Seguridad II

Actividad 1

1.1. ¿Que es una Autoridad de Certificación (CA)? ¿Qué función desarrolla durante la fase de “handshaking” del protocolo **https**? Explicalo con tus palabras.

Una Autoridad de Certificación es una entidad de confianza, encargada de verificar sitios web y otras entidades.
- Confirman la identidad del titular certificado: Garantiza que la web es de quien dice ser.
- Emisión de certificados: Emite los certificados que garantizan que la identidad es valida.
-Desmostracion de la validez de los certificados: Demuestra que los certificados emitidos continúan siendo validos y no han sido manipulados.

1.2. Visita las páginas web siguientes y consulta la información del certificado de servidor que se utiliza. Completa el siguiente cuadro:

Web	Autoridad de Certificación	Validez	Algoritmo de firmado
https://www.digicert.com/	DigiCert, Inc.	Emitido el: lunes, 18 de abril de 2022, 2:00:00 Vencimiento el: viernes, 5 de mayo de 2023, 1:59:59	Huella digital SHA-256: A2 26 BC F5 13 62 20 5E AD 89 7B 8D 36 F8 F6 F8 55 90 F4 9E E8 70 1C 4E 99 DB 84 10 21 7B 66 ED Huella digital SHA-1: 2B EB D6 FE AE C1 C2 EF 43 6C EB 66 5A 4C 31 72 93 74 48 82
https://www.bbva.es/	DigiCert Inc	Emitido el: jueves, 5 de mayo de 2022, 2:00:00 Vencimiento el: miércoles, 10 de mayo de 2023, 1:59:59	Huella digital SHA-256: 5F 84 A0 6D 0F 03 54 47 30 D7 42 C0 7B 77 02 2B E2 30 F8 DD 33 4C D1 BA E5 6A 1F 75 87 CD BE 83 Huella digital SHA-1: 08 52 A9 96 C8 F4 F4 9A B6 6D 6E DB 39 70 BF 23 90 AF E2 79
https://www.pccoste.es/	Let's Encrypt	Emitido el: viernes, 14 de octubre de 2022, 9:21:26 Vencimiento el: jueves, 12 de enero de 2023, 8:21:25 (El certificado no es valido)	Huella digital SHA-256: 63 F7 E6 D2 34 50 C8 C2 37 02 03 82 CA 54 BE A0 8C 8B 68 64 CC D0 D0 6D 4B 54 67 53 A8 DD 7E A9 Huella digital SHA-1: 41 EC 16 E2 75 5E B8 89 14 86 0F 3F 46 90 59 8D F9 62 3A 04
https://adsalsa.com/	Let's Encrypt	Emitido el: sábado, 24 de septiembre de 2022, 23:47:59 Vencimiento el: viernes, 23 de diciembre de 2022, 22:47:58	Huella digital SHA-256: 9A 87 4E 4E 39 3D 14 96 F5 94 C3 09 9B 0A 61 EF 91 F8 7D A6 39 D6 DA AA 44 D5 8C A5 4B 13 D0 63 Huella digital SHA-1: 01 D4 D0 83 1C 60 B2 B5 54 CF F6 8F E5 08 D1 BC A1 68 C4 8B

1.3 Investiga qué significado tienen los siguientes símbolos que aparecen al acceder a páginas web, mediante el protocolo https y Firefox:

- Candado verde: Se ha realizado la conexión con la pagina cuya dirección web aparece en la barra de direcciones y la conexión entre Firefox y el sito web está cifrada.
- Candado gris tachado en rojo: La conexión entre Firefox y la pagina web solo esta parcialmente encriptada.
- Candado gris con triangulo amarillo: La conexión entre Firefox y la pagina solo esta encriptada parcialmente y/o el certificado es autofirmado o no lo a emitido una entidad verificada.

1.4 ¿Qué diferencia existe entre la criptografía simétrica y la asimétrica?

En la criptografía simétrica, la información se cifra con una única clave y se descifra con la misma.
En la cartografiara asimétrica, existen dos claves, una privada y otra publica, con la publica se cifra la información y con la privada, se descifra.

1.5 ¿Qué significa el concepto de intercambio de claves entre cliente y servidor en el contexto de HTTPS?

En estos casos, la información esta cifrada de forma asimétrica, por lo tanto, se utilizan una clave publica y una privada para encriptar y desencriptar la información. El navegador, cifra una clave con la clave publica del servidor y la envía, entonces en este momento, tanto el servidor como el cliente disponen de la misma clave para cifrar y descifrar la información.

