CMD SIN SECRETOS

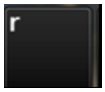
BY: WHITE DARKNNESS

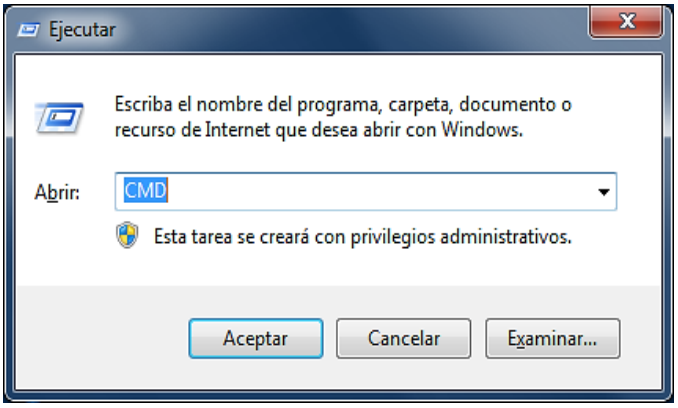
Version 2.0

hack x crack
WWW.HACKXCRACK.ES

CMD sin secretos ;)

Ok, si aún no sabes usar esta famosísima ventanita negra, ESO SE ACABÓ!!!! porque aprenderás desde cero :)

Para abrirla aplasta al mismo tiempo las teclas  +  y en la ventanita que te acaba de salir escribe CMD y da enter ;)

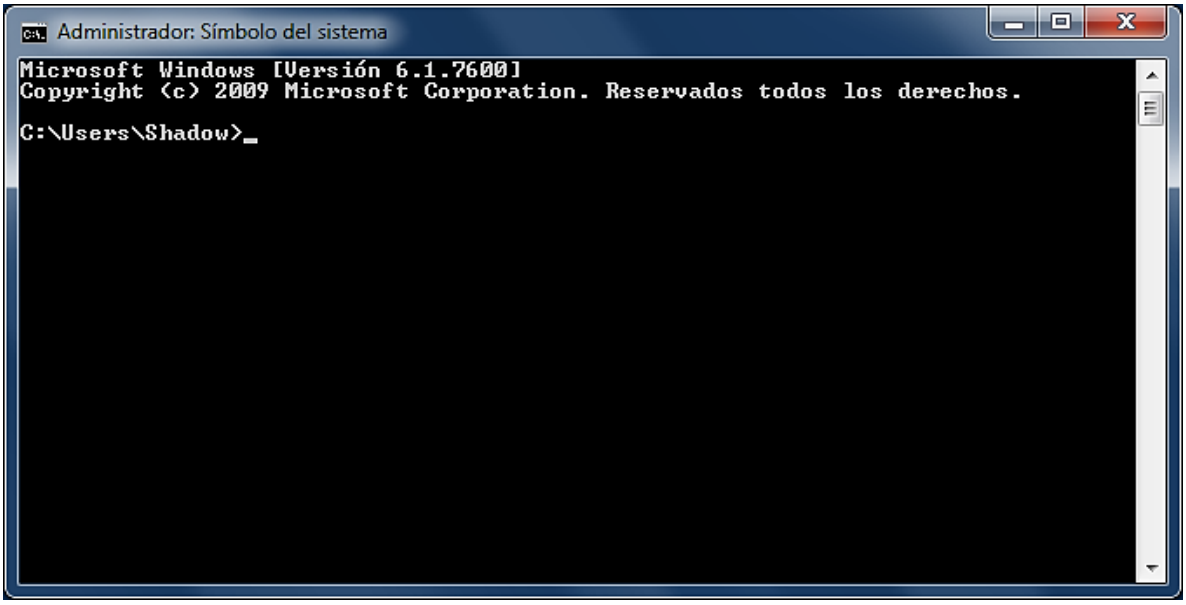


El CMD se conoce por muchos nombres:

-Línea o Interfaz de Comandos -Símbolo del Sistema -Procesador de Comandos -Shell del Sistema -Consola de Windows - Intérprete de Comandos -*Terminal*

Puedes decirle como quieras, pero olvídate más de ventanita negra :)

Y aquí está el CMD, te lo presento :)

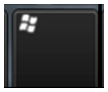
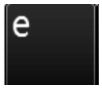


