DESPLEGAR SITIO HTTPS APACHE UBUNTU

PABLO HORCAJADA GONZALEZ y PABLO BÉJAR THOMAS

Profesor: Guillermo Bellettini

Fecha 28/01/2021

Clase: Despliegue Web

Contenido

Configuración Inicial

Instalación paquetes necesarios

Openssl

```
root@ubu-VirtualBox:~# apt-get install openssl
```

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be upgraded:
  openssl
1 upgraded, 0 newly installed, 0 to remove and 491 not upgraded.
Need to get 0 B/613 kB of archives.
After this operation, 1.024 B disk space will be freed.
(Reading database ... 126222 files and directories currently installed.)
Preparing to unpack .../openssl_1.1.1-1ubuntu2.1~18.04.14_amd64.deb ...
Unpacking openssl (1.1.1-1ubuntu2.1~18.04.14) over (1.1.1-1ubuntu2.1~18.04.4) .
..
Setting up openssl (1.1.1-1ubuntu2.1~18.04.14) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
```

Apache2

```
root@ubu-VirtualBox:~# apt-get install apache2
```

-Nos preguntará si queremos continuar, por lo que diremos que “y”.

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.2-0
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.2-0
0 upgraded, 9 newly installed, 0 to remove and 491 not upgraded.
Need to get 1.713 kB of archives.
After this operation, 6.932 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

t

```
Processing triggers for libc-bin (2.27-3ubuntu1) ...
Processing triggers for ureadahead (0.100.0-21) ...
Processing triggers for systemd (237-3ubuntu10.24) ...
Processing triggers for ufw (0.36-0ubuntu0.18.04.1) ...
root@ubu-VirtualBox:~#
```

Entidad Certificadora

Creación de claves publica y privada

```
root@ubu-VirtualBox:~# openssl genrsa -des3 -out ca.key 4096
```

-Nos pedirá una contraseña dos veces (para verificar). En este caso será “Madrid01”.

```
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................................
.....................................................................++++
.....................++++
e is 65537 (0x010001)
Enter pass phrase for ca.key:
Verifying - Enter pass phrase for ca.key:
```

Comprobación claves

-Comprobamos que se ha creado el fichero.

```
root@ubu-VirtualBox:~# ls -la ca.key
-rw------- 1 root root 3311 ene 28 11:45 ca.key
```

-Comprobamos el contenido de dicho fichero.

```
root@ubu-VirtualBox:~# cat ca.key
```

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,3813D8306C556736

PVDqHvB4hf5RZw+ysd4qE+W+jqYfmj+OkgUjcetsWjWGAYLKCLj2/giMwSkIsrj5
kQ90AmT5diKSzTTplDL32wPPiCgYJU4wasqlZKZsB7KfxZYcu5i3etn5JqggKl0F
fJZNtdTe4hWqkM6zc3b6tgIaYYIgTamzMVaeMDbLD54eunMTWJ0vzF6f1GkH6jQM
RsnUxsn2yCQa1W/eHzW04zLx2Wtngr3w+ZXrsigp+SivGb410UwE5mzwWykyJe8u
cSF/YG585xoRzDMYP52J+QTTbXgr1GSo4biNNgN4DGVZCrXcWHOlq+3QX/VQtNF1
9/vVVP+CZlQQbtX2n8QbkX04s8y8GxfoIarwh9A+cAUivgrff0qyU+rMbttT6HU9
nCjBjWsIFlMlzLp3yziAajNbrD4H3fN89RZYwJvlNrdnMIC30x5fM5+YL39mA4TT
iHfGXP2lEDmGafJ8VKJht3oqkNv26Il74IxOEysIwquMZ8Pf6xg34w6u9rzgxEer
rqRlorg7cvDINHJx8RGeMqIrmy/Ak96rDDAqrAfg4ECf0SiYOHz5CBIyiQJsSeZO
xZ19giDq3TLJdltMBvRjwfSu8cL0SqsHhAlUnRgzCMJ9M4hrMscdghLjv/CqB6X+
uSyFBvip2ebYCGpXuDa2+3Dx9BquaAKXRldL4+nji0SRtR6CrYv6XpsPCfOqChBB
```

