CONTRASEÑAS

EN WINDOWS XP

Ernesto Castelán Chávez
Sir_Lance

ADVERTENCIA

Este texto es puramente educativo y de aprendizaje. El autor no se hace responsable del mal uso que se le pueda dar a la información proporcionada.

Teoría

¿Qué es una contraseña?

En informática una contraseña es una clave que permite el acceso a algún recurso y que brinda seguridad en las comunicaciones. La contraseña evita el acceso de usuarios sin autorización y normalmente debe mantenerse en secreto ante aquellos a quien no se les permite el acceso. En los sistemas informáticos actuales cada contraseña está ligada a un único usuario por lo que la contraseña puede ser cambiada o se puede negar el acceso a un usuario sin afectar a los demás.

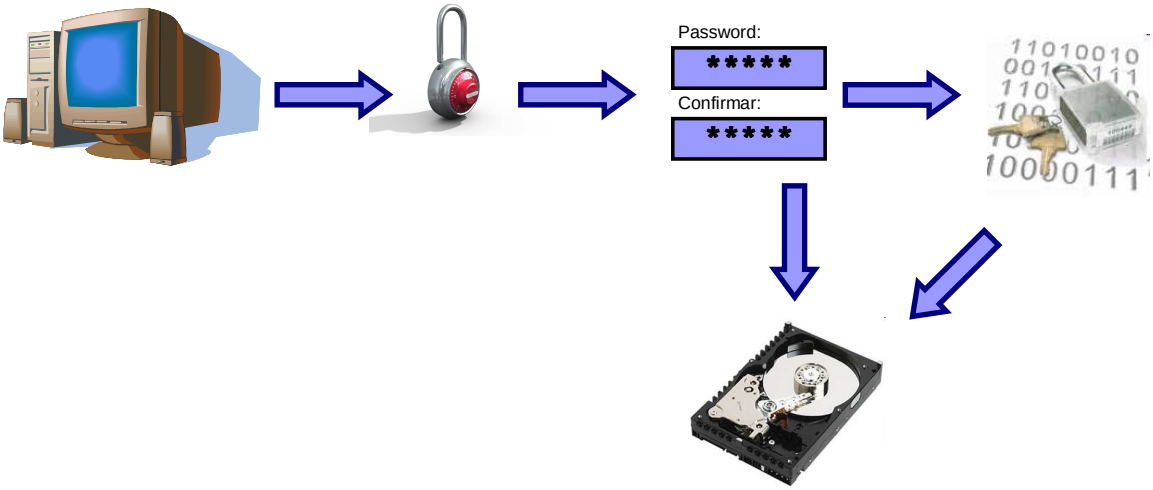
Historia de las contraseñas

El uso de contraseñas se remonta a la antigüedad pues el ser humano siempre ha tenido la necesidad de mantener información importante en secreto y asegurarse que quien la reciba sea quien debía recibirla. Centinelas que vigilaban alguna locación, pedían el santo y seña al que quería pasar y solamente le permitían el acceso a aquella persona que conociera la contraseña. Las claves y contraseñas jugaron un papel muy importante en las guerras y campañas militares.

En la era moderna, las contraseñas son usadas para controlar el acceso a sistemas operativos de computadoras, teléfonos celulares, decodificadores de TV por cable, cajeros automáticos, etc.

¿Cómo funcionan las contraseñas?

A la hora de crear una cuenta de usuario o de restringir un recurso, se nos pide teclear la contraseña por primera vez. Generalmente debemos introducirla dos veces para evitar errores de tecleo. Una vez que hemos establecido la contraseña, ésta es almacenada en un medio permanente como un archivo o una base de datos en el disco duro.



Anteriormente las contraseñas eran guardadas tal cual en algún archivo de texto escondido en el sistema. Este método era sumamente inseguro ya que si alguien averiguaba o encontraba dicho archivo, las contraseñas podían ser vistas inmediatamente y el equipo así como la información sensible eran vulnerables.

Actualmente, antes de guardar una contraseña, el sistema le aplica una serie de operaciones matemáticas para convertirla en información imposible de interpretar a simple vista, es decir codifica o cifra la contraseña.

Pasemos a explicar los siguientes conceptos, pues son básicos para la comprensión de lo que se explicará más adelante.

- Al hecho de cifrar o codificar la contraseña (o cualquier dato) se le llama **encriptar**.
- El método, los pasos o el proceso interno que se sigue para cifrar la contraseña se le conoce como **algoritmo**.
- El resultado de codificar la contraseña (es decir la contraseña ya cifrada) se llama **hash** (en plural **hashes**)

Generalmente los algoritmos que se usan para cifrar contraseñas son irreversibles, es decir que una vez encriptada la contraseña NO puede ser desencriptada. De esta manera, si tenemos acceso al archivo donde se guardan los hashes, no podemos "deshacer" el proceso para ver las contraseñas.

Contraseña **Algoritmo** **Hash**

Pero si los hashes no se pueden "deshacer", ¿Cómo sabe entonces el sistema que he introducido la clave correcta?

