Informe Sobre laboratorio 1

Presentado Por:

Anderson Rene Gómez Aza

Sebastián Misael Rodríguez Bernal

Dirigido a:

Juan Albarracín

Énfasis en seguridad informática

ETITC

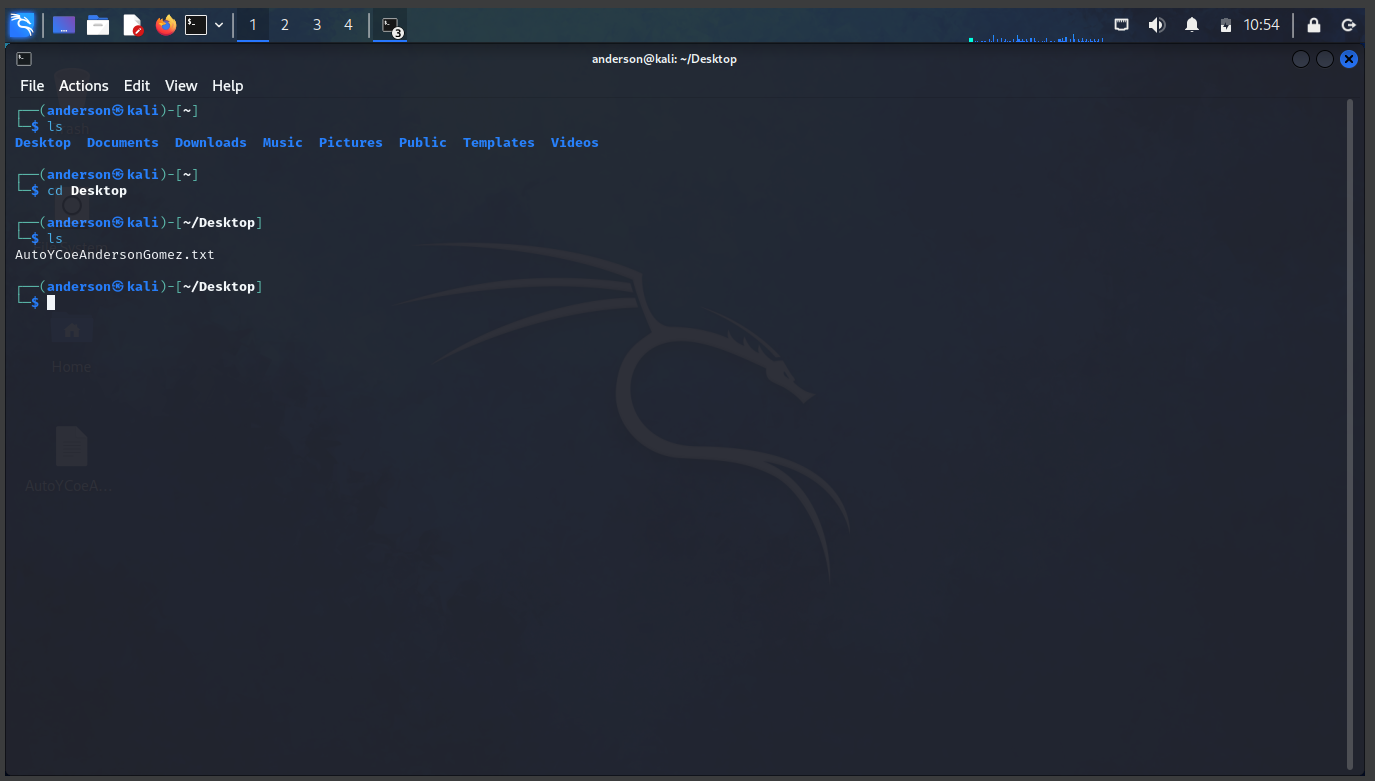
2024

Solución Anderson Rene Gómez Aza

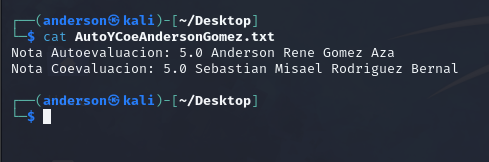
1. Instalar Kali Linux por medio de maquina virtual



