

Pràctica 4: Llocs web virtuals. Llocs web segurs amb SSL/TLS

1- Llocs webs segurs amb SSL/TLS

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'enciptació de dades) a les comunicacions. TLS (Seguretat de Capa de Transport) és l'evolució del protocol SSL (Capa de Connexió Segura). Les versions de TLS utilitzades 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 xifra 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) Certificats autosignats i b) Certificats signat per una **Autoritat de Certificació (CA)**.

g) Un certificat 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 signat per una CA podem tenir comunicacions enciptades i ens assurem 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. Normalment 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 enciptades. Els 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'autenticació no sigui necessària però si que és necessari la privacitat de les comunicacions. Si es vol posar una botiga virtual o es treballa per una organització gran llavors sí que és necessari per proporcionar autenticació i enciptació.

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 autenticat.

l) Enllaços:

- [Guia de seguretat d'Apache](#)
- [Handshake de la connexió d'un client a un servidor per mitjà d'HTTPS](#)

2- Abans de començar

- a) Crea una carpeta de nom **m08uf1pr4** dins de la carpeta **m08uf1** que vas crear a la pràctica **m08uf1pr2**.
- b) Copia el fitxer **Vagrantfile** que vas crear a la pràctica **m08uf1pr2** dins de la carpeta **m08uf1pr4**.
- c) Crea una carpeta de nom **projecte** dins de **m08uf1pr4** que està configurada per ser compartida amb **/var/www/html** de la màquina virtual d'acord amb la configuració del fitxer **Vagrantfile**.
- d) Modifica el fitxer **Vagrantfile** dins de **m08uf1pr4**:
- El paràmetre **config.vm.hostname** serà igual a **daw2-xyyyzz-m08uf1pr4.fjeclot.net** a on **xyyyzz** són les 2 primeres lletres del teu nom, 1r cognom i 2n cognom.
 - El paràmetre **v.name** serà igual a **daw2-xyyyzz-m08uf1pr4** a on **xyyyzz** són les 2 primeres lletres del teu nom, 1r cognom i 2n cognom.
 - Comprova que el paràmetre **v.cpus** és igual a **2** i **v.memory** és igual a **2048** (és a dir, 2GiB)
 - Assegura't que la màquina virtual treballa amb **Adaptador Pont** i **DHCP**. Comprova que el paràmetre **config.vm.network** és **"public_network"**.
 - Comprova que la màquina física comparteix el directori **projecte** amb el directori **/var/www/html** de la màquina virtual amb els permisos, propietari i grup correctes. Dins de **Vagrantfile** comprova que pots trobar la següent línia de configuració:
`config.vm.synced_folder "/projecte", "/var/www/html", owner: "www-data", group: "www-data"`
 - Comprova que s'instal·larà **aptitude**, **net-tools**, **git**, **nano**, **apache2**, **php**, mòdul de PHP per **Apache2**.
 - Comprova que l'usuari **vagrant** té permisos per treballar dins del directori **/var/www/html** de la màquina virtual.
- e) Crea i posa en marxa la nova màquina virtual. Des de dins de **m08uf1pr4** executa: **vagrant up**
- f) Si el procés de posada en marxa s'atura perquè et demana quina targeta de xarxa de la màquina **host** vols utilitzar, hauràs d'escollir **wlp7s0** si vols treballar amb **WiFi** o **enp8s0f1** per treballar amb **Ethernet** (o sigui, el **cable**).
- g) Un cop en marxa, accedeix a la màquina virtual, executant dins **m08uf1pr4**: **vagrant ssh**
- h) Des de dins de la màquina virtual, comprova:
- La seva adreça IP via adaptador pont. Executa: **ip -4 -br add show dev eth1**
 - El nom de sistema de la màquina virtual que ha de ser el mateix que **config.vm.hostname** de **Vagrantfile**. Executa: **hostname --fqdn**

3- Generació d'un certificat autosignat i una clau pública

- a) Comprova que el paquet de software **openssl** està instal·lat. Executa **openssl version** i comprova que treballes amb la versió 1.1 o superior.
- b) Crea una carpeta de nom **cert** dins del directori personal d'usuari **vagrant**. 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 **cert** i fent ús del programa **openssl**, genera una parella de **clau privada i pública** per poder treballar amb **criptografia asimètrica (o clau pública)**, utilitzant l'**algorisme RSA**, amb una longitud de la clau que serà de **4096 bits** que s'emmagatzemarà utilitzant el format **PEM**. El nom del fitxer amb les claus serà **daw2.pem**. Executa:

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

Ara tens un fitxer de nom **daw2.pem** amb la parella de clau privada i pública necessàries per treballar amb certificats digitals. a partir del fitxer **daw2.pem** es pot [extreure la clau pública](#).

