**PRÁCTICA 3 – CRIPTOGRAFÍA 1**

**NOTA**

La carpeta volume\_data está en la carpeta lab\_xx de cada sesión, y se mete en la de cada contenedor

La carpeta shared está dentro de Kali o de Ubuntu

Para pasarles algo, se copia en la carpeta volume\_data correspondiente y estará en su carpeta shared

Para entrar en shared de Kali por ejemplo, cd .. dos veces y cd shared

Para pasar algo de Kali a Ubuntu, meterlo en la carpeta shared de Kali, copiarlo de la Kali de volume\_data a la Ubuntu de volume\_data y estará en la shared de ubuntu

**OFUSCAR INFO EN IMÁGENES CON STEGHIDE**

steghide embed -cf fotop3.jpg -ef mensaje.txt

Poner la contraseña que quieras

Para extraer el mensaje:

steghide extract -sf fotop3.jpg

cat mensaje.txt y te sale el mensaje.

**CRIPTOGRAFÍA SIMÉTRICA**

**Cifrar un archivo utilizando un algoritmo de clave simétrica fuerte**

encriptar archivo: openssl enc -aes-128-ecb -in archivo.txt -out archivo\_cifrado.enc

desencriptarlo: openssl enc -d -aes-128-ecb -d -in archivo\_cifrado.enc -out archivo\_descifrado.txt

**Cifrado de imágenes – modo ECB**

convertir una imagen a ppm y separar cabecera y cuerpo:

convert image.png image.ppm

head -n 3 image.ppm > cabecera.txt

tail -n +4 image.ppm > cuerpo.bin

unirla: cat cabecera.txt <fichero con el cuerpo cifrado> > <nombre de la unión>.ppm

gimp imagenunida.ppm -> la abre

Aún cifrando el cuerpo, se intuyen las líneas del dibujo, lo cual puede llevar a filtraciones de datos

**Cifrado de imágenes – modo CBC**

encriptar el cuerpo con un vector de inicialización generado:

generar el vector -> openssl rand -hex 16 y pegarlo al final del siguiente comando

openssl enc -aes-128-cbc -e -in cuerpo.bin -out cuerpocifrado.enc -iv 772d117623d77dad384c69c9559cc141

Ahora no se intuyen las lineas del dibujo

**Cifrado de discos – crear una carpeta que cifre automáticamente lo que metas dentro**

• Instala el software de cifrado de disco: sudo apt install ecryptfs-utils

• Crea una carpeta para cifrar en tu directorio home. Si usas una existente, asegúrate de que esté vacía (si no, haz una copia de seguridad de su contenido... por si acaso \*+,-./)

• Cifra la carpeta montándola bajo el sistema de ficheros ecryptfsà mount -t ecryptfs (sí, el punto de montaje y la carpeta son los mismos. Por ejemplo, mount -t ecryptfs /home/ssiuser/secure /home/ssiuser/secure). Necesitarás permisos de root

• Elije un algoritmo de cifrado simétrico apropiado de acuerdo con la teoría.

• Elije 32 bytes para la clave.

• Elije No en la opción plaintext passthrough.

• Elije No a cifrar nombres de archivo (aunque este es un detalle menor)

• Responde Yes a las dos preguntas siguientes (aparecen si este es el primer uso de cifrado de disco en el sistema operativo, que debería)

• Comprueba con el comando mount que el punto de montaje está montado como cifrado.

• Copia o crea un archivo de texto en la carpeta cifrada. ¿Puedes leerlo?

• Desmonta el punto de montaje cifrado con sudo umount /home/secure. ¿Puedes leer su contenido ahora? (por favor, ¡sal de la carpeta antes de desmontarla! \*+,-./)

• Móntalo de nuevo con los mismos parámetros. ¿Puedes volver a leer el contenido?

**Introducción al cracking de contraseñas sin conexión**

**John the Ripper para romper OpenSSL**

Necesitamos un diccionario: disponible en rockyou.txt en el directorio wordlist de Kali

Crea un fichero a descifrar de la misma forma que lo hiciste en el ejercicio L3B2\_SYMCRIPT (con la contraseña “password”), pero usando el formato AES-128-CBC. Como dijimos, debes procesarlo previamente con la utilidad openssl2john instalada en el contenedor Kali de la infraestructura del Lab 3 (el paquete john predeterminado de Ubuntu no lo incluye). Almacena la salida en un archivo y recuerda bien el formato de la hash que te extrae que le has puesto en el parámetro -m

openssl enc -aes-128-cbc -in lab3Cifrar.txt -out mensaje.txt -pass pass:password

/usr/share/john/openssl2john.py -c 1 -m 2 mensaje.txt > secret.hash

john --wordlist=/wordlist/rockyou.txt secret.hash

john --show secret.hash

**John the Ripper + contraseñas de usuario + generador de listas de palabras Crunch**

Hacerlo en kali

Primero, unir los ficheros passwd y shadow con unshadow

sudo unshadow /wordlist/passwd /wordlist/shadow > /home/ssiuser/unshadowed.txt

Ahora, generar diccionario personalizado con Crunch

Sabemos que la contraseña tiene la forma **testXYZ** donde **XYZ** puede ser tres letras minúsculas o tres números. Vamos a generar una lista de palabras usando **crunch**:

* **Para contraseñas con tres letras minúsculas:**

crunch 7 7 -t test@@@ -o /home/ssiuser/custom\_wordlist.txt

* **Para contraseñas con tres números y más dígitos:**

crunch 10 10 -t test%%%... -o /home/ssiuser/custom\_wordlist2.txt

Esto generará dos listas separadas. Para unir ambas listas en un solo archivo:

cat /home/ssiuser/custom\_wordlist.txt /home/ssiuser/custom\_wordlist2.txt > /home/ssiuser/custom\_wordlist.txt

Ahora, usar john the ripper con el diccionario personalizado

john --wordlist=/home/ssiuser/custom\_wordlist.txt /home/ssiuser/unshadowed.txt

john --show /home/ssiuser/unshadowed.txt

**"Fuerza bruta pura" con John the Ripper**

• Elimina el archivo john.pot que está en el directorio .john oculto de la carpeta en la que estás trabajando. Si no lo haces, y john ya ha descifrado una contraseña en una ejecución anterior, john te informará de que la contraseña ya ha sido descifrada y no calculará nada, ¡aunque queden algunas contraseñas sin descifrar!

rm -rf ~/.john/john.pot

Ejecuta john en modo incremental

john --incremental --max-length=4 archivo\_con\_hash