SEGURIDAD EN SISTEMAS OPERATIVOS

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

Curso 2018-19

Práctica [1]. Administración de la seguridad en Linux

Sesión [5]. Cifrado de archivos

Autor[1]: Matilde Cabrera González

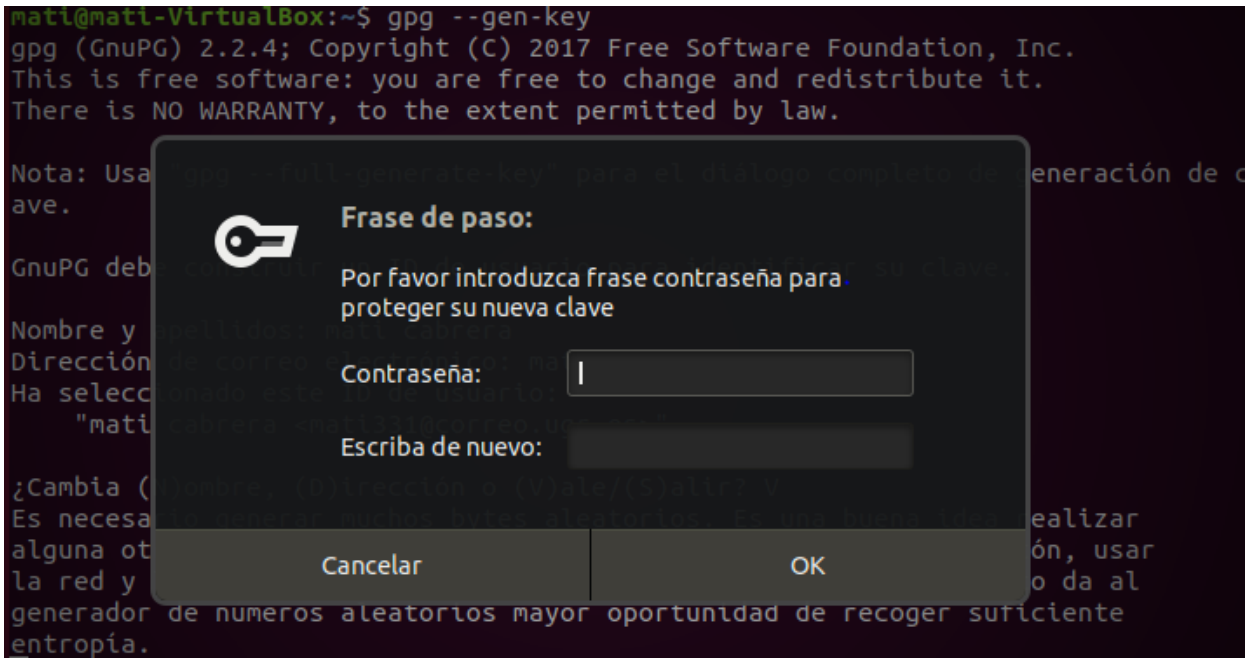
Ejercicio 1.

a) Utiliza la herramienta gpg para crear unas claves personales.

```
mati@mati-VirtualBox:~$ gpg --gen-key
gpg (GnuPG) 2.2.4; Copyright (C) 2017 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Nota: Usa "gpg --full-generate-key" para el diálogo completo de generación de clave.

GnuPG debe construir un ID de usuario para identificar su clave.

Nombre y apellidos: mati cabrera
Dirección de correo electrónico: mati331@correo.ugr.es
Ha seleccionado este ID de usuario:
    "mati cabrera <mati331@correo.ugr.es>"

¿Cambia (N)ombre, (D)irección o (V)ale/(S)alir? V
Es necesario generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/consola, mover el ratón, usar
la red y los discos) durante la generación de números primos. Esto da al
generador de números aleatorios mayor oportunidad de recoger suficiente
entropía.
Es necesario generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/consola, mover el ratón, usar
la red y los discos) durante la generación de números primos. Esto da al
generador de números aleatorios mayor oportunidad de recoger suficiente
entropía.
gpg: clave 0F4FBBDD93F7F984 marcada como de confianza absoluta
gpg: creado el directorio '/home/mati/.gnupg/openpgp-revocs.d'
gpg: certificado de revocación guardado como '/home/mati/.gnupg/openpgp-revocs.d/7CF111E64BE7F3278
BEB439A0F4FBBDD93F7F984.rev'
claves pública y secreta creadas y firmadas.

pub   rsa3072 2018-11-02 [SC] [caduca: 2020-11-01]
      7CF111E64BE7F3278BEB439A0F4FBBDD93F7F984
uid                      mati cabrera <mati331@correo.ugr.es>
sub   rsa3072 2018-11-02 [E] [caduca: 2020-11-01]

mati@mati-VirtualBox:~$
```