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]:**FJE CLOT**
- e) Organizational Unit Name (eg, section) []:**CFGS**
- f) Common Name (eg, YOUR name) []: **<Escriu el teu nom d'usuari de Github>**
- g) Email Address []: **<L'adreça de correu que vas utilitzar per crear el teu usuari de Github>**
- h) A challenge password []: **<en blanc, o sigui, que no escriguis res. Prem Enter>**
- i) An optional company name []: **<en blanc, o sigui, que no escriguis res. Prem Enter>**

Comprova ara que s'ha generat el fitxer **daw2.csr** amb la petició de creació del certificat de seguretat.

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 assegura't que les dades són correctes a la secció **Issuer**, i que la validesa és d'un any a la secció **Validity**.

4- Configuració d'un lloc web virtual segur

a) Utilitzant llocs web virtuals (o virtualhosts) poden allotjar 1 o més llocs webs amb un únic servidor web. En aquest moment, tenim en marxa per defecte 2 llocs webs virtuals:

- El lloc web NO SEGUR per defecte que escolta pel port 80/tcp i treballa amb HTTP i que s'identifica com **000-default** dins del directori **/etc/apache2/sites-enabled**.
- El lloc web SEGUR per defecte que escolta pel port 443/tcp i treballa amb HTTPS i que s'identifica com **default-ssl.conf** dins del directori **/etc/apache2/sites-enabled**.

Desactivarem aquests 2 llocs webs virtuals per defecte executant:

- **sudo a2dissite 000-default.conf**
- **sudo a2dissite default-ssl.conf**

i a continuació executarem la següent ordre perquè els canvis tinguin efecte:

- **sudo systemctl restart apache2**

b) Instal·la en els directori adequats del teu servidor la parella **clau de pública/privada** i el **certificat de seguretat autosignat** que vas generar als apartats 3.c i 3.e de la pràctica. Hauràs de copiar els fitxers **daw2.crt** a **/etc/ssl/certs** i el fitxer **daw2.pem** a **/etc/ssl/private**:

- **sudo cp daw2.crt /etc/ssl/certs**
- **sudo cp daw2.pem /etc/ssl/private**

c) Aquests fitxers necessiten els permisos i propietaris adequats per poder ser utilitzats per l'**Apache2** i no ser visibles per usuaris sense permisos per fer-ho. Executa les següents ordres:

- **sudo chmod 644 /etc/ssl/certs/daw2.crt**
- **sudo chgrp ssl-cert /etc/ssl/private/daw2.pem**
- **sudo chmod 640 /etc/ssl/private/daw2.pem**

d) Crea un arxiu de configuració d'**apache2** de nom **daw2s.conf** per crear un nou lloc web segur per la màquina virtual dins del directori **/etc/apache2/sites-available**. Aquest fitxer de configuració:

- Farà que **Apache2** utilitzi el certificat de seguretat i la clau creades a l'apartat 3.c i 3.e.
- Farà que **Apache2** redireccioni les connexions **http** pel port **80/tcp** cap a **https** pel port **443/tcp**.

El contingut del fitxer de configuració **daw2s.conf** serà aquest:

```
<IfModule mod_ssl.c>
  <VirtualHost *:443>
    ServerAdmin vagrant@daw2-xyyzz-m08uf1pr4.fjeclot.net
    ServerName daw2-xyyzz-m08uf1pr4.fjeclot.net
    DocumentRoot /var/www/html
    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>
<VirtualHost *:80>
  DocumentRoot /var/www/html
  ServerName daw2-xyyzz-m08uf1pr4.fjeclot.net
  Redirect permanent / https://daw2-xyyzz-m08uf1pr4.fjeclot.net
</VirtualHost>
```

NOTA: Recorda que **xyyzz** són les 2 primeres lletres del teu nom, 1r cognom i 2n cognom.

f) Per evitar el molest missatge de warning **AH00558: apache2: Could not reliably determine the server's fully.....**, afegeix al final del fitxer **/etc/apache2/apache2.conf** la directiva:

```
#
ServerName daw2-xyyzz-m08uf1pr4.fjeclot.net
```

NOTA: Recorda que **xyyzz** són les 2 primeres lletres del teu nom, 1r cognom i 2n cognom.

g) Crea dins **/var/www/html** un nou fitxer **index.html** amb el següent contingut:

```
<html>
  <title>
    Lloc web segur de daw2-xyyzz-m08uf1pr4.fjeclot
  </title>
  <body>
    Lloc web segur daw2s utilitzant un certificat digital autosignat<br>
    <i>Creador del lloc: Nom i Cognoms</i><br>
  </body>
</html>
```