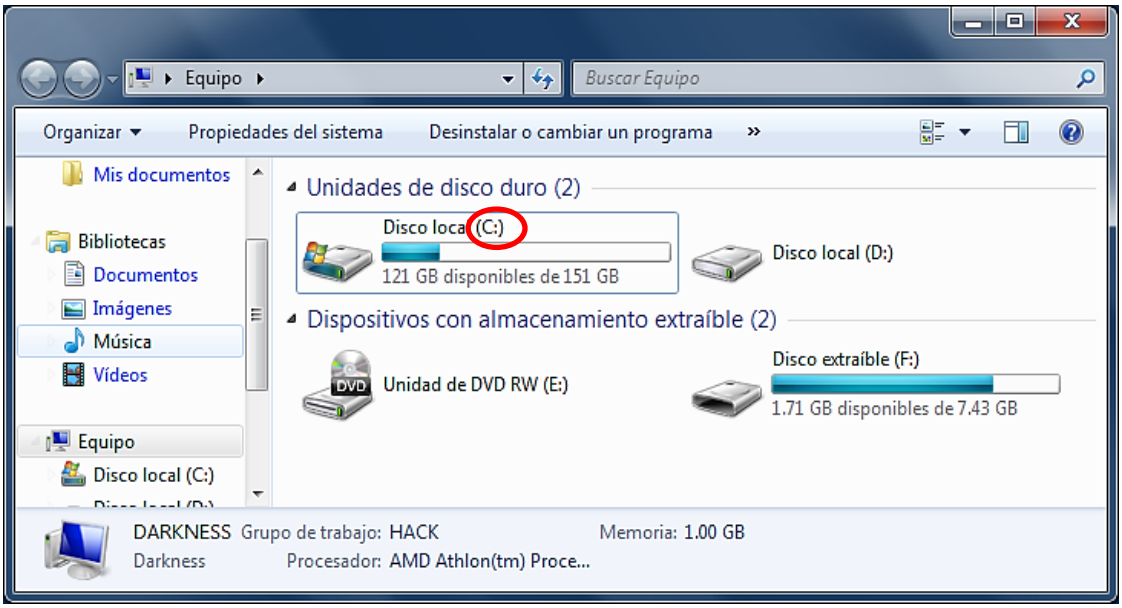
Como vemos, la Shell *"tiene un cursor parpadeando que parece estar esperando nuestras instrucciones"*, no te preocupes ahora mismo te explico como funciona y que significan todo eso ;)

Lo primero que llama la atención es esto: **C:\Users\Shadow>**
Qué significa??? Eso se llama ***DIRECTORIO***, OJO!!! Que no se te olvide y no lo pierdas de vista porque a continuación lo comentaremos.

Observación: El carácter **>** (mayor que) no forma parte del directorio, tan solo indica que la interfaz acepta comandos. Por eso en la ***Shell de Phyton*** también está presente (Tienes un excelente manual sobre este lenguaje en aquí) Claro, no por eso deja de ser útil para otras cosas :)

Vamos a verlo parte por parte; primeramente allí está una **C** mayúscula con dos puntitos, lo cual me dice que estoy dentro del *disco C*. Bueno y donde rayos está eso???

Aplasta al mismo tiempo las teclas  +  se abrirá una ventana como la siguiente que sin duda ya la habrás mirado muchas veces ;)



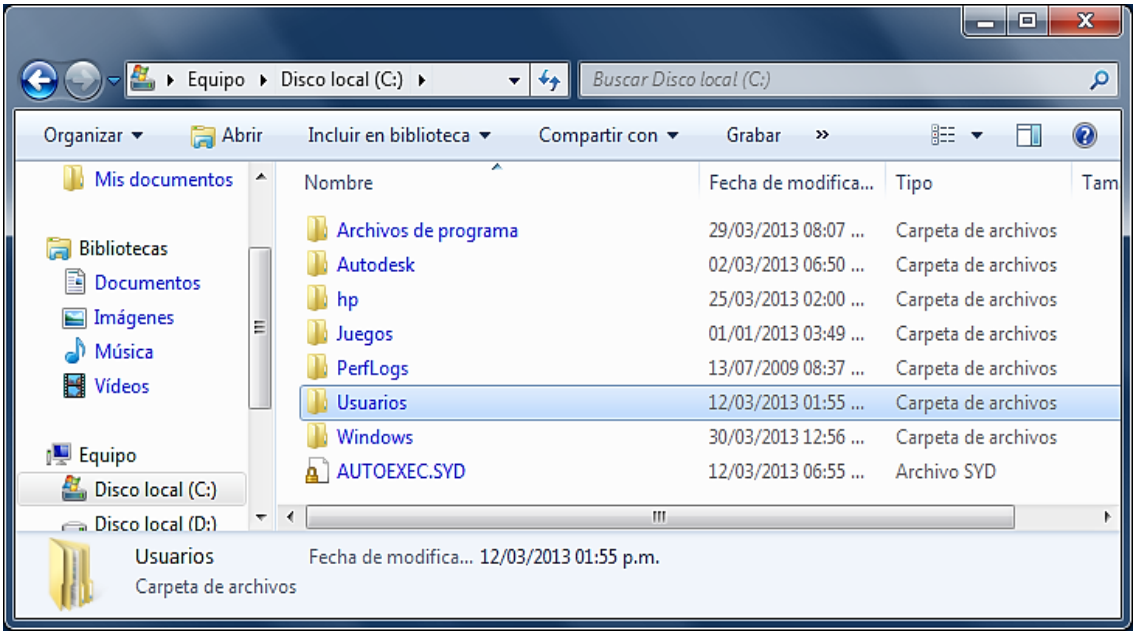
Aquí es donde encontramos las unidades de disco duro que tenemos. Lo único que nos importa es lo que encerré en el circulito rojo :)

-AAaahhh!!! Se parece a la C con dos puntitos que andamos buscando.