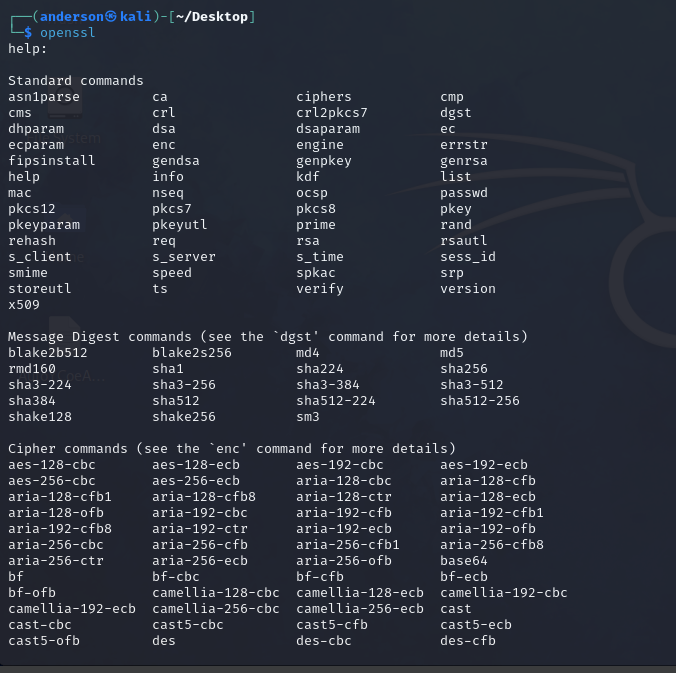
1. Creamos texto plano AutoyCoe Anderson



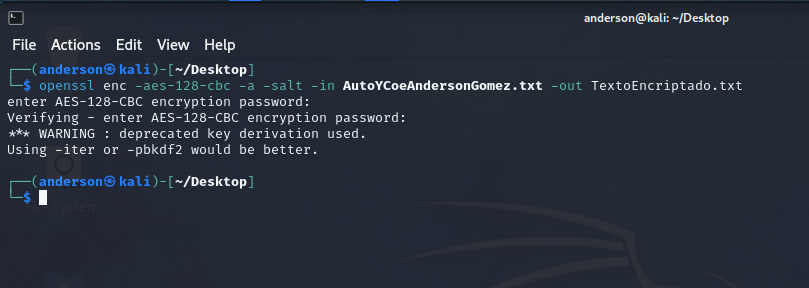
1. Vemos el contenido del archivo plano



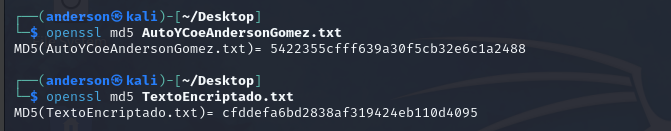
1. Comprobamos la librería openSSL
   1. OpenSSL es una herramienta de código abierto y una biblioteca de criptografía que se utiliza ampliamente en sistemas operativos Unix-like, incluyendo Kali Linux. Proporciona funciones para la creación y administración de certificados digitales, así como para la encriptación y descifrado de datos.
   2. OpenSSL es una herramienta esencial para realizar una amplia gama de tareas relacionadas con la seguridad, como la creación de claves criptográficas, la generación de certificados SSL/TLS, la firma y verificación de mensajes digitales, y la encriptación de datos en tránsito.



