Práctica: Cifrado seguro de archivos en una instancia EC2 usando OpenSSL

Objetivos de la práctica

- Comprender qué significa cifrar y descifrar información.
- Usar OpenSSL aplicando buenas prácticas modernas (-pbkdf2, -iter).
- Diferenciar entre texto en claro y texto cifrado.
- Aprender dos métodos de cifrado:
    - Con contraseña
    - Con archivo de clave (más profesional)
- Relacionar estos conceptos con HTTPS, bases de datos cifradas o AWS KMS.

Recursos necesarios

- Cuenta AWS Academy o estándar
- Instancia EC2 Ubuntu o Amazon Linux (t2.micro)
- Clave .pem
- Conexión SSH

Enunciado de la práctica

1️⃣Conexión a la instancia EC2

Crea una instancia EC2 con Ubuntu / Amazon Linux.

Descarga tu clave .pem.

Conéctate:

```
ssh -i clave.pem ubuntu@IP_PUBLICA
```

2️⃣Comprobar si OpenSSL está instalado

```
openssl version
```

Si no está instalado:

```
sudo apt update
sudo apt install openssl -y
```

3️⃣Creación de un documento con información sensible

```
echo "Nombre: Alicia Blanco
DNI: 12345678Z
Email: ana@example.com" > datos.txt
```

Comprobamos la creación y contenido del archivo

```
cat datos.txt
```

4️⃣Cifrado seguro (con COntraseña)

Usaremos AES-256-CBC + PBKDF2 + 100.000 iteraciones.

Cifrar archivo

```
openssl enc -aes-256-cbc -salt -pbkdf2 -iter 100000 -in datos.txt -out
datos_cifrados.enc
```

Introduciremos una contraseña que debemos recordar

Vemos el archivo cifrado

```
ls -l
cat datos_cifrados.enc
```

Si todo ha ido bien, debe ser ilegible

5️⃣Intento de descifrado sin clave (debe fallar)

```
openssl enc -aes-256-cbc -d -pbkdf2 -iter 100000 -in datos_cifrados.enc
```

Nos aparecerá un mensaje de error

6️⃣Descifrar correctamente

```
openssl enc -aes-256-cbc -d -pbkdf2 -iter 100000 -in datos_cifrados.enc -out
datos_descifrados.txt
```

Vemos el contenido

```
cat datos_descifrados.txt
```

7️⃣Comparación de Archivos

```
ls -lh datos*
diff datos.txt datos_descifrados.txt
```

8️⃣Cifrado con archivo de clave Este método es muy usado en aplicaciones reales.

6.1 Crear una clave secreta aleatoria

```
openssl rand -base64 32 > clave.key
```

6.2 Cifrar usando el archivo de clave

```
openssl enc -aes-256-cbc -salt -pbkdf2 -iter 100000 -in datos.txt -out
datos_key.enc -pass file:./clave.key
```

6.3 Descifrar usando el archivo de clave

```
openssl enc -aes-256-cbc -d -pbkdf2 -iter 100000 -in datos_key.enc -out
datos_key_descifrado.txt -pass file:./clave.key
```

Verificar:

```
cat datos_key_descifrado.txt
```

Actividades

Deberéis elaborar un documento que contenga:

A. Capturas obligatorias

- Contenido de datos.txt
- Cifrado con contraseña
- Error al descifrar sin clave
- Descifrado correcto
- Cifrado usando archivo de clave
- Descifrado usando archivo de clave

B. Preguntas teóricas

- ¿Por qué es más seguro usar -pbkdf2 y -iter 100000?
- Diferencia entre cifrar y ocultar un archivo.
- ¿Qué ocurre si se pierde la contraseña usada para cifrar?
- Diferencias entre:
    - cifrado con contraseña
    - cifrado con archivo de clave