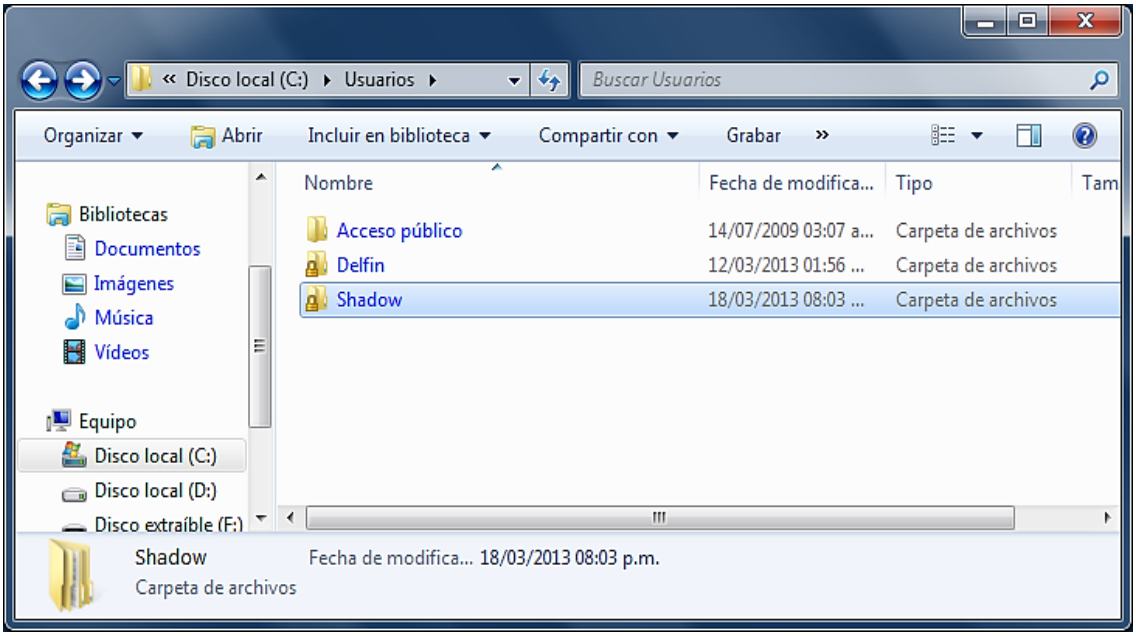
Hombre que brillante eres ya la encontraste, pero que estás esperando ábrelo :)

NOTA: Desde hoy la C con dos puntitos se llama **DISCO C**

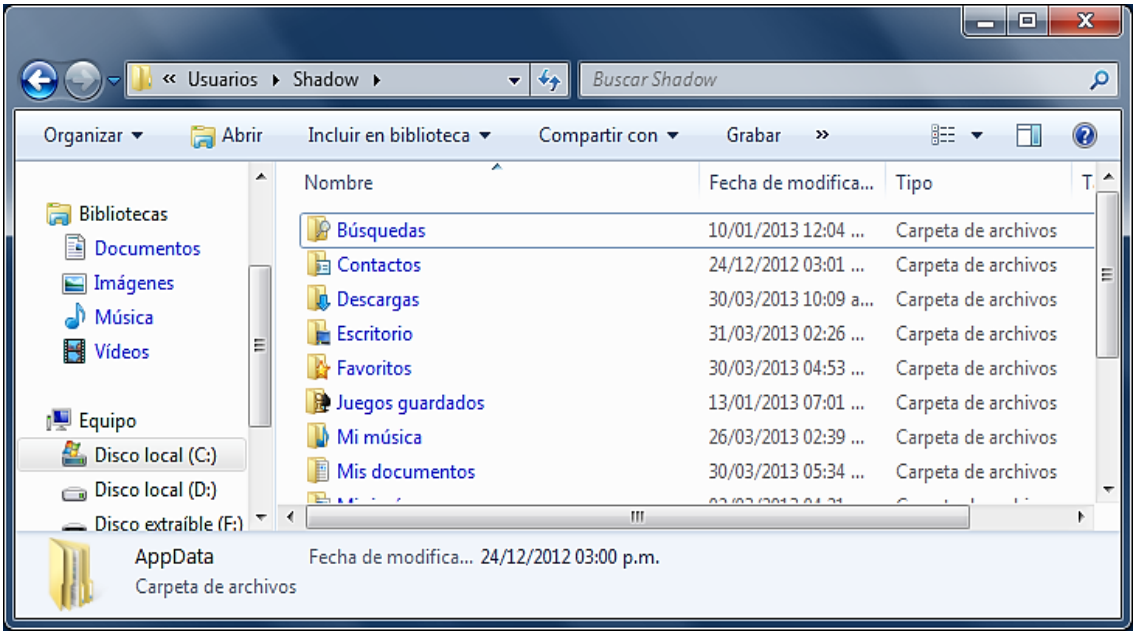
Ahora vemos que una diagonal separa al Disco C de la palabra **Users** (Usuarios) Esto significa que aparte de estar dentro del C también estamos dentro de Users o de Usuarios. Entonces busca esa carpeta y ábrela :)



