SEGURIDAD EN SISTEMAS OPERATIVOS

4º Grado en Informática – Complementos de Ing. del Software

Curso 2017-18

Práctica [1]. Administración de la seguridad en Linux

Sesión [5]. Cifrado de archivos

Autor[1]: Rubén Calvo Villazán

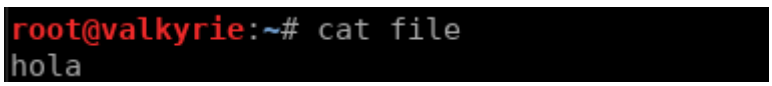
Ejercicio 1.

a) Claves personales generadas con la herramienta gpg:

```
$> gpg --list-keys
/root/.gnupg/pubring.kbx
------------------------
pub   rsa3072 2017-11-18 [SC] [expires: 2019-11-18]
      53D82B560F06A578CC254F605AF413EC9E643E33
uid           [ultimate] valkyrie <valkyrie@random.org>
sub   rsa3072 2017-11-18 [E] [expires: 2019-11-18]

pub   rsa4096 2017-11-18 [SC]
      5804F4E2A654C3F68387E75500FFFF0079184D7B
uid           [ultimate] valkyrie ("Random CommMent82376") <valkyrie@random.org>
sub   rsa4096 2017-11-18 [E]
```

b) Cifrar un archivo:



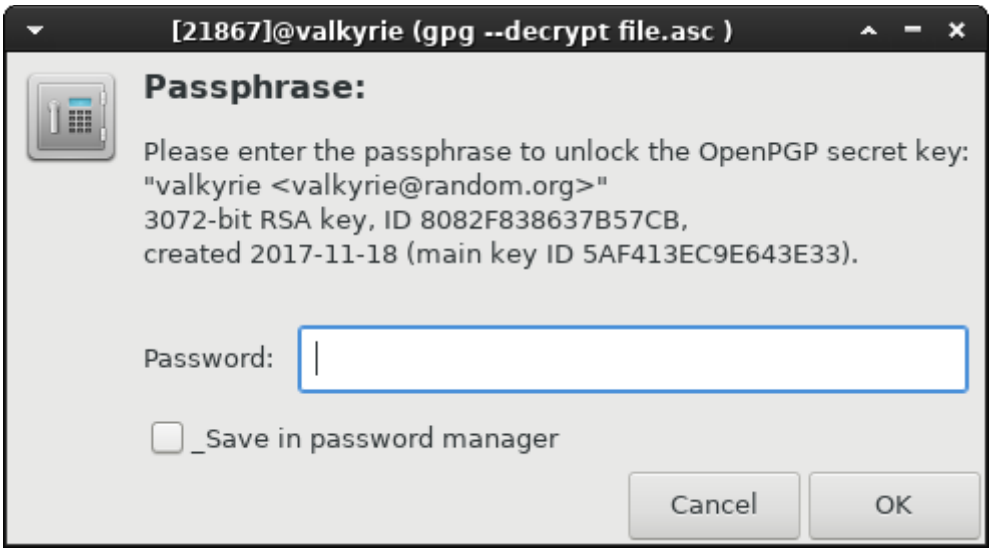
---

1 Como autor declaro que los contenidos del presente documento son originales y elaborados por mi. De no cumplir con este compromiso, soy consciente de que, de acuerdo con la "Normativa de evaluación y de calificaciones de los estudiantes de la Universidad de Granada" esto "conllevará la calificación numérica de cero … independientemente del resto de calificaciones que el estudiante hubiera obtenido ..."

```
root@valkyrie:~# gpg --output file --encrypt --recipient valkyrie file
File 'file' exists. Overwrite? (y/N) y
root@valkyrie:~# ls
 Desktop     file  'Nmap complete scan'         System  'VirtualBox VMs'
 Downloads   Home   PlantillaDocPracticas.odt   To-do
root@valkyrie:~# cat file
[illegible]
```