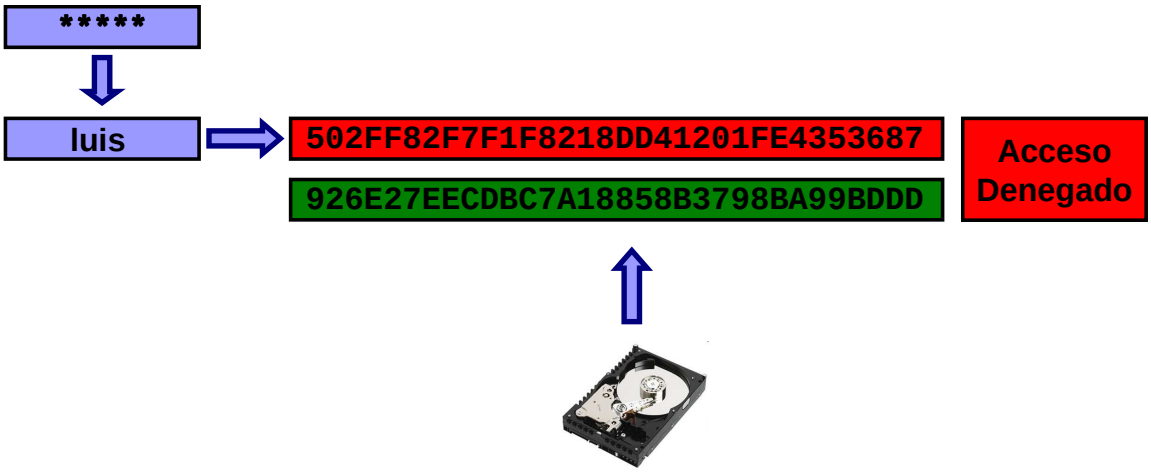
Cuando una contraseña es encriptada, el algoritmo usado generará un hash. En teoría, el hash es único para cada contraseña por lo que la misma contraseña siempre resultará en el mismo hash.

pepe	926E27EECDBC7A18858B3798BA99BDDD
PEPE	41E74C6D258C53D1336677F34DCA5C84
password	5F4DCC3B5AA765D61D8327DEB882CF99
Jabón	FFB12D591858EDE312E0BA2A9FAF7322
Jamón	6E5B2F2E74E718B5091BAD0FF4A7A85E

No importa que las contraseñas sean muy parecidas, el hash será sustancialmente diferente, como podemos observar con "pepe - PEPE" y "jabón - jamón".

Una parte de la seguridad del sistema depende del algoritmo usado para encriptar las contraseñas, pues hay algoritmos más seguros que otros. En este ejemplo se usó un algoritmo llamado MD5.

Una vez que nuestra contraseña ya está almacenada en el sistema y tratamos de acceder al recurso protegido, se nos pedirá confirmar nuestra identidad por medio de la contraseña. Cuando la introducimos el sistema calculará el hash y se comparará con el hash almacenado previamente. Si los hashes son iguales se permite el acceso, en caso contrario se niega. Esto es más o menos lo que haría nuestra computadora si iniciamos sesión y colocamos la contraseña incorrecta:



Pero si introducimos la contraseña correcta:

¿Cómo averiguar una contraseña?

Si bien las contraseñas están pensadas para proteger datos y recursos, al mismo tiempo son la parte más débil de cualquier sistema de seguridad puesto que deben ser recordadas por humanos y los humanos no somos perfectos. Hay muchas maneras de averiguar la contraseña de un usuario.

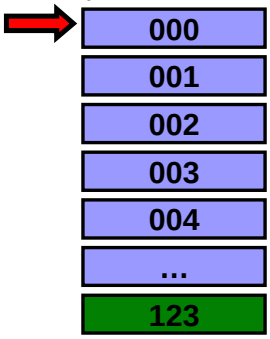
La debilidad de las contraseñas consiste en que los usuarios frecuentemente:

- Usamos la misma contraseña para varias cuentas
- Usamos las contraseñas que vienen por defecto (como “administrador” o “1234”)

- Usamos contraseñas muy fáciles de adivinar (nuestro nombre, el nombre de la novia, fechas de nacimiento y cumpleaños, etc…)
- Anotamos las contraseñas en lugares inseguros (en un papelito debajo del teclado por ejemplo)

Las contraseñas pueden ser averiguadas de muchas maneras, explicaré unas cuantas, que son bastante conocidas:

- **Ingeniería social:** La forma más antigua y quizás la más efectiva. Consiste en engañar o extorsionar al usuario para que él mismo proporcione la contraseña. Por ejemplo haciéndonos pasar por el administrador y diciéndole *"estamos dando mantenimiento a todas las cuentas y encontramos un problema de corrupción de datos en la suya, por favor sería tan amable de proporcionarnos su contraseña para que lo arreglemos y pueda trabajar sin problemas".* Funciona más seguido de lo que se pueden imaginar.
- **Ataque de fuerza bruta:** Consiste en obtener un hash y probar una a una todas las posibles contraseñas. Imaginemos que tenemos un candado de esos de bicicletas con una combinación de tres dígitos. Probaremos todas las combinaciones, una a una, hasta que encontremos la correcta.