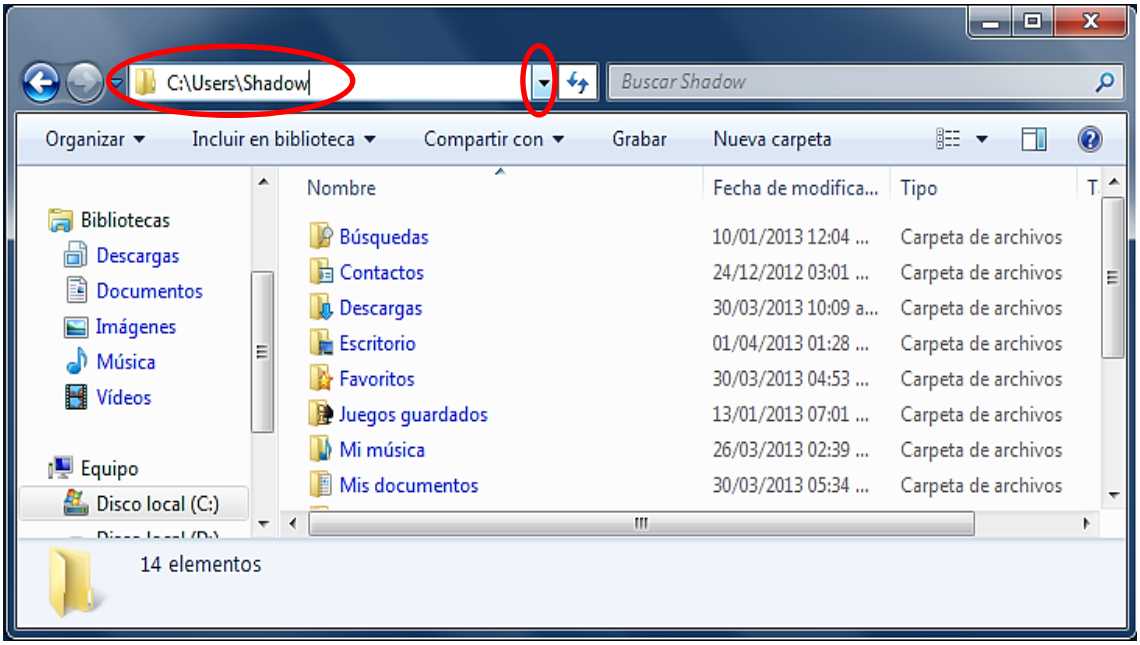
Ya vamos acabando, solo nos queda encontrar la palabra **Shadow,** este es el nombre que le pusiste a tu cuenta de usuario (No es lo mismo que el nombre del Equipo) En este caso el usuario se llama Shadow.



Listo por fin terminamos, si lo has hecho bien te debió quedar algo como esto:

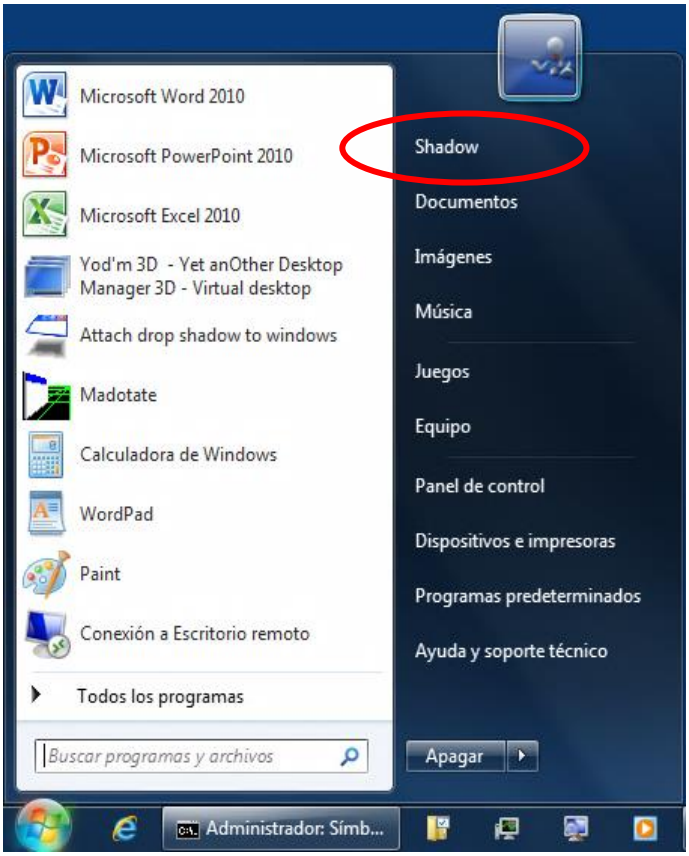


Por consiguiente podemos concluir que el CMD nos está diciendo que estamos dentro de esta carpeta (llamada carpeta personal). Para comprobar que entramos bien dale clic a la flechita de la barra de direcciones y verás que es exactamente el mismo directorio que tiene el CMD ;)



NOTA: Fíjate como un directorio se separa por una diagonal, pero esa diagonal siempre va a estar inclinada a la **IZQUIERDA**, o sea así: **** (Contrabarra) No es lo mismo que esta otra inclinada a la derecha: **/** (Barra)

Ahora que si tienes Windows 7, puedes acceder más fácil a este directorio desde inicio y después en Shadow (O el nombre que te diste como usuario)



Hay muchas formas de abrir la consola. Aquí están dos más:

-Escribiendo CMD en la parte que dice: "*Buscar programas y archivos*"

-Dando clic donde dice: "Todos los programas", después abrir la carpeta "Accesorios" y por último en "Símbolo del Sistema"