Creación certificada

```
root@ubu-VirtualBox:~# openssl req -new -x509 -days 365 -key ca.key -out ca.crt
```

-Nos pedirá una contraseña, en este caso “Madrid01”.

```
root@ubu-VirtualBox:~# openssl req -new -x509 -days 365 -key ca.key -out ca.crt

Enter pass phrase for ca.key:
```

-Nos pedirá los datos de: país, provincia, localidad, organización, nombre y correo.

```
Enter pass phrase for ca.key:
Can't load /root/.rnd into RNG
140026252304832:error:2406F079:random number generator:RAND_load_file:Cannot op
en file:../crypto/rand/randfile.c:88:Filename=/root/.rnd
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Madrid
Locality Name (eg, city) []:Madrid01
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Daw Despliegue
Organizational Unit Name (eg, section) []:Daw
Common Name (e.g. server FQDN or YOUR name) []:Pablo
Email Address []:pablodespliegue@ceu.es
```

Servidor Web Seguro

Creación cavles publica y privada

```
root@ubu-VirtualBox:~# openssl genrsa -des3 -out server.key 4096
```

-Nos pedirá una contraseña dos veces (para verificar). En este caso será “Madrid01”.

```
Generating RSA private key, 4096 bit long modulus (2 primes)
..............................++++
.........................................++++
e is 65537 (0x010001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
```

Comprobación creación clave privada servidor

-Comprobamos que se ha creado el fichero.

```
root@ubu-VirtualBox:~# ls -la server.key
-rw------- 1 root root 3311 ene 28 11:51 server.key
```

-Comprobamos el contenido de dicho fichero.

```
root@ubu-VirtualBox:~# cat server.key
```

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,FC4A444307796357

evxtP7GMqh5BbuaNjcSh9wqTiWFZH/H6OEHZIWvYyFuS2hoBXLwqtbeIkQIBKxQ8
bJg5RLUde7uOFjwRtoXO07MKkNYwVOb5+sRVEWjW2aj2WQ9fPGYO0DEaGdXwkalm
OeeUoMWuKYQTz3Wmu9QfPY2/Zw7woa7QNvlAke3VP6oeUGvE0gdEQO/KGma4SNUH
anqzUPTuMYyw5S26//DXwyOIFCajPZkMVui3n6ODgwNJeYRewLmiUH4mOXiCMBqq
R+w+npSXEviqpDDBPcvJuTQfR8Dk8SpqyuxQO2D5nZRsinmoP06Uu2kH1jA0ZmrV
dmwTB9uGqXKcMVIB5nnzJuq4qeWQ3348hbPQOAHq9NPGqFgAuOaa1ZsaSRJPirAI
```

Petición de creación petición certificado

```
root@ubu-VirtualBox:/# openssl req -new -key server.key -out server.csr
```

-Nos pedirá la contraseña y acto seguido que rellenemos unos datos.

```
Enter pass phrase for server.key:
Can't load /root/.rnd into RNG
139747591971264:error:2406F079:random number generator:RAND_load_file:Cannot o
en file:../crypto/rand/randfile.c:88:Filename=/root/.rnd
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Madrid
Locality Name (eg, city) []:Madrid
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Daw Despliegue
Organizational Unit Name (eg, section) []:Daw
Common Name (e.g. server FQDN or YOUR name) []:Pablo
Email Address []:pablodespliegue@ceu.es
```

-Y unos datos extra.

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:pablo
An optional company name []:pablo2
```

Comprobación Certificado

```
root@ubu-VirtualBox:/# ls -la server.csr
-rw-r--r-- 1 root root 1809 ene 30 12:47 server.csr
```

