Práctica 2

Criptografía

Antes de empezar

Estas tareas comenzarán a realizarse durante las clases prácticas y, la parte que no dé tiempo a finalizar en ese horario, se terminarán como trabajo individual del alumno.

Lo más conveniente para la correcta realización de la práctica es que se utilicen los ordenadores de los laboratorios y la máquina virtual generada en la práctica 0 de seguridad en Linux. Vamos a establecer conexiones entre las diferentes máquinas por lo que si preferís llevar vuestro propio ordenador, debéis conectaros a la red a través de cable.

Instalación de paquetes necesarios para realizar la práctica

1. Necesitamos un descompresor zip:

   sudo apt-get install unzip

2. Instalamos las herramientas de desarrollo:

   sudo apt-get install build-essential

3. Instalamos el programa que nos va a permitir generar esteganogramas:

   $ sudo apt-get install steghide

4. Paquetes necesarios para el ataque mediante fuerza bruta:

   $ sudo apt-get install libpth-dev libbz2-dev libassuan-dev libgcrypt20-dev libgpg-error-dev zlib1g-dev

5. Necesitamos un diccionario de contraseñas potente:
   $ wget http://downloads.skullsecurity.org/passwords/john.txt.bz2

   Lo descomprimimos:

   $ bunzip2 john.txt.bz2

6. Descargamos el programa PGPCrack-NG que nos va a permitir averiguar una clave de un fichero cifrado mediante fuerza bruta:

$*wget* https://github.com/kholia/PGPCrack-NG/archive/master.zip

Descomprimimos:

$ unzip master.zip

Compilamos:

$cd PGPCrack-NG-master

$ make

No debería darnos ningún erro al compilar. Volvemos a nuestro directorio de usuario:

$cd ..

El objetivo de está práctica va a ser enviar un mensaje secreto a un compañero. El mensaje va a estar protegido con cifrado simétrico y además lo vamos a ocultar en una imagen cuyo proceso va a estar también protegido con contraseña, la cual estableceremos mediante Diffie-Hellman entre ambos interlocutores.

1. Creamos un fichero de texto con el mensaje que queremos enviar:

   echo –e "El mensaje que queramos" | tee –a mensaje.txt

2. Ciframos el fichero con clave simétrica:

   $gpg –c mensaje.txt

Le damos una clave que podría parecer segura: "asdf1234". Tendría que aparecer un fichero encriptado "mensaje.txt.gpg"

3. Para el proceso esteganográfico neceistamos una clave. Vamos a establecer el intercambio de esta clave mediante Diffie-Hellman. Lo primero es elegir un par de números lo suficientemente complejos como para realizar el intercambio:

   p: número primo (por ejemplo el 997)

   a: raíz primitiva de p (por ejemplo el 7)

Cada alumno debe pensar en un número privado X < p. Para generar la clave pública debemos aplicar la siguiente fórmula: Y = (a^X) mod p (podemos utilizar la calculadora de Windows para realizar esta operación o bien en Linux accediendo a python *$python3* para salir

de python escribimos *quit()*). Ahora tenemos que pasar el resultado de esta operación a nuestro compañero para ello lo haremos mediante ssh:

$ echo –e "la clave pública es Y" | tee –a pkPubUOxxxxx.txt

donde Y es el valor de pkPub y se lo enviamos mediante scp a la cuenta alumno de vuestro compañero:

$scp pkPubUOxxxxxx.txt alumnossi@ipCompañero:.

Ahora para saber la clave publica de nuestro compañero hay que mirar el fichero pkPubUOxxxxxxxx.txt que nos habrá dejado él:

$cat /home/alumnossi/pkPubUOxxxxxx.txt

Con la clave "pkPubCompañero" que no envió nuestro compañero generamos la clave que usaremos en el proceso esteganográfico de la siguiente manera: pkPrv = (pkPubCompañero^X) mod p.

4. Descargamos una imagen jpg que queramos desde Windows y la enviamos a nuestro sistema Linux con winscp.
5. Ahora vamos a ocultar el mensaje cifrado en un esteganograma usando como password la que hemos intercambiado con Diffie-Hellman (pkPrv):

   $ steghide embed –cf imagen.jpg –ef mensaje.txt.gpg

6. Enviamos el esteganograma a nuestro compañero mediante la cuenta alumnossi:

   $scp imagen.jpg alumnossi@ipCompañero:.

7. Extraemos el mensaje del esteganograma que nos ha enviado nuestro compañero

   $steghide extract –sf /home/alumnossi/imagen.jpg

8. Y ahora procedemos a averiguar la clave de encriptación por fuerza bruta:

   $cat john.txt | ./PGPCrack-NG-master/PGPCrack-NG mensajesecreto.txt.gpg

9. Una vez sabemos la clave desencriptamos el mensaje:

   $gpg mensajesecreto.txt.gpg

10. Y pro fin leemos el mensaje secreto:

    $cat mensajesecreto.txt

11. Podéis intentar encriptar el fichero con otra clave y probar su robustez.