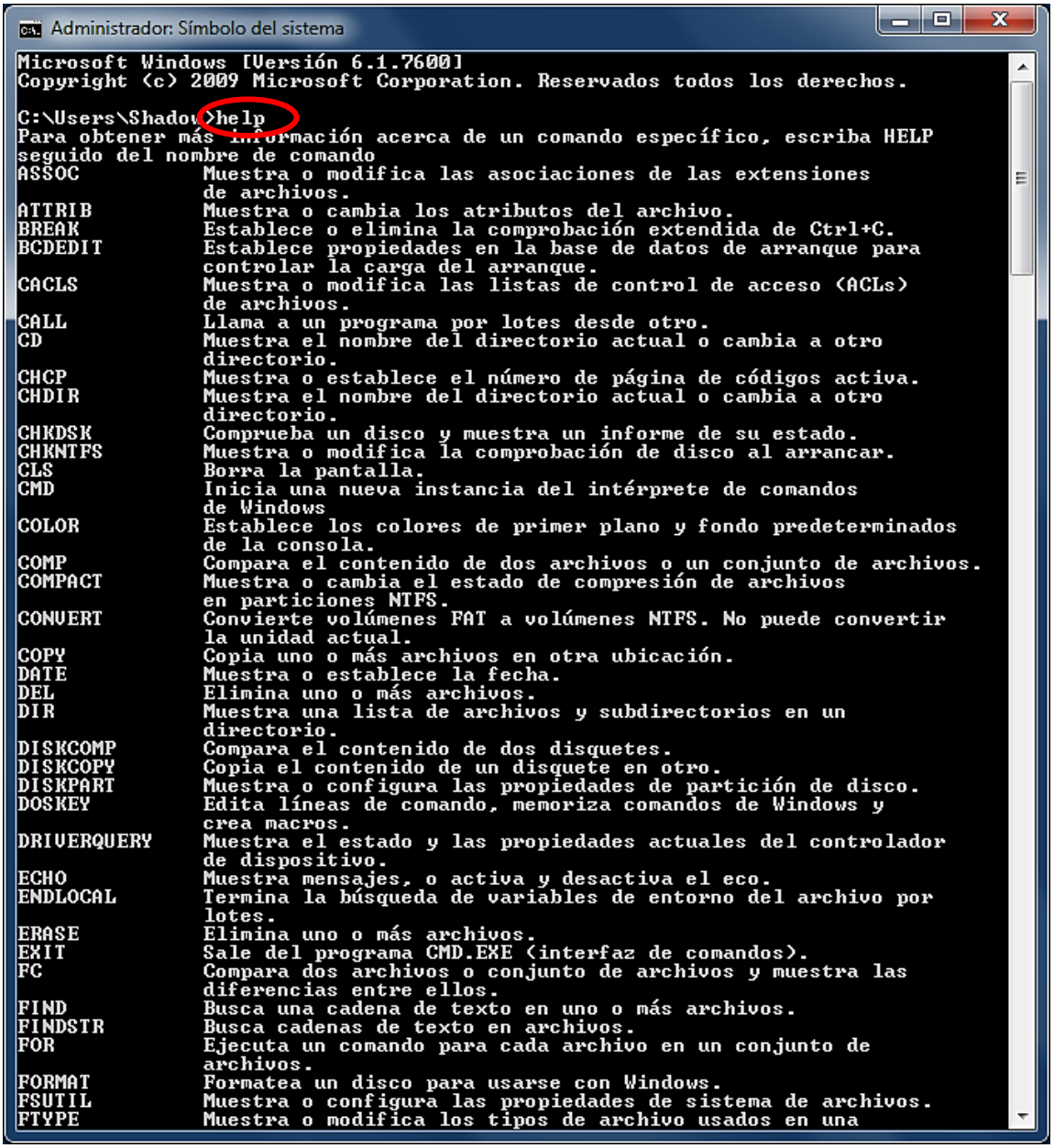
-Mmm… pues todo me parece bien, pero lo que me interesa es aprender a usar esta famosísima línea de comandos. Te diste cuenta??? ya no la llamé ventanita negra ;)

Precisamente para allá iba y también te darás cuenta de que todo lo que expliqué tenía un propósito ;)

No pierdas de vista el directorio que acabamos de encontrar, porque vamos a hacer unos cuantos experimentos sobre el :)

Vamos a lo nuestro!!!

Con este procesador de comandos podemos realizar muchas tareas sin necesidad de usar el ratón, solo tenemos que saber cuales son los comandos que debemos usar. Para averiguarlo teclea **help** (ayuda) en el CMD y da enter.



Vaya!!! Aunque hice la ventana más larga no alcanzaron a mirarse todos los comandos; pero no te asustes!!! Verás que es más fácil de lo que piensas ;) En la parte izquierda están algunos de los comandos que podemos usar (Ojo!!! he dicho algunos) y *en la parte derecha está una breve descripción de cada uno.*

Vamos a usar uno de los más básicos, me refiero al CD (**C**hange **D**irectory)

