Restablecer la password de cualquier tipo de cuenta de usuario local de Windows

Con esto se podrá recuperar la contraseña de los usuarios registrados en un equipo local sin necesidad obviamente de entrar en el sistema, de manera que no se tenga que introducir la clave anterior para restablecer una nueva passw, de modo que genera una nueva contraseña para el usuario en la que seleccionemos, incluido administradores locales. Así también como el poder manipular otras configuraciones adicionales.

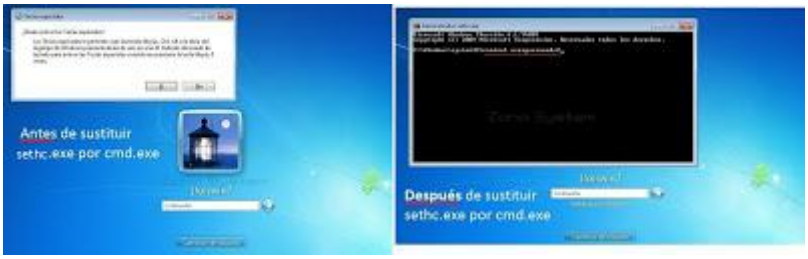

Figura 1: Iniciando consola de recuperación de passwords antes de iniciar sesión en el sistema.

Esto es un **pequeño hack descarado** y un agujero de seguridad grande. Funciona en versiones Windows XP/Vista/ 7 / 8 / 8.1/10 tanto en arquitecturas de x86 y x64.
Me imagino que la razón será por si algún usuario que solo tenga una cuenta y cambia la passw de esta en un momento de su vida se olvida de ella, pueda iniciar sesión con una nueva clave y acceder al sistema con la cuenta de usuario en cuestión.

ACTUALIZO (30/07/2015):
Con la reciente salida de Windows 10, simplemente decir que esta característica sigue funcionando.

Ya que un sistema operativo Windows siempre y cuando siga cumpliendo estos dos requisitos:
- Funcionalidad por defecto de las stickykeys (sethc.exe), con pulsación de 5 veces seguidas en la tecla mayus.
- Se pueda acceder a las consolas .msc: lusrmgr.msc o de "netplwiz".

Cumpliendo estas dos características anteriores este tutorial seguirá sirviendo para restablecer las passwords de administrador Windows.
Y en el caso de Windows 10 esto sigue siendo así...

Una forma de evitar esto y añadir un obstáculo más de seguridad, sería establecer una contraseña al acceso de la BIOS, para no poder realizar bootstrap a un USB o CD/DVD, también sería aconsejable si la BIOS lo permite deshabilitar la opción de hacer booting con "medios extraibles desmontables" (USB) y lo mismo con la lectora/grabadora CD/DVD. Y ya si somo muy paranoicos a parte de la password para el acceso y configuración a la BIOS, establecer otra aún a un nivel más bajo o anterior que sería establecer otra antes de que el equipo realice el POST (*Power On Self Test*) de arranque (esto también si la configuración de la BIOS lo permite).

En este tutorial voy intentar explicar todos los pasos al detalle a seguir y definir comando básicos, con el fin de que cualquier usuario pueda entenderlo.

[1] - Encemos el PC y booteamos el Live CD de instalación de Microsoft Windows (nos valdría cualquier versión sería lo mismo. Simplemente tendremos que tener acceso a una "Consola de recuperación"). En este caso me base un Windows 7 Ultimate.
Una vez se nos carga el LiveCD de la instalación de Windows, y accedemos a la primera ventana del asistente de instalación.
Pulsamos en 'Siguiente' -> Reparar el equipo -> esperamos que se nos carge las 'opciones de recuperación de sistema' -> pulsamos en 'Siguiente' -> se nos mostrará una nueva ventana en la que elegimos la opción "Símbolo del sistema".

Figura 2: Siguiente en el asistente de instalación de Windows.

Figura 3: Sección "Reparar el equipo" en el asistente de instalación de Windows.

Figura 4: Opciones de recuperación del sistema.

Figura 5: Símbolo de sistema, como opción de recuperación del sistema.

