Práctica BRS: GPG usando Linux

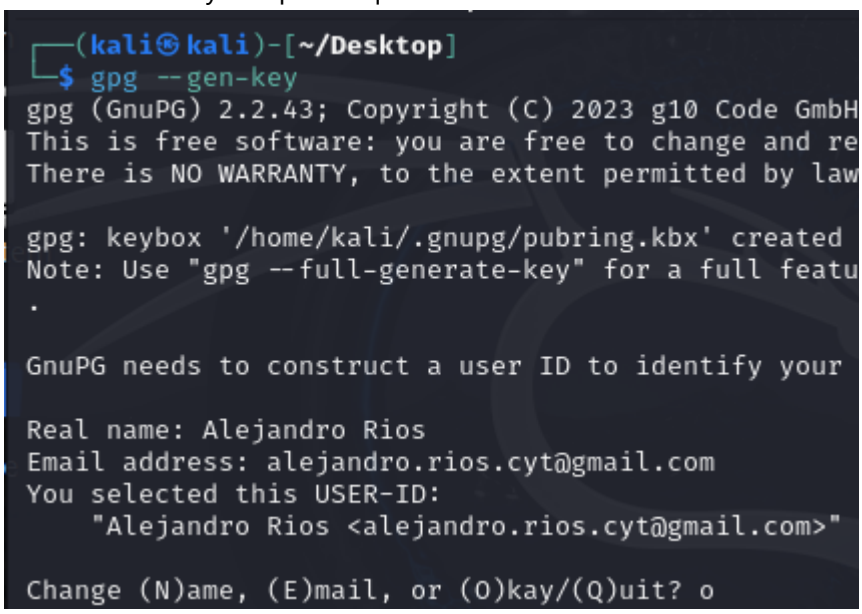
Requisitos previos

- PC con acceso a Internet
- Máquina virtual con Kali Linux (o cualquier otra distribución)
- Software PuTTY

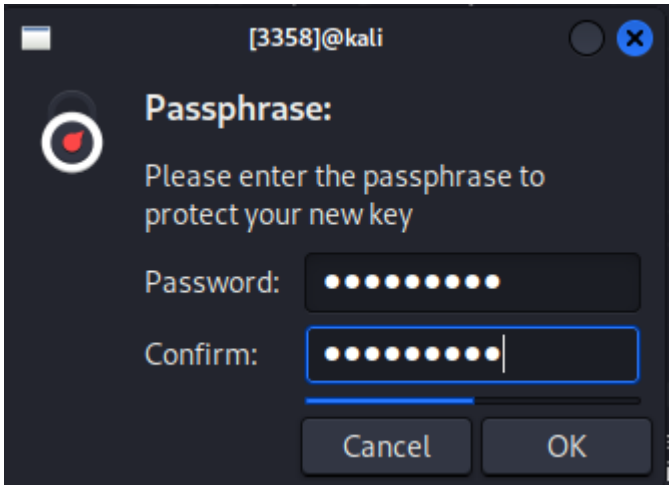
Proceso

1. Creación llaves GPG

- Ejecutaremos el comando `gpg --gen-key` en la terminal de nuestra Linux. Nos pedirá nuestro nuestro nombre e email y nos pedirá que confirmemos los datos.



- Una vez hecho, nos pedirá una `passphrase` (**pandora27** en mi caso) para proteger las claves.



- Tras darle a `OK` y esperar un poco, nos generará las claves y nos mostrará un breve resumen de lo que hemos hecho.

```
pub   rsa3072 2024-11-07 [SC] [expires: 2027-11-07]
      BEF8E2067346FC16FF70B02D9768B4491FE6864F
uid                      Alejandro Rios <alejandro.rios.cyt@gmail.com>
sub   rsa3072 2024-11-07 [E] [expires: 2027-11-07]


┌──(kali㉿kali)-[~/Desktop]
└─$
```

- Para ver todas las claves que tenemos usaremos el comando `gpg --list-keys`

```
┌──(kali㉿kali)-[~/Desktop]
└─$ gpg --list-keys
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2027-11-07
/home/kali/.gnupg/pubring.kbx
-----------------------------
pub   rsa3072 2024-11-07 [SC] [expires: 2027-11-07]
      BEF8E2067346FC16FF70B02D9768B4491FE6864F
uid           [ultimate] Alejandro Rios <alejandro.rios.cyt@gmail.com>
sub   rsa3072 2024-11-07 [E] [expires: 2027-11-07]
```