Contraseña: mati

[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 ..."



b) Una vez creadas, utilízalas para cifrar y descifrar un archivo.

Intentamos cifrar archivo2:

```
mati@mati-VirtualBox:~$ cat archivo2
F   UID   PID  PPID PRI  NI    VSZ   RSS WCHAN  STAT TTY        TIME COMMAND
4  1000   851   714  20   0 212296  6104 poll_s Ssl+ tty1       0:00 /usr/lib/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=ubuntu gnome-session --session=ubuntu
4  1000   853   851  20   0 478520 117204 ep_pol Sl+ tty1       0:28 /usr/lib/xorg/Xorg vt1 -displayfd 3 -auth /run/user/1000/gdm/Xauthority -background none -noreset -keeptty -verbose 3
0  1000  1095   851  20   0 642312 15236 poll_s Sl+  tty1       0:00 /usr/lib/gnome-session/gnome-session-binary --session=ubuntu
```

```
mati@mati-VirtualBox:~$ gpg --output archivo2encrypt --encrypt archivo2
No ha especificado un ID de usuario (puede usar "-r")

Destinatarios actuales:

Introduzca ID de usuario. Acabe con una línea vacía: mati cabrera

Destinatarios actuales:
rsa3072/885B03CA904D1F9D 2018-11-02 "mati cabrera <mati331@correo.ugr.es>"

Introduzca ID de usuario. Acabe con una línea vacía:
mati@mati-VirtualBox:~$ ls
archivo1  archivo2encrypt  Descargas   Escritorio  matikey_priv.pgp  Música     Público  Vídeos
archivo2  archivo3         Documentos  Imágenes    matikey_pub.pgp   Plantillas  snap
```

```
mati@mati-VirtualBox:~$ cat archivo2encrypt
mati@mati-VirtualBox:~$ gpg --output archivo2enc
 --encrypt archivo2encry
```

Ahora lo desciframos:

```
mati@mati-VirtualBox:~$ gpg --decrypt archivo2encrypt
gpg: cifrado con clave de 3072 bits RSA, ID 885B03CA904D1F9D, creada el 2018-11-02
      "mati cabrera <mati331@correo.ugr.es>"
F   UID   PID  PPID PRI  NI    VSZ   RSS WCHAN  STAT TTY        TIME COMMAND
4  1000   851   714  20   0 212296  6104 poll_s Ssl+ tty1       0:00 /usr/lib/gdm3/gdm-x-session -
-run-script env GNOME_SHELL_SESSION_MODE=ubuntu gnome-session --session=ubuntu
4  1000   853   851  20   0 478520 117204 ep_pol Sl+ tty1       0:28 /usr/lib/xorg/Xorg vt1 -displ
ayfd 3 -auth /run/user/1000/gdm/Xauthority -background none -noreset -keeptty -verbose 3
0  1000  1095   851  20   0 642312 15236 poll_s Sl+  tty1       0:00 /usr/lib/gnome-session/gnome-
session-binary --session=ubuntu
```

c) Agrupate con un compañero e intercambiar un archivo cifrado por cada uno que el otro debe
descifrar.