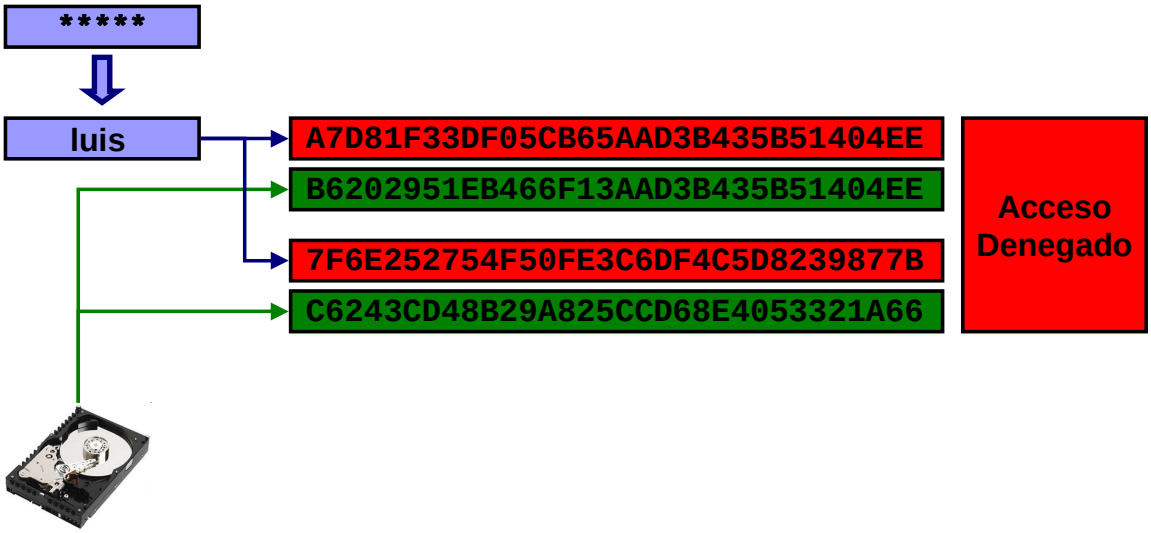


Pero las contraseñas informáticas pueden tener letras, números y símbolos, y pueden contener un gran número de elementos que permiten infinidad de combinaciones, por lo cual debemos establecer un límite de longitud y los caracteres que queremos probar (por ejemplo intentar sólo con letras minúsculas y números). Entre más caracteres y más longitud seleccionemos el proceso será más tardado porque el número de combinaciones posibles crece exponencialmente, a veces puede llegar a durar años. Pero si la contraseña es corta y no contiene caracteres extraños el proceso puede acortarse considerablemente. Es como si la clave del candado de la bicicleta fuera 001 sólo debemos hacer un intento antes de poder abrirlo.

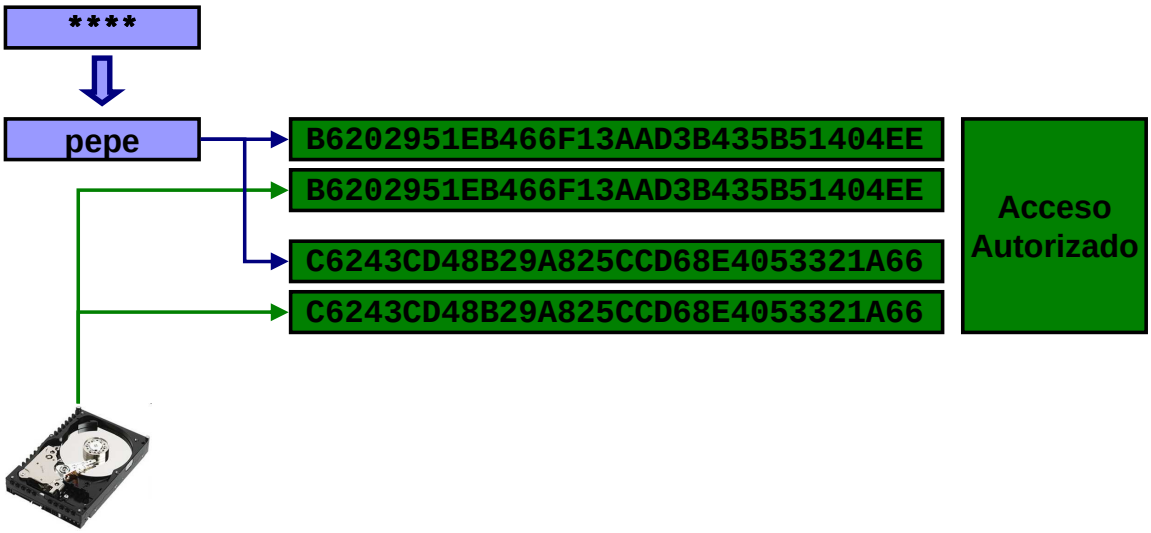
- **Ataque de diccionario:** Es muy parecido al proceso anterior, excepto que en vez de probar todas las contraseñas posibles, nos limitamos a unas cuantas contraseñas comunes almacenadas en una lista llamada "diccionario". Funciona con contraseñas sencillas y obvias, pero debido al número limitado de contraseñas disponibles en un diccionario muchas veces falla. Algunos programas permiten hacer alteraciones a cada palabra del diccionario como es invertir la palabra, añadir mayúsculas, añadir un número al final, etc… lo cual nos da más posibilidades de hallar la contraseña que buscamos.