1. Realizamos el comando openssl enc -aes-128-cbc -a -salt -in archivo\_original -out archivo\_encriptado
   1. openssl: Este es el nombre del comando que invoca el programa OpenSSL. OpenSSL es una herramienta de código abierto y una biblioteca de criptografía que proporciona varias funciones criptográficas para asegurar datos en tránsito o en reposo.
   2. enc: Esta es una suborden dentro de OpenSSL que se utiliza para encriptar y desencriptar archivos.
   3. -aes-128-cbc: Especifica el algoritmo de cifrado que se utilizará para encriptar los datos. En este caso, se está utilizando AES (Advanced Encryption Standard) con una clave de 128 bits en modo CBC (Cipher Block Chaining). AES es un algoritmo de cifrado ampliamente utilizado y considerado seguro.
   4. -a: Esta opción indica que se desea codificar la salida en formato Base64. La codificación en Base64 convierte los datos binarios en una forma de texto legible que es útil para transferencias de datos que no admiten caracteres especiales.
   5. -salt: Esta opción agrega sal (un valor aleatorio) al proceso de encriptación. La sal mejora la seguridad del cifrado al hacer que cada ejecución del comando genere una salida diferente, incluso si los mismos datos se cifran.
   6. -in archivo\_original: Especifica el nombre del archivo de entrada que se va a encriptar. En este caso, "archivo\_original" es el nombre del archivo que contiene el texto plano que se desea encriptar.
   7. -out archivo\_encriptado: Especifica el nombre del archivo de salida donde se guardarán los datos encriptados. En este caso, "archivo\_encriptado" es el nombre del archivo que contendrá el texto plano encriptado.

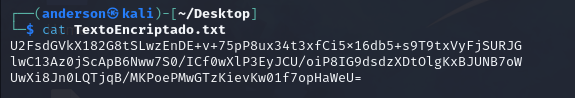


1. Realizamos los hash de ambos archivos con el comando openssl md5 nombre del archivo
   1. El comando openssl md5 nombre:archivo es utilizado para calcular el hash MD5 de un archivo específico. Aquí está el desglose de cada parte del comando:
      1. openssl: Como se mencionó anteriormente, este es el nombre del comando que invoca el programa OpenSSL, una herramienta de código abierto que proporciona varias funciones criptográficas.
      2. md5: Esto indica que se utilizará el algoritmo de hash MD5 para calcular el hash del archivo. MD5 (Message Digest Algorithm 5) es un algoritmo de resumen criptográfico ampliamente utilizado para producir un resumen único y fijo de datos, generalmente utilizado para verificar la integridad de archivos y contraseñas.
      3. nombre:archivo: Esta parte del comando especifica el nombre del archivo del cual se desea calcular el hash MD5. Aquí, "nombre" es el nombre que deseas asignar al archivo y "archivo" es el nombre real del archivo del que deseas calcular el hash.

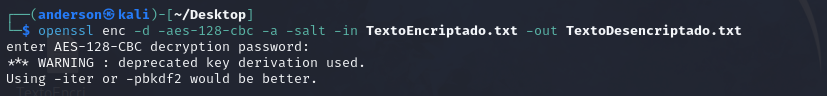


* 1. Como podemos ver los hash son diferentes ya que el contenido de los 2 archivos con completamente diferentes con eso ya nuestros hash generados deben ser diferentes

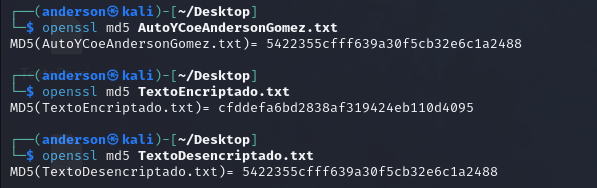
1. Revisamos el contenido del archivo encriptado con la encriptación aes 128 cbc



1. Desencriptamos el archivo con el comando openssl enc -d -aes-128-cbc -a -salt -in nobre del archivo encriptado -out nombre del archivo que creara con el texto plano desencriptado



1. Creamos los hash de los 3 archivos



* 1. Como evidenciamos en el texto plano y archivo original el hash es el mismo por lo cual la desencriptación de los archivos esta correcta

1. Revisamos el contenido de los 3 archivos para verificar que se haya encriptado y desencriptado bien

