ACTIVIDAD 15 – CERTIFICADOS DIGITALES

Administración servidor web HTTPS (Apache2) en Ubuntu Server: -- mod_ssl, default_ssl – certificados digitales.

Instalamos ssl, para ello ponemos el siguiente comando

```
root@ubuntu10:/etc# apt-get install openssl
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... 0%
```

Una vez instalado vamos a comprobar que tenemos los módulos de ssl

```
root@ubuntu10:/etc/apache2/mods-available# ls
actions.conf          cern_meta.load     httpd.conf          proxy_ftp.load
actions.load          cgid.conf          ident.load          proxy_http.load
alias.conf            cgid.load          imagemap.load       proxy.load
alias.load            cgi.load           include.load        proxy_scgi.load
asis.load             charset_lite.load  info.conf           reqtimeout.conf
auth_basic.load       dav_fs.conf        info.load           reqtimeout.load
auth_digest.load      dav_fs.load        ldap.conf           rewrite.load
authn_alias.load      dav.load           ldap.load           setenvif.conf
authn_anon.load       dav_lock.load      log_forensic.load   setenvif.load
authn_dbd.load        dbd.load           mem_cache.conf      speling.load
authn_dbm.load        deflate.conf       mem_cache.load      ssl.conf
authn_default.load    deflate.load       mime.conf           ssl.load
authn_file.load       dir.conf           mime.load           status.conf
```

Ahora activamos el módulo con el siguiente comando

```
root@ubuntu10:/etc/apache2/mods-available# a2enmod ssl
Enabling module ssl.
See /usr/share/doc/apache2.2-common/README.Debian.gz on how to configure SSL and
 create self-signed certificates.
Run '/etc/init.d/apache2 restart' to activate new configuration!
root@ubuntu10:/etc/apache2/mods-available#
```

Ahora habilitamos el sitio que se nos ha creado por defecto

```
root@ubuntu10:/etc/apache2/sites-available# a2ensite default-ssl
Enabling site default-ssl.
Run '/etc/init.d/apache2 reload' to activate new configuration!
root@ubuntu10:/etc/apache2/sites-available#
```

Ahora vamos a habilitar los certificados con los siguientes comandos

```
root@ubuntu:/etc/ssl/private# openssl genrsa -des3 -out ubuntu.key 1024
```

```
root@ubuntu:/etc/ssl/private# openssl req -new -key ubuntu.key -out server.csr
```

```
root@ubuntu:/etc/ssl/private# openssl x509 -req -days 365 -in server.csr -signke
y ubuntu.key -out ubuntu.crt
```

Ahora comprobamos que tenemos los certificados creados

```
root@ubuntu:/etc# cd ssl
root@ubuntu:/etc/ssl# cd private
root@ubuntu:/etc/ssl/private# ls
server.csr  ssl-cert-snakeoil.key  ubuntu.crt  ubuntu.key
```

Y nos vamos al sitio por defecto para configurarlo de la siguiente manera

```
GNU nano 2.2.2          Archivo: default-ssl          Modificado

      </Directory>

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

      #   A self-signed (snakeoil) certificate can be created by installing
      #   the ssl-cert package. See
      #   /usr/share/doc/apache2.2-common/README.Debian.gz for more info.
      #   If both key and certificate are stored in the same file, only the
      #   SSLCertificateFile directive is needed.
      SSLCertificateFile    /etc/ssl/private/ubuntu.crt
      SSLCertificateKeyFile /etc/ssl/private/ubuntu.key_
```

Ahora nos vamos al navegador del cliente y ponemos la https://10.33.10.3 , pero el final de la práctica no me sale

MARÍA ÁNGELES PEÑASCO SÁNCHEZ – ACTIVIDAD 15 – TEMA 4 – SRI