Para poder utilizar las claves para cifrar otro archivo y mandarlo a un compañero necesito tener la clave pública y privada en diferentes archivos:

```
mati@mati-VirtualBox:~$ gpg --armor --export --output matikey_pub.pgp mati cabrera
mati@mati-VirtualBox:~$ ls
archivo1  archivo3    Documentos  Imágenes         Música      Público  Vídeos
archivo2  Descargas   Escritorio  matikey_pub.pgp  Plantillas  snap
```

```
mati@mati-VirtualBox:~$ cat matikey_pub.pgp
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBFvc0hwBDAC11sLlmpZvoPk4EKwMLAgLWzE7BANA0BR2qMa/dEIuyi6/Cp9j
ns1fNET7hpE7EeMYLIOg2cm1XqgTULyjyq3EoJobZu6K93gFHBA3saD4/feOwyMS
/OhbhJJzCNHev9mb0cO4/JPt4JZoHzW4mRnkWj7vWznKjan6F21ZAU1h3W4uW0ZL
TXOJmoF3PyoQI+nbV/EQpDe2FqE62ua+21Rkqcx2r9L4evrJVJZu2mCB5QgX01dT
/9EKlzn+NCh4tXvPqvsZz1chSijIm2ZzDnlHh8MkGjsXKAs5rh/PldLYrwJ7nzYN
xsv4vxPtZFCJyqXMrt3DJ/S8d4HR+IP1WwyY2LOAwgd4IpbXSmCqO6PdmUSakPgP
jHungiJOrjbJHKX5GpgQom7IE5u2xJxDysfi91hpRsqAb/O14evABEj2ww9yTrtv
g2mx/3MoROgT5A5yR4MBlkzBs2l4cRMiweZ4/ZEg8i73Xy4M2eSpDyKxINYjr3MW
BIvfRMEENG7RlGMAEQEAAbQkbWF0aSBjYWJyZXJhIDxtYXRpMzMxQGNvcnJlby51
Z3IuZXM+iQHUBBMBCgA+FiEEfPER5kvn8yeL60aD0+73ZP3+YQFAlvc0hwCGwMF
CQPCZwAFCwkIBwIGFQoJCAsCBBYCAwECHgECF4AACgkQD0+73ZP3+YQ2Vwv/WdtB
Rq4PKcUA82/oS599fMs7t2LYE1CP2Bg2FilY6ayRcCY+RxPDrdMWdaUfzejKmu6d
7I/p4Xw5Ou9xYxv/MqzWSvUnZMPRlieSmoNTZ5TomV224bf26LzDEIklBH6OeKoy
75VXZxAFQUYq0lBCY+apPz/00wzhpNHY5U6eZKtZSlkFbCPYcNNr8vgOgmNAQ5UW
```

```
mati@mati-VirtualBox:~$ gpg --armor --export-secret-key --output matikey_priv.pgp mati cabrera
mati@mati-VirtualBox:~$ ls
archivo1  archivo3    Documentos  Imágenes         matikey_pub.pgp  Plantillas  snap
archivo2  Descargas   Escritorio  matikey_priv.pgp  Música           Público     Vídeos
mati@mati-VirtualBox:~$ cat matikey_priv.pgp
-----BEGIN PGP PRIVATE KEY BLOCK-----

lQWGBFvc0hwBDAC11sLlmpZvoPk4EKwMLAgLWzE7BANA0BR2qMa/dEIuyi6/Cp9j
ns1fNET7hpE7EeMYLIOg2cm1XqgTULyjyq3EoJobZu6K93gFHBA3saD4/feOwyMS
/OhbhJJzCNHev9mb0cO4/JPt4JZoHzW4mRnkWj7vWznKjan6F21ZAU1h3W4uW0ZL
TXOJmoF3PyoQI+nbV/EQpDe2FqE62ua+21Rkqcx2r9L4evrJVJZu2mCB5QgX01dT
/9EKlzn+NCh4tXvPqvsZz1chSijIm2ZzDnlHh8MkGjsXKAs5rh/PldLYrwJ7nzYN
xsv4vxPtZFCJyqXMrt3DJ/S8d4HR+IP1WwyY2LOAwgd4IpbXSmCqO6PdmUSakPgP
jHungiJOrjbJHKX5GpgQom7IE5u2xJxDysfi91hpRsqAb/O14evABEj2ww9yTrtv
g2mx/3MoROgT5A5yR4MBlkzBs2l4cRMiweZ4/ZEg8i73Xy4M2eSpDyKxINYjr3MW
BIvfRMEENG7RlGMAEQEAAf4HAwIYYUFEDvFwUOO/5taFXjUau35Xm3z52gCxz729
```