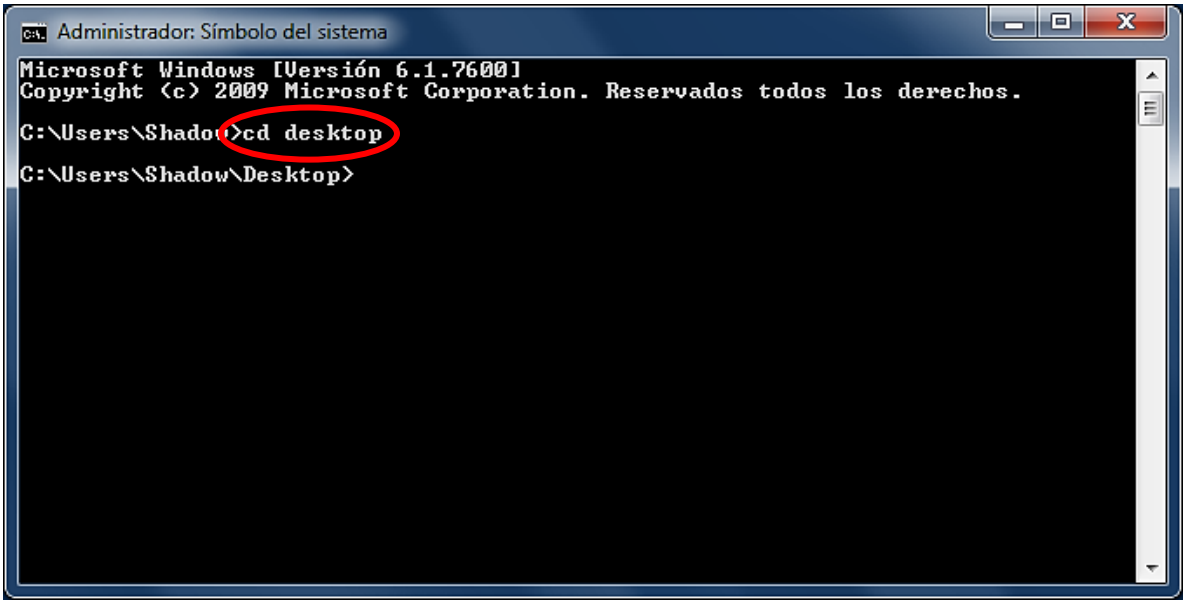
Si no lo has notado los comandos van ordenados alfabéticamente por si estabas tardando en hallarlo :)

Ok, su descripción dice: "Muestra el nombre del directorio actual o cambia a otro directorio"

Como ya sabemos, nosotros estamos dentro de este directorio: **C:\Users\Shadow** por lo cual estaremos trabajando en esa parte a menos que nos movamos a otro lugar, por ejemplo si queremos desplazarnos hasta el escritorio tendríamos que escribir cd escritorio y dar enter, pero si te sale algo como esto: *"El sistema no puede encontrar la ruta especificada."* Quiere decir que tienes que poner escritorio en inglés.

-Que bueno que sé algo de inglés, ya decía yo que haberme ido para los United States tenía que servirme de algo :) Entonces tengo que escribir ***cd desk****.*

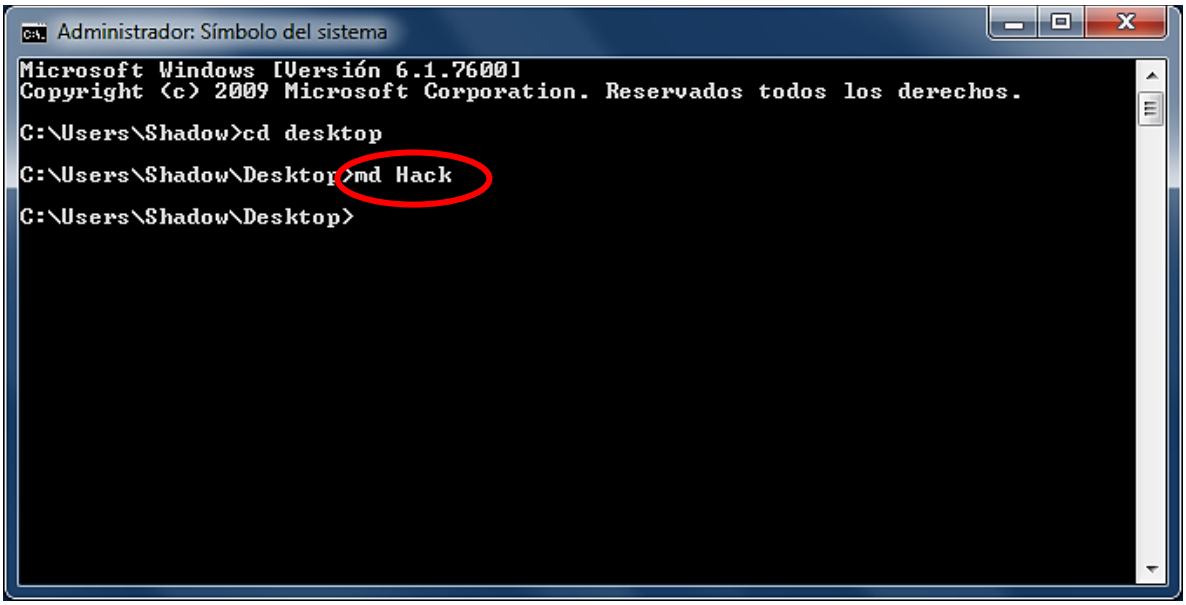
I'm sorry, pero aunque escritorio si se dice desk, escritorio de computadora es **desktop** ;)



Como ves ya accedimos al escritorio :) Ahora busquemos otro *comando interno* del CMD (después entenderás porque dije interno) Que te parece el que dice MD (**M**ake **D**irectory)