El problema de las contraseñas en Windows XP

Todos conocemos las cuentas de usuario de Windows XP, que nos permiten tener nuestro escritorio y documentos separados del de los otros usuarios. El problema de las contraseñas de usuario en Windows XP y versiones anteriores es que por cada contraseña almacena dos hashes; uno generado por el algoritmo LM y otro por el NTLM. Veamos como funciona si introducimos una contraseña incorrecta:

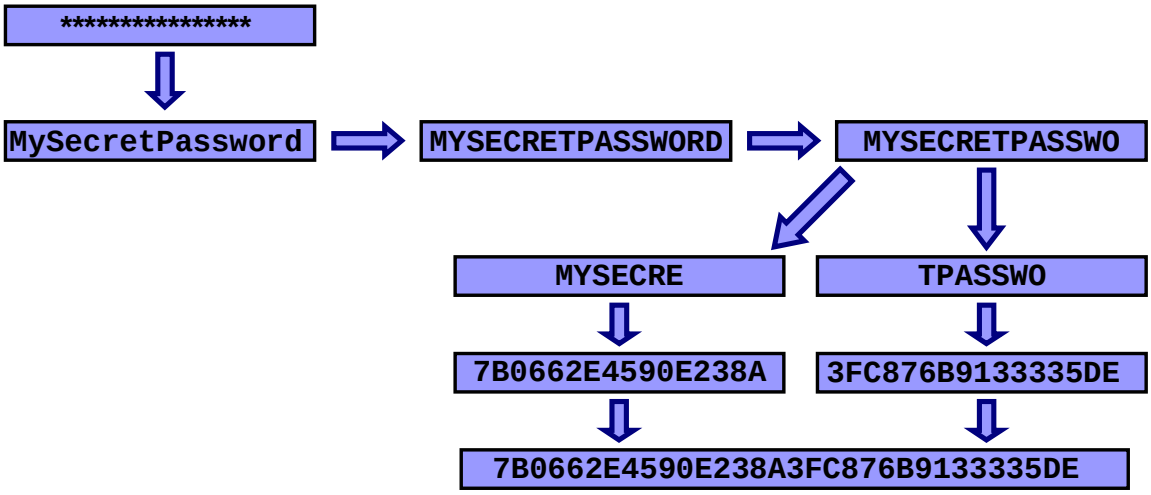


Y cómo funciona si introducimos la contraseña correcta:

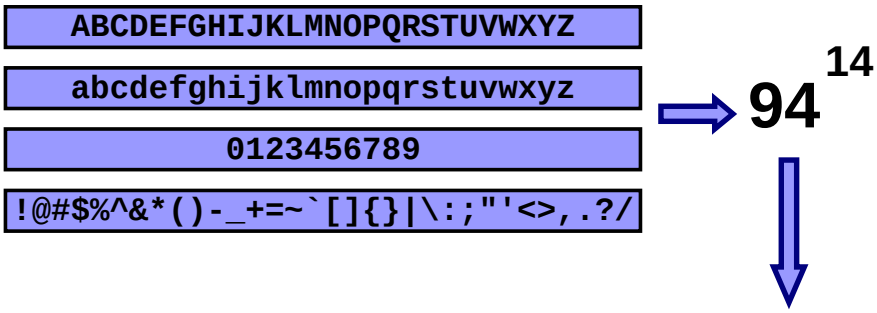


Es lógico pensar que si se comparan dos hashes en vez de uno, el sistema debe ser por lo menos el doble de seguro, pero enseguida veremos que no es ni la mitad de seguro, puesto que el algoritmo LM tiene muchas debilidades. Veamos de manera general cual es su algoritmo:

1. El usuario introduce la contraseña
2. La contraseña se convierte a mayúsculas
3. La contraseña se corta a 14 caracteres
4. Se divide en dos partes de 7 caracteres
5. Se calcula el hash de cada parte de manera individual
6. Se unen los dos hashes



¿Y bien? ¿De qué nos sirve saber todo esto? Hagamos unos cálculos. Hay 26 letras en el abecedario anglosajón, cada letra se puede escribir en mayúscula o minúscula, además de haber 10 dígitos (del 0 al 9), y digamos 32 símbolos (!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/). Si quisiéramos tener una contraseña de un solo carácter tendríamos 94 posibles contraseñas (26 mayúsculas + 26 minúsculas + 10 dígitos +32 símbolos). Para una contraseña de 14 caracteres tendríamos que elevar 94 a la 14, con la ayuda de una calculadora obtenemos un numerote de más de ¡4 mil cuatrillones de posibles contraseñas! Una PC casera moderadamente rápida puede codificar 4 millones de contraseñas por segundo. Si hiciéramos un ataque de fuerza bruta, ayudándonos de nuestra calculadora (y si no fallan mis cálculos), podríamos tardar hasta ¡33 billones de años! es decir 33 millones de millones de años, lo cual es una eternidad.



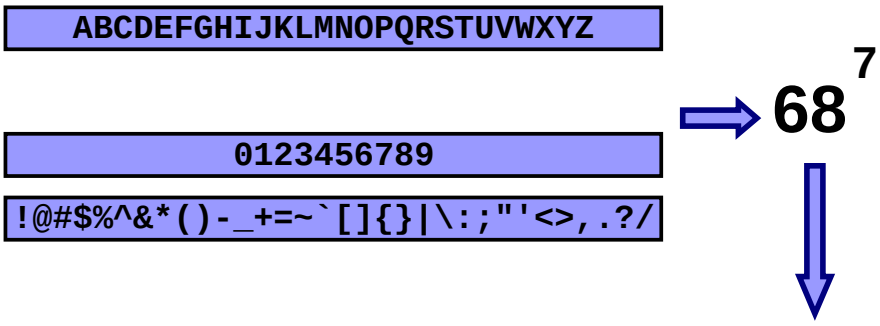
4 205 231 901 698 742 834 534 301 696

(cuatro mil cuatrillones)

33 billones de años

(33 millones de millones)

¿Pero que pasa con el algoritmo LM? Que sólo permite 26 letras posibles (por que no hay minúsculas) más los números y símbolos. Además de que divide la contraseña en dos partes de 7 caracteres, así que no importa que tu contraseña sea de 14 caracteres por que es como si tuvieras dos contraseñas de 7. Si quisiéramos tener una contraseña de un solo carácter tendríamos tan solo 68 opciones posibles. Con una contraseña de 7 caracteres tenemos tan solo 6 billones de posibles contraseñas, lo cual se queda corto contra los 4 mil cuatrillones. Si calculamos el tiempo máximo que nos llevaría encontrar la contraseña por fuerza bruta serían más o menos 20 días, lo cual comparado con 33 mil millones de años, no es nada.



