este caso, se establece en 4 megabytes.
noerror	Esto indica que dd continuará leyendo y escribiendo a pesar de los errores de entrada/salida.
sync	Ordena a dd que escriba los datos de manera sincrónica, lo que significa que los datos se escriben inmediatamente en el dispositivo de salida en lugar de almacenarse en la memoria caché y luego escribirse más tarde.
status=progress	Proporciona una barra de progreso que muestra el progreso de la copia.

Este comando está copiando datos desde el dispositivo /dev/sdb al dispositivo /dev/sdc utilizando un tamaño de bloque de 4 megabytes, ignorando los errores de entrada/salida, escribiendo de manera sincrónica y mostrando el progreso de la operación. Para este apartado he creado dos espacios virtuales con VirtualBox y los he montado en Kali Linux, uno de ellos de 5GB y otro de 10GB.



4. **Para finalizar comprueba que las copias son identicas al original haciendo una comprobación *hash*. usando los comandos *md5sum* y *sha1sum*.**

Dejo una imagen con lsblk para que se compruebe el proceso.



Podemos observar que tienen el mismo sha1sum y md5sum.