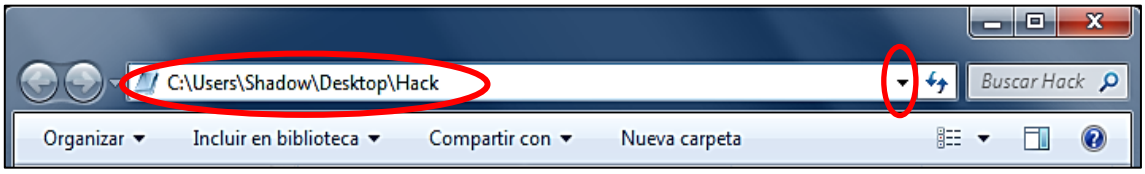
Su pequeña descripción dice: *"Crea un directorio".* Probémoslo, escribe MD y el nombre que quieras darle a tu directorio, el mío se va a llamar Hack (No pierdas de vista tu escritorio)

Nota: Puede que sobre el comentario pero siempre es necesario dar enter para que el comando se ejecute.



-Dios!!! Me acaba de aparecer una carpeta en el escritorio que se llama Hack.

Así es, ábrela y de nuevo da clic a la flechita de la barra de direcciones:



-Según mis cálculos esto quiere decir que un directorio es una carpeta, porque es lo mismo que está en el CMD pero aparte tiene el nombre Hack que es la carpeta que acabamos de hacer y de abrir.

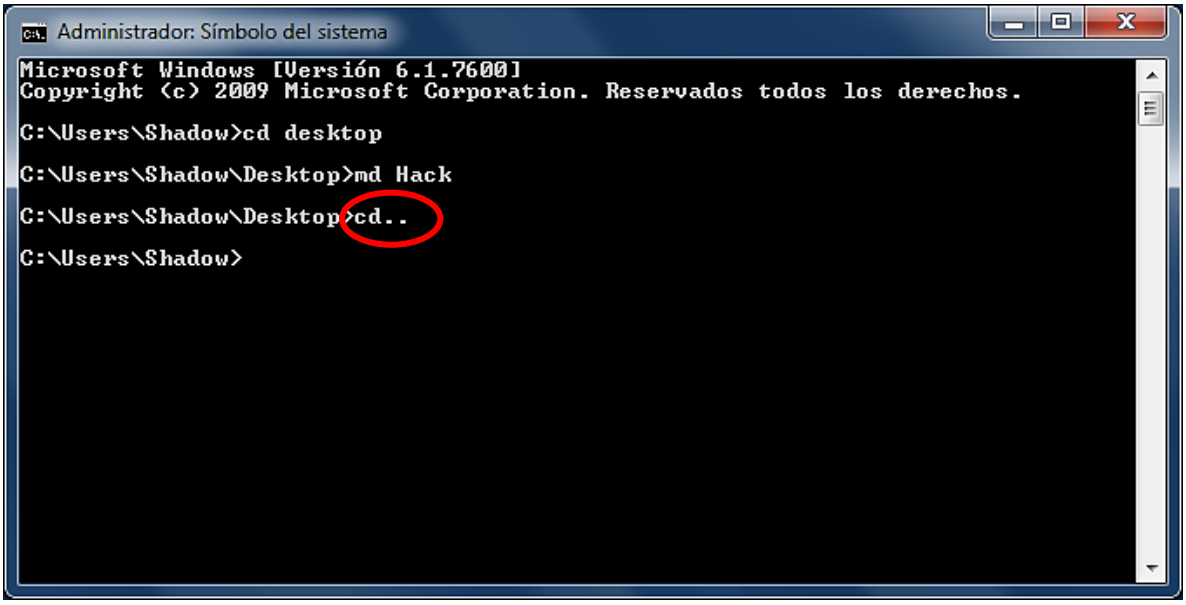
Muy bien!!!! Te felicito.

-Muchas gracias, yo sabía que un día estarías orgulloso de mí, creo que voy a llorar.

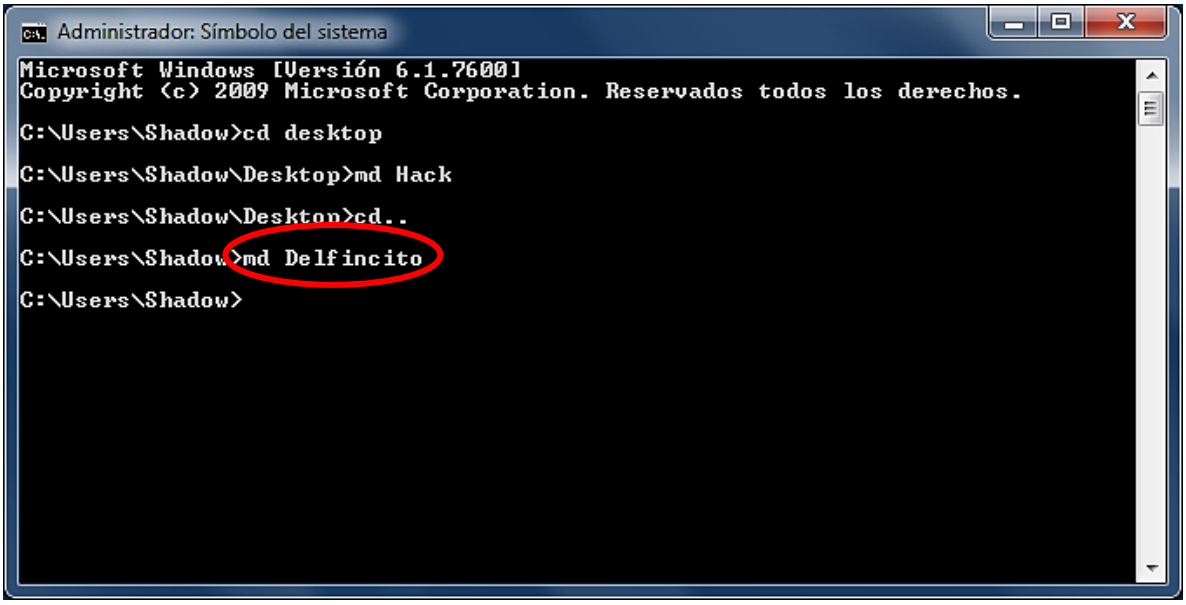
Hombre no te aceleres que todavía tienes mucho por aprender. Hagamos un experimento más :)