6 722 988 818 432

(6 billones)

20 días

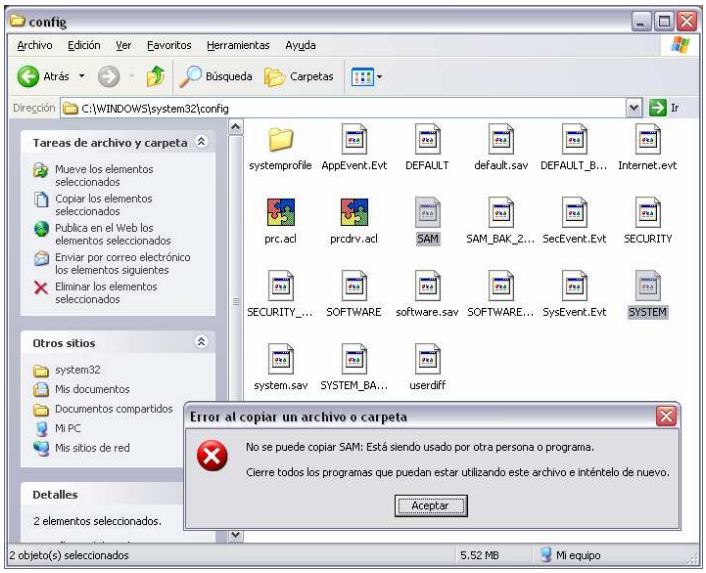
Práctica

¿Cómo obtener una contraseña de Windows XP?

Bien, hemos llegado a lo interesante, la parte donde nos ensuciaremos las manos. Supongamos que hemos olvidado la contraseña de nuestra cuenta de usuario, o que un maligno virus la cambió. Así que tenemos acceso al equipo y a otras sesiones, pero no a la nuestra. Veamos como recuperar la contraseña olvidada utilizando lo que hemos aprendido.

Al principio dijimos que los hashes de las contraseñas se almacenaban en el disco duro. Windows XP guarda sus contraseñas en dos archivos:

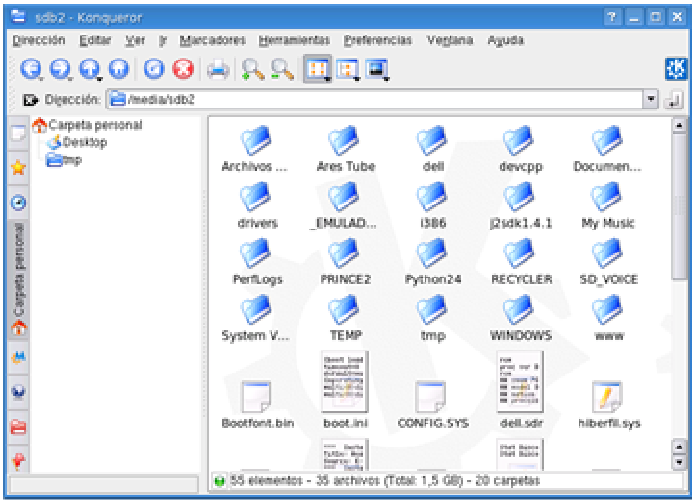
```
C:\windows\system32\config\SAM
C:\windows\system32\config\SYSTEM
```



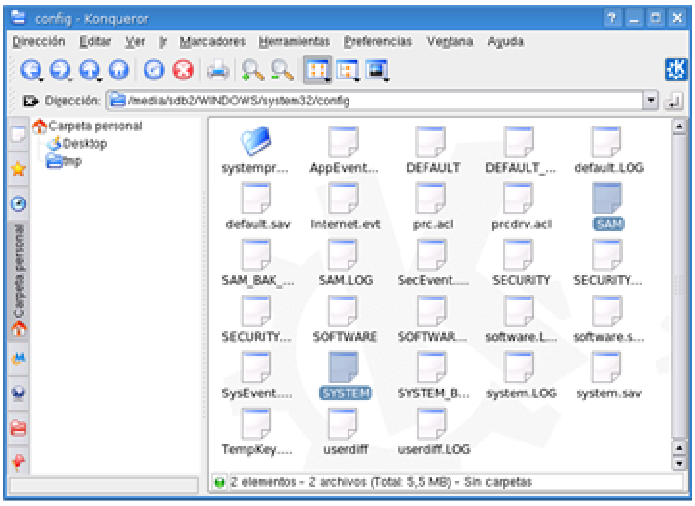
¡Bien! Lo tenemos, copiemos los archivos y listo.

Mmm parece que esos archivos no se dejan copiar. Claro, Windows los está protegiendo para evitar que sean modificados, copiados o borrados. Era demasiado fácil como para ser verdad. Bueno, afortunadamente todo tiene solución. Copiaremos los archivos con la ayuda de Linux.