Actividad 2

Configura el vhost que atiende al dominio backoffice.ddaw.es configurado en la práctica 1 de la unidad para que solo atienda a peticiones https. Para eso tendrás que:
1. Crear un certificado autofirmado y la clave privada correspondiente.
2. Crear un nuevo vhost que atienda las peticiones https para el dominio correspondiente.
3. Crear una redirección permanente del tráfico del vhost, de http a https. En este enlace puedes encontrar información de cómo hacerlo.

- Instalar las librerias y herramientas openssl:

apt-get install openssl libssl-dev
sudo a2enmod ssl
systemctl restart apache2

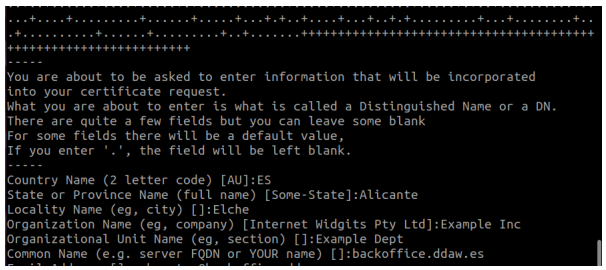
- Crear el certificado de servidor y la carpeta donde se guardara:

sudo mkdir -p /etc/ssl/01-es-ddaw-backoffice

cd /etc/ssl/01-es-ddaw-backoffice

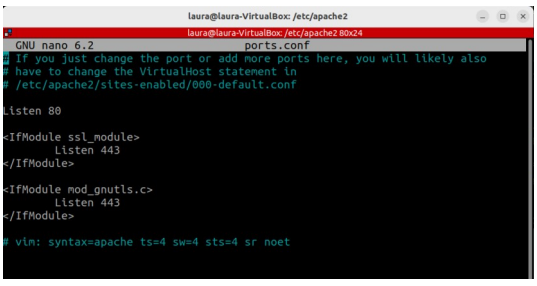
sudo openssl req -new -x509 -nodes -days 365 -newkey rsa:2048 -out /etc/ssl/01-es-ddaw-backoffice/server.crt -keyout /etc/ssl/01-es-ddaw-backoffice/server.key

- Seguir los pasos que te pide el comando:



- Comprobamos que nuestro servidor escuche por el puerto 443:

cd etc/apache2
sudo nano ports.conf



En nuestro caso, ya esta, si no es así, habría que incorporarlo.

- Añadimos las directivas necesarias al VirtualHost correspondiente:
cd /etc/apache2/sites-available
sudo nano 003-es-ddaw-backoffice.conf
(Resaltado aparecen los cambios en el fichero)

VirtualHost *:80>
ServerAdmin webmaster@localhost
ServerName backoffice.ddaw.es
ServerAlias www.backoffice.ddaw.es
DocumentRoot /var/www/01-es-ddaw-backoffice
ErrorLog ${APACHE_LOG_DIR}/003-es-ddaw-backoffice-error.log
CustomLog ${APACHE_LOG_DIR}/003-es-ddaw-backoffice-access.log combined
</VirtualHost>
<VirtualHost _default_:443>
ServerName backoffice.ddaw.es
DocumentRoot /var/www/01-es-ddaw-backoffice
SSLEngine On
SSLCertificateFile /etc/ssl/01-es-ddaw-backoffice/server.crt
SSLCertificateKeyFile /etc/ssl/01-es-ddaw-backoffice/server.key
</VirtualHost>

- Se activa con el comando a2ensite, se comprueba que los archivos están correctos y se reinicia el servidor:

sudo a2ensite 003-es-ddaw-backoffice.conf
sudo apache2ctl configtest
sudo systemctl restart apache2

- Accedemos a la direccion: https://backoffice.ddaw.es/

Vemos que se accede correctamente

- Crear una redirección permanente a este dominio.

cd /etc/apache2/sites-available
sudo nano 003-es-ddaw-backoffice.conf

(Resaltado aparecen los cambios en el fichero)

<VirtualHost *:80>
ServerAdmin webmaster@localhost
ServerName backoffice.ddaw.es
ServerAlias www.backoffice.ddaw.es
DocumentRoot /var/www/01-es-ddaw-backoffice
Redirect permanent / https://backoffice.ddaw.es
ErrorLog ${APACHE_LOG_DIR}/003-es-ddaw-backoffice-error.log
CustomLog ${APACHE_LOG_DIR}/003-es-ddaw-backoffice-access.log combined
</VirtualHost>
<VirtualHost _default_:443>
ServerName backoffice.ddaw.es
DocumentRoot /var/www/01-es-ddaw-backoffice
SSLEngine On
SSLCertificateFile /etc/ssl/01-es-ddaw-backoffice/server.crt
SSLCertificateKeyFile /etc/ssl/01-es-ddaw-backoffice/server.key
</VirtualHost>

Tras este ultimo cambio, entra directamente con la direccion anterior a la nueva direccion con https