Tendré que enviar y recibir la clave publica, con la clave pública del compañero cifro “archivo3”

obteniendo como resultado “archivo3.asc” y se lo mando para que el compañero lo descifre:

```
mati@mati-VirtualBox:~$ gpg --import jorge_pubkey.gpg
gpg: clave 68350B92E99C8C5D: clave pública "Jorge Soler Padial (Seguridad en Sis
temas Operativos) <gorgue@correo.ugr.es>" importada
gpg: Cantidad total procesada: 1
gpg:               importadas: 1
mati@mati-VirtualBox:~$ gpg --armor --recipient gorgue@correo.ugr.es --encrypt a
rchivo3
gpg: C8DBB56C9E4DC0C4: No hay seguridad de que esta clave pertenezca realmente
al usuario que se nombra
sub  rsa4096/C8DBB56C9E4DC0C4 2018-11-08 Jorge Soler Padial (Seguridad en Sistem
as Operativos) <gorgue@correo.ugr.es>
 Huella clave primaria: D169 648F 9188 039C F005  2EBE 6835 0B92 E99C 8C5D
      Huella de subclave: E348 AB32 5C0A D621 575D  9D95 C8DB B56C 9E4D C0C4

No es seguro que la clave pertenezca a la persona que se nombra en el
identificador de usuario. Si *realmente* sabe lo que está haciendo,
puede contestar sí a la siguiente pregunta.

¿Usar esta clave de todas formas? (s/N) s
```

El compañero me envía “texto.txt.asc” cifrado con mi clave publica antes enviada. Vamos a proceder a descifrarlo y guardar la salida en “texto.txt”, mostramos su contenido:

```
mati@mati-VirtualBox:~$ gpg --decrypt texto.txt.asc --output texto.txt
gpg: Atención: "--output" no se considera una opción
uso: gpg [opciones] --decrypt [filename]
mati@mati-VirtualBox:~$ gpg --output texto.txt --decrypt texto.txt.asc
gpg: cifrado con clave de 3072 bits RSA, ID 885B03CA904D1F9D, creada el 2018-11-
02
      "mati cabrera <mati331@correo.ugr.es>"
mati@mati-VirtualBox:~$ ls
archivo1             archivo3      Imágenes          Plantillas     Vídeos
archivo2             archivo3.asc  jorge_pubkey.gpg  Público
archivo2_aes.enc     Descargas     matikey_priv.pgp  snap
archivo2_descifrado  Documentos    matikey_pub.pgp   texto.txt
archivo2encrypt      Escritorio    Música            texto.txt.asc
mati@mati-VirtualBox:~$ cat texto.txt
Este Fichero solo lo puede leer Mati
mati@mati-VirtualBox:~$
```

Ejercicio 2.

Utiliza la herramienta openssl para cifrar y descifrar un archivo con un algoritmo y clave de tu elección.

