**Manual de Práctica 11 – Encriptación**

**Edgar Gael Sanchez Hernandez**

**Materia:** Administración de Redes

**Docente:** Ana Claudia Zenteno Vázquez

**Objetivo**: Que el alumno ejecute comandos como MD5 y las diferentes versiones de SHA para generar checksum de un determinado archivo.

1. Realice un cuadro comparativo de descripción y opciones de los siguientes comandos:
   1. md5sum
   2. sha1sum
   3. sha256sum
   4. sha512sum

|  |  |  |
| --- | --- | --- |
| Comando | Descripción | Opciones |
| md5sum | Calcula y muestra el valor hash MD5 de uno o más archivos. | - -b: Muestra el valor hash en binario. <br> - -c: Compara el valor hash calculado con un valor hash proporcionado en un archivo. <br> - -t: Muestra el nombre del archivo antes del valor hash. |
| sha1sum | Calcula y muestra el valor hash SHA-1 de uno o más archivos. | - -b: Muestra el valor hash en binario. <br> - -c: Compara el valor hash calculado con un valor hash proporcionado en un archivo. <br> - -t: Muestra el nombre del archivo antes del valor hash. |
| sha256sum | Calcula y muestra el valor hash SHA-256 de uno o más archivos. | - -b: Muestra el valor hash en binario. <br> - -c: Compara el valor hash calculado con un valor hash proporcionado en un archivo. <br> - -t: Muestra el nombre del archivo antes del valor hash. |
| sha512sum | Calcula y muestra el valor hash SHA-512 de uno o más archivos. | - -b: Muestra el valor hash en binario. <br> - -c: Compara el valor hash calculado con un valor hash proporcionado en un archivo. <br> - -t: Muestra el nombre del archivo antes del valor hash. |

1. Seleccione un archivo aleatorio (.docx, imagen, pdf, etc) y pruebe con este los comandos listados anteriormente.

De forma similar a

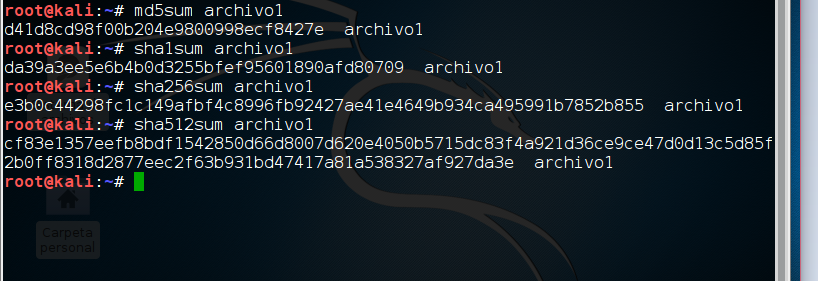


Imagen de la pantalla de un computador

Descripción generada automáticamente con confianza media

Responda las siguientes preguntas:

* ¿Por qué las salidas de cada comando son totalmente distintas en forma y dimensión?

R= Diferencias en la implementación del comando: Cada comando puede estar diseñado por diferentes desarrolladores, lo que lleva a variaciones en la forma en que se presentan los resultados.

Configuración y opciones: Los comandos pueden tener diferentes opciones y configuraciones que afectan la salida. Por ejemplo, algunos comandos pueden tener opciones para mostrar información adicional o formatear la salida de una manera específica.

Diferencias en la naturaleza de los datos: La salida puede variar dependiendo de los datos de entrada y del propósito del comando. Por ejemplo, la salida de un comando que lista archivos puede ser diferente en diferentes directorios o sistemas de archivos.

* ¿Cuál de los comandos anteriores es mejor y por qué?

R= se prefiere sha256sum debido a su mayor seguridad y eficiencia.

* En sus palabras, para qué sirve un checksum.

R= Un checksum es un valor numérico único que se calcula a partir de un conjunto de datos, como un archivo o un conjunto de datos de red.

1. Obtenga y comparta los códigos generados por correo electrónico. Coloque ahí mismo el archivo para que sea posible descargarlo. Pida a su compañero descargue el archivo y efectue las mismas operaciones de obtención de códigos y compárelos con el código enviado por correo. ¿es el mismo código?
2. Si el archivo fuera modificado ¿obtiene el mismo código?
3. Refiérase al capítulo 4 del libro de Antonio Villalón que se encuentra en

<http://es.tldp.org/Manuales-LuCAS/SEGUNIX/unixsec-2.1.pdf>

y Analice los comandos crypt y pgp

R= Crypt:

crypt es un comando de cifrado que se utiliza para encriptar y desencriptar archivos en sistemas Unix y Linux. Utiliza un algoritmo de cifrado simple y estándar llamado "crypt", que es un algoritmo de cifrado de clave simétrica. El comando crypt requiere que el usuario proporcione una contraseña para cifrar o descifrar un archivo. La desventaja de crypt es que utiliza un algoritmo de cifrado relativamente débil en comparación con los estándares modernos, por lo que no se recomienda su uso para aplicaciones de seguridad críticas.