[2] - Cuando se nos muestra la ventana de símbolo del sistema, ejecutada por defecto como Administrador local.
Escribimos lo siguiente:

```
C:
cd \windows\system32
ren sethc.exe sethc.ejm
copy cmd.exe sethc.exe
exit
```

Después de cada instrucción, para la confirmación presionamos la tecla Enter.

Figura 6: Renombrando fichero sethc por una consola cmd.

Explicación:
sethc.exe -> Fichero ejecutable que hace llamada a las StickyKeys (teclas pegajosas o teclas espeiales), esta lo que hace es que cuando, por ejemplo, pulsamos la tecla "Shift" (mayusculas, derecha o izquierda) del teclado 5 veces seguidas, nos salga una ventana que nos permite activar o desactivar dichas teclas.
cmd.exe -> Fichero ejecutable que hace llamada al Símbolo del sistema de Windows

> ***C:*** Entramos en la unidad c: por defecto, o la letra que tengamos asignada al disco local donde almacenemos la instalación de Windows.
> Con el comando ***cd***: Entramos en los direcctorios de del disco local especificados, que en este caso es donde se encuentras los ficheros en los que haremos las modificaciones necesarias.
> Con el comando ***ren***: Básicamente lo que se está haciendo es, renombrar, cambiándole la extensión, al fichero original 'sethc.exe' por 'sethc.ejm'. Por que ejm?, es indiferente podemos poner lo que queramos, siempre que no supere las 3 letras de extensión. Elegí: ejm (ejemplo) "por poner algo". Pero como ya digo esto no tiene relavancia, simplemente se hace para que no se tenga concordancia cuando posteriormente se copie la cmd.exe por sethc.exe.
> Con el comando ***copy***:Después se copia la cmd.exe por sethc.exe, como sethc.exe lo habíamos renombrado a sethc.ejm el fichero sethc.exe no existe, supuestamente. Entonces lo que hacemos es crear una cmd.exe original pero con el nombre sethc.exe. De este modo, se conseguiría que cuando llamemos a las StickyKeys, se nos abra un Símbolo del sistema (CMD).
> Con el comando ***exit***: Salimos del símbolo del sistema.

[3] - Una vez acabado el paso 2, reiniciamos el PC en el botón "Reiniciar" en la ventana de 'Opciones de recuperación del sistema'.
Iniciamos el equipo sin bootear el LiveCD de instalación de Windows, es decir que lo inicializamos de manera normal.

[4] - En la pantalla de bienvenida, pulsamos 5 veces seguidas la tecla "Shift" (Mayusculas) izquierda o derecha, nos funcionará igual.
Ahora, se nos abrirá el cmd.exe o Símbolo del sistema de Windows.
Y escribimos:

control userpasswords2

Nota: También podríamos poner: **netplwiz**, es lo mismo y nos llevaría a la misma ventana gráfica.
Sería lo mismo. La diferencia (creo recordar...) está en que netplwiz era el fichero que abría y daba acceso a dicha ventana de control de cuentas de usuario en sistemas Windows NT y 2000, este aún se conserva en Windows XP, Vista y 7. Aunque añadieron una segunda vía de acceso: control userpasswords2, que es exactamente lo mismo.

[5] - Se nos abrirá la ventana de 'Cuentas de usuario', si no apareciese en ese momento en la pantalla de bienvenida, reiniciamos y volvemos a realizar el paso 4 y no tendrá que aparecer.
Pues en esta ventana podremos restablecer la constraseña del usuario que seleccionemos. En este ejemplo, se trata de una cuenta tipo Adminsitrador con el nombre de usuario "1loiswin7". Una vez seleccionamos el usuario podemos pulsar en el botón "Restablecer contraseña" he introducir la constraseña nueva sin necesidad de que nos pregunta la contraseña que hubiese anteriormente.
'Aplicamos' y 'Aceptamos' los cambios. (O simplemente 'Aceptar' sería lo mismo).

Figura 7: Iniciada consola con las StickyKeys y restableciendo passw de administrador de Windows.

Aunque en la captura de pantalla de arriba no muestro la ficha o pestaña "Opciones avanzadas" de la ventana 'Cuentas de usuario', en esta podremos elegir una cuenta de usuario de tipo 'limitada' y cambiarla por una de tipo 'Administrador' o viceversa, así como también agregar dicho usuario seleccionado a un grupo local que hubiesemos creado previamente o los incluidos por defecto del sistema, esto solo para Windows XP. En Windows Vista o 7 veremos otro aspecto similar en el que podremos administrar las contraseñas de la base de datos local SAM de Windows y entrar en la ventana 'Usuario y grupos locales' (lusrmgr.msc) con la cual también podremos realizar lo mismo que en Windows XP.

[6] - Y por último iniciamos sesión en el sistema con el nombre de usuario y contraseña que restablecimos. Y ya estaremos dentro, para hacer las modificaciones necesarias, así como cambiar a una nueva contraseña o lo que fuese.

[7] - Ahora, como paso final, dejaremos o restableceremos los ficheros modificados

(sethc y cmd) a su estado original o default.
Para ello una vez que estamos ya dentro del sistema ejecutamos un "Símbolo del sistema" como administrador. Para ello, vamos a:
Inicio -> Todos los programas -> Accesorios -> y botón derecho en 'Símbolo de sistema' -> Ejecutar como administrador.
Si tenemos ativado el UAC (*User Account Control*) de Windows, nos saldrá una ventana informativa 'Control de cuentas de usuario', que nos preguntará si deseamos que se hagan cambios en el sistema, le decimos que si.

Una vez abierto el CMD y estar situados en la ubicación:
C:\Windows\System32

En el caso de no estarlo, escribimos en el CMD:

C:
cd windows\system32

Una vez estemos en dicho direcctorio (lo cual por defecto lo está, si ejecutando el CMD con privilegios administrativos) simplemente tendríamos que escribir en el CMD:

del sethc.exe
ren sethc.ejm sethc.exe
exit

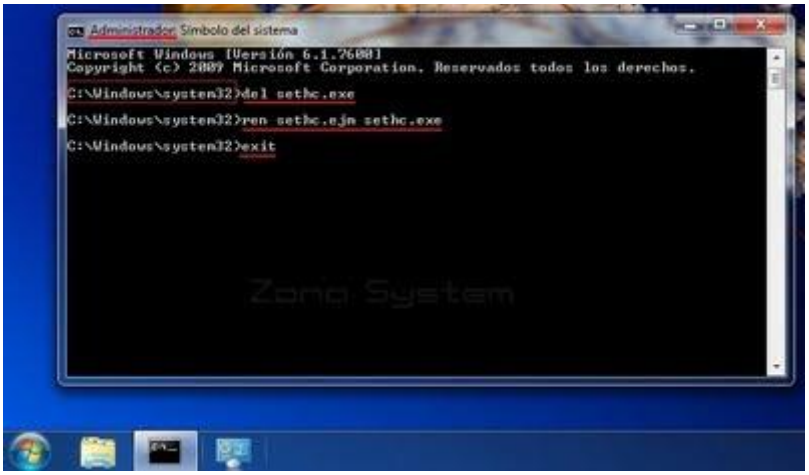

Figura 8: Restableciendo el orden de los ficheros renombrados anteriormente.

Explicación:
> Con el comando **del**: Borra ficheros y direcctorios, en este caso borraría el fichero sethc.exe.
> Y los comandos **ren**: (renombrar nombres de ficheros) y **exit** (salir del CMD), ya se comentaran anteriormente.

Lo que se está haciendo, es borrar el fichero sethc.exe que es una copia del cmd.exe original. Después renombramos el fichero sethc.ejm a sethc.exe, el sethc.ejm que es el fichero del sethc original. Por lo tanto, lo dejamos como estaba para que a la hora de llamar a la ejecución de las StickyKeys este se ejecute correctamente.
Y con la copia del cmd borrada y el fichero del sethc en su estado original, daremos por acabado la configuración.

Espero que este tutorial ayude aquell@s usuari@s, que no recuerdan su contraseña y de este modo haiga una solución al problema. Y no utilizar este pequeño hack maliciosamente...