SANOG 16

Apache 2.2 with SSL

In /etc/rc.conf, add the following line

apache22_enable="YES"

To start apache run

$ /usr/local/etc/rc.d/apache22 start

Creating the SSL Certificates:

$ cd /usr/local/etc/apache22/

$ openssl genrsa -des3 -out server.key 1024

A passphrase is requested, to protect the key,** between 4-23 characters.

This passphrase will be needed at every apache restart, since the apache server does not know the passphrase to unlock the key.

Enter a passphrase for the key, for example '1234' (this is required) but we will get rid of it (so we don't have to type the passphrase every time we type apache):

$ cp server.key server.key.org

$ openssl rsa -in server.key.org -out server.key

Once again, type your passphrase ('1234'), and now the file “server.key” will contain an *un*encrypted key.

Create Certificate Request

$openssl req -new -key server.key -out server.csr

Answer similarly to the following, replacing the values for YOUR domain name:

```
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]:BT
State or Province Name (full name) [Some-State]:.  <- just type .
Locality Name (eg, city) []:Paro
Organization Name (eg, company) [Internet Widgits Pty]:SANOG 16
Organizational Unit Name (eg, section) []:Workshop 3
Common Name (eg, YOUR name) []:www.phil.ws3.conference.sanog.org
Email Address []:regnauld@nsrc.org

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:      (just press return)
An optional company name []:  (just press return)
```

You have now generated your Certificate Signing Request. We need to SIGN it now:

Self Signing your Own Certificate

$ openssl x509 -req -days 3650 -in server.csr -signkey server.key -out server.crt

You should see output similar to this:

Signature ok
subject=/C=BT/L=Paro/O=SANOG 16/OU=Workshop 3/
CN=www.phil.ws3.conference.sanog.org/emailAddress=regnauld@nsrc.org
Getting Private key

Enabling SSL

Edit /usr/local/etc/apache22/httpd.conf file, find the line:

 # Include etc/apache22/extra/httpd-ssl.conf

and UNcomment it:

Include etc/apache22/extra/httpd-ssl.conf

Edit **/usr/local/etc/apache22/extra/httpd-ssl.conf**

Two lines control where the Certificate and Key are located, these are:

SSLCertificateFile "/usr/local/etc/apache22/server.crt"

and

SSLCertificateKeyFile "/usr/local/etc/apache22/server.key"

This is the default, and this is where we have placed our certificate – so we can just leave it alone. Find the line:

ServerName www.phil.ws3.conference.sanog.org:443
ServerAdmin your@email.addr.ess

Now, restart apache:

/usr/local/etc/rc.d/apache22 restart

Now, try to access, using a web browser on your computer:

httpS://www.YOURDOMAIN.ws3.conference.sanog.org

What do you observe ?