Práctica 2.3: GPG Linux

Vamos a suponer el escenario del uso de GPG en una distribución de Linux. En este caso haremos uso de gpg que suele venir instalado por defecto en las distribuciones Linux.

En nuestro caso utilizaremos un servidor Ubuntu mediante línea de comandos.

1. Creación de las llaves GPG

La primera cosa que necesitamos saber es como crear las llaves GPG.

Utilizaremos el comando gpg—gen-key para realizar esta acción y rellenaremos los datos como se nos pide por pantalla.

Seguidamente nos pedirá una contraseña para proteger nuestra key.

NOTA: puede que en este proceso nos pida también los datos del algoritmo de cifrado y la fecha de expiración.

En este caso utilizaremos RSA ya que es más seguro que el cifrado DSA.

Una vez generada la key podemos verla con el comando gpg -k

Y podemos ver los archivos generados en el directorio /root/.gnupg

2. Exportación de las claves públicas

Exportaremos la clave pública en un archivo llamado “mi-clave-publica.key” con el comando:

```
# gpg --export -a “Usuario” > mi-clave-publica.key
```

3. Envio de la clave a un servidor de claves

Por ejemplo el servidor de la red iris

4. Exportación de la clave privada

La opción utilizada en este caso es: --export-secret-key

Y nos pedirá la contraseña que se introdujo durante la creación de la clave.

5. Importar una clave pública

Para poder comunicarnos con otros interlocutores necesitamos la clave pública.

Descargaremos la clave pública “.key” y se puede importar a nuestro anillo de claves.

Por seguridad, GPG no considera de confianza la clave imoprtada. Para ello, se puede editaremos la clave y le otorgaremos la confianza con los siguientes comandos:

```
gpg—edit-key “nombre”
fpr
sign
```

y con el comando “quit” salimos.

Ahora podemos ver que ha cambiado la clave con gpg –k.

6. Importar una clave privada

Si por algún motivo tuviéramos que importar una clave privada podemos hacerlo con el siguiente comando

```
gpg—allow-secret-key—import privada.key
```

7. Borrar una clave pública

```
gpg—delete-key “nombre_usuario”
```

8. Borrar una clave privada

gpg—delete-secret-key “nombre_usuario”

9. Encriptación simétrica de archivos

Si quisiéramos encriptar nuestros propios archivos podríamos hacer uso de una encriptación simétrica ya que utilizaríamos nuestra clave privada para encriptar y desencriptar el fichero, pero no podríamos compartir el fichero con nadie ya que tendríamos que pasarle también nuestra clave privada.

Usamos el parámetro -c para usar encriptación simétrica y nos pedirá que introduzcamos una contraseña al fichero, no nos pide la contraseña de nuestra clave privada.

Si vemos el directorio veremos un nuevo fichero con extensión .gpg que será el archivo encriptado.

Si quisiéramos volver a ver el contenido del fichero tendremos que desencriptarlo primero

gpg -o <archivo_descifrado> -d <archivo_cifrado>

10. Encriptación asimétrica con clave pública

Será necesario importar clave pública, encriptar el fichero y enviarlo al destinatario de la clave.

ENTREGA:

El objetivo es la práctica de todas las posibles opciones que nos brinda GPG.

Para ello crearemos el par de claves, exportaremos la clave pública y la subiremos a un servidor de claves, por ejemplo el de la red iris.

No bajaremos una clave pública de un compañero, la importaremos a nuestro anillo y cifraremos un mensaje. Después enviaremos el mensaje cifrado al compañero propietario de la clave. Y tendrá que descifrarlo.

Captura del anillo de claves y del proceso de descifrado del mensaje del compañero con nuestra clave.