

# SERVIDORES WEB

## DE ALTAS PRESTACIONES

José David Torres de las Morenas

### Práctica 4

Lo primero que vamos a hacer es instalar un certificado SSL autofirmado, en cualquiera de las dos máquinas con servidor web activamos SSL en apache y creamos el certificado autofirmado.

```
root@ubuntu:/home/ubuntu# a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
    service apache2 restart
root@ubuntu:/home/ubuntu# systemctl restart apache2.service
root@ubuntu:/home/ubuntu# mkdir /etc/apache2/ssl
root@ubuntu:/home/ubuntu# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.crt
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to '/etc/apache2/ssl/apache.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Granada
Locality Name (eg, city) []:Granada
Organization Name (eg, company) [Internet Widgits Pty Ltd]:AsignaturaSwap
Organizational Unit Name (eg, section) []:AsignaturaSwap
Common Name (e.g. server FQDN or YOUR name) []:AsignaturaSwap
Email Address []:asignaturaswap@swap.com
```

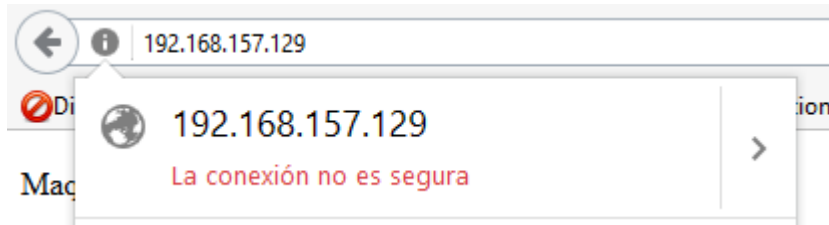
Ahora debemos modificar el archivo de configuración que se encuentra en la ruta /etc/apache2/sites-available/default-ssl.conf y modificar las siguientes líneas:

```
# A self-signed (snakeoil) certificate can be created by installing
# the ssl-cert package. See
# /usr/share/doc/apache2/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/apache2/ssl/apache.crt
SSLCertificateKeyFile   /etc/apache2/ssl/apache.key
```

Ahora activamos el sitio default-ssl y reiniciamos apache con las siguientes instrucciones:

```
a2ensite default-ssl
service apache2 reload
```

Y ya podemos acceder al navegador y ver que la navegación ahora no es segura en la dirección de la máquina donde hemos instalado el certificado:



## CONFIGURACIÓN DEL CORTAFUEGOS

Vamos a crear un nuevo archivo .sh donde guardaremos nuestro script con la siguiente instrucción:

```
sudo touch scriptIptables.sh
```

A continuación modificamos el archivo para guardar en el nuestro siguiente script:

```
sudo nano scriptIptables.sh
```

```
iptables -F
iptables -X
iptables -Z
iptables -t nat -F

iptables -P INPUT DROP
iptables -P OUTPUT DROP

iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

iptables -A INPUT -i eth0 -p tcp -m multiport --dports 22,80,443 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -m multiport --sports 22,80,443 -m state --state ESTABLISHED -j ACCEPT

iptables -L -n -v
```

Tras esto, podemos ver la salida por pantalla de este script con la siguiente instrucción:

```
sh scriptIptables.sh
```

```
root@ubuntu:/etc# sh scriptIptables.sh
Chain INPUT (policy DROP 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source            destination
  0      0 ACCEPT    all  --  lo      *        0.0.0.0/0         0.0.0.0/0
  0      0 ACCEPT    tcp    --  eth0    *        0.0.0.0/0         0.0.0.0/0          multiport d
ports 22,80,443 state NEW,ESTABLISHED

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source            destination

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source            destination
  0      0 ACCEPT    all  --  *       lo      0.0.0.0/0         0.0.0.0/0
  0      0 ACCEPT    tcp    --  *       eth0    0.0.0.0/0         0.0.0.0/0          multiport s
ports 22,80,443 state ESTABLISHED
```