CONFIGURACIÓ D'UN SERVIDOR APACHE SEGUR AMB UN CERTIFICAT AUTOSIGNAT (HTTPS)

Crear un certificat autosignat i configurar-lo en Apache de forma que en accedir a l'URL https://www##.aula218.lan s'establisca una connexió segura.

Creem un certificat autosignat:

1- Instal·lem les eines necessàries (OpenSSL):

sudo apt-get install openssl

2- Generar una clau privada

sudo openssl genrsa -out /etc/ssl/private/aula218.key 2048

3- Generar el certificat autosignat amb la clau privada.

sudo openssl req -new -x509 -key /etc/ssl/private/aula218.key -out /etc/ssl/certs/aula218.crt -days 365

Al realizar aquest comando, ens demanarà la següent informació:

> Country Name (2 letter code): Ex: ES
> State or Province Name (full name): Ex: València
> Locality Name (eg, city): Ex: València
> Organization Name (eg, company): Ex: aula218
> Common Name: www##.aula218.lan

Configuració d'Apache per HHTPS:

1- Activem els mòduls SSL a Apache:

sudo a2enmod ssl
sudo a2ensite default-ssl
sudo systemctl restart apache2

2- Configurem el lloc virtual amb SSL:

Editem el fitxer de configuració SSL per Apache :

sudo nano /etc/apache2/sites-available/default-ssl.conf

Ens assegurem que les següents línies estiguen així:

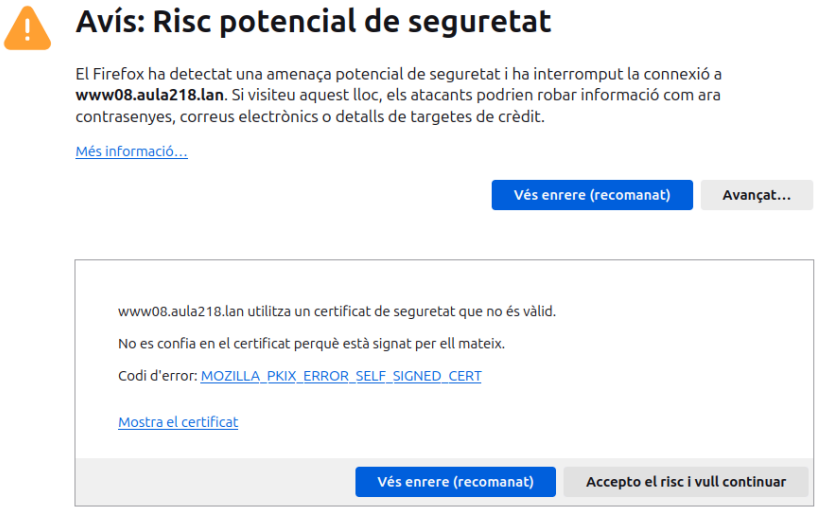
```
<VirtualHost *:443>
	ServerAdmin webmaster@localhost
	ServerName www08.aula218.lan

	DocumentRoot /var/www/html

	ErrorLog ${APACHE_LOG_DIR}/error.log
	CustomLog ${APACHE_LOG_DIR}/access.log combined

	#   SSL Engine Switch:
	#   Enable/Disable SSL for this virtual host.
	SSLEngine on

	#   Self-signed certificate and private key
	SSLCertificateFile	/etc/ssl/certs/aula218.crt
	SSLCertificateKeyFile   /etc/ssl/private/aula218.key

	# Uncomment or delete unnecessary lines
	#SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt
	#SSLCACertificatePath /etc/ssl/certs/
	#SSLCACertificateFile /etc/apache2/ssl.crt/ca-bundle.crt
	#SSLCARevocationPath /etc/apache2/ssl.crl/
	#SSLCARevocationFile /etc/apache2/ssl.crl/ca-bundle.crl

	<FilesMatch "\.(?:cgi|shtml|phtml|php)$">
		SSLOptions +StdEnvVars
	</FilesMatch>

	<Directory /usr/lib/cgi-bin>
		SSLOptions +StdEnvVars
	</Directory>
</VirtualHost>
```

3- Activem el lloc i reiniciem Apache:

sudo a2ensite default-ssl.conf
sudo systemctl restart apache2

S'ha aconseguit establir una connexió segura? El navegador mostra algun avís? Justifica les respostes i documenta-les.

Si, s'ha aconseguit establir una connexió segura.



Com que el certificat és autosignat, el navegador mostrarà un avís que indica que la connexió no és privada o que el certificat no ha estat emès per una autoritat de certificació reconeguda.

Encara que la connexió estigui encriotada, el navegador alerta que el certificat no és de confiança. Es pot continuar al lloc ignorant l'avís, el que implica que la connexió seguirà sent segura.

Seguint les instruccions del punt 1 els membres restants del grup hauran d'instal·lar i
configurar un certificat per al seu domini.

Els altres membres de l'equip han de seguir el mateix procés, substituint el domini www08.aula218.lan pel seu domini específic. Al igual que abans:

1- Crear una clau privada i el certificat autosignat.

2- Configurar apache modificant default-ssl.conf per a que utilitze el certificat i la clau correcta i que el nom del servidor sigua el domini corresponent.

3- Activar el lloc i reiniciar Apache:
sudo a2ensite default-ssl.conf
sudo systemctl restart apache2

Les instruccions eren correctes i fàcils d'entendre? Justifica les respostes

- Las instrucciones eran bastantes claras; lo único que me llevó a confusión era: 'www##.aula218.lan', donde ## era la ip del equipo, igual ponerlo en dicha línea podría ser mejor de cara a los demás usuarios.

OPINIONS:

Paula: Aquesta activitat m'ha servit per aprendre com funciona la seguretat en el connexions HHTPS. He aprés a generar un certificat i integrar-lo en un servidor Apache, cosa que ens permet establir una connexió segura amb el nostre domini.

Vero: Por lo general es una práctica fácil y rápida, pero surgió un problema con el apache en el que no me dejaba reiniciarlo. El problema era una extensión errónea en la línea 33 de la configuración de Apache. Una vez corregido dicho conflicto, pude seguir con la práctica de forma correcta.

Andrea: el desarrollo de la actividad se ha realizado sin ningún problema. Los pasos a seguir son claros y el resultado es el esperado.

Ion: Una práctica bastante sencilla, y es una buena forma de practicar la implementación de SSL y entender la infraestructura de certificados en un entorno local.