cesarin.wordpress.com

Quitar o resetear contraseña de Windows con chntpw en Backtrack

3 minutos

CHNTPW (Change NT Password), es una utilidad de Linux, diseñado para sobreescribir, resetear, cambiar o modificar passwords de las cuentas de usarios Windows, esta herramienta viene por defecto en Backtrack 4 r2, sino se la puede descargar e instalar en la distribución Linux de su preferencia.

Para quitar o cambiar la contraseña de algún usuario de una máquina Windows, procedemos de la siguiente manera:

– Arrancamos el equipo Windows a traves del CD Live con la distribución BAcktrack (o la que tenga instalada chntpw)

– Una vez iniciado el sistema backtrack desde el CD Live, abrimos la consola y realizamos los siguientes pasos:

– Creamos una carpeta/directorio, con cualquier nombre, por ejemplo Windows7, con el siguiente comando:

 # mkdir /media/Windows7

En mi caso, he creado un directorio con el nombre Windows7 en el directorio /media/

– Montar la partición Windows en el Backtrack:

 # mount -t ntfs-3g /dev/sda2 /media/Windows7

Explicación breve:

mount -> comando para montar la partición

-t ntfs-3g -> El sistema de archivos de nuestra partición Windows, en este caso, NTFS

/dev/sda2 -> Dispositivo en el que está nuestra partición Windows

/media/Windows7 -> Directorio que creamos en el paso anterior, donde vamos a montar la partición Windows

– Nos ubicamos dentro de dicho directorio:

 # cd /media/Windows7

– Ahora accedemos al directorio donde se encuentra el SAM SYSTEM de Windows que es donde se almacenan las contraseñas de los usuarios, ubicada en /Windows/System32 /config:

 # cd /media/Windows7/Windows/System32/config

– Estando en esta ubicación, procedemos a ejecutar el chntpw, utilizando el siguiente comando:

 # /pentest/password/chntpw/chtnpw -l SAM SYSTEM

Aquí, nos mostrará el listado de usuarios del sistema.

– Ahora nos ubicamos en el usuario del sistema que querramos quitar la contraseña de la siguiente manera:

 # /pentest/password/chntpw/chtnpw -u <Usuario> SAM SYSTEM

En el mensaje que nos muestra le damos la orden que no, ingresando la n

– En esta parte se muestran las opciones que tiene chntpw para

actuar en el usuario seleccionado, usamos la opción 1 para quitar el password

– Guardar los cambios?? Ponemos [y]es

– Finalmente reiniciamos el sistema e ingresamos a Windows, se podrá observar que se puede ingresar sin poner contraseña del usuario que le borramos la contraseña

It’s all….