Práctica 2.3: Acceso seguro con Nginx

Tabla de Contenido

Requisitos antes de comenzar la práctica

- La práctica Instalación de Nginx o la práctica Autenticación básica ha de estar funcionando correctamente.
- No empezar la práctica antes de tener la práctica anterior funcionando y comprobada.

1. Introducción

El acceso seguro mediante certificados TLS/SSL es una obligación en cualquier sitio web que se precie al que queramos acceder.

1.1. Prerequisitos

Durante la por tarea el nombre usaremos del dominio `example.com` que estés utilizando.

Necesitaremos un nombre de servidor y un registro DNS para nuestro servidor.

- Un registro `A` con `example.com` apuntando a la IP de nuestro servidor.
- Un registro A con `www.example.com` apuntando a la IP de nuestro servidor.

Alternativamente para las pruebas podemos modificar el archivo `hosts` para crear estos registros para las pruebas.

2. Configuración de Nginx

2.1. Nombre de servidor

Crearemos el fichero para nuestro dominio que suponemos `/etc/nginx/sites-available/example.com` y estableceremos la directiva `server_name` apropiadamente.

```
$ sudo nano /etc/nginx/sites-available/example.com
```

Modificaremos la opción `server_name`

Fragmento del fichero `/etc/nginx/sites-available/example.com`

```
server_name example.com www.example.com;
```

Comprobaremos que no hemos introducido ningún error de sintáxis en la configuración.

```
$ sudo nginx -t
```

Reiniciaremos el servicio

```
$ sudo systemctl reload nginx
```

3. Configuración del cortafuegos

Si no tenemos instalado un cortafuegos, usaremos `ufw`

```
$ sudo apt install ufw
```

Comprobaremos si el cortafuegos está activo y cuales son los perfiles que tiene activado.

```
$ sudo ufw status
```

Activaremos el perfil para permitir el tráfico HTTPS

```
$ sudo ufw allow ssh ①
$ sudo ufw allow 'Nginx Full'
$ sudo ufw delete allow 'Nginx HTTP' ②
```

① Permitir la conexión SSH

② Borrar las reglas HTTP en caso de que estuvieran para evitar duplicación

Comprobaremos el status que debe ser parecido a este

```
$ sudo ufw status
Status: active
To                 Action   From
--                 ------   ----
Nginx Full         ALLOW    Anywhere
Nginx Full (v6)    ALLOW    Anywhere(v6)
```

Activaremos el cortafuegos

```
$sudo ufw --force enable
```

4. Generar un certificado autofirmado

El certificado almacenará información básica acerca del sitio web, y estará acompañada de un fichero de clave privada que permite al servidor manejar los datos cifrados enviados al servidor.

Crearemos la clave SSL y el certificado con el comando `openssl`.

```
$ sudo openssl req -x509 -nodes -days 365 \ ①
       -newkey rsa:2048 -keyout /etc/ssl/private/example.com.key \ ②
       -out /etc/ssl/certs/example.com.crt ③
```

① Utilizamos `\` para dividir el comando en varias lineas

② Cambiar por el nombre de nuestro dominio

③ Idem del anterior

Salida del comando `openssl`

```
Generating a RSA private key
....+++++
.....................................+++++
writing new private key to '/etc/ssl/private/example.com.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]:Andalucía
Locality Name (eg, city) []:Granada
Organization Name (eg, company) [Internet Widgits Pty Ltd]:IZV
```

```
Organizational Unit Name (eg, section) []:WEB
Common Name (e.g. server FQDN or YOUR name) []:example.com ①
Email Address []:webmaster@example.com
```

① Pondremos nuestro nombre de dominio

5. Configuración

Añadiremos a la configuración de nuestro sitio `example.com` (que ya tenías antes hecho) el uso de certificado SSL.

Fichero `example.com`

```
server {
  listen 80;
  listen 443 ssl;
  server_name example.com www.example.com;
  root /var/www/example.com/html;
  ssl_certificate /etc/ssl/certs/example.com.crt;
  ssl_certificate_key /etc/ssl/private/example.com.key;
  ssl_protocols TLSv1 TLSv1.1 TLSv1.2 TLSv1.3;
  ssl_ciphers HIGH:!aNULL:!MD5;

  location / {
    try_files $uri $uri/ =404;
  }
}
```

Comprobaremos la configuración:

```
$ sudo nginx -t
```

y recargaremos el servidor

```
$ sudo systemctl reload nginx
```

6. Prueba

Por último, si no lo hemos hecho, configuraremos el DNS para que el nombre de nuestro dominio nos lleve a la dirección IP de nuestro servidor web. Accede a la dirección de tu servidor web y enseñale al profesor su funcionamiento.