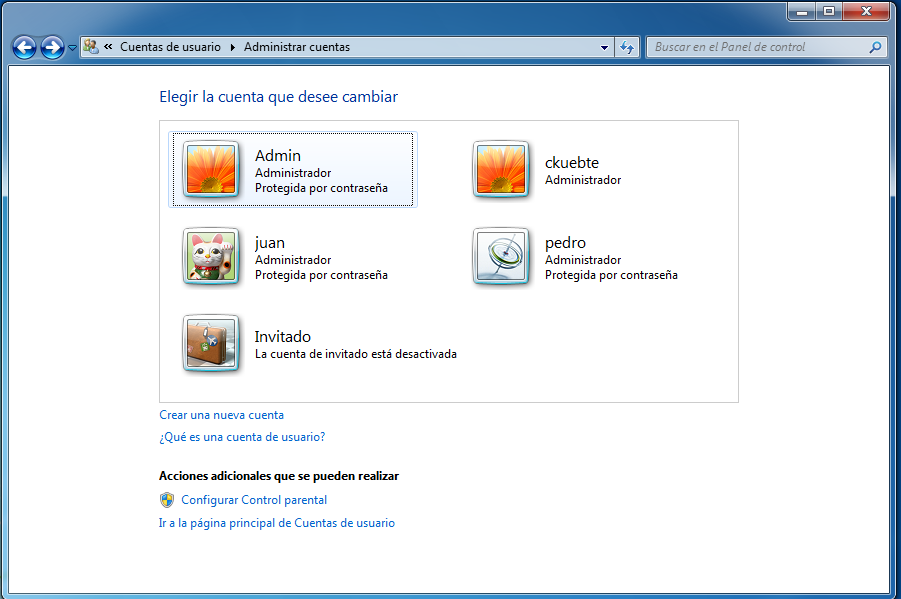
Práctica modificación de contraseñas en Windows / Linux

06/12/2017

Athos Orío Choperena

# Windows:

En esta práctica vamos a resetear las contraseñas en un equipo windows. Para ello, lo primero vamos a crear algunos usuarios con contraseña.



Ahora, vamos a arrancar con una live cd (puede ser windows Linux o la que sea) para cambiar los archivos del sistema. En windows, cuando presionamos 5 veces seguidas la tecla mayúscula, se ejecuta el archivo sethc.exe. Este archivo sirve para activar teclas especiales relacionadas con la accesibilidad.

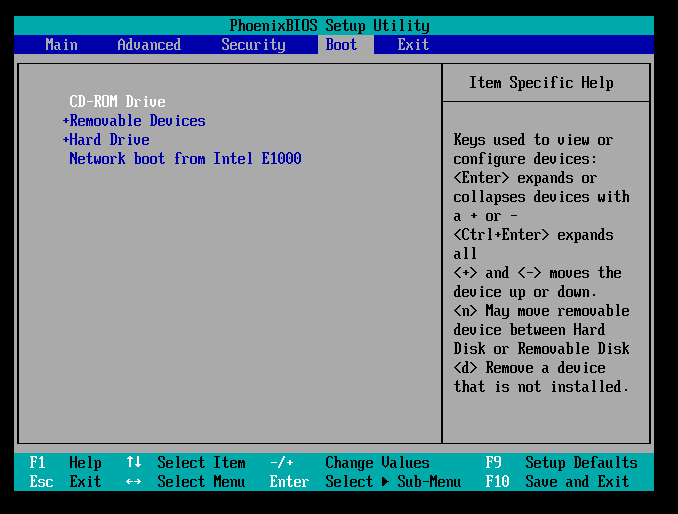
Por otro lado, el comando control userpasswords2 abre una ventana para poder crear, borrar y modificar usuarios.

El objetivo es cambiar el nombre al ejecutable cmd.exe y ponerle el nombre sethc.exe, de esta forma conseguiremos que cuando presionemos 5 veces las mayúsculas se ejecute la consola de comando en vez de las teclas especiales, una vez ahí, desde la consola, ejecutaremos control userpasswords2 y desde ahí resetearemos las contraseñas.

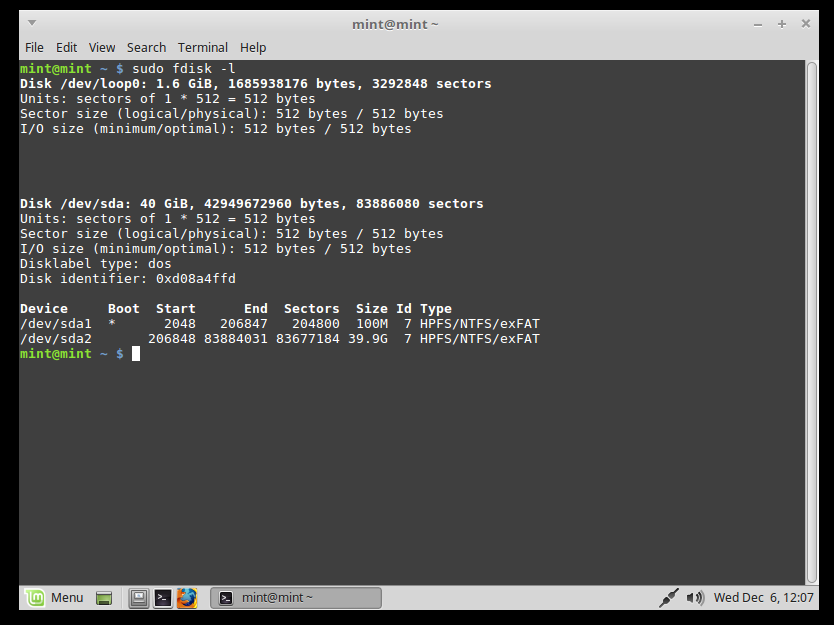
Ahora muestro el proceso de cómo se hace.

## 1.- Arrancar desde un live cd

Configuramos la máquina para que arranque desde un cd/dvd o usb, y lo metemos en la unidad. Tras esto arrancamos la máquina.



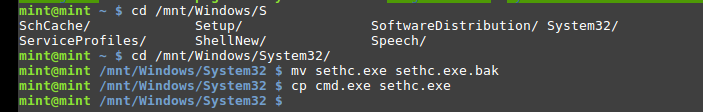
Hacemos un fdisk –l para ver las unidades de disco duro que nos detecta.



Como vemos, tenemos una unidad con dos volúmenes. Sda1 con 100 megas y sda2 con 40gb, sda2 es nuestro objetivo así que vamos a montarla



Ahora vamos a ir a windows\system32, renombraremos el archivo sethc.exe para poder restaurarlo más tarde, y duplicaremos el archivo cmd.exe con el nombre sethc.exe



Ahora, arrancamos la máquina de forma normal (sin el cd de la live metido). Como se puede ver en el siguiente gif, presionamos 5 veces la tecla mayúsculas, y se nos abrirá la consola, ejecutamos el comando control userpasswords2 y podremos restablecer las contraseñas

<controluserpasswords2.gif>

Ahora arrancamos la máquina y probamos a entrar sin introducir la contraseña.

<login-without-pass.gif>

# Linux:

Tenemos (por lo menos) dos formas para hacerlo en Linux.

## 1.- Quitar x en archivo password:

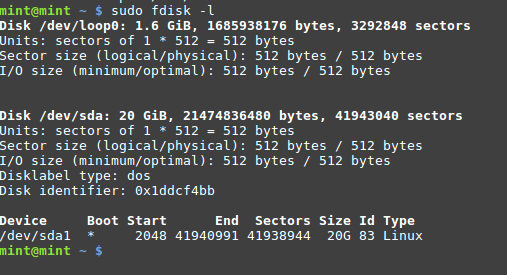
Para esto, arrancaremos una maquina Linux, pero con una live cd.

En el siguiente gif se puede comprobar que… si dejamos la contraseña en blanco, no podemos acceder al sistema

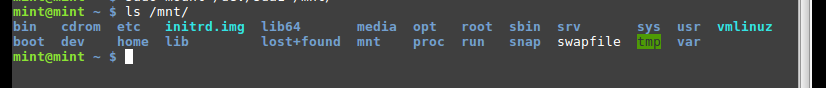
<ubuntu-login-fail.gif>

Ahora, arrancamos desde una live cd, para ello, configuramos la BIOS (como hemos hecho anteriormente) para que arranque desde un dispositivo externo.

Con fdisk comprobamos las unidades del sistema



Ahora lo montamos.



Ahora, editaremos el archivo /etc/passwd y eliminaremos la “x” que hay entre el primer y segundo “:”

<remove-x-passwd-file.gif>

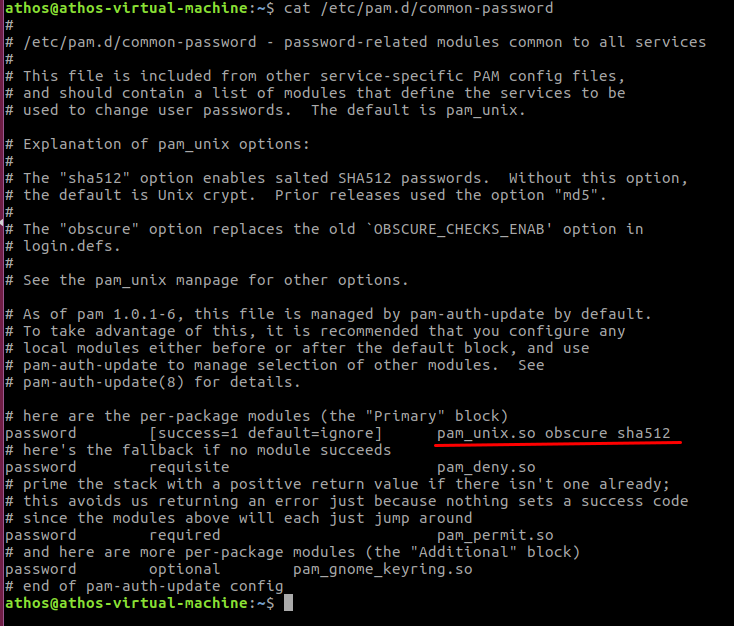
Ahora arrancamos el sistema normalmente, podremos acceder simplemente pinchando en la flecha. Tras esto, podremos cambiar la contraseña del usuario con el comando passwd. Si el usuario tiene permisos sudo, podremos cambiar también la contraseña de root con sudo passwd.

En el siguiente gif, podemos comprobar, como al principio no tenemos permisos para leer el archivo shadow, y tras cambiar las contraseñas podemos verlo.

<reset-linux-password.gif>

## 2.- Generar una contraseña y sustituirla:

Para esto, primero arrancaremos desde una live (como en el caso anterior), montaremos la unidad y revisaremos el archivo /etc/pam.d/common-password para ver como encripta este sistema que estamos vulnerando.



Como vemos en la imagen anterior, el sistema encripta con sha512, entonces lo que tenemos que hacer, es buscar una herramienta que encripte con ese algoritmo, y generaremos nuestra propia contraseña.

En una consola Linux, podemos generar la contraseña sha512 con el siguiente comando

python -c "import crypt,random,string; print crypt.crypt(raw\_input('clear-text password: '), '\$6\$' + ''.join([random.choice(string.ascii\_letters + string.digits) for \_ in range(16)]))"

Como se puede ver en el siguiente gif

<sha512-hash-generator.gif>

Copiaremos la contraseña, y la introduciremos en el archivo shadow. Tras esto, podremos acceder al sistema con la nueva contraseña generada.