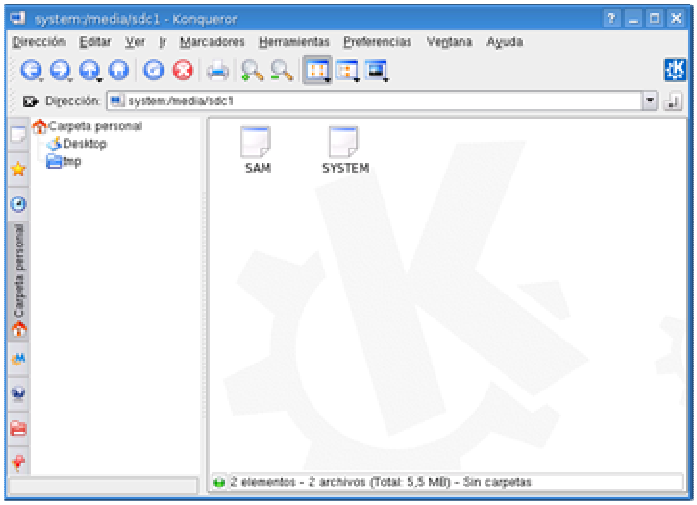
Este texto no pretende profundizar, ni explicar el funcionamiento de Linux y de sus características, así que seré muy breve. Linux es un sistema operativo como lo es Windows, que permite administrar los archivos, los dispositivos (monitor, mouse, teclado), y todo el PC. Si iniciamos nuestra PC Con Linux, Windows ya no se estará ejecutando, así que no estará protegiendo nada. En este ejemplo utilizaremos Knoppix (www.knoppix-es.org), un Linux que se descarga, se quema en un CD, se mete al ordenador, reinicias y ya estás en Linux, sin instalar nada. Debes haber configurado tu BIOS para arrancar desde el CD, pero eso no lo voy a explicar. En resumen, utilizaremos Linux sólo para copiar los archivos que Windows no quiere que copiemos.



Una vez que estamos en Linux, abrimos el disco duro y si hay más de uno, verificamos que sea el correcto. Como vemos las clásicas carpetas de Windows *(“Archivos de programa”, “WINDOWS”, “Doccuments and Settings”)* deducimos que es el disco duro correcto.

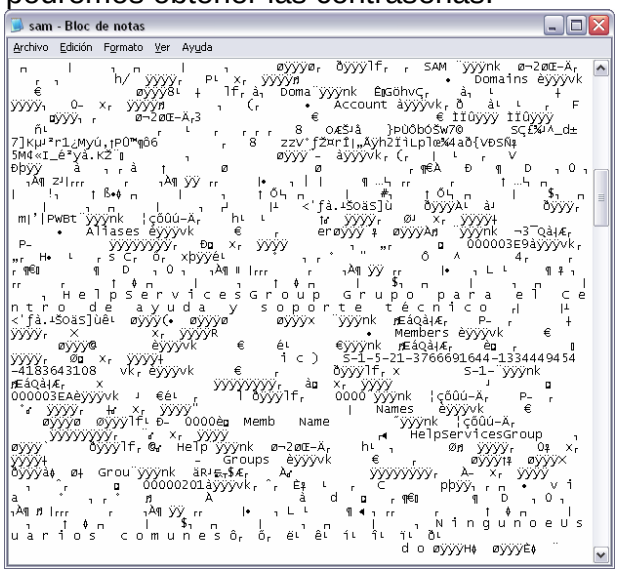


Vamos a la carpeta *“WINDOWS/system32/config”*, seleccionamos los archivos antes mencionados *“SAM”* y *“SYSTEM”*, y presionamos *Ctrl+C*.

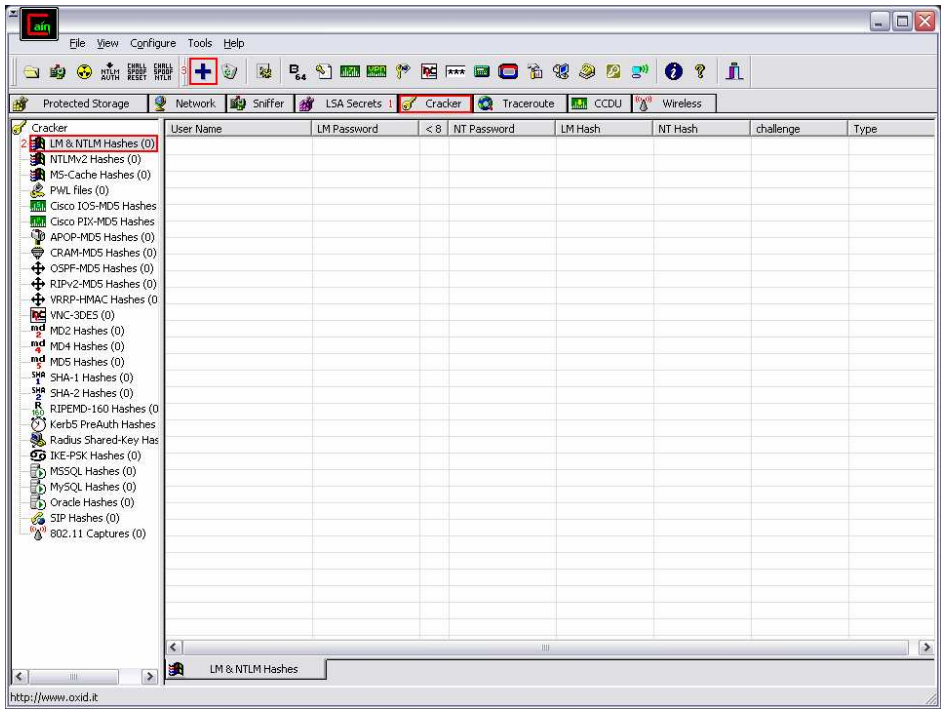


Conectamos nuestra memoria USB y copiamos los archivos en ella presionando *Ctrl+V*.