-Comprobamos el contenido de dicho archivo con los datos que hemos rellenado cifrados.

```
root@ubu-VirtualBox:/# cat server.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIFADCCAugCAQAwgY0xCzAJBgNVBAYTAkVTMQ8wDQYDVQQIDAZNYWRyaWQxDzAN
BgNVBAcMBk1hZHJpZDEXMBUGA1UECgwORGF3IERlc3BsaWVndWUxDDAKBgNVBAsM
A0RhdzEOMAwGA1UEAwwFUGFibG8xJTAjBgkqhkiG9w0BCQEWFnBhYmxvZGVzcGxp
ZWd1ZUBjZXUuZXMwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQC2mvlO
WqO9Zg29rZdkjpVdV+jfeX65BqJfwW8Nh7UpQtzWDw91e+WAYeAlHEtqPVTGme7+
3iVTztjU3L3yE4dbYfvfYVmm4ckQFYVnlnft97+OMp1sm2piYDaNkcLVbV1QoJUd
xghILOmoiMQ3Jn+3kqiTCCIsUxEjqdc0fnYX8jYjlOzJtrNM9xFTE/OERVKRiHyu
tkFY2nFT6lKcclS6JI4sfboTm4LBDn2o1W5xhT6krtG6qMTi+nicc+mQsK6ZGEno
```

-Firmamos el certificado con el cable publica.

```
root@ubu-VirtualBox:/# openssl x509 -req -days 365 -in server.csr -CA ca.crt -C
Akey ca.key -set_serial 01 -out server.crt
```

-Nos pedirá la contraseña para verificar.

```
Signature ok
subject=C = ES, ST = Madrid, L = Madrid, O = Daw Despliegue, OU = Daw, CN = Pab
lo, emailAddress = pablodespliegue@ceu.es
Getting CA Private Key
Enter pass phrase for ca.key:
```

Configuración ficheros

Comprobación ficheros apache2

-Accedemos a la siguiente ruta para ver los ficheros que se han instalado con apache2.

```
root@ubu-VirtualBox:~# cd /etc/apache2/sites-available
root@ubu-VirtualBox:/etc/apache2/sites-available#
```

-Comprobamos que los ficheros se han instalado con un "ls".

```
root@ubu-VirtualBox:/etc/apache2/sites-available# ls
000-default.conf  default-ssl.conf
```

Accesibilidad del servidor web seguro a las claves

-Movemos las claves y el certificado a otra carpeta para que el servidor las pueda encontrar.

```
root@ubu-VirtualBox:/# mv server.key /etc/ssl/private/server.key
```

```
root@ubu-VirtualBox:/# mv server.crt /etc/ssl/certs/server.crt
```

-Comprobamos que se encuentran en los directorios correspondientes.

```
root@ubu-VirtualBox:/etc/ssl/certs# ls -la server.crt
-rw-r--r-- 1 root root 1992 ene 30 12:59 server.crt
```

```
root@ubu-VirtualBox:/etc/ssl/private# ls -la server.key
-rw------- 1 root root 3311 ene 28 11:51 server.key
```

-Accedemos al fichero generado por apache para añadir los valores adecuados.

```
root@ubu-VirtualBox:/# nano /etc/apache2/sites-available/default-ssl.conf
```

-Comentamos estas dos líneas.

```
 #SSLCertificateFile      /etc/ssl/certs/ssl-cert-snakeoil.pem
 #SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
```

-Añadimos los valores que contienen los ficheros anteriores.

```
#   A self-signed (snakeoil) certificate can be created by ins$
#   the ssl-cert package. See
#   /usr/share/doc/apache2/README.Debian.gz for more info.
#   If both key and certificate are stored in the same file, o$
#   SSLCertificateFile directive is needed.
#SSLCertificateFile      /etc/ssl/certs/ssl-cert-snakeoil.pem
#SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
SSLCertificateFile /etc/ssl/certs/server.crt
SSLCertificateKeyFile /etc/ssl/private/server.key
```

