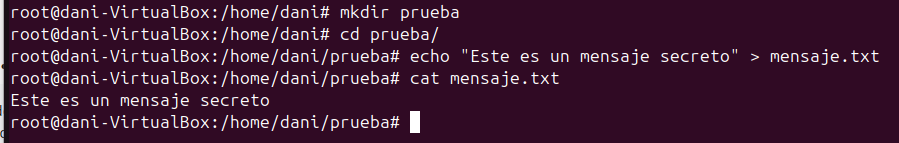
CRIPTOGRAFIA 2

Comparación de hashes SHA-256 en Linux

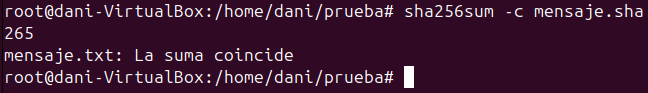
1. Creación de archivo de prueba



2.- Generar hash sha-256

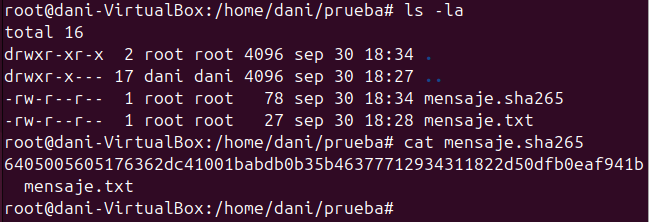


3.- Verificar integridad del archivo:



La opcion –c significa “check”

Contenido del archivo cifrado:



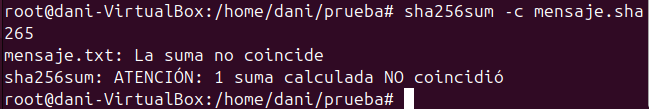
Sha256sum –c calcula el hash alamacenado del archivo (primer campo) y toma el nombre del archivo (segundo campo) para comprobar que el archivo no ha sido modificado.

4.- Simulación de un cambio en el archivo (ataque):

Modificación del archivo:

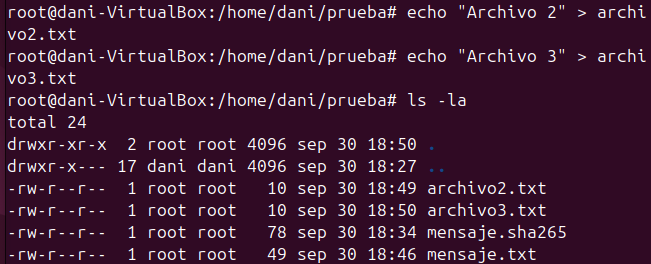


Comprobación del hash al modificar el archivo:



6.-Verificación de varios archivos

Creación de los archivos:



Generación de hashes en los archivos:



Con esto nos habrá creado los hashes en los archivos y el nombre de cada archivo.

Ahora vamos a verificar los hashes con el archivo donde hemos metido la información “hashes.sha256”:

