RESETEAR CLAVE WINDOWS CON BACKTRACK 4

BackTrack es una herramienta de auditoría de penetración en sistemas informáticos y cuenta con un amplio abanico de utilidades para ello y es distribuida en forma de LIVE CD de Linux.

Vamos a ver como podemos dejar en blanco la contraseña de un usuario en un equipo con Windows mediante este sistema.

Para emplear BT4 insertar el CD y arrancar el equipo desde el mismo.

Aparecerá un menú, seleccionar la primera opción BT4 FrameBuffer 1024

Tras el arranque aparecerá una pantalla en negro donde escribiremos startx y pulsaremos enter. Esto hará que se inicie el modo gráfico.

Pulsaremos ALT + F2 y en la ventana que aparece escribiremos terminador y enter.

A continuación tendremos que ver cual es el estado de particiones de nuestro disco duro y encontrar la que tiene Windows instalado, escribiremos fdisk -l y pulsaremos enter.

Aparecerá una lista con todas las particiones del equipo algo como:

/dev/sda1
/dev/sda2

… Dependiendo del número de particiones del disco.

Si sabemos que Windows está sobre la primera partición entonces deberemos de montar esa partición para poder trabajar en ella,

mount -t ntfs /dev/sda1 /mnt/

Una vez montada la partición, tenemos que localizar el fichero SAM que, normalmente está en %SYSTEMFOLDER%/System32/Config/SAM

con el comando de Linux ls podéis ver lo que hay en las carpetas.

Una vez localizado el fichero escribiremos:

chntpw -i /mnt/ RUTA DEL FICHERO SAM --->>> chntpw -i /mnt/windows/system32/config

Ojo a las mayúsculas y minúsculas en la ruta.

Aparecerá un menú con las distintas opciones. Seleccionar el usuario que queremos resetear y aplicar la opción de resetear password.

OJO!! La opción de cambiar el password puede fallar y dañar el SAM. Mejor resetearlo.

Reiniciar el equipo.