Ahora estamos a una sola clase del repaso hacia el examen y viendo un poco más a fondo Windows:)
No sé si sabían, pero han agregado la palabra "**Hacker**" en la **RAE** (nombrando la entidad ya deben saber que tipo de atrocidad voy a decir), pero lo han definido como un delincuente. Me causa un poco de pena por la Academia, ya que le sigue sacando prestigio y da el parámetro real que es el "lo vi en la tele". Si bien en parte se apega a ciertas costumbres y deformaciones del idioma, hay muchas cosas que no sólo están erroneamente definidas sino que van dándole pie al invento de palabras sin sentido (**güisqui y jipi** en la cabecera de la tabla). Nosotros seguiremos siendo lo que somos, sin importar lo que al otro le parezca. Si nos definen como piratas, entonces redefinamos eso con respecto al tiempo en el que vivimos. En fin, si alguien os acosa con esto díganle que se vaya a comer **almóndigas**.

Hoy le daremos un buen vistazo al tema de las **contraseñas** en este sistema operativo.
Hablemos de **SAM**.

"¿El gordito que perseguía a Frodo en El Señor De Los Anillos?"

No, Manolo. ¿Por qué estaría, yo, hablando de eso? -.-
SAM es el abreviado de **Security Account Manager**. Éste corresponde a una **base de datos** que almacena las **contraseñas** del sistema, tanto para acceso remoto como para acceso local.

"Muy interesante, y ésto ¿se hackea?"

Bueno, se podría decir que sí. Hay que tener algunas cosas en cuenta:

- El SAM tiene las contraseñas almacenadas en forma de **hashes** (LM para los sistemas antes de NT y NTLM para los sistemas NT).
- Está **alojado** en C:/Windows/system32/config/SAM.
- Está **montado** en HKLM/SAM.

Esto quiere decir que seguramente dependerá del poder de **cómputo** para ver en cuánto tiempo podemos **crackear** el hash y encontrar la coincidencia buscada, como hicimos en las clases pasadas.

Si tuviesemos que enfrentarnos a una contraseña muy fuerte, me vería obligado a resistir la tentación de crackearlo y todo el entrenamiento anterior sería en vano... ¿O no?

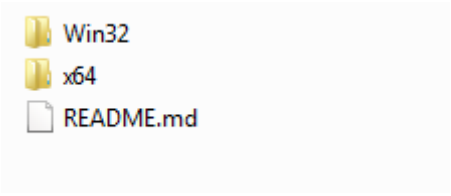
"¿Cuál es la posibilidad de obtener estos hashes? Suponiendo que están en una base de datos, debe ser algo protegido."

Exactamente. Windows utiliza una llave para cifrar este archivo, que se denomina **Syskey** o system key. Esta claro que la protección es suficiente para que una persona no pueda leerlo, pero la clave está dentro del sistema operativo obviamente y nosotros deberíamos encontrar la manera de atacar.

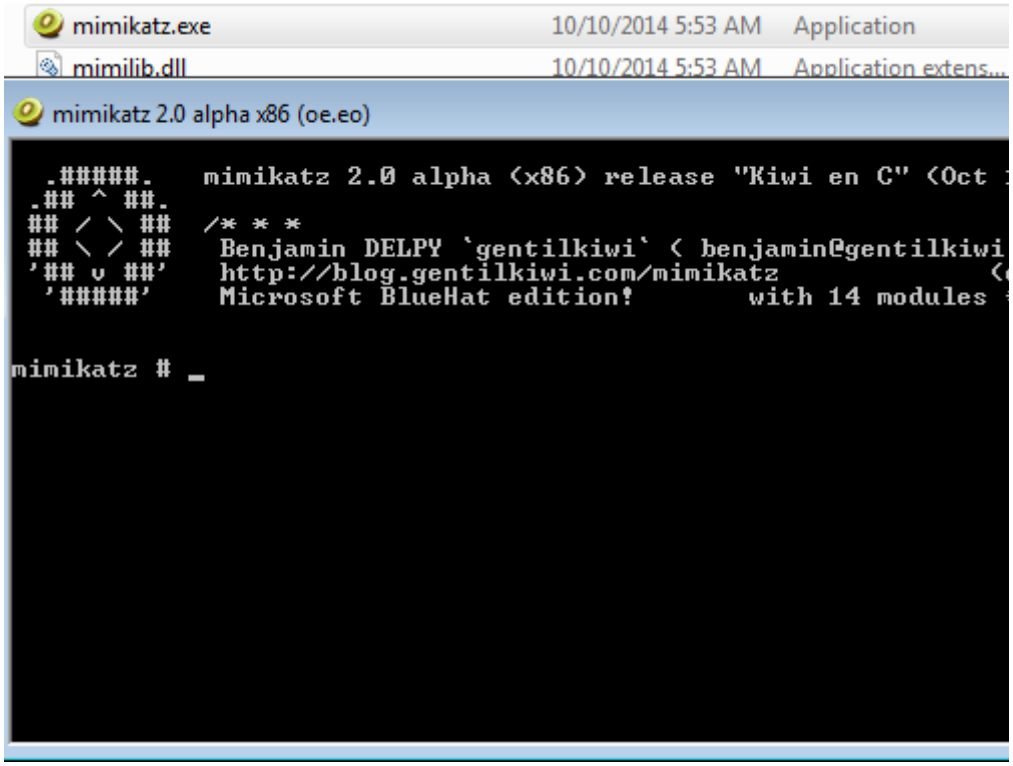
Vamos a utilizar una herramienta llamada **Mimikatz**.