2. Exportar la claves

- Usaremos el comando `cd ~/.gnupg` para irnos al directorio oculto donde se encuentran las claves GPG de nuestro sistema (se almacenan ahí por defecto)

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cd ~/.gnupg

┌──(kali㉿kali)-[~/.gnupg]
└─$ ls
openpgp-revocs.d  private-keys-v1.d  pubring.kbx  pubring.kbx~  trustdb.gpg

┌──(kali㉿kali)-[~/.gnupg]
└─$
```

- Ejecutamos el comando `gpg --export -a nombreAsignado > mi-clave-publica.key`, siendo `nombreAsignado` el nombre que hayamos introducido al crear la clave. En mi caso `Alejandro Rios`

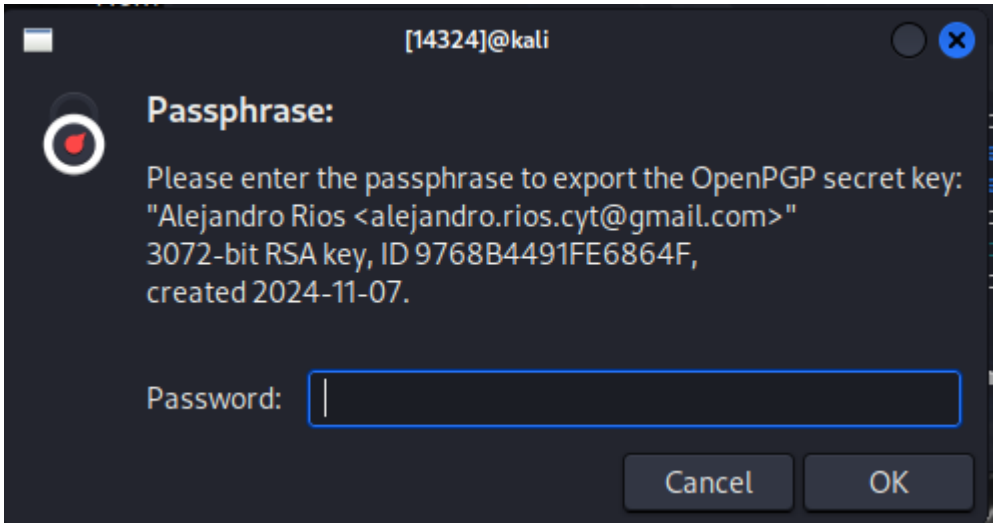
```
┌──(kali㉿kali)-[~/.gnupg]
└─$ gpg --export -a "Alejandro Rios" > mi_clave_publica.key

┌──(kali㉿kali)-[~/.gnupg]
└─$ ls -l
total 24
-rw-rw-r-- 1 kali kali 2472 Nov  7 14:28 mi_clave_publica.key
drwx------ 2 kali kali 4096 Nov  7 14:09 openpgp-revocs.d
drwx------ 2 kali kali 4096 Nov  7 14:09 private-keys-v1.d
-rw-rw-r-- 1 kali kali 1987 Nov  7 14:09 pubring.kbx
-rw------- 1 kali kali   32 Nov  7 14:07 pubring.kbx~
-rw------- 1 kali kali 1280 Nov  7 14:18 trustdb.gpg
```

- Con el comando `gpg --export-secret-key -a nombreAsignado > mi-clave-publica.key` haremos exactamente lo mismo, pero exportaremos la clave privada.

```
┌──(kali㉿kali)-[~/.gnupg]
└─$ gpg --export-secret-key -a "Alejandro Rios" > mi_clave_secreta.key
```

- Nos pedirá la contraseña que introdujimos anteriormente y tras darle a OK se exportará clave.




```
┌──(kali㉿kali)-[~/.gnupg]
└─$ ls -l
total 32
-rw-rw-r-- 1 kali kali 2472 Nov  7 14:32 mi_clave_publica.key
-rw-rw-r-- 1 kali kali 5229 Nov  7 14:32 mi_clave_secreta.key
drwx------ 2 kali kali 4096 Nov  7 14:09 openpgp-revocs.d
drwx------ 2 kali kali 4096 Nov  7 14:09 private-keys-v1.d
-rw-rw-r-- 1 kali kali 1987 Nov  7 14:09 pubring.kbx
-rw------- 1 kali kali   32 Nov  7 14:07 pubring.kbx~
-rw------- 1 kali kali 1280 Nov  7 14:18 trustdb.gpg
```

3. Importar una clave pública