Habilitación SSL Apache

-Habilitamos el modo ssl de apache.

```
root@ubu-VirtualBox:/# a2enmod ssl
```

-Para activarlo, no pedirá que reiniciamos apache.

```
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create
self-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
```

-Reiniciamos apache.

```
root@ubu-VirtualBox:/# systemctl restart apache2
```

-Activamos el archivo por defecto de “default-ssl”.

```
root@ubu-VirtualBox:/# a2ensite default-ssl.conf
```

-Para activarlo, no pedirá que recarguemos apache.

```
Enabling site default-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
```

-Recargamos apache2.

```
root@ubu-VirtualBox:/# systemctl relaod apache2
```

-Accedemos al directorio donde están los archivos de configuración para ver si están activado (al estar en verdes, significan que lo están).

```
root@ubu-VirtualBox:/etc/apache2/sites-enabled# ls
000-default.conf  default-ssl.conf
```

-Reiniciamos apache.

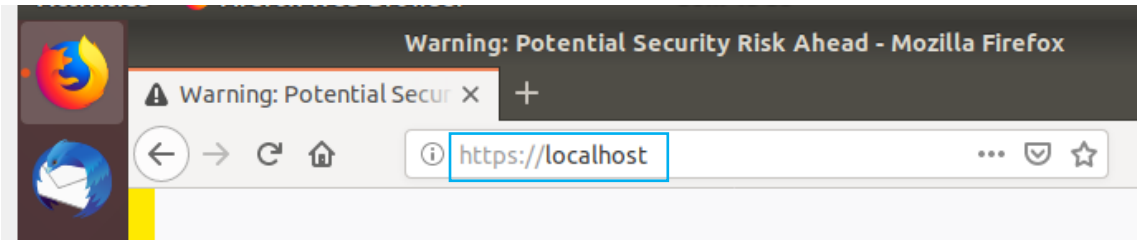
```
root@ubu-VirtualBox:/# systemctl restart apache2
```

-Introducimos la contraseña que hemos puesto en los certificados (Madrid01).

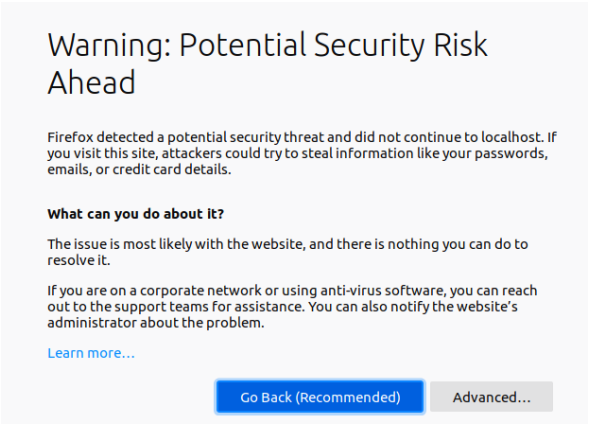
```
Enter passphrase for SSL/TLS keys for 127.0.1.1:443 (RSA): ********
```

