**PRÁCTICA N° 3**

Cifrado y firma digital con el uso de GPG

1. **OBJETIVOS**
   1. Comprender cómo funciona el cifrado y la firma digital en Linux mediante GPG.
   2. Realizar tareas de cifrado y firma digital para asegurar la información en dispositivos Linux.
   3. Garantizar la confidencialidad, integridad y autenticidad en el intercambio de información autenticidad ante posibles ataques.
2. **MARCO TEÓRICO**
   1. **GPG**

GNU Privacy Guard (GPG) es una herramienta de software libre y de código abierto que permite realizar cifrado y firmas digitales de datos. Está basado en el estándar OpenPGP (Pretty Good Privacy) y es compatible con una amplia variedad de clientes de correo electrónico y aplicaciones de cifrado. Se emplea principalmente para proteger la privacidad y seguridad de los datos mediante el cifrado de archivos y correos electrónicos. Su funcionamiento se basa en la criptografía de clave pública, en la que cada usuario dispone de un par de claves: una clave pública y una clave privada.

Algunas características importantes son las siguientes

* **Cifrado de mensajes:** GPG permite cifrar texto, archivos y correos electrónicos para asegurar que solo el destinatario autorizado pueda acceder al contenido. Combina el cifrado de clave pública y simétrico para proteger la información.
* **Firma Digital:** Los usuarios pueden firmar digitalmente mensajes y archivos para validar su autenticidad e integridad. Esto ayuda a prevenir la suplantación de identidad y asegura que los datos no hayan sido alterados durante su transmisión.
* **Generar claves:** GPG permite generar pares de claves criptográficas: una clave pública, que puede compartirse, y una clave privada, que debe mantenerse confidencial. La clave pública se utiliza para cifrar mensajes, y solo su clave privada correspondiente puede descifrarlos.
* **Verificación de Identidad:** los usuarios pueden confirmar la identidad de otros mediante la verificación de sus claves públicas, garantizando una comunicación segura y evitando interacciones con impostores.

1. **TRABAJO PREPARATORIO**
   1. Explicar la diferencia entre cifrado simétrico y asimétrico. También entre clave pública y clave privada.
   2. Consultar que es una firma digital, su utilidad, proceso de verificación y su importancia en la seguridad en dispositivos Linux.
   3. Describir que es GPG y su utilidad, así como la forma de instalar y configurar en Linux.
2. **EQUIPO Y MATERIALES**

* Oracle VM Virtual Box o VMWare Player.
* Máquina virtual con distribución Ubuntu/Debian que actúe como dispositivo Linux.
* Internet.

1. **PROCEDIMIENTO**

**Instalación de GPG**

* Se verifica si se encuentra instalado con el comando gpg –version, caso contrario instalar con el siguiente comando sudo apt install gnupg.

**Generación de par de claves**

* Para generar la clave pública y privada se utiliza el siguiente comando: gpg --full-generate-key. Luego se llena la información de la siguiente manera:

Tipo de clave: Seleccionar RSA y RSA (predeterminado).

Tamaño de clave: Ingresar 4096 (recomendado para mayor seguridad).

Duración de la clave: Ingresar 0 para que no expire, dado el caso que es una práctica.

Identidad: Ingresar un nombre, email y un comentario opcional.

Contraseña: Establecer una contraseña para proteger la clave privada.

* Luego se verifica la creación de claves públicas y privadas con los comandos: gpg --list-keys, gpg --list-secret-keys respectivamente,

**Cifrado de archivos**

* Se crea un archivo de prueba con el comando echo y luego se cifran el archivo usando la clave pública del destinatario con el comando: gpg --encrypt --recipient "correo@destinatario.com" archivo.txt. Como resultado se genera el archivo archivo.txt.gpg.

A computer screen shot of text

Description automatically generated

**Descifrado de archivos**

* Para descifrar el archivo se usa la clave publica creada con el comando: gpg --decrypt archivo.txt.gpg.

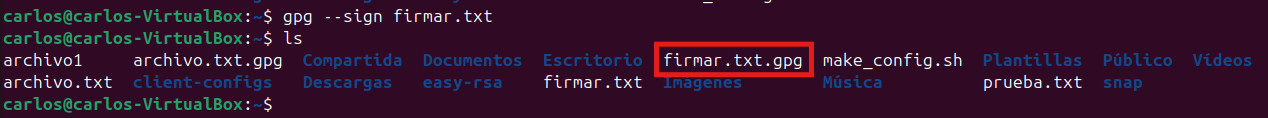
**A screenshot of a computer

Description automatically generated**

Luego se muestra una ventana, como donde se debe ingresar la contraseña creada para la generación de la clave publica y como resultado se descifra el archivo y se muestra su contenido.

**Firma digital de archivos**

* Para esto primero se crea un archivo de prueba, el cual será firmado (firmar.txt,) De este modo con el comando gpg --sign firmar.txt se firma el documento y se genera el archivo firmar.txt.gpg

****

Luego para verificar que el archivo firmado posea integridad y autenticidad, se utiliza el comando gpg --verify mensaje.txt.sig

**Exportar e Importar Claves**

* Para exportar la clave publica y compartirlo con personas de confianza se usa el comando gpg --export --armor "tu\_correo@ejemplo.com" > clave\_publica.asc y para importar claves públicas de terceros se realiza con el comando gpg --import clave\_publica\_companero.asc, lo cual es útil para verificar la integridad y autenticidad del archivo firmado.

**Revocar una clave**

* Para revocar una clave se debe crear un archivo de revocación, el cual se usa para invalidar una clave pública en el futuro si esta se encuentra comprometida. Para esto se usa el comando gpg --output revocacion.asc --gen-revoke "juan@example.com"

A screenshot of a computer program

Description automatically generated

De este modo el archivo revocacion.asc se puede usar para revocar la clave cuando sea necesario.

1. **INFORME**
   1. Documentar las configuraciones aplicadas.
   2. Presentar las capturas de pantalla, con la debida explicación de los resultados mostrados. Además, indicar el impacto en la seguridad.
   3. Realizar el proceso de firma separada y explicar sus casos de uso. Además, las diferencias que tiene con firma adjunta.
2. **REFERENCIAS**

**[1] "Cómo utilizar GPG para cifrar y firmar mensajes" DigitalOcean. https://www.digitalocean.com/community/tutorials/how-to-use-gpg-to-encrypt-and-sign-messages. (accessed Dec 16. 2024)**