Servicios de Alto Nivel en Redes Informáticas

Práctica 4 : “Apache y SSL”

Acedo Legarre, Aitor.
Puértolas Rebollar, Cristina.
Año 2002/2003.
4º Ingeniería Informática.

ENTORNO HW

vendor_id : GenuineIntel
model name : Intel(R) Celeron(TM) CPU 1300MHz
cpu MHz : 1300.038
cache size : 256 KB

ENTORNO SW

Linux version 2.4.18 (gcc version 2.95.4 20011002 (Debian prerelease))

SOFTWARE Y DESCARGAS

```
lynx http://httpd.apache.org/dist/httpd/apache_1.3.27.tar.gz
lynx ftp://ftp.modssl.org/source/mod_ssl-2.8.14-1.3.27.tar.gz
lynx ftp://ftp.openssl.org/source/openssl-0.9.7.tar.gz

gzip -d -c apache_1.3.27.tar.gz | tar xvf -
gzip -d -c mod_ssl-2.8.14-1.3.27.tar.gz | tar xvf -
gzip -d -c openssl-0.9.7a.tar.gz | tar xvf -
```

COMPILADOR DE 'C' E INTÉRPRETE DE PERL

Para comprobar las versiones del compilador de c e intérprete de Perl a tener en cuenta en la instalación de Apache, haremos 'dpkg -l <nombre_paquete>', pudiendo ver si esta instalado o no, junto con la versión incluida en esta instalación:

```
/ Name       Version      Description
==============================================================
ii  perl-base      5.004.05-1.1   Fake package assuring that one of the
-base
ii  gcc            2.95.2-13      The GNU C compiler.
```

Ambas versiones son suficientes para las ampliaciones / dependencias en / de la instalación de apache.

PASOS PREVIOS A LA INTALACIÓN DEL APACHE

Creación de un usuario sin privilegios en la máquina denominado 'apache', este usuario no tendrá un shell para entrar en la máquina.

UID=1008
GID=1008

Esta es la línea que nos quedará en el fichero /etc/passwd después de crear nuestro usuario virtual:

```
apache:x:1008:1008:,,,:/home/apache:/bin/false
```

CONFIGURACIÓN DE LA INSTALACIÓN DE APACHE (mod_ssl)

1. Construir OpenSSL

```
$ cd openssl-0.9.7a
$ ./config
$ make
$ cd ..
```

2. Construir e instalar SSL-aware Apache

```
$ cd mod_ssl-2.8.14-1.3.27
$ ./configure --with-apache=../apache_1.3.27 \
  --with-ssl=../openssl-0.9.7a \
  --prefix=/usr/local/apache
$ cd ..
$ cd apache_1.3.27
# make
# make certificate
```

La salida que obtenemos una vez completado el formulario que resulta de configurar el certificado es :

```
This Certificate belongs to:
  localhost
  sutra@lr07.cps.unizar.es
  Sanri Team
  Cps
  Zaragoza, Aragon, ES

  This Certificate was issued by:
  Snake Oil CA
  ca@snakeoil.dom
  Certificate Authority
  Snake Oil, Ltd
  Snake Town, Snake Desert, XY
  Serial Number: 01

Certificate Fingerprint:
8E:A4:82:40:BF:CC:6D:6B:75:25:F2:61:52:3A:CB:79

**************************************************************************
RESULT: Server Certification Files

o  conf/ssl.key/server.key

    The PEM-encoded RSA private key file which you configure
    with the 'SSLCertificateKeyFile' directive (automatically done
    when you install via APACI). KEEP THIS FILE PRIVATE!

o  conf/ssl.crt/server.crt

    The PEM-encoded X.509 certificate file which you configure
    with the 'SSLCertificateFile' directive (automatically done
    when you install via APACI).

 o  conf/ssl.csr/server.csr

   The PEM-encoded X.509 certificate signing request file which
   you can send to an official Certificate Authority (CA) in order
   to request a real server certificate (signed by this CA instead
   of our demonstration-only Snake Oil CA) which later can replace
   the conf/ssl.crt/server.crt file.

      # make install
```

Y la salida que obtenemos al hacer exitosamente el 'make install' es:

```
+--------------------------------------------------------------+
| You now have successfully built and installed the            |
| Apache 1.3 HTTP server. To verify that Apache actually       |
| works correctly you now should first check the               |
| (initially created or preserved) configuration files         |
|                                                              |
|   /usr/local/apache/conf/httpd.conf                          |
|                                                              |
| and then you should be able to immediately fire up           |
|                                                              |
| Apache the first time by running:                            |
|  /usr/local/apache/bin/apachectl start                       |
|                                                              |
| Or when you want to run it with SSL enabled use:             |
|                                                              |
|   /usr/local/apache/bin/apachectl startssl                   |
|                                                              |
| Thanks for using Apache.       The Apache Group              |
|                                http://www.apache.org/        |
|                                                              |
+--------------------------------------------------------------+
```