NOTA: **Nom i Cognoms** són els teus de veritat i sense accents, i **xyyzz** són les 2 primeres lletres del teu nom, 1r cognom i 2n cognom.

h) Activa el nou lloc web virtual segur de **daw2-xyyzz-m08uf1pr4.fjeclot.net**. Executa l'ordre:

- `sudo a2ensite daw2s.conf`

i) Assegura't que el mòdul **SSL** del servidor **Apache** està carregat per poder treballar amb HTTPS. Executa:

`sudo a2enmod ssl`

j) Reinicia **Apache2**. Executa:

- `sudo systemctl restart apache`

k) Comprova que el servei apache2 està en execució (running) i actiu (active) i no hi ha cap error d'arrancada. Executa:

- `sudo systemctl status apache2`

l) Comprova que el servidor **apache2** escolta pels ports **80/tcp** i **443/tcp**. Executa:

- `sudo netstat -atupn | grep apache2`

i comprova que el resultat és del tipus:

tcp	0	0 0.0.0.0:80	0.0.0.0:*	LISTEN	1625/apache2
tcp	0	0 0.0.0.0:443	0.0.0.0:*	LISTEN	1625/apache2

a on el **PID** d'**apache2** (en aquest cas **1625**) pot ser un número diferent al de l'exemple però els valors dels ports **80** i **443** han de ser els mateixos.

5- Accedint al lloc segur des de la teva màquina física amb el navegador Firefox

a) Modifica el fitxer **hosts** de la teva **màquina física** de manera que relacioni l'adreça IP de la teva màquina virtual amb el seu nom **daw2-xyyzz-m08uf1pr4.fjeclot.net** (a on **xyyzz** són les 2 primeres lletres del teu nom, 1r cognom i 2n cognom). El fitxer **hosts** es troba a:

- **/etc** dins de **Linux**
- **C:\Windows\System32\Drivers\etc** dins de **Windows**

b) Des del navegador **Firefox** de la teva màquina física, estableix una connexió segura amb el servidor Apache2 de la màquina virtual utilitzant la següent URL:

https://daw2-xyyzz-m08uf1pr4.fjeclot.net

a on **xyyzz** són les 2 primeres lletres del teu nom, 1r cognom i 2n cognom.

NOTA: En el moment de connectar-te per primera vegada, el navegador mostra el missatge **“Avís: Risc potencial de seguretat”**. Fes click a l'opció **Avançat...** A continuació fes clic a **Accepto el risc i vull continuar**. Un cop acceptat el risc de seguretat, comprova que pots accedir a la web del lloc virtual

c) Comprova que has carregat correctament el certificat digital autosignat en el teu navegador. Des del menú de **Firefox** obre **Paràmetres** → **Privadesa i seguretat** → **Seguretat** → **Certificats** → **Mostra els certificats**. Selecciona la pestanya **Servidors**, troba el certificat del servidor **daw2-xyyzz-m08uf1pr4.fjeclot.net:443** (a on **xyyzz** són les 2 primeres lletres del teu nom, 1r cognom i 2n cognom) i fes clic a **Visualitza** per comprovar que les dades coincideixen amb les dades del certificat que es poden veure executant l'ordre de l'apartat 3.f.

d) Finalment, comprova que una connexió a **http://daw2-xyyzz-m08uf1pr4.fjeclo.net** (o sigui a **http** no a **https**) des de la màquina física es redirecciona automàticament a **https://daw2-xyyzz-m08uf1pr4.fjeclo.net**. Recorda que **xyyzz** són les 2 primeres lletres del teu nom, 1r cognom i 2n cognom.

Forma de lliurament de la pràctica

1- Lliurament el dia: Comença el dia **31-1-24**

2- Comprovació:

- a) De l'arrancada de la màquina virtual amb Vagrant i del nom de sistema de la màquina virtual utilitzant la segona ordre de l'apartat **2.h**.
- b) Del contingut del certificat autosignat **daw2.crt** utilitzant la instrucció de l'apartat **3.f**. S'ha de veure clarament: **Serial Number**, **Issuer** i **Validity**.
- c) Que El servidor **apache2** dins de la màquina virtual està escoltant pel port **80/tcp** i **443/tcp** utilitzant la instrucció de l'apartat **4.l**.
- d) De la Connexió segura des de la màquina física a **http://daw2-xyyzz-m08uf1pr4.fjeclo.net** (a on **xyyzz** són les 2 primeres lletres del teu nom, 1r cognom i 2n cognom).
- e) Visualització del certificat de seguretat s'ha afegit a navegador tal i com s'explica a l'apartat **5.c**.
- f) De la **redirecció http** cap a **https** tal i com s'explica a l'apartat **5.d**.