Comprobación funcionamiento servidor web

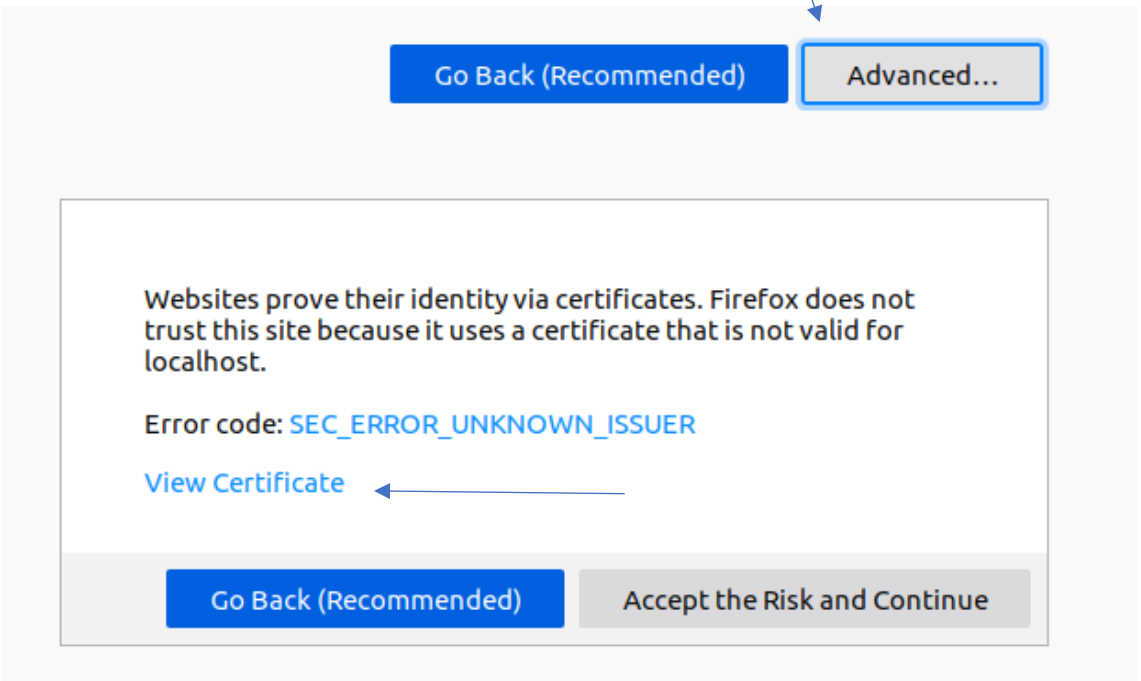
-Abrimos el navegador y nos vamos a la siguiente dirección.



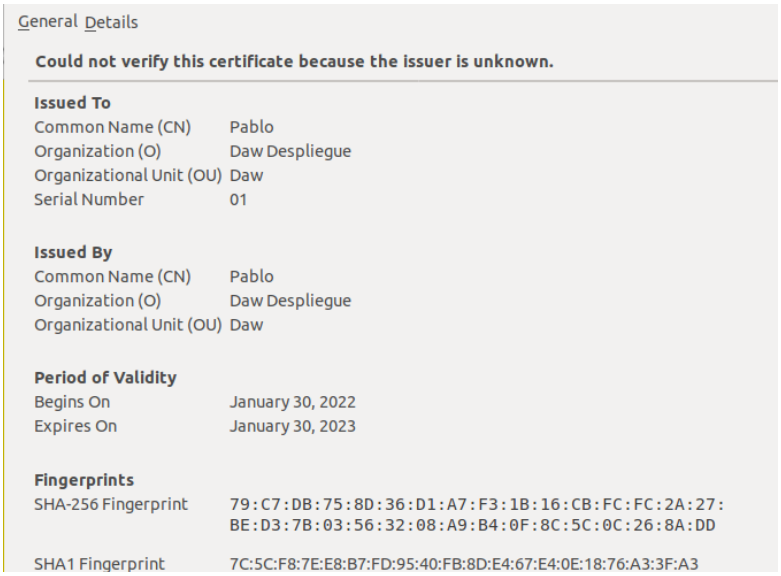
-Vemos que nos muestra un aviso en el certificado, por lo que hemos hecho todo lo anterior correctamente.



-Accedemos el certificado para asegúranos que es el nuestro.



-Comprobamos finalmente que el certificado contiene nuestros datos.



-Aceptamos los riegos y continuamos para ver que el certificado funciona y se ha guardado correctamente y podemos acceder a la página.