FICHERO DE CONFIGURACIÓN 'httpd.conf'

```
##
## httpd.conf -- Apache HTTP server configuration file
##

### Section 1: Global Environment
#
# El servidor Apache correrá en modo standalone, es decir,
# independiente al demonio inetd.
#
ServerType standalone

#
# ServerRoot: Directorio raíz del arbol de directorios del servidor,
# en el cual se encuentran ficheros de configuración, de error, y logs.
# También colgarán de aquí los fuentes de nuestras páginas estáticas.
#
ServerRoot "/usr/local/apache"

#
# PidFile: Fichero donde el servidor debe registrar el número de
# identificador de proceso con el que se inicia.
#
PidFile /usr/local/apache/logs/httpd.pid

#
# SocreBoardFile: Fichero utilizado para guardar la información de
# los procesos del servidor.
#
ScoreBoardFile /usr/local/apache/logs/httpd.scoreboard

#
# KeepAlive: Activa o desactiva la opción de aceptar conexiones
# persistentes al servidor.
#
KeepAlive On
```

```
#
# MaxKeepAliveRequests: Número máximo de peticiones permitidas durante
# una conexión persistente.
#
MaxKeepAliveRequests 100

#
# KeepAliveTimeout: Numero de segundos que se ha de esperar para la
# siguiente petición desde el mismo cliente en la misma conexión.
#
KeepAliveTimeout 15

#
# MaxRequestsPerChild: número de peticiones que cada proceso hijo puede
# realizar, antes de que el hijo muera. Si = 0, infinitas.
#
MaxRequestsPerChild 0

#
# Port: Puerto al cual estará escuchando el servidor en modo
# standalone.
#
Port 8080

##
##  SSL Support
##
## Cuando se provea de SSL , el servidor deberá escuchar a los puertos
## 8080 y 8443 según el estándar del protocolo http y https
## respectivamente.
##

<IfDefine SSL>
Listen 8080
Listen 8443
</IfDefine>

#
# Como queremos que corra httpd de un modo más seguro, nos hemos creado
# el usuario 'apache' sin shell, que será propietario de ese servicio.

User apache
Group apache

#
# ServerAdmin: Dirección a la que se podrá enviar correo electrónico
# (como cliente) en caso de fallos o problemas del servidor.
#

ServerAdmin sutra@Lr07.cps.unizar.es

#
# ServerName: cadena de texto que representa a la máquina en la que
# esta corriendo el servicio.
# Hemos puesto localhost porque estamos en modo de prueba, pero lo suyo
# sería indicar la IP de la máquina, así también será independiente de
# la resolución de nombres (DNS).
# ServerName 155.154.210.194
```

ServerName localhost

```
#
# DocumentRoot: Directorio desde el cual serviremos los documentos.
#

DocumentRoot "/usr/local/apache/htdocs"

#
# Cada directorio al cual Apache tiene acceso puede ser configurado con
# respecto a qué servicios y cualidades tienen permisos sobre dicho
# directorio.
#
# La primera configuración de todas es la más restrictiva, que luego
# iremos modificando para nuestro caso particular.
#

<Directory />
    Options FollowSymLinks
    AllowOverride None
</Directory>

#
# Desde el directorio raíz de nuestro servidor...
#

<Directory "/usr/local/apache/htdocs">
    Order allow,deny
    Allow from all
</Directory>

#
# Las líneas que siguen previenen que todos aquellos ficheros
# que comiencen por .ht en nuestro servidor web no se puedan acceder
# desde cualquier cliente. Deshabilitadas por motivos de seguridad.
#

<Files ~ "^\.ht">
    Order allow,deny
    Deny from all
    Satisfy All
</Files>

# Permisos especiales para cumplir los requisitos de la práctica.
# Antes de nada cabe mencionar que el orden de las etiquetas
# deny y allow del tag 'Order' tienen significados por defecto:
#
# Order deny, allow --> por defecto das permiso a todos, y
# evalúa SI EXISTEN las etiqueta deny y después la allow.
#
# Order allow, deny --> por defecto niegas los permisos a todos, y
# evalúa SI EXISTEN las etiquetas allow y después deny.
#
# Dar permiso a todos a la página principal.

<Files index.html>
        Order deny,allow
        Allow from all
</Files>
```

```
# Dar permiso sólo a esta máquina.

<Files tuIP.html>
        Order deny,allow
        Deny from all
        Allow from 127.0.0.1
</Files>

# Dar permiso a las máquinas que pertenecen a la subred del
# laboratorio.

<Files laboratorio.html>
        Order deny,allow
        Deny from All
        Allow from 155.210.154.0/24
        Allow from 127.0.0.1
</Files>

# Denegar el acceso a la máquina cuya IP sea 155.210.154.193.

<Files niegaIP.html>
        Order deny,allow
        Deny from 155.210.154.193
</Files>

# Acceso restringido a través de contraseñas.

<Files erestu.html>
       AuthName "Gente_del_laboratorio"
       AuthGroupFile /dev/null
       AuthType Basic
       AuthUserFile /usr/local/apache/passwd/.htpasswd
       Require valid-user
</Files>
```

CREACIÓN DEL FICHERO DE CONTRASEÑAS PARA EL ACCESO RESTRINGIDO

Ejecutar el siguiente comando si el fichero de contraseñas se crea por primera vez:

```
/usr/local/apache/bin/htpasswd -c <fichero_de_pass_nuevo>
```

Si queremos añadir un usuario nuevo ejectuar el siguiente comando:

```
sudo ../htpasswd ../passwd/.htpasswd sanri
```

**Nota: Refresco de navegador para autentificación no sirve, se queda con la sesión del último usuario autentificado todo el rato. (Esto ocurre con autentificación básica)

CONTRASEÑA DE ACTIVACIÓN DEL MODULO SSL

```
$ cd /usr/local/apache/bin
# sudo ./apachectl startssl

Apache/1.3.27 mod_ssl/2.8.14 (Pass Phrase Dialog)
Some of your private key files are encrypted for security
reasons.
In order to read them you have to provide us with the pass
phrases.
Server Lr07.cps.unizar.es:8443 (RSA)
Enter pass phrase:
(KEY: "debian rules")
```