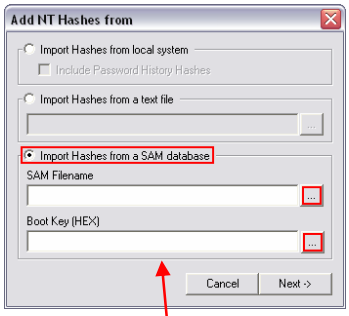
Ahora regresamos a Windows. Abramos el archivo con el bloc de notas, y así podremos obtener las contraseñas.



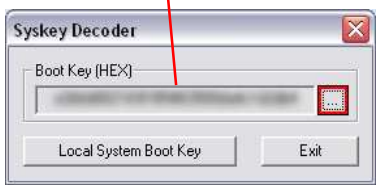
Parece que el archivo está dañado por que no se ven las contraseñas por ninguna parte, pero no es así. Recordemos que las contraseñas son encriptadas por el sistema, por eso instalaremos “Cain & Abel” (www.oixid.it) que es un programa de recuperación de contraseñas muy completo y nos ayudará en estas tareas. Instalamos pues el programa y lo ejecutamos. Algunos antivirus lo detectan como programa maligno, puesto que a veces utiliza algunas técnicas “sucias”, para realizar algunas de sus opciones.



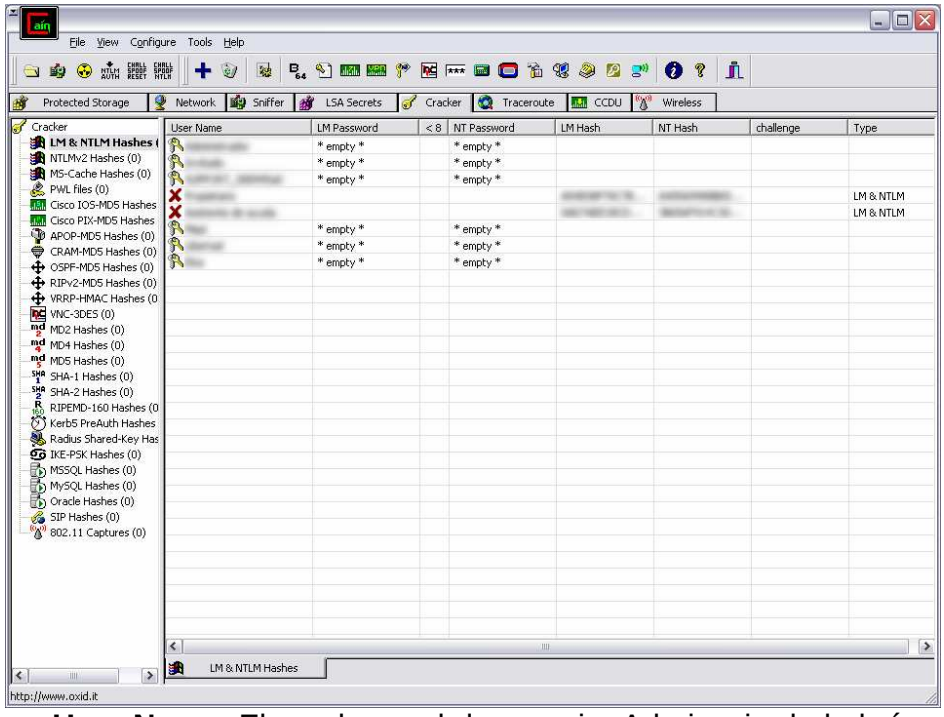
Vamos a la pestaña *“Cracker”* y en la lista a la derecha tenemos muchas opciones. Cada opción corresponde a un algoritmo diferente. Seleccionamos *“LM & NTLM Hases”* pues estos son los algoritmos que usa Windows. Ahora presionamos el botón de más que se ve arriba para añadir nuestro archivo SAM.



Seleccionaremos la opción *"Import Hases from a SAM database"* y donde nos pone *"SAM Filename"* picamos en los tres puntos y seleccionamos el archivo SAM que copiamos a nuestra memoria. Luego, donde nos pone *"Boot Key"* picamos en los tres puntitos y nos sale otra ventana.

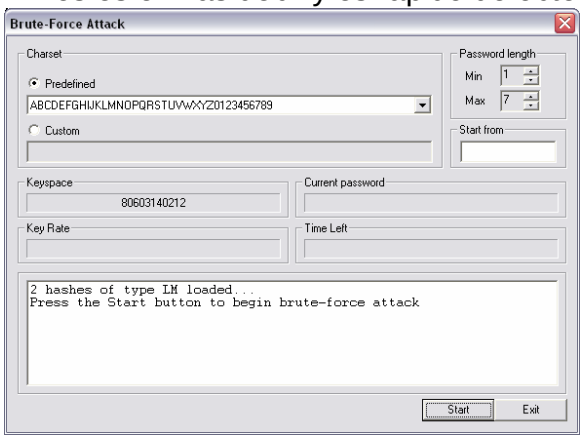


Picamos de nuevo en los tres puntitos y seleccionamos el archivo SYSTEM. Automáticamente debe de aparecer un código, lo seleccionamos y lo copiamos. Cerramos esta ventanita, en la anterior donde nos pedía *"Boot Key"* pegamos el código obtenido. Finalmente presionamos *"Next"*. ¡Ahora sí! Podemos ver los nombres de usuarios de la PC y otros datos interesantes.