Entramos a la página https://github.com/gentilkiwi/mimikatz/releases/tag/2.0.0-alpha-20141010 para **descargar** la aplicación en cualquiera de los 2 formatos de comprimido que queramos (.7z o .zip).

Luego de descomprimir los archivos en algun lado, veremos 3 archivos. Entren a la carpeta Win32 si tienen un sistema operativo de 32 bits, o a la otra carpeta si tenemos uno de 64 bits.

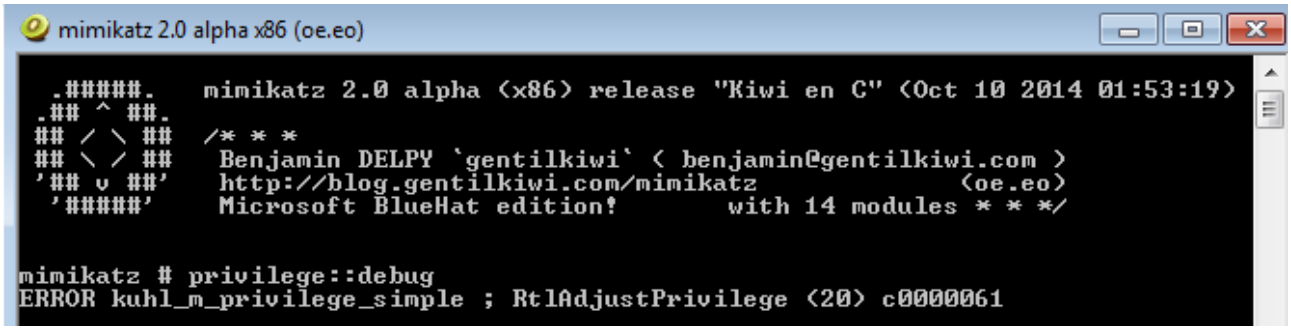


Yo estoy usando un W7 de 32 bits, así que entraré en esa carpeta.
Luego de eso, ejecutamos el único ejecutable que vemos allí, y nos abrirá una consola de comandos propia del programa.

