DAW Práctica 2.3: Autentificación y control de acceso

Elabora un documento donde figuren todos los pasos realizados con las pantallas significativas, explicando cada uno de los pasos.

En esta práctica se implementará la autentificación para obtener un control de acceso en Nginx y Apache.

Procedimiento:

Nginx

1. En este caso, se utilizará la herramienta **openssl** para crear las contraseñas. Podemos comprobar una lista de los paquetes instalados con dpkg -l. Si queremos filtrar esa lista a únicamente lo que nos interesa, podemos añadir | grep openssl.

   ```
   dpkg -l | grep openssl
   ```

2. En caso de no encontrarlo, se deberá instalar.

3. Para almacenar nuestros usuarios y contraseñas deberemos crear un fichero oculto en /etc/nginx llamado .htpasswd. El formato que seguirá este archivo es ***nombreDeUsuario:$ContraseñaCrifrada***.

4. Para crear cada uno de los usuarios que tengan acceso nuestro servicio, nos podemos ayudar del siguiente comando:

   ```
   sudo sh -c "echo 'nombre_usuario':$(openssl passwd -apr1)' >> /etc/nginx/.htpasswd"
   ```

5. Comenta qué hace el comando.

6. Crea al menos dos usuarios y confirma que sus contraseñas aparecen cifradas en el documento.

7. Se deberá modificar el fichero de configuración de nuestro servidor web. Primero se elegirán qué recursos estarán protegidos. Nginx permite añadir restricciones a nivel de servidor o en un location (directorio o archivo) específico. En este caso vamos a proteger el document root (la página principal) de nuestro sitio. Para ello, añadiremos lo siguiente al fichero de configuración en la sección de la raíz:

```
location / {
        try_files $uri $uri/ =404;
        auth_basic "Zona restringida";
        auth_basic_user_file /etc/nginx/.htpasswd;
}
```

8. Comprobar que no hay errores de configuración.

9. Reiniciar el servicio.

10. Probar si realmente solicita una autentificación y si realiza su función.

11. ¿Qué error aparece si no realizamos la autentificación? ¿Podrías realizar un html qué aparezca en lugar de ese error?

Apache

1. Por cambiar, en Apache se puede utilizar el comando htpasswd para crear la contraseña. Esta instrucción en nuestro sistema se debería encontrar dentro del paquete apache2-utils. Comprueba que este paquete se encuentra dentro del sistema.

2. En caso de no encontrarlo, se deberá instalar.

3. Se creará un fichero oculto en /etc/apache2 llamado .htpasswd. Utilizando el comando htpasswd directamente podemos crear el fichero con el primer usuario:

   ```
   htpasswd -c /etc/apache2/.htpasswd nombre_ejemplo
   ```

   ¿Qué utilidad tiene la extensión -c?

4. Añade más usuarios utilizando el comando htpasswd.

5. Comprueba que las contraseñas de los diferentes usuarios que has creado en el fichero aparecen cifradas.

6. Este método para crear usuarios con contraseña es igual de válido que el implementado para Nginx. Confírmalo creando un nuevo usuario con su contraseña utilizando la otra implementación.

7. Se deberá modificar el fichero de configuración de nuestro host virtual de Apache. Para ello añadiremos lo siguiente:

```
<Directory "/var/www/html/SERVIDORWEB">
        AuthType Basic
        AuthName "Acceso Restringido"
        AuthUserFile /etc/apache2/.htpasswd
        Require valid-user
</Directory>
```

Si en lugar de archivos que se encuentran en un directorio, se quiere implementar en una localización en concreto (como en el caso de Nginx), la configuración será similar modificando la etiqueta **Directory + "ruta"** por **Location + "ruta"**.

8. Comprobar posibles errores de sintaxis.

9. Reiniciar el servicio.

10. Probar el correcto funcionamiento de la autentificación.

11. Si quieres eliminar un usuario únicamente deberás modificar el fichero htpasswd. En cambio, si quieres modificar una contraseña, no es necesario eliminar el usuario y crearlo de nuevo. Es posible modificar una contraseña volviendo a ejecutar el comando htpasswd con un nombre de usuario que ya existe dentro del fichero. Modifica la contraseña de un usuario y comprueba que se ha actualizado.

12. Crea un html que aparezca cuando no queramos meter las credenciales y no nos autoricen el acceso.