Quiero recalcar que la carpeta se creó en el escritorio porque actualmente estamos trabajando precisamente allí, pues recuerda que nos movimos del directorio en el que estábamos al principio, de lo contrario la carpeta hubiera

aparecido aquí: **C:\Users\Shadow.** Para demostrar nuestra teoría tenemos que retroceder. Escribe el comando *CD pero seguido de dos puntos* y da enter.



Ahora nuevamente estamos donde empezamos, entonces hagamos otra carpeta y veamos que sucede, ya sabes escribe MD y el nombre que le quieras dar, yo le voy a poner *Delfincito* :)



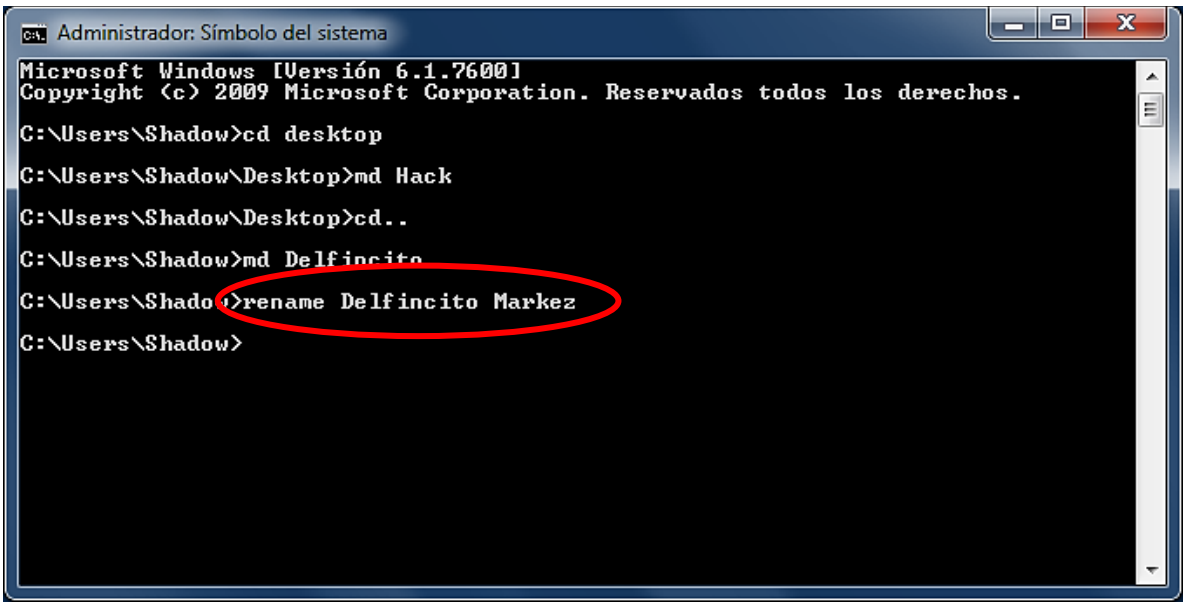
-Esta vez la carpeta NO me salió en el escritorio, sino en la ventana que tiene como directorio ***C:\Users\Shadow*** *porque nosotros nos regresamos allí con el comando* ***CD..*** *Ahora sí entendí :)*

Perfecto creo que ya has entendido la importancia que tiene un directorio cuando estamos usando la consola ;)

Antes de pasar a otro tema quisiera que analizáramos el comando RENAME (renombrar). Aunque creo que no hace falta escribir su descripción aquí la tienes: *"Cambia el nombre de uno o más archivos"*

Nota: Los comandos Ren y Rename significan lo mismo y sirven exactamente para lo mismo.

Probémoslos!!! Escribe rename, el nombre del archivo y después el *nuevo* nombre que quieras que tenga. Yo voy a renombrar la carpeta *Delfincito* a *Markez*, por lo tanto debo hacer esto:



Te reto a cambiar el nombre de la carpeta Hack a Crack (Recuerda que la carpeta Hack está aquí: **C:\Users\Shadow\Desktop** y no aquí: **C:\Users\Shadow**) Suerte!!!

Apunte: Usa el comando cls (**Cl**ean **S**creen) para limpiar la pantalla de todos los comandos usados y con **color a** le das mi estilo favorito al cmd :)

Pequeño paréntesis

Aclarando Dudas :)

Vamos a intentar despejar algunas cuestiones que pudieron haber quedado unas líneas más arriba ;)

Para empezar cuando abriste el CMD quizá obtuviste