

LABORATORIO 3

- A. Realizaremos la configuración de un servidor web seguro.
- B. Material por grupo que se necesitara:
 - Un CPU por grupo
 - Bajarse y traer la ultima versión de apache web server (AWS) para Windows
 - Bajarse y traer la ultima versión de openssl para AWS Windows
 - Un sitio web con un par de páginas web.
- C. Procedimiento:
 - 1. Instalar Apache y Openssl
 - 2. Configuring Apache

Change at least the following parameters in `Apache-dir/conf/httpd.conf`:
[Replace all occurrences of `www.my-server.com` with the real domain name!]

- `Listen 443` (So your server listens on the standard SSL port)
- `ServerName www.my-server.com`

3. Creating a test certificate

```
openssl req -config openssl.cnf -new -out my-server.csr
```

This creates a certificate signing request and a private key. When asked for "Common Name (eg, your websites domain name)", give the exact domain name of your web server (e.g. **www.my-server.dom**). The certificate belongs to this server name and browsers complain if the name doesn't match.

```
openssl rsa -in privkey.pem -out my-server.key
```

This removes the passphrase from the private key. You **MUST** understand what this means; `my-server.key` should be only readable by the apache server and the administrator.

You should delete the `.rnd` file because it contains the entropy information for creating the key and could be used for cryptographic attacks against your private key.

```
openssl x509 -in my-server.csr -out my-server.cert -req -signkey my-server.key -days 365
```

This creates a self-signed certificate that you can use until you get a "real" one from a certificate authority. (Which is optional; if you know your users, you can tell them to install the certificate into their browsers.) Note that this certificate expires after one year, you can increase `-days 365` if you don't want this.

Create an `Apache/conf/ssl` directory and move `my-server.key` and `my-server.cert` into it.

4. Configuring Apache and `mod_ssl`

Find the `LoadModule` directives in your `httpd.conf` file and add this after the existing ones, according to the file you have found in the distribution:

LABORATORIO 3

LoadModule ssl_module modules/ApacheModuleSSL.so

Add the following to the end of httpd.conf:

```
# see http://www.modssl.org/docs/2.8/ssl\_reference.html for more info
SSLMutex sem
SSLRandomSeed startup builtin
SSLSessionCache none

SSLLog logs/SSL.log
LogLevel info
# You can later change "info" to "warn" if everything is OK

<VirtualHost www.my-server.dom:443>
SSLEngine On
SSLCertificateFile conf/ssl/my-server.cert
SSLCertificateKeyFile conf/ssl/my-server.key
</VirtualHost>
```

5. Copiar el sitio web en el directorio correspondiente de Apache