Descifrar el archivo:

```
root@valkyrie:~# gpg --decrypt file.asc
gpg: encrypted with 3072-bit RSA key, ID 8082F838637B57CB, created 2017-11-18
      "valkyrie <valkyrie@random.org>"
hola
```



c) Descifrar asimétricamente (con dos llaves):

```
root@valkyrie:~# gpg --export -a "valkyrie" > public.key
root@valkyrie:~# cat public.key
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBFoQOEQBDACvdx5g0i6ZPtCayfuJd3jg1vUShwbNiR5iIkHJYRErlb0ZrGvi
VpCpH5jejSaGcZO3yNAtplJ9CSLEWqSnQk1Urs1gys98ZcbkKjrEaEN9iAplTr7p
SkuwaZfXTqqzcLpKgPfXqi8vRE5KKqfIlK4pQci9UbdkUzCeWRmFKyX8sO00acd4
OpPOnh5CrznwhXBfhvpARDsvFUw3nxMizfpGpYUHwsp4sxi8rkByxCSyOlbtRw9c
wx6mb7aFCtdZ8PWkBmozN5WHhTutSugOY57b1VghwS+siGPPmszo9b/b1iAwk8xg
j6/qKKIp1bW2f34Bur7MqPqVPlh8zts6A6M8vUxRk1GzYli2fdfRXyL3oXYMIfus
NK/w3I6l9GPBAFwDTVShFzV9h1M2cWJro7s29ZnDmqVX9lM6spUClAW3o6xm7Gny
```

```
root@valkyrie:~# gpg -e -u "valkyrie" -r "valkyrie" file
```

En este caso sustituir un nombre (“valkyrie”) por el del compañero

```
root@valkyrie:~# gpg --decrypt file.gpg
gpg: encrypted with 3072-bit RSA key, ID 8082F838637B57CB, created 2017-1
1-18
      "valkyrie <valkyrie@random.org>"
hola
```

Ejercicio 2.

Encriptar/Desencriptar con openssl:

Usando aes256:

```
root@valkyrie:~# openssl aes-256-cbc -a -salt -in file -out file.enc
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
```

```
root@valkyrie:~# cat file
hola
root@valkyrie:~# cat file.enc
U2FsdGVkX1+0aZ0st4h5bHdcYovLpt/tOUIxkWRY2H4=
```

```
root@valkyrie:~# openssl aes-256-cbc -d -a -in file.enc -out file.new
enter aes-256-cbc decryption password:
root@valkyrie:~# cat file.new
hola
```

Ejercicio 3.

a) Heartbleed:

Heartbleed es un agujero de seguridad de software en la biblioteca de código abierto OpenSSL, solo vulnerable en su versión 1.0.1f, que permite a un atacante leer la memoria de un servidor o un cliente, permitiéndole por ejemplo, conseguir las claves privadas SSL de un servidor.

Esta vulnerabilidad compromete las claves secretas usadas para identificar los proveedores de servicios o incluso para encriptar el tráfico, los usuarios y contraseñas y hasta el propio contenido.

Permitiéndole a los atacantes escuchar comunicaciones, robar información directamente del servicio o hasta hacerse pasar por servicios y usuarios.

b) Cómo saber si nuestro sistema la sufre:

Como solo es vulnerable la version 1.0.1, podemos comprobar nuestra version de openssl:

```
root@valkyrie:~# openssl
OpenSSL> version
OpenSSL 1.1.0g  2 Nov 2017
OpenSSL>
```

O comprobar nuestro dominio con la página:

https://filippo.io/Heartbleed/

Si vemos la información oficial:

- OpenSSL 1.0.1 through 1.0.1f (inclusive) are vulnerable
- OpenSSL 1.0.1g is NOT vulnerable
- OpenSSL 1.0.0 branch is NOT vulnerable
- OpenSSL 0.9.8 branch is NOT vulnerable

c) Cómo arreglarla:

Para arreglarla lo recomendable es actualizar openssl a la versión más reciente.

Para ubuntu:

```
$> sudo apt-get update
$> sudo apt-get dist-upgrade
```