Vamos a usar cifrado simétrico aes-256-ofb visto en la asignatura SPSI, se hacen bloques de 256b, el modo ofb es un cifrado por flujo, donde un bloque depende del anterior.

```
mati@mati-VirtualBox:~$ openssl enc -aes-256-ofb -in archivo2 -out archivo2_aes.enc
enter aes-256-ofb encryption password:
Verifying - enter aes-256-ofb encryption password:
mati@mati-VirtualBox:~$ ls
archivo1          archivo2encrypt  Documentos  matikey_priv.pgp  Plantillas  Vídeos
archivo2          archivo3         Escritorio  matikey_pub.pgp   Público
archivo2_aes.enc  Descargas        Imágenes    Música            snap
mati@mati-VirtualBox:~$ xxd archivo2_aes.enc
00000000: 5361 6c74 6564 5f5f d77c 11ea d9c7 00ed  Salted__.|......
00000010: 9991 1a8a 973f e38a 41f9 c18c caf7 9987  .....?..A.......
00000020: 0d6b e03f dbd9 aa3f fcab 1e38 0809 6926  .k.?...?...8..i&
00000030: abb4 6ca9 2ff8 6e82 bc41 f4f7 6945 7b3e  ..l./.n..A..iE{>
00000040: ef92 00ac 0b7c 7de2 83b3 6b95 bb35 f9a6  .....|}...k..5..
00000050: 96b8 a762 75b2 ed79 3be1 1400 6dc8 f9df  ...bu..y;...m...
00000060: e382 f2fb 241f abd7 9a56 198c 3b77 2ca8  ....$....V..;w,.
00000070: b65d 69dc bc30 fce8 a16b ac25 009a bdc6  .]i..0...k.%....
00000080: 80ba 59aa 2fcc 3cbd 89b7 f40c ac9a 3445  ..Y./.<.......4E
00000090: 50f8 c806 621e 0d6d c292 f914 2193 e342  P...b..m....!..B
000000a0: 37d5 4265 5a2a 8664 c9a9 7e89 84cc a419  7.BeZ*.d..~.....
000000b0: 84e6 53fe d8fd 01f2 5da2 9bcf d4f4 f220  ..S.....]...... 
000000c0: 4ef6 36ab aa1b ec68 1e6b da2c 2263 f1e6  N.6....h.k.,"c..
000000d0: 9b41 e536 3175 95f1 8415 7be7 e18d f51b  .A.61u....{.....
000000e0: 98e3 4f60 6a75 2514 5e22 828f e8a6 5b64  ..O`ju%.^"....[d
000000f0: 9028 ab66 f827 1a30 208c 8b7e 2bad 91f2  .(.f.'.0 ..~+...
00000100: 7b5f f938 4b12 9b0d ec17 1bf8 13e1 4c68  {_.8K.........Lh
00000110: f839 7993 00e9 2c5d bcce c101 dd2e f70b  .9y...,]........
00000120: d62b 9679 6e6f 95a5 263b 9423 85e6 ad39  .+.yno..&;.#...9
00000130: bf66 a98f b546 ed0e a272 4183 ef8c f5cd  .f...F...rA.....
00000140: 7148 3f1a 63b8 a4e5 7a84 ec96 1a95 7bde  qH?.c...z.....{.
00000150: 451d c31b efc3 45d6 91bc 33ba 0be0 eda3  E.....E...3.....
00000160: a059 a8fc aec6 af54 c237 4ce0 7c36 356a  .Y.....T.7L.|65j
00000170: b267 cccc c966 f0cf 3f07 0900 5635 8114  .g...f..?...V5..
00000180: 5c3f 8696 16b2 b480 c70a b05c 73e4 b521  \?.........\s..!
00000190: f19d 6b39 e296 d1de 8ae7 e5e7 28e8 83a2  ..k9........(...
000001a0: fa7b 7187 ae02 d28d 9f2b 16f3 a789 0930  .{q......+.....0
000001b0: 5e06 73a6 69df 0794 1441 d189 6dbb 74be  ^.s.i....A..m.t.
000001c0: a1d0 b686 6b89 7536 606d 501c 7340 0c7b  ....k.u6`mP.s@.{
000001d0: aa28 bc02 9cf0 6f1b 958c 12d6 7fa2 954b  .(....o........K
000001e0: b99e 7a75 39c8 fbfc 877a d6c5 8cd6 0bde  ..zu9....z......
000001f0: 97cf 1041 5255 8f71 2f3f d8ad 0212 7209  ...ARU.q/?....r.
00000200: 6a56 7a6d 396e 7b32 c015 0c6d 4131 948c  jVzm9n{2...mA1..
00000210: b34b b050 2ad2 98e5 c895 1149 25c5 5879  .K.P*......I%.Xy
00000220: 919d 561f d368 8804 575c 0dd4 94ca 0916  ..V..h..W\......
00000230: 2fe3 6b23 c5e8 60e1 a80f 132d ee6f ea3b  /.k#..`....-.o.;
00000240: 3d26 3831 1d26 54bb 9ac2 628a            =&81.&T...b.
mati@mati-VirtualBox:~$
```

Clave usada: mati. Ahora vamos a descifrar el mismo archivo, para ello usamos la opción -d. El resultado lo guardamos en archivo2_descifrado y lo visualizamos para ver el resultado.

```
mati@mati-VirtualBox:~$ openssl enc -aes-256-ofb -d -in archivo2_aes.enc -out archivo2_descifrado
enter aes-256-ofb decryption password:
mati@mati-VirtualBox:~$ cat archivo2_descifrado
F   UID   PID  PPID PRI  NI    VSZ   RSS WCHAN  STAT TTY        TIME COMMAND
4  1000   851   714  20   0 212296  6104 poll_s Ssl+ tty1       0:00 /usr/lib/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=ubuntu gnome-session --session=ubuntu
4  1000   853   851  20   0 478520 117204 ep_pol Sl+ tty1       0:28 /usr/lib/xorg/Xorg vt1 -displayfd 3 -auth /run/user/1000/gdm/Xauthority -background none -noreset -keeptty -verbose 3
0  1000  1095   851  20   0 642312 15236 poll_s Sl+  tty1       0:00 /usr/lib/gnome-session/gnome-session-binary --session=ubuntu

mati@mati-VirtualBox:~$
```

Ejercicio 3.

