Pràctica 4: Llocs webs segurs. Autenticació i encriptació amb HTTPS

1- Introducció

a) HTTPS és el resultat d'afegir una capa de software que implementa el protocol SSL/TLS per sota de la capa que implementa el protocol HTTP. Per tant, HTTPS no és un protocol per ell mateix sino la combinació de HTTP sobre SSL/TLS. Tots dos protocols són de nivell d'aplicació.

b) SSL/TLS són protocols criptogràfics que permeten afegir autenticació i privacitat (per mitjà de l'encriptació de dades) a les comunicacions. TLS (Seguretat de Capa de Transport) és l'evolució del protocol SSL (Capà de Connexió Segura). Les versions de TLS utilizades avui dia són les 1.0, 1.1 i 1.2. L'última versió de SSL va ser la 3.0.

c) Per mitjà de HTTPS es pot afegir **autenticació** del servidor i també si és necessari, del client. L'autenticació del servidor assegura al client que "el servidor és realment qui diu que és",

d) Per realitzar la autenticació d'un servidor, cal que tingui instal.lat un **certificat**. Les comunicacions segures per mitjà de SSL/TLS utilitzen certificats norma **X.509**. Aquests certificats permeten l'**autenticació** per mitjà d'un sistema de criptografia asimètrica coneguda amb el nom de criptografia de clau pública.

e) Per mitjà de HTTPS es pot afegir **privacitat** (o **confidencialitat**) a les comunicacions entre el client i el servidor web. Per tant, podem establir connexions segures tot i que la xarxa en la qual ens trobem sigui insegura (per exemple, una wifi). Per afegir privacitat s'utilitza un sistema de criptografia de clau simètrica que xifrar les les dades entre el client i servidor. La clau simètrica canvia a cada sessió de connexió. El servidor i el client s'intercanvien la clau de simètrica que s'utilitza a cada sessió de connexió per mitjà d'un sistema de criptografia asimètrica.

f) El **certificat** és molt important perquè assegura l'autenticitat d'una o de les dues parts de la comunicació. Es pot assegurar l'autenticitat del servidor, del client o de tots 2 a l'hora. Existeixen dos tipus de certificats: **a)** Certificitats autosignats i **b)** Certificats signat per una **Autoritat de Certificació** (CA).

g) Un certificació signat per una CA i instal·lat en un servidor, assegura al client que una autoritat externa en la qual es confia (l'autoritat de certificació o CA) confirma que el posseïdor del certificat és realment qui afirma ser. Una CA pot ser una autoritat governamental o una empresa de prestigi reconegut. La Generalitat, el ministeri de l'interior o empreses com Verisign són exemples de CA. Per mitjà d'un certificat signar per una CA podem tenir comunicacions encriptades i ens assegurem de l'autenticitat del servidor o també a vegades del client (per exemple, quan paguem impostos per internet).

h) Els certificats signats per una CA s'han de pagar, però hi ha la possibilitat d'aconseguir un certificat de seguretat a la web de Let's Encrypt. Els certificats de Let's Encrypt s'han de renovar cada sis mesos. Normalmet els certificats tenen una durada de 1 a 10 any o més.

i) Un certificat autosignat és un certificat en la qual una entitat es certifica a ella mateixa. Evidentment, si ens connectem a un servidor amb un certificat autosignat no podem assegurar l'autenticitat però com a mínim les dades viatgen encriptades. El certificats autosignats són de franc (me'ls faig jo mateix).

j) Un certificat autosignat pot ser suficient per una organització petita a on tothom es coneix i l'autènticació no sigui necessària però si que és necessiti la privacitat de les comunicacions. Si es vol posar una botiga virtual o es treballa per una organització gran llavor sí que és necessari per proporcionar autenticació i encriptació.

k) Si el client no té un certificat es poden introduir mecanismes d'autenticació que demanin a l'usuari un nom i una contrasenya per poder ser autentificat.

l) Enllaços:

* Guia de seguretat d'Apache
* Handshake de la connexió d'un client a un servidor per mitjà d'HTTPS

2- Genera un certificat autosignat i una clau pública

a) Instal·la el paquet de software **openssl**.

b) Com usuari del sistema crea una carpeta de nom **certificats**. Fes que només sigui de **rwx** pel propi usuari i que la resta d'usuaris i grups del sistema no tinguin cap permís.

c) Des de dins de **certificats** i fent ús del programa **openssl**, genera una **clau privada RSA** de **4096 bits** encriptada utilitzant l'algorisme d'encriptació **AES-256**, emmagatzemada utilitzant el format **PEM** i de nom **daw2.pem**. Executa:

```
openssl genpkey -algorithm RSA -out daw2.pem -pkeyopt rsa_keygen_bits:4096 -aes256
```

Si et demana una “pash phrase”, introdueix **Daw2019@**. Aquesta “pash phrase” et serà demanada cada cop que vulguis utilitzar la clau privada **daw2.pem**.

d) Ara genera una petició de **certificat CSR** pel servidor. El fitxer amb el certificat s'anomenarà **daw2.csr**. Executa:

```
openssl req -new -key daw2.pem -out daw2.csr
```

