Pràctica 2: Autenticació i encriptació amb certificats de seguretat SSL/TLS

1- Introducció

1- 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.

2- 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.

3- 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",

4- 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 del sistema de criptografia asimètrica tambe coneguda amb el nom de criptografia de clau pública.

5- 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.

6- 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).

7- 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).Els certifiacats signats per una CA s'han de pagar.

8- 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).

9- 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

10- Si el client no té un certificat es poden introduir els mecanismes d'autenticació que vam veure a la pràctica anterior per demanar a l'usuari un nom d'usuari i una contrasenya i que s'autentifiqui.

11- Links:

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

2- Configura HTTPS amb Apache en el servidor debian

a) Crea el següent fitxer **index.html** dins de **/var/www/html**:

```
<html>
      <title>
            Lloc web segur amb connexió HTTPS
      </title>
      <body>
            <h2>P&agrave;gina d'inici del lloc web segur</h2>
            Aquesta web nom&eacute;s &eacute;s accesible via https<br>
            <i>Creador del lloc: "el teu compte de l'escola"</i><br>
      </body>
</html>
```

b) Instal·la en el teu servidor un certificat de seguretat autosignat i una clau pública, seguint els següens passos:

1r pas) Descarrega el certificat **daw2.crt** i la clau pública **daw2.key** del següent enllaç: http://www.collados.org/daw2/m08/uf1/daw2.tar.gz

2n pas) Descomprimeix **daw2.tar.gz**. Un cop descomprimit, obtindràs 2 fitxers: **daw2.crt** i **daw2.key**. Aquest 2 fitxers són una clau pública (**daw2.key**) i un certificat autosignat de seguretat (**daw2.crt**). Copia el fitxer **daw2.crt** a **/etc/ssl/certs**. Copia el fitxer **daw2.key** a **/etc/ssl/private**.

c) Modifica l'arxiu de configuració del lloc web segur amb les següents directives:

* **SSLEngine** --> **on**.
* **SSLCertificateFile** --> **/etc/ssl/certs/daw2.crt**.
* **SSLCertificateKeyFile** --> **/etc/ssl/private/daw2.key**.

d) Activa el mòdul **SSL** del servidor **Apache**. Executa: **a2enmod ssl.** Després reinicia **Apache2.**

e) Comprova que s'ha activat amb l'ordre. Executa: **apachectl -M**. El nom del mòdul un cop activat és **ssl_module**. Comprova també que el servidor **Apache2** ara també **escolta** pel **port 443/tcp**.

f) Activa el lloc web segur. Executa: **a2ensite default-ssl.conf**. Comprova que s'ha creat el link a l directori **/etc/apaches2/sites-enabled**. Després reinicia **Apache2.**

3- Configura la màquina client

a) Comprova l'adreça IP del servidor. Des del navegador, estableix una connexió segura amb el servidor.

b) En el moment de connectar-te, el navegador dóna l'avís que la connexió no és segura. Fes click a l'opció **Avançat** i comprova el motiu d'aquest avís.

c) Afegeix l'excepció de seguretat i aconsegueix el certificat. Visualitza el certificat. Comprova que el número de sèrie és **00:C3:3C:87:7E:DA:EF:07:1D** i que la data de venciment és el **12/01/19**.

d) Confirma l'excepció de seguretat i comprova que pots accedir via HTTPS al lloc web segur.

e) Comprova que has carregat el certificat en el teu navegador. Des de **Firefox**, ves a Edita --> Preferències --> Avançat --> Avançat --> Certificats --> Visualitza els certificats, i troba el certificat **daw2.crt**.

f) Tanca el navegador i torna a connectar-te al lloc virtual. Comprova que ara has entrat directament perquè el certificat està carregat. **NOTA:** Compte amb els paràmetres de configuració de l'historial del navegador. Si s'esborra tot cada vegada que atures el navegador llavors cada vegada que posis en marxa el navegador, et torna a demanar l'entrada de l'excepció de seguretat.

g) Comprova que passa si realitzes una connexió via **http** al servidor. Quina web virtual ens mostra el servidor?

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

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

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

c) Des de dins de **.certificats** i fent ús de l'**openssl**, genera una **clau privada RSA** de **1024 bits** encriptada utilitzant el mètode **Triple-DES**. Utilitza com a *pass phrase* --> **asix2**. Fes que el fitxer amb la clau s'anomeni **asix2m08.key**. Llegeix *"Step 1: Generate a private key"* de la pagina web" http://www.akadia.com/services/ssh_test_certificate.html

d) Genera una petició de **certificat CSR** pel servidor. El fitxer amb el certificat s'anomenarà **asix2m08.csr**. Llegeix *"Step 2: Generate a CSR (Certificate Signing Request)"* de la pagina web http://www.akadia.com/services/ssh_test_certificate.html. Les respostes a les preguntes realitzades per l'ordre de creació del certificat han de ser 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]:FJECLOT
e) Organizational Unit Name (eg, section) [ ]:CFGS_ASIX2
f) Common Name (eg, YOUR name) [ ]: El teu nom
g) Email Address [ ]: La teva adreça de l'escola
h) A challenge password [ ]: <en blanc>
i) An optional company name [ ]: ETPC

e) Genera un certificat autosignat d'un any de validesa de nom **asix2m08.crt**. Llegeix *"Step 4: Generating a Sef-Signed Certificate"* de la web: http://www.akadia.com/services/ssh_test_certificate.html. Comprova que s'ha generat el certficat autosignat **asix2m08.crt**.

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

openssl x509 -in daw2m08.crt -noout -text

i comprova que el contingut és correcte.

5- Com conèixer el nivell de seguretat SSL d'una pàgina web (HTTPs)

a) Quan ens connectem a través de SSL estem més segurs a la xarxa que no fent-ho. Ara comprovareu a partir d'una pàgina web l'anàlisi de la seguretat de la pàgina web (amb el que al SSL es refereix). És capaç de dir-nos els seus punts dèbils, mostrant els resultats i una puntuació després d'un escaneig.

b) A partir de la pàgina https://www.ssllabs.com/ssldb/index.html feu un escaneig de les següents pàgines:

1- Google
2- Facebook
3- Escola del Clot

c) Mostreu informació sobre:

1- Gràfica de resum
2- El seu certificat
3- Quan expira
4- La clau utilitzada (key)
5- L'algoritme

Forma de lliurament de la pràctica

1- Lliurament el dia **13-1-16** a les **15.00h.**

2- Comprovació:

a)Servidor escoltant pel port **443**.

b)Realització de la connexió segura des del client al servidor.

c)Comprovació del certificat de seguretat descarregat en el client.

d)Creació d'un certificat autosignat **asix2m08.crt** i de clau pública **asix2m08.key**.

e) Mostra la puntuació d'escaneig de l'**Escola del Clot**.