Taller 1: Criptografía Simétrica y Esteganografía

Para el desarrollo de este taller debe crear un informe en formato `.doc` o formato `.odt` en el cual debe colocar las respuestas a todas las preguntas **resaltadas en negritas** que encuentre en las siguientes Secciones. Al finalizar el taller envíe su respectivo informe al profesor. El informe debe incluir su nombre y número de cédula al principio.

1. Criptografía Simétrica con OpenSSL

Para realizar encriptado simétrico utilizaremos la interfaz de linea de comandos de la biblioteca OpenSSL.

1. Ejecute el comando "`openssl`". Esto abre la terminal interactiva de OpenSSL.
2. Dentro de la terminal de OpenSSL ejecute el comando "`help`". **Identifique en la sección titulada "Cipher commands" cuales algoritmos de cifrado puede utilizar OpenSSL**.
3. Cierre la terminal de OpenSSL con el comando "`exit`".
4. Cifre el archivo "taller_1.pdf" utilizando el comando "`openssl aes-256-cbc -a -in taller_1.pdf -out taller_1.enc`"[1]. La opción "`-a`" de OpenSSL indica que el archivo de salida debe ser codificado en formato Base64. Sin esta opción, el archivo de salida sería un archivo binario.
5. Para descifrar el archivo ejecute el comando "`openssl aes-256-cbc -d -a -in taller_1.pdf -out taller_1.enc`". Nótese la opción adicional "`-d`" que indica que la operación a realizar es un desencriptado.

2. Ataques de Fuerza Bruta con John the Ripper

John the Ripper es una herramienta para aplicar ataques de diccionario a archivos encriptados. Para poder utilizarla en las computadoras del laboratorio hace falta compilarla primero. Para esto ejecute los siguientes pasos:

1. Instale los siguientes paquetes con el comando "`apt`" como usuario `root`:
   - build-essential
   - libssl-dev
   - git
   - zlib1g-dev
   - yasm
   - libgmp-dev
   - libpcap-dev
   - pkg-config
   - libbz2-dev
2. Entre al subdirectorio "src" de la distribución de John the Ripper y ejecute el comando "`./configure && make -s clean && make -sj 2`"
3. Cuando termine la compilación encontrará el programa `john` en el subdirectorio "run" de John the Ripper.

Probaremos utilizar John the Ripper para obtener el password de cifrado de un par de claves SSH[2].

[1] Este comando pedirá la clave de cifrado dos veces para su verificación.
[2] La teoría y uso de las claves de SSH se estudiarán en la clase de Criptografía Asimétrica y en el taller 2

1. Abra una terminal en el subdirectorio "run" de John the Ripper.
2. Cree un par de claves ssh con el siguiente comando "`ssh-keygen -t rsa -C 'taller'`". Cuando el comando pregunte el nombre del archivo de claves a generar coloque "prueba_rsa". Cuando el comando pregunte la clave de cifrado coloque "Beatles".
3. Copie el archivo "words.txt" adjunto a este enunciado dentro del mismo subdirectorio "run".
4. Ejecute el siguiente comando dentro del subdirectorio "run": "`./ssh2john prueba_rsa >prueba_rsa.hash`". Esto genera un archivo "prueba_rsa.hash" el cual describe al archivo "prueba_rsa" de
5. Ejecute el comando "`./john --wordlist=words.txt prueba_rsa.hash`".
6. **Cuando John termine ejecute el comando "`./john --show prueba_rsa.hash`" para verificar el password descifrado** .

Esto describe el uso general de John the Ripper. Mediante esta herramienta es posible romper claves de cifrado de una considerable cantidad de archivos. La documentación sobre el uso de John the Ripper se encuentra en forma de archivos de texto dentro del subdirectorio "doc" de John the Ripper.

3. Esteganografía básica

En esta sección utilizaremos tres técnicas para esconder un archivo dentro de otro.

3.1. Ocultando Archivos con la Terminal

La forma más sencilla de ocultar un archivo dentro de otro es concatenando ambos archivos utilizando el comando "`cat`". Esto es factible al utilizar un archivo binario como archivo portador. El archivo a ocultar puede ser tanto binario como de texto.

1. **Tome nota del tamaño en Megabytes del archivo "mono.png" incluido con este enunciado.**
2. Ejecute el comando: "`cat duke.mp3 >> mono.png`". **Tome nota del tamaño resultante del archivo "mono.png"**.
3. Para extraer el archivo "duke.mp3" ocultado, utilize el comando "`cat mono.png | tail -c+212518 > duke_2.mp3`". **¿Que acción realiza el comando "`tail -c+212518`" en la tubería anterior?**. Puede usar el comando "`man tail`" para justificar su respuesta.
4. **Utilize el comando "`vbindiff duke.mp3 duke_2.mp3`" para verificar que los dos archivos .mp3 son iguales**.

3.2. Ocultar un Archivo Dentro de una Imágen JPEG con la Terminal

El formato de archivo `.jpg` siempre comienza con los bytes `0xFFD8`. Luego el archivo está compuesto por una serie de secciones que siempre tienen la siguiente forma:

- El primer byte de la sección es `0xFF`, seguido de un byte que indica el tipo de sección.
- Luego siguen dos bytes en formato *big endian* que indican la longitud de la sección, incluyendo los dos bytes de longitud pero excluyendo los dos bytes de la cabecera de sección.

Aprovechando esta estructura es posible ocultar información dentro de las secciones de JPEG.

1. Ejecute el comando "`hexdump -C img1.jpg`". **Verifique que efectivamente el archivo sigue el formato indicado anteriormente. Indique cual es el código y la longitud de la primera sección del archivo (la que sigue a los bytes de inicio** `0xFFD8`).

2. Ejecute el comando "`cat img1.jpg | head -c 4 >> carrier.jpg`". **Utilizando el comando "`hexdump -C`" verifique que el archivo "carrier.jpg" solo contiene 4 bytes**.

3. **Verifique que el tamaño en bytes del archivo "SarahTheSpaceSpy.js" es de 2641 bytes**. Luego ejecute el comando "`echo -en '\x0A\x64' >> carrier.jpg`". **Utilizando el comando "`man echo`" investiguen que hacen las opciones "`-e`" y "`-n`" del comando "`echo`"**.

4. Ejecute el comando "`cat img1.jpg | tail -c+7 | head -c 14 >> carrier.jpg`". **¿Que se está copiando en el archivo "carrier.jpg" con este comando?**.

5. Ejecute el comando "`cat SarahTheSpaceSpy.js >> carrier.jpg`".

6. Ejecute el comando "`cat img1.jpg | tail -c+21 >> carrier.jpg`". **¿Por que se utiliza la opción "`-c+21`" en el comando "`tail`" en la tubería anterior?**.

7. Abra el archivo "carrier.jpg" con un visor de imágenes. **Luego verifique que el archivo "SarahTheSpaceSpy.js" está efectivamente escondido dentro de "carrier.jpg" utilizando el comando "`hexdump -C`"**.

El archivo "hackme.jpg" contiene un archivo oculto el cual fue insertado utilizando esta técnica. Extraiga este archivo oculto e indique en su informe que contiene dicho archivo[3].

[3] Puede utilizar el comando "`file`" para determinar el tipo del archivo oculto una vez que lo extraiga.