Este es un ejercicio interesante. A nivel práctico habrá quien le saque partido y habrá quien no, pero no por ello deja de una oportunidad de aprender y experimentar con nuestro sistema.

El objetivo es conseguir un fichero encriptado, que si se monta y se introduce la password correcta, se convierte en un sistema de ficheros donde podemos guardar datos confidenciales: cuentas del banco, tarjetas de crédito, datos personales de clientes, fotos de nuestra vecina en la ducha, la lista NOC de los mejores agentes de la CIA... y esas cosas que tenemos en nuestro disco duro y que no queremos que nadie vea. Y si se desmonta, es solo un fichero inocente lleno de basurilla informática completamente ilegible.

¿Mola o no mola?

Pues empecemos con un poco de teoría, vamos a hablar del dispositivo loop.

El dispositivo loop Es un seudo-dispositivo que hace que un archivo se comporte y sea accesible como un dispositivo de bloque (un HD, CD-ROM, etc...).

Antes de utilizarse, un dispositivo loop debe asociarse a un fichero existente en nuestro sistema de ficheros. La asociación permite que el archivo se comporte como un bloque 'especial' de ficheros, y si el archivo contiene un sistema de ficheros completo, este puede ser montado como si fuera un dispositivo de disco.

El ejemplo más fiel a lo que pretendemos hacer es el de una imagen ISO.

Los dispositivos /dev/zero y /dev/urandom:

/**dev**/**zero** es un archivo especial que provee tantos caracteres null como se lean desde él.

Uno de los usos típicos es proveer un flujo de caracteres para sobreescribir información. Otro uso puede ser para generar un archivo "limpio" de un determinado tamaño.

/**dev**/**urandom** es lo mismo, solo que en lugar de null provee basurilla informática, es decir, caracteres aleatorios. En lugar de generar un archivo "limpio" generará un archivo lleno de mierda ilegible.

Para lo que pretendemos hacer es mejor utilizar /dev/urandom

El comando dd (duplicate disk)

El comando dd se utiliza para copiar un archivo de un origen a un destino, de acuerdo a determinadas opciones, alguno lo habréis usado para crear un diskete de arranque a partir de una imagen... ¿no os suena eso a cómo se copia una ISO? :P

Aquí (http://linux.die.net/man/1/dd) tenéis una lista de las opciones de dd, nosotros vamos a

usarlo de la siguiente manera:

dd if=dispositivo de entrada of=dispositivo de salida bs=tamaño del bloque count=nº de bloques (cada bloque será del tamaño especificado con 'bs')

El comando losetup

losetup se utiliza para asociar dispositivos loop a ficheros o dispositivos de bloque, para desasociarlos y para chequear su estado. Además, entre sus opciones encontramos la opción '-e encryption', lo que nos va a permitir la encriptación de nuestro fichero.

Bueno, pues vamos allá!!

Lo primero que vamos a hacer es cargar en el kernel las herramientas que necesitamos:

uno:~# modprobe cryptoloop