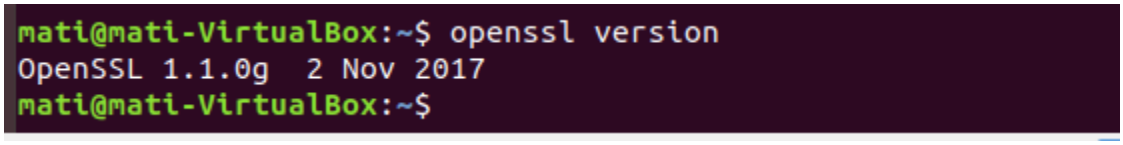
Busca información sobre esta vulnerabilidad para contestar a las siguientes cuestiones:
• Heartbleed
En abril de 2004 se detectó una importante vulnerabilidad en la biblioteca criptográfica openssl conocida con el nombre “heartbleed” que afectó a más de la mitad de los servidores mundiales. Puede tener más detalles de la misma en http://heartbleed.com, y en multitud de artículos publicados en Internet dada su relevancia.

a) ¿En qué consiste la misma?
El error Heartbleed es una grave vulnerabilidad en la biblioteca de software criptográfico OpenSSL. Esta debilidad permite robar la información protegida, en condiciones nomales, por el cifrado SSL / TLS utilizado para proteger Internet. SSL /TLS proporciona seguridad de comunicación y privacidad a través de Internet para aplicaciones como web, correo electrónico, mensajería instantánea (IM) y algunas redes privadas virtuales (VPN).

El error Heartbleed permite que cualquier persona en Internet lea la memoria de los sistemas protegidos por las versiones vulnerables del software OpenSSL. Esto compromete las claves secretas utilizadas para identificar a los proveedores de servicios y para cifrar el tráfico, los nombres y contraseñas de los usuarios y el contenido real. Esto permite a los atacantes espiar las comunicaciones, robar datos directamente de los servicios y usuarios y suplantar servicios y usuarios.

b) ¿Cómo saber si nuestro sistema la sufre?

Actualmente esta versión no se instala por defecto, no la tengo en el dispositivo de las practicas, aunque si la tuve que poner en otra maquina por darme un error la versión openssl 1.1.0g



c) ¿Cómo podemos subsanarla?

En la misma página de openssl se muestran sus vulnerabilidades https://www.openssl.org/news/vulverabilities.html.

La mejor forma de subsanar esta vulnerabilidad es teniendo el equipo lo mas actualizado posible, la versión usada por defecto como podemos ver en el ejercicio anterior es la 1.1.0 pero ya está la versión 1.1.1

Para tener el equipo actualizado, tenemos las ordenes sudo “apt-get update” y sudo “apt-get upgrade”. O si quieres probar una versión especifica se puede descargar desde la página oficial https://www.openssl.org/source/old/, o siguiendo los siguientes pasos:

cd /usr/local/src

sudo wget -c https://www.openssl.org/source/openssl-1.1.1-pre9.tar.gz

sudo cp openssl-1.1.1-pre9.tar.gz /opt

cd /opt/

sudo tar xvfz openssl-1.1.1-pre9.tar.gz

cd /opt/ openssl-1.1.1-pre9

sudo ./config --prefix=/usr/local/openssl --openssldir=/usr/local/openssl

sudo make

sudo make install

SI NO DA FALLO EL MAKE

sudo rm /usr/bin/openssl

sudo ln -s /usr/local/openssl/bin/openssl /usr/bin/openssl

openssl version

Este ejemplo es para instalar la última versión disponible de openssl, probado en una máquina virtual, pero serviría para cualquier versión que queramos probar.