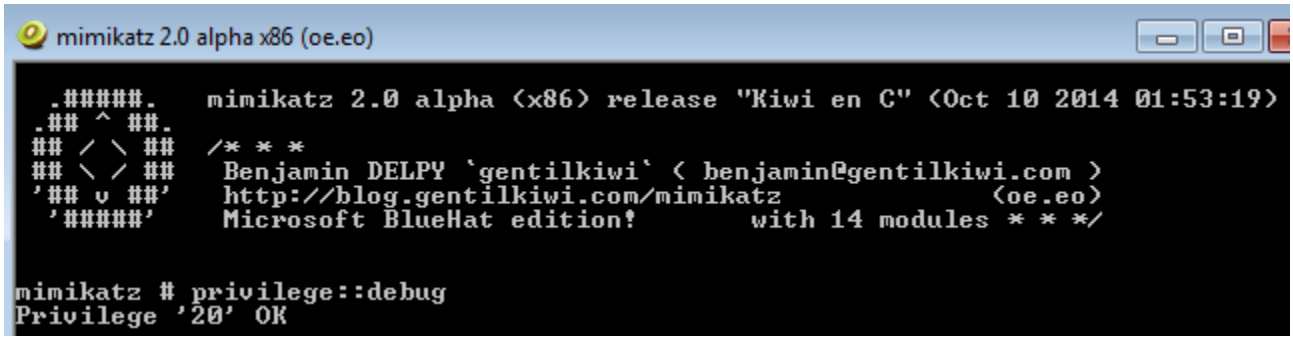


Este programa se agarra de ciertos parámetros para dar información de las contraseñas del sistema. Pero para eso necesita permisos especiales. Intentemos de abrirlo con doble click y usemos el comando "**privilege::debug**".

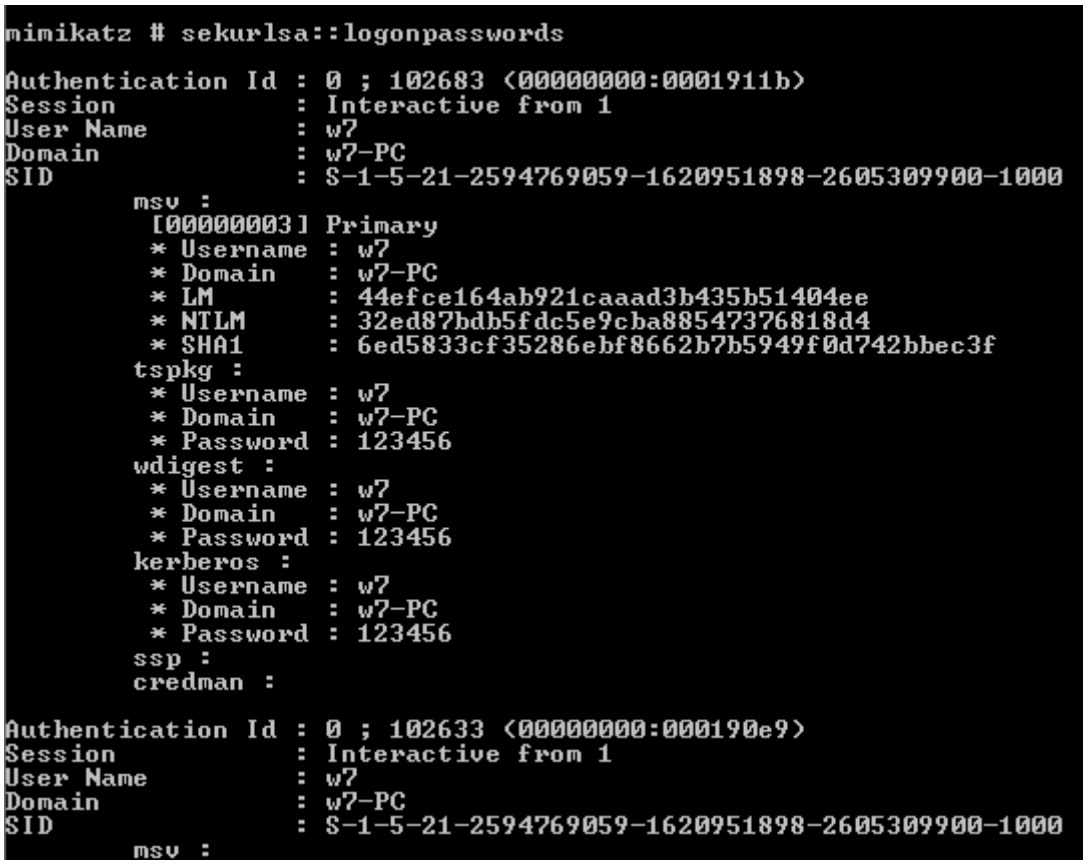
Si **no** lo estamos ejecutando con algun usuario de alto **privilegio**, veremos este error.