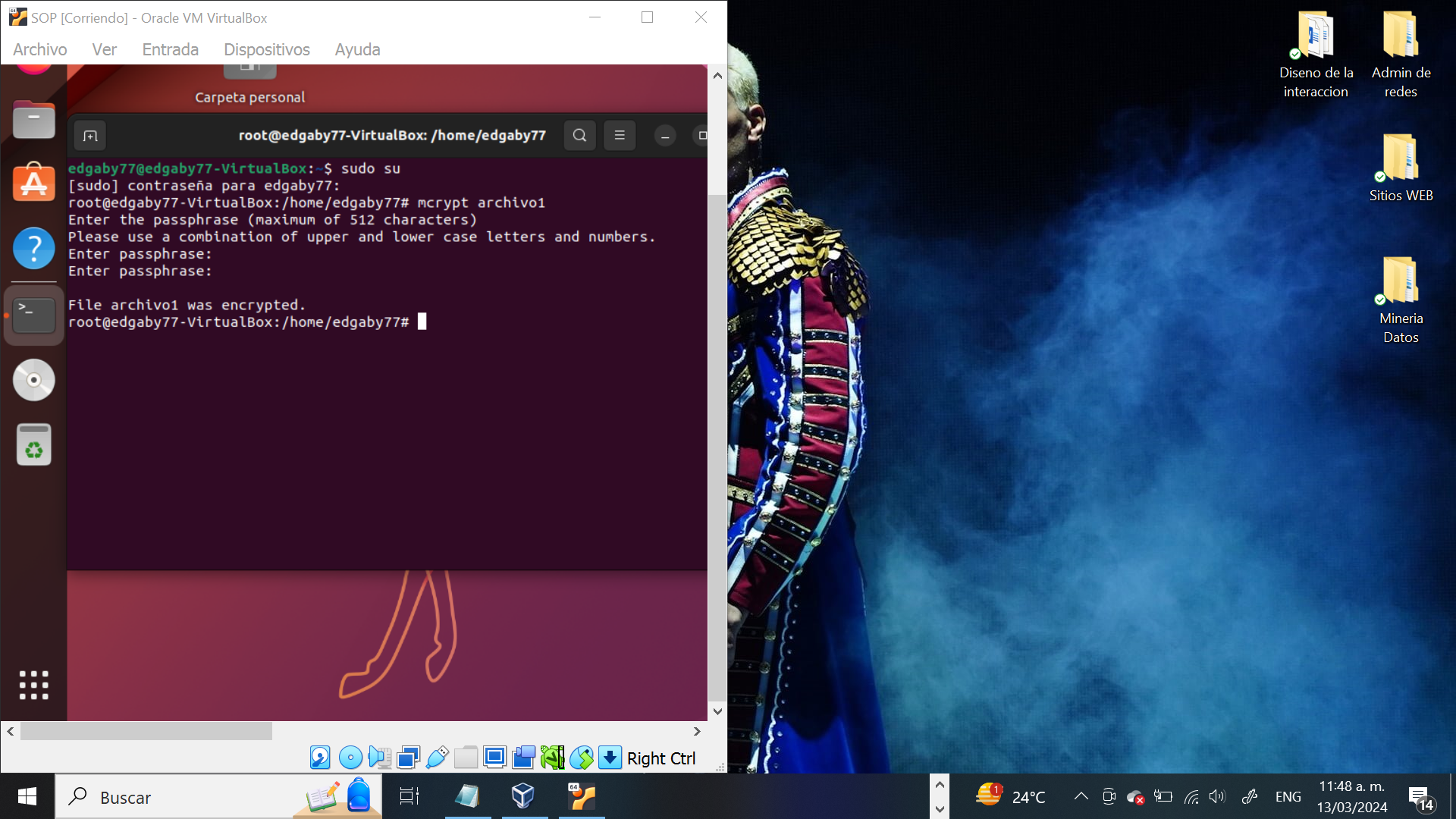
PGP (Pretty Good Privacy):

PGP es una suite de software de criptografía que proporciona cifrado de datos, firmas digitales y otras funciones relacionadas con la seguridad de la información. PGP utiliza un enfoque de criptografía de clave pública, donde cada usuario tiene un par de claves: una clave pública y una clave privada. La clave pública se utiliza para cifrar mensajes que solo el propietario de la clave privada puede descifrar, mientras que la clave privada se utiliza para firmar mensajes y descifrar los mensajes cifrados con la clave pública correspondiente. PGP es ampliamente utilizado para asegurar la comunicación por correo electrónico y otros medios digitales.

Aplique alguno de estos dos comandos a un archivo y comparta su practica con capturas.

Captura de pantalla de computadora

Descripción generada automáticamente



¿Cuál es la diferencia de usar crypt y pgp a usar md5 y sha?

R=Crypt y PGP se utilizan para cifrar y proteger la confidencialidad de los datos, mientras que MD5 y SHA se utilizan para generar valores hash que se utilizan para verificar la integridad de los datos. Cada uno tiene su propio propósito y se utiliza en diferentes contextos de seguridad.