Aquesta ordre et demana suministrar algunes dades per crear la petició de certificat de seguretat. Un conjunt de respostes que es poden donar són les següents:

a) Country Name (2 letter code) [AU]:**ES**
b) State or Province Name (full name) [Some-State]:**B**
c) Locality Name (eg, city) [ ]:**B**
d) Organization Name (eg, company) [Internet Widgits Pty Ltd]:**DAW2**
e) Organizational Unit Name (eg, section) [ ]:**DAW2**
f) Common Name (eg, YOUR name) [ ]: **<El teu nom. El de veritat. Sí, l'autèntic>**
g) Email Address [ ]: **<La teva adreça de github de la primera pràctica de Git>**
h) A challenge password [ ]: **<en blanc, o sigui, que no escriguis res. Prem Enter>**
i) An optional company name [ ]: **DAW2**

e) Genera un certificat de seguretat autosignat d'**un any** de validesa de nom **daw2.crt**. Executa:

```
openssl x509 -req -days 365 -in daw2.csr -signkey daw2.pem -out daw2.crt
```

f) Comprova que el certifiacat s'ha creat correctament. Visualitza el contingut del certificat amb l'ordre:

```
openssl x509 -in daw2.crt -noout -text
```

i comprova que el contingut és correcte.

3- Configura un nou lloc web virtual segur

a) Crea la carpeta **/var/www/html/daw2s**. Crea el fitxer **index.html** dins de **/var/www/html/daw2s** amb el següent contingut:

```
<html>
      <title>
            Web segura d'inici del lloc www.daw2s.net
      </title>
      <body>
            Web segura d'inici de www.daw2s.net<br>
            <i>Creador del lloc: Nom i Cognoms</i><br>
      </body>
</html>
```

NOTA: Nom i Cognom són els teus de veritat i sense accents.

b) Instal·la en el teu servidor el **certificat de seguretat autosignat** i la **clau pública** que vas generar a l'apartat 2 de la pràctica. Hauràs de **c**opiar el fitxer **daw2.crt** a **/etc/ssl/certs** i el fitxer **daw2.pem** a **/etc/ssl/private**. Assegura't en els 2 casos que permisos, propietaris i grups siguim iguals que els de la resta de fitxers que es troben en el mateix directori.

c) Crea un arxiu de configuració d'un lloc virtual **www.daw2s.net** de **daw2s.conf** i desa-ho dins del directori **/etc/apache2/sites-available**. El contingut del fitxer de configuració serà:

```
<IfModule  mod_ssl.c>
   <VirtualHost  *:443>
         ServerAdmin  webmaster@daw2s.net
         ServerName  www.daw2s.net
         ServerAlias  web.daw2s.net
         DocumentRoot  /var/www/html/daw2s
         ErrorLog  ${APACHE_LOG_DIR}/error.log
         CustomLog  ${APACHE_LOG_DIR}/access.log  combined
         DirectoryIndex  index.html  index.php
         SSLEngine  on
         SSLCertificateFile  /etc/ssl/certs/daw2.crt
         SSLCertificateKeyFile  /etc/ssl/private/daw2.pem
   </VirtualHost>
</IfModule>
```

d) Redirecciona totes les peticions a **http** cap a **https**. Afegeix al final de **daw2s.conf** la següent configuració:

```
   <VirtualHost  *:80>
         ServerName  www.daw2s.net
         DocumentRoot  /var/www/html/daw2s
         Redirect permanent / https://www.daw2s.net
   </VirtualHost>
```

e) Activa el lloc web virtual **www.daw2s.net** executant **`a2ensite daw2s.conf`**

f) Carrega el mòdul **SSL** del servidor **Apache**. Executa: **`a2enmod ssl`**. Comprova que s'ha carregat amb l'ordre. Executa: **`apachectl -M`**.

g) Reinicia **Apache2**. Si et demana una passphrase, és la que vas introduir dins la clau **daw2.pem** al segon punt de la pràctica. Comprova que el servidor **Apache2** s'executa i **escolta** pel **port 443/tcp**.

4- Accedint al lloc segur des de la màquina client amb el navegador Firefox

a) Comprova l'adreça IP de la màquina virtual a on has creat el lloc virtual segur **www.daw2s.net**.

b) Modifica el fitxer **/etc/hosts** (Linux) o **c:\windows\system32\drivers\etc\hosts** (Windows) i afegeix una nova línia a on surti l'adreça IP del servidor debian i el nom del lloc virtual.

c) Des del navegador, estableix una connexió segura amb el servidor Apache2 utiltizant la següent URI:
https://www.daw2s.net

NOTA: En el moment de connectar-te, el navegador dóna l'avís ***"La connexió no és segura"***. Fes click a l'opció **Avançat**. A continuació **afegeix una excepció de seguretat** i fes clic al botó per obtenir el certificat del servidor. Un cop confirmada l'excepció de seguretat, comprova que pots accedir a la web del lloc virtual **www.daw2s.net**.

d) Comprova que has carregat el certificat en el teu navegador. Des de **Firefox**, obre Edita --> Preferències --> Privadesa i seguretat --> Seguretat --> Certificats --> Visualitza els certificats. Troba el certificat del servidor **www.daw2s.net** i visualitza'l.

e) Comprova que si realitzes una connexió a **http://www.daw2s.net** (http no https) es redirecciona cap a la connexió segura.

Forma de lliurament de la pràctica
1- Lliurament el dia: Comença el dia **15-1-21**
2- Comprovació:
- **a)** Comprovació del certificat autosignat **daw2.crt** i de clau pública **daw2.key**.
- **b)** Servidor escoltant pel port **443**
- **c)** Connexió segura des del client a **https://www.daw2s.net**
- **d)** Comprovació del certificat de seguretat en el client.
- **e)** Comprovació de la **redirecció http** cap a **https**.