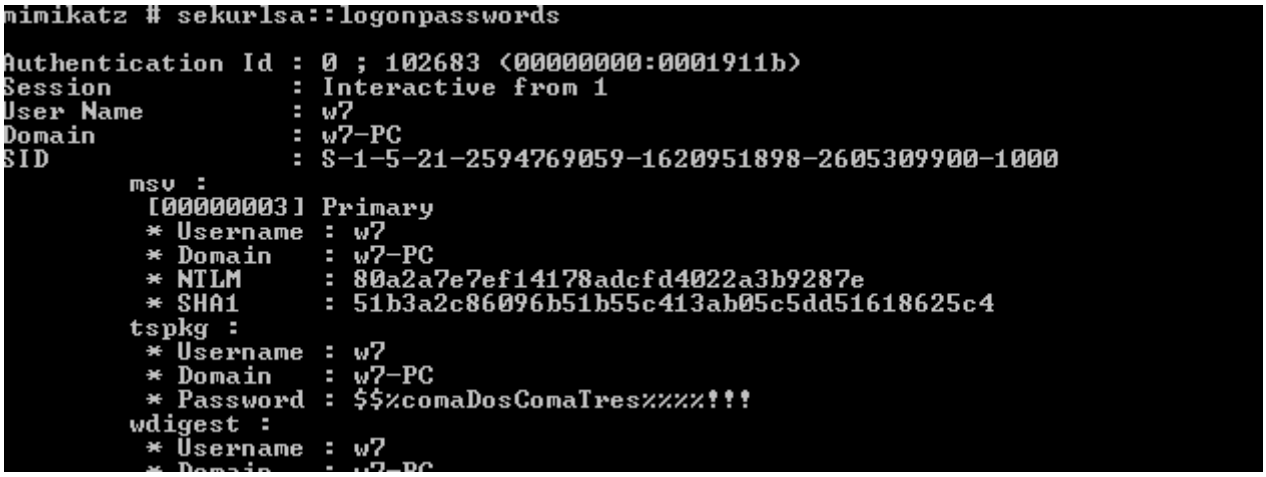
Entoinces, démosle click derecho y ejecutar como **administrador**, para que podamos ver si era ése el problema.



Claramente lo era.
Ya obtuvimos privilegios necesarios para conocer la contraseña. Ahora escribamos el comando "**sekurlsa::logonpasswords**", para obtener las contraseñas del sistema.



Nos vuelca en la consola, las contraseñas y los hashes. Como ven, mi **contraseña** era **123456** lo cual no era muy fuerte. Pero intentemos cambiar la **contraseña** por algo bien **potente** como: "$$ %comaDosComaTres%%%%!!!" (sin las comillas).



Así que igualmente lo hace de manera limpia. Por el **tiempo** que nos llevó, ya sabemos que no utiliza un sistema de crackeo por fuerza bruta, sino que **descifra** la **SAM** con la **Syskey**. Esto es una ventaja para el atacante, ya que el tiempo es siempre el mismo aunque la contraseña sea demasiado

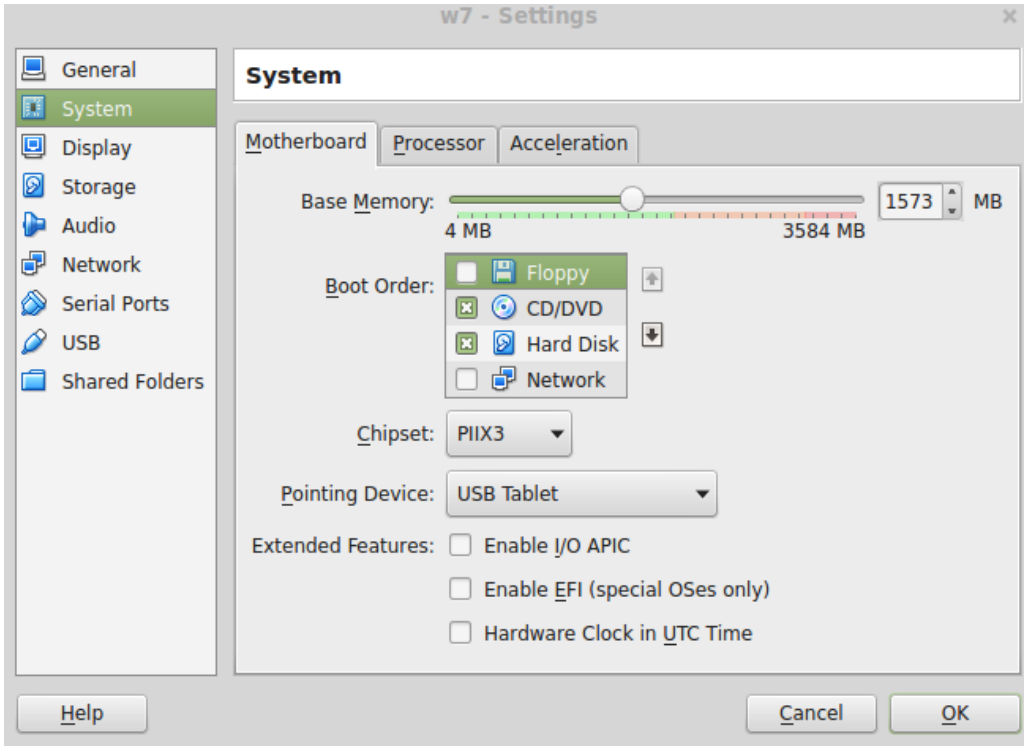
fuerte.

NOTA: si prestaron atención, se darán cuenta que en la primera contraseña, nos aparecía el hash **LM** y en la segunda contraseña ya no aparecía. Esto sucede porque LM puede usar hasta un **máximo de 14 caracteres**.

Esta herramienta es excelente si podemos usar la cuenta del administrador. Pero, lo que sucedería en caso de usar una cuenta de **invitado** es **nada**, tal y como vimos antes.

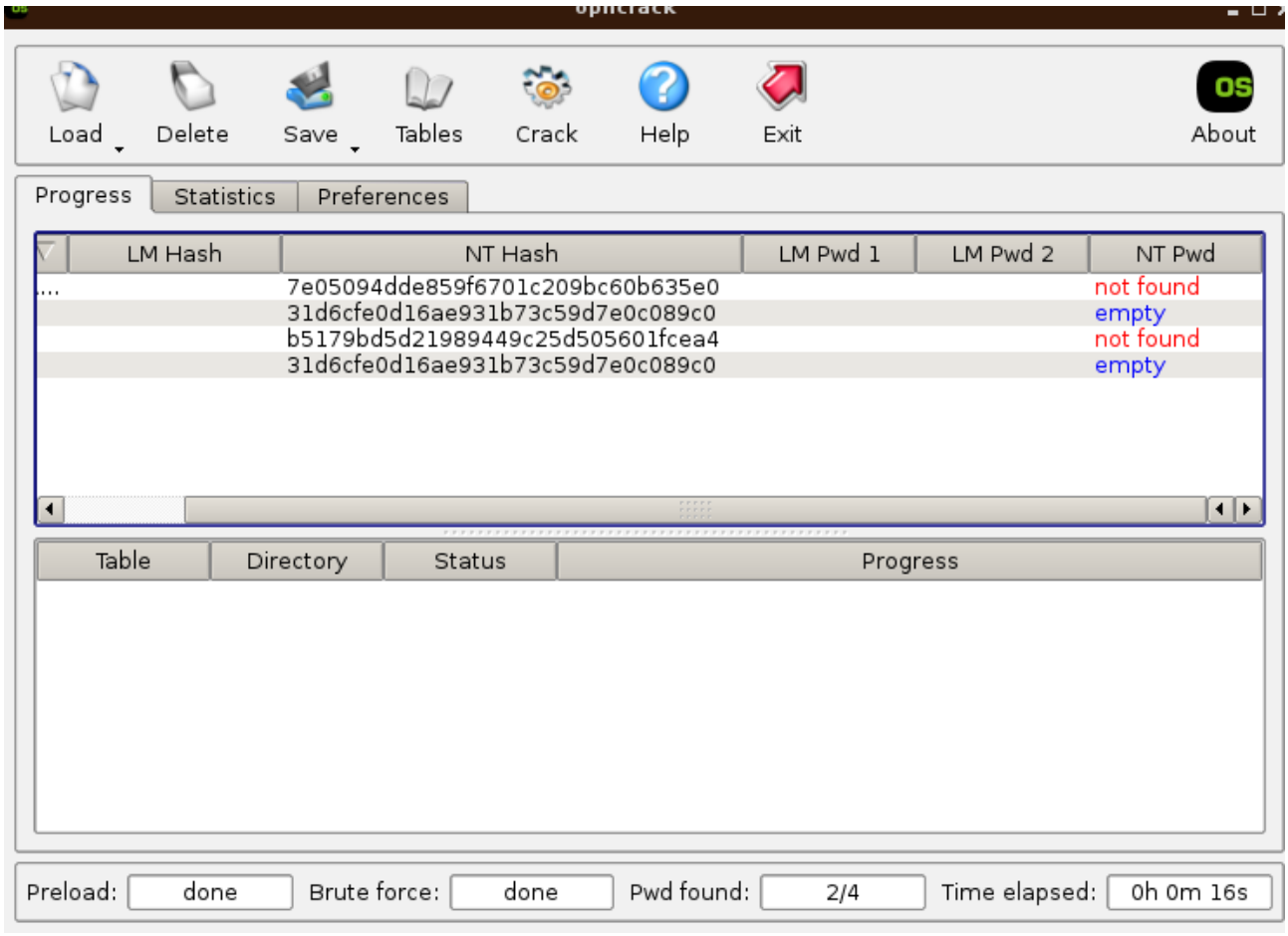
El problema es que ésta no es la única forma de conseguir la contraseña. Si tuviesemos un sistema operativo basado en **Linux**, esto es cuestión de tiempo para realmente obtener todo. Así que tenemos una herramienta basada en ese sistema operativo pero que tiene todo automatizado -aunque en otro momento veremos otrsa técnicas mucho más eficientes y potentes-. Ésto no solamente simplifica las cosas para cualquier persona que no sepa utilizar Linux, sino para cualquier persona que simplemente sepa como bootear otro dispositivo que no sea el disco.
La herramienta se llama **Ophcrack** y se encuentra en
http://ophcrack.sourceforge.net/download.php.
Si bajamos en la página veremos que están los **liveCD** -que no son otra cosa que sistemas booteables que se pueden ejecutar sin tener que ser instalados-. Allí descargamos el ophcrack del sistema operativo que queramos. Es importante por las tablas que van a ir allí. Este programa utiliza **fuerza bruta** -para el lado del atacante esto podría ser un último recurso- para conseguir su objetivo, y aquí dependerá de la viveza del **administrador** para sobrevivir a este ataque.