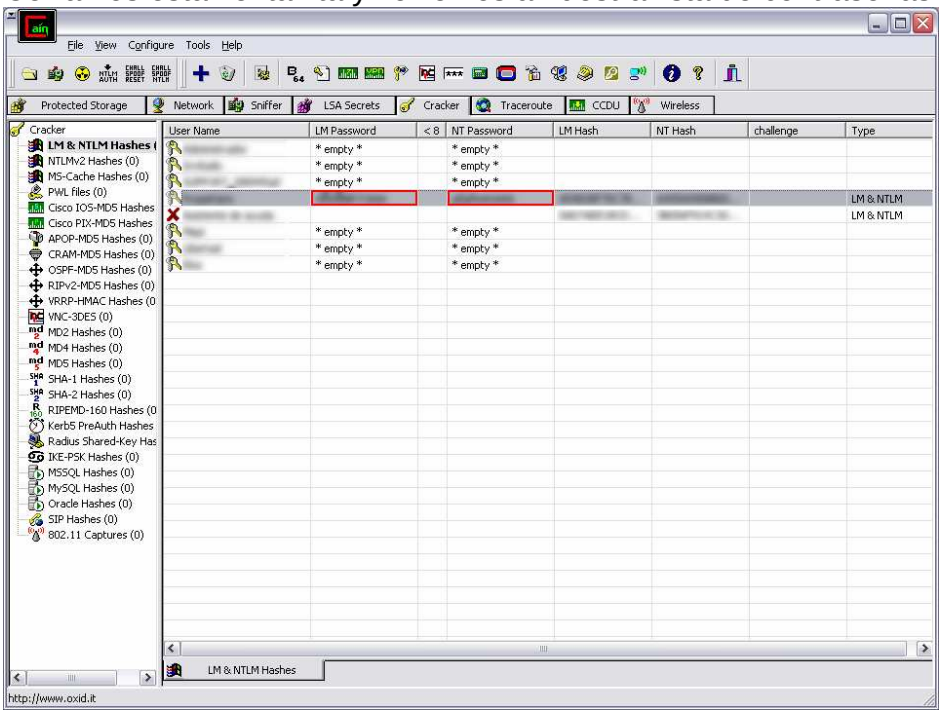
- **User Name:** El nombre real de usuario. A la izquierda habrá unas llavecitas si la contraseña ha sido descifrada, o una equis roja si no es así.
- **LM Password:** La contraseña LM, es decir la más fácil de obtener pero no la real. Si dice *"empty"* es que el usuario no tiene contraseña.
- **< 8:** Si hay un asterisco significa que la contraseña real es de menos de 8 caracteres de largo.
- **NT Password:** La contraseña real, pero la que es más difícil de obtener.
- **LM Hash:** El hash LM, el más débil.
- **NT Hash:** El hash NTLM, el más robusto.
- **Challenge:** Una opción de seguridad del sistema de la que no nos ocuparemos ahora.
- **Type:** Tipo de contraseña. Todas deberían ser del mismo tipo (LM & NTLM).

Como las contraseñas son encriptadas con un algoritmo irreversible tendremos que hacer un ataque de fuerza bruta, pero tranquilos que no tardaremos 20 días, ni mucho menos 33 billones de años. Seleccionamos la contraseña que nos interesa, y le damos clic derecho. Seleccionamos la opción *"Brute-Force Atack > LM Hashes"*. Le haremos el ataque de fuerza bruta al algoritmo LM, pues como vimos es el más débil y es rápido de obtener.



En *"Charset"* especificamos los caracteres con los que vamos a trabajar. Seleccionar sólo letras y números es una buena opción, puesto que la mayoría de los usuarios normales no usan símbolos en sus contraseñas y se reduce el tiempo de espera a unas 4 ó 5 horas. Cabe aclarar que si la contraseña tiene un carácter que no hayamos seleccionado, no podrá ser averiguada. Obtener la contraseña es una cuestión de probabilidades. Hacemos clic el botón de *"Start"* para que comience a trabajar.

Sólo queda esperar a que termine el proceso. Una vez que termine habremos averiguado la contraseña LM. Como ya tenemos la contraseña en mayúsculas, a la computadora le tomará unas fracciones de segundo averiguar la contraseña real. Cerramos esta ventanita y volvemos a nuestra lista de contraseñas.



Ahora en *"LM Password"* veremos la contraseña que hemos encontrado y en *"NT Password"* se mostrará la contraseña real.

A modo de conclusión

Todos los procesos aquí explicados, deberían funcionar con cualquier versión de Windows anterior a XP, pero en realidad sólo lo he comprobado en Windows XP. En Windows Vista los procesos funcionan pero el sistema ya no almacena el hash LM, por lo que averiguar la contraseña puede llevar mucho más tiempo.

En realidad, cuando una contraseña es más larga que 14 caracteres Windows XP no almacena el hash LM, dificultando averiguarla. Pero una contraseña de más de 14 caracteres es rara.

Sitiografía

http://es.wikipedia.org/wiki/Contraseña
http://es.wikipedia.org/wiki/Hash
http://en.wikipedia.org/wiki/LM_hash
http://en.wikipedia.org/wiki/Security_Account_Manager
http://es.wikipedia.org/wiki/Criptografía