

Servicios SSL APACHE

[El Servidor SSL Para Correo se definió en la practica de correos por lo que se omite en esta practica.]

Una vez instalado el servidor apache se instalan las librerias de SSL:

*** aptitude install openssl openssl-blacklist openssl-blacklist-extra**

ahora nos movemos a la carpeta /etc/apache2 en donde crearemos de forma temporal las llaves SSL para despues moverlas a la carpeta de destino final, los comandos para ellos son: openssl genrsa -des3 -out rgb2gray.key.

se nos pedira contrasena pero dejaremos limpio los campos,

despues openssl req -new -key rgb2gray.key -out certificado.csr este nos pedira variso datos de la identidad del sitio,y finalmente generamos nuestra llave auto firmada con el comando openssl x509 -req -days 365 -in certificado.csr -signkey rgb2gray.key -out certificado firmado.crt

con ello tendremos los archivos necesarios

```
root@zepeda-NVA53:/etc/apache2/sites-available# openssl x509 -req -days 365 -in certificadorgb2gray.csr -signkey rgb2gray.key -out certificadofirmado.crt
certificadorgb2gray.csr: No such file or directory
root@zepeda-NVA53:/etc/apache2/sites-available# openssl x509 -req -days 365 -in certificadorgb2gray.csr -signkey rgb2gray.key -out certificadofirmado.crt
Signature ok
subject=/C=MX/ST=Jalisco/L=Guadalajara/O=CUCEI/OU=INFORMATICA/CN=rgb2gray.com/emailAddress=peanut@rgb2gray.com
Getting Private key
Enter pass phrase for rgb2gray.key:
```

Ahora solo es necesario crear un virtual host con la siguiente informacion

```
<IfModule mod_ssl.c>
    <VirtualHost _default_:443>
        ServerAdmin webmaster@localhost
        ServerName rgb2gray.com
        ServerAlias www.rgb2gray.com
        DocumentRoot /var/www/rgb2gray
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
        SSLEngine on
        SSLCertificateFile /etc/ssl/certs/certificadofirmado.crt
        SSLCertificateKeyFile /etc/ssl/private/rgb2gray.key
        #SSLOptions +FakeBasicAuth +ExportCertData +StrictRequire
        <FilesMatch "\.(cgi|shtml|phtml|php)$">
            SSLOptions +StdEnvVars
        </FilesMatch>
        <Directory /usr/lib/cgi-bin>
            SSLOptions +StdEnvVars
        </Directory>

        BrowserMatch "MSIE [2-6]" \
            nokeepalive ssl-unclean-shutdown \
            downgrade-1.0 force-response-1.0
        BrowserMatch "MSIE [17-9]" ssl-unclean-shutdown

    </VirtualHost>
</IfModule>
```

cabe mencionar que las llaves deben de moverse a esas carpetas que se especifican, ahora solo se reinicia apache y todo quedara listo para ser usado.