Javier García Peña

Generación y activado de certificado autofirmado SSL:

Podemos generar un certificado oficial si tenemos un servidor real conectado a internet(los más fácil es contratar uno) pero en el caso de esta práctica nos autofirmaremos uno, el cual nos dará un aviso de que no es fiable en los navegadores.

Para generarlo ejecutaremos como usuario root:
“a2enmod ssl”
“service apache2 restart”
“mkdir /etc/apache2/ssl”
“openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.crt”

Una vez ejecutemos estos comandos tendremos que rellenar los datos para el certificado ssl, una vez terminemos vamos a configurar el archivo /etc/apache2/sites-available/default-ssl, y dentro añadiremos después de la linea donde pone “SSLEngine on”:
SSLCertificateFile /etc/apache2/ssl/apache.crt
SSLCertificateKeyFile /etc/apache2/ssl/apache.key

Ya estará todo preparado para que activemos el archivo que acabamos de editar con el comando:
a2ensite default-ssl

Ahora solo nos queda reiniciar apache para que se den los cambios.
service apache2 reload

Configuración del firewall iptables:

Para facilitar el uso y asegurarnos de que el firewall está siempre activo, creamos un script con la configuración de este que sera iniciado mediante crontab cada vez que la máquina arranque.

```
# (1) Eliminar todas las reglas (configuración limpia)
iptables -F
iptables -X
iptables -Z
iptables -t nat -F

# (2) Política por defecto: denegar todo el tráfico
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

# (3) Permitir cualquier acceso desde localhost (interface lo)
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# (4) Abrir el puerto 22 para permitir el acceso por SSH
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT

# (5) Abrir los puertos HTTP (80) de servidor web
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT

# (6) Abrir los puertos HTTPS (443) de servidor web
iptables -A INPUT -p tcp --dport 443 -j ACCEPT
```

```
iptables -A OUTPUT -p tcp --sport 443 -j ACCEPT
```