Voy a hacerlo en la máquina virtual (obviamente). Así que una vez descargado el Ophcrack, en el menú de la máquina virtual vamos a **Devices -> CD/DVD Devices -> Choose a virtual CD/DVD Disk File...** Allí elegimos la **imagen** (extensión .iso) de lo que descargamos. Luego, apagamos la máquina (me acabo de dar cuenta que lo hice de manera desordenada, perdón) y vamos a Settings -> en la parte izquierda vamos a **System-> en la pestaña Motherboard tenemos que asegurarnos de que el booteo del CD este por encima del de Hard Disk.**

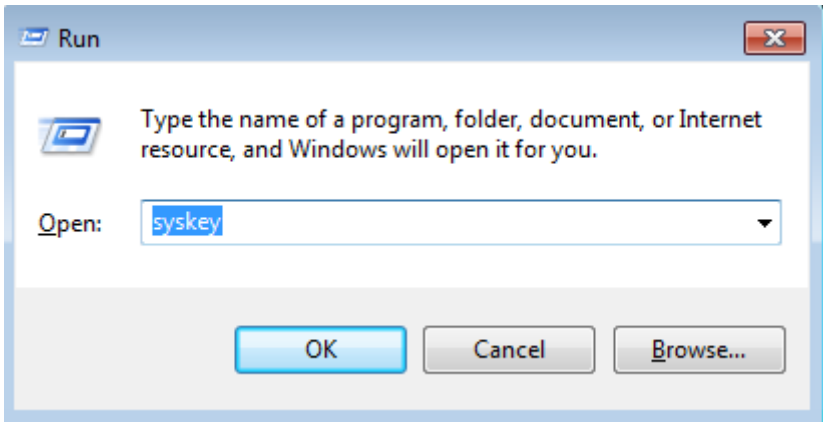


Ahora iniciamos la máquina virtual nuevamente, e iniciará automáticamente este menú al cual le damos a la primera opción.

Luego vendrá esta pantalla del entorno gráfico y empezará a intentar **crackear** las contraseñas sin que nosotros le digamos nada. Es importante saber que utiliza un ataque de fuerza bruta por diccionario, así que si tenemos una **table rainbow** que queramos usar en nuestro poder, lo podemos hacer. Allí vemos que tardó 16 segundos en sacar que 2 estaban vacías y las otras no fueron posibles porque no estaban en el diccionario -aunque era 123456-.

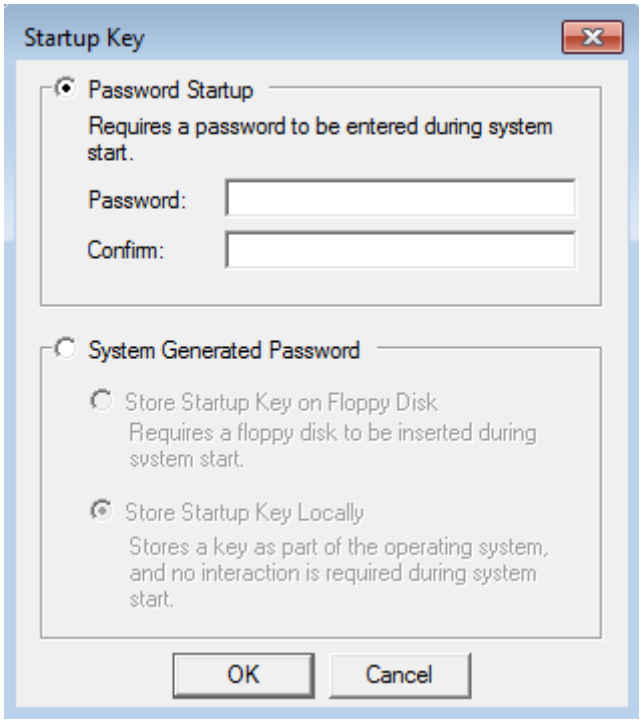


Bueno, no fue una clase muy profunda pero está bueno ver ciertos ataques por más simples que fueran. Aquí vimos que si un atacante tiene **acceso físico** al lugar y sin las protecciones necesarias, seguro que obtiene las contraseñas. ¿Cómo **protegernos** de ésto? Bueno primero podríamos hacer que un usuario normal no utilize las cuentas de **Administrador por defecto**, ni dejar a esta cuenta **sin contraseña alguna**. Es más, si podemos, utilizemos una clave **fuerte** y **extensa**.
Lo segundo sería ponerle una **contraseña** al **BIOS** para que no puedan entrar y cambiar el booteo al CD.
Pero hay una tercera cosa que podemos hacer. El **syskey** que usamos para cifrar el SAM también puede ser utilizado en el inicio para que, antes de entrar al Windows nos pida la contraseña de la Syskey y además es una buena práctica para no alojar esta clave en el sistema.
Para hacer ésto, iniciamos el ***run*** o ***ejecutar*** y escribimos "**syskey**", sin comillas obviamente.

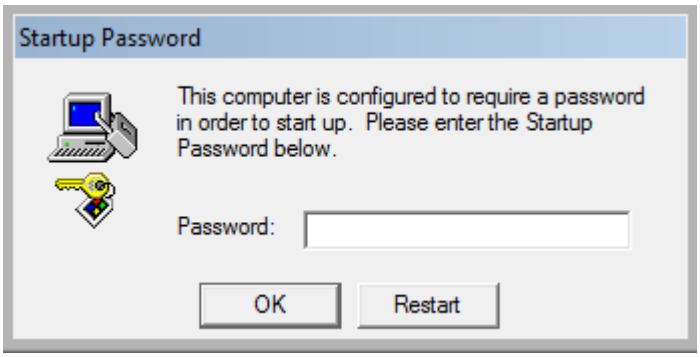


Muy bien, nos abrirá esta ventana a la que le daremos en el botón de ***update***.

Y vemos que está elegida la opción de abajo. Elegimos la de arriba y le ponemos una contraseña (no va a reemplazar a la de la sesión. Simplemente es una aparte).



Luego, si volvemos a iniciar el sistema operativo, antes de que aparezcan las sesiones o demás, veremos esta ventana a la cual le damos la contraseña que tuvimos antes.



Eso sí, si utilizamos el Mimikatz luego de abierta la sesión, no tendrá problemas con esto pues la **SAM** estará corriendo siempre en **segundo plano**.

Pueden seguirme en Twitter: @RoaddHDC

Cualquier cosa pueden mandarme mail a: r0add@hotmail.com

Para donaciones, pueden hacerlo en bitcoin en la dirección siguiente:
1HqpPJbbWJ9H2hAZTmpXnVuoLKkP7RFSvw

Roadd.
