Alumno: Rodrigo Vila

Experto Universitario de la Información

Modulo 6 Unidad 4: Seguridad de Comunicaciones y Redes

Ejercicio Número 1 Unidad 4:

Servicios de Seguridad OSI

Estos son algunos servicios que podemos aplicar

- Autenticación
- Control de Accesos
- Confidencialidad de Datos
- Integridad de Datos
- Non Repudiation
- Monitoreo y Logging

Seleccionar uno y desarrollarlo y explicarlo mediante un ejemplo.

Integridad de Datos:

Descripción:

La integridad de datos es un servicio de seguridad en el modelo OSI que garantiza que la información enviada y recibida no ha sido alterada o manipulada durante su transmisión. Este servicio asegura que los datos permanezcan completos, precisos y confiables desde su creación hasta su destino final.

La integridad de los datos puede ser comprometida por varios factores, como errores en la transmisión, ataques maliciosos (por ejemplo, la inserción de datos falsificados) o fallos en los sistemas de almacenamiento. Para garantizar la integridad de los datos, se utilizan técnicas como sumas de verificación, algoritmos de hash, y firmas digitales, que permiten detectar cualquier modificación no autorizada en los datos.

Ejemplo:

Supongamos que estás trabajando en un banco que envía instrucciones de transferencia de fondos electrónicamente. Es crucial que estas instrucciones no se modifiquen durante el envío, ya que cualquier alteración podría resultar en la pérdida o transferencia incorrecta de fondos.

Para garantizar la integridad de los datos, antes de enviar las instrucciones, se aplica un algoritmo de hash (por ejemplo, SHA-256) a las instrucciones de transferencia, generando un hash único. Este hash se envía junto con las instrucciones de transferencia.

Al llegar al destino, el sistema receptor aplica el mismo algoritmo de hash a las instrucciones recibidas y compara el hash resultante con el que fue enviado. Si ambos coinciden, se garantiza que las instrucciones no han sido modificadas durante la transmisión. Si hay alguna discrepancia, se sabe que los datos fueron alterados y la transferencia es bloqueada para evitar un error o fraude.

Conclusión:

Este servicio es esencial en cualquier sistema donde la exactitud y confiabilidad de los datos son cruciales, como en transacciones financieras, comunicaciones de datos sensibles, o cualquier otro entorno donde la integridad de los datos debe ser protegida.

¿Cómo generar un hash SHA-256 de un archivo para verificar su integridad utilizando Kleopatra (herramienta vista en ésta cursada)?

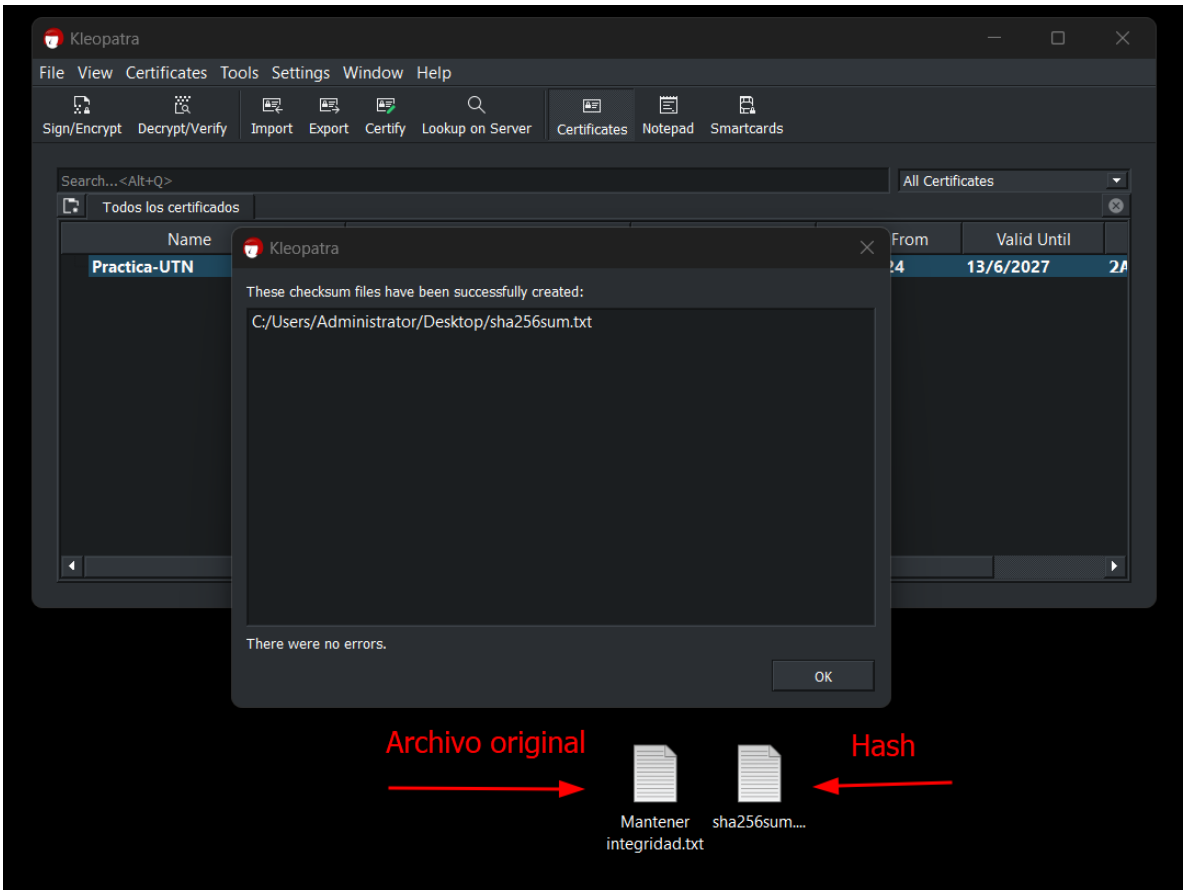
1. Hash de un archivo con Kleopatra:

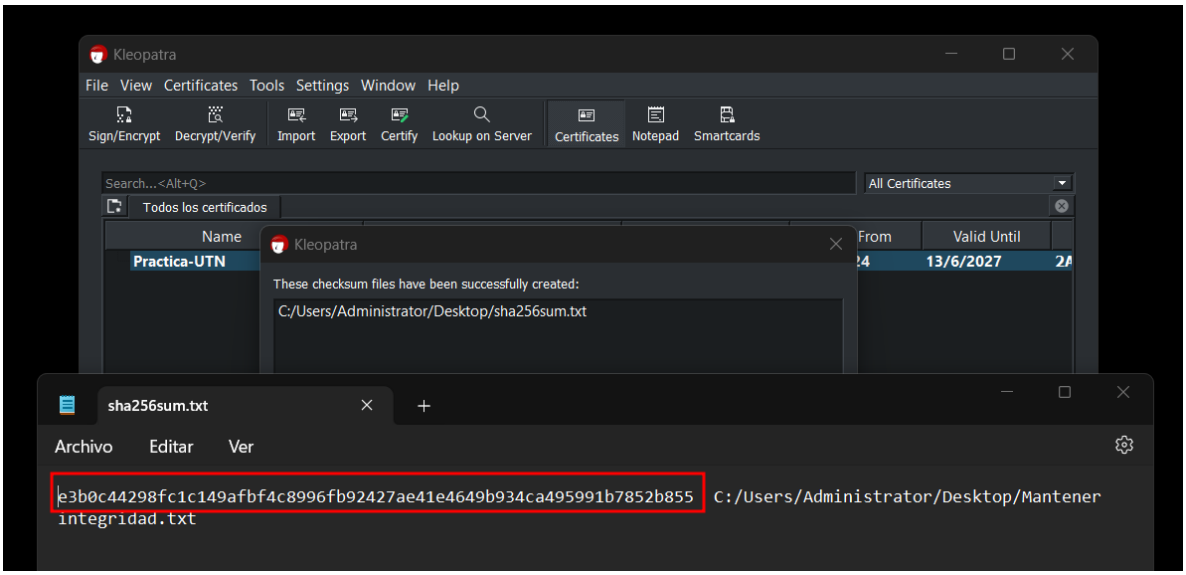
Kleopatra es una herramienta para gestión de claves GPG/PGP, que también puede calcular hashes.

Pasos:

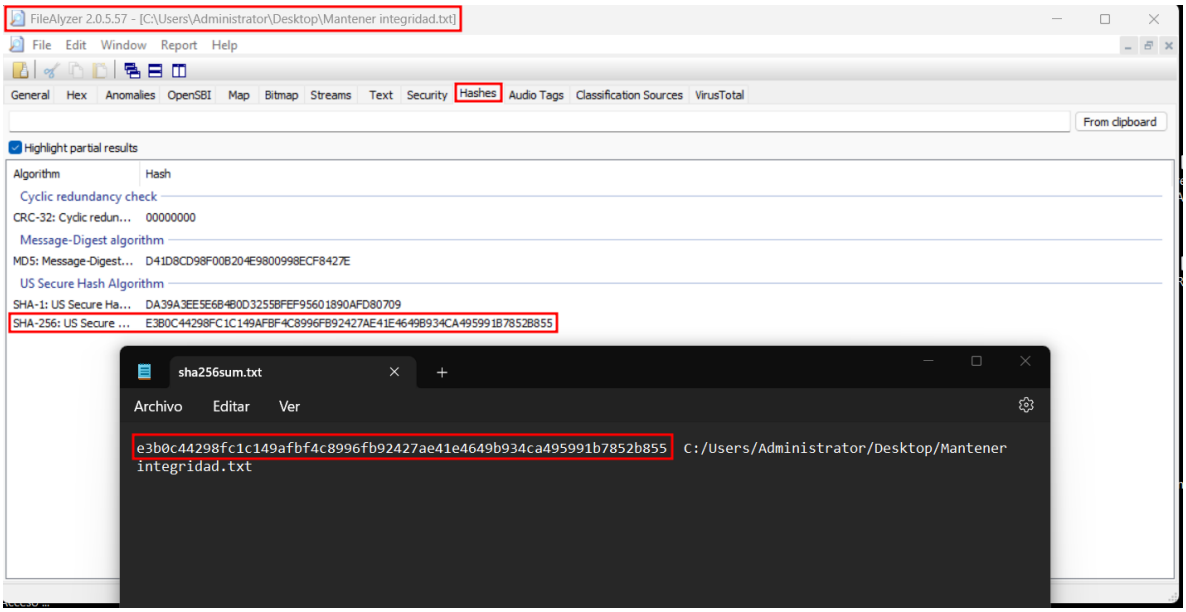
1. Abre Kleopatra.
2. Haz clic en el menú "File" (Archivo) y selecciona "Create Checksum Files" (Crear Archivos de Suma de Verificación).
3. Selecciona el archivo que deseas hashear.
4. En la ventana emergente, selecciona "SHA-256" como el algoritmo de hash.
5. Kleopatra generará un archivo con el hash SHA-256 del archivo seleccionado.

Este hash puede ser utilizado para verificar la integridad del archivo en el futuro.



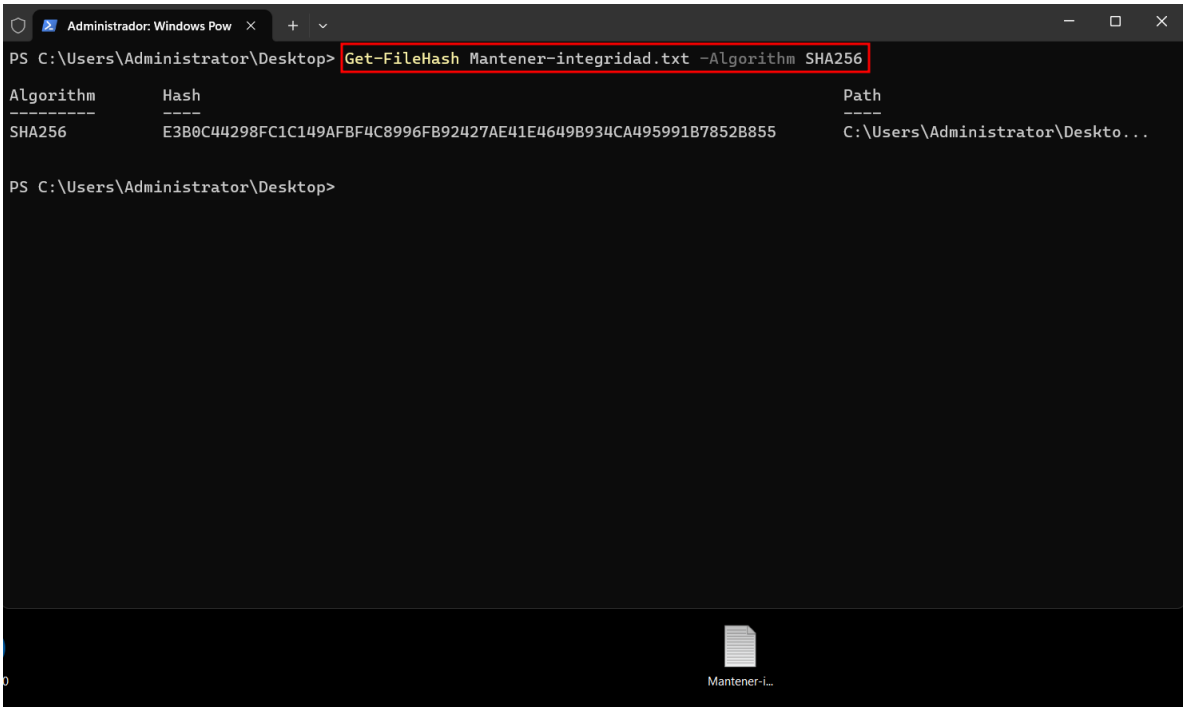


¿Cómo comprobar el hash para verificar que el archivo no haya sido modificado utilizando FileAlyzer (herramienta vista en clase)?



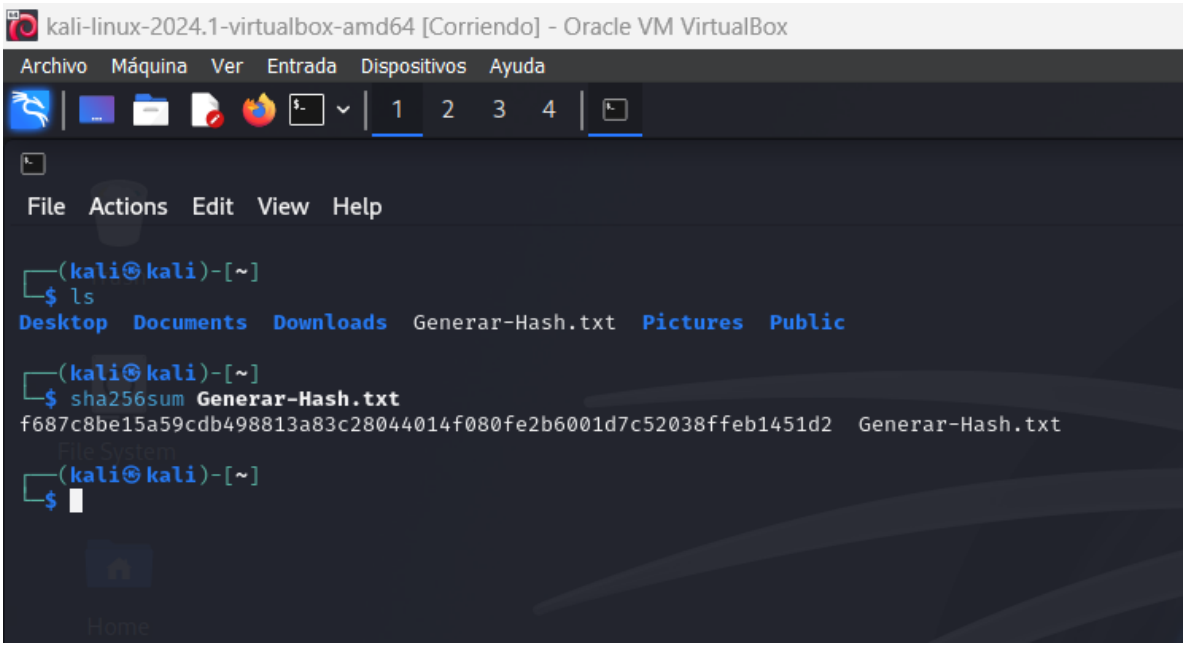
Generar hash desde PowerShell (Windows):

Cmd: Get-FileHash nombre_del_archivo -Algorithm SHA256



Generar hash desde terminal Linux:

Cmd: sha256sum nombre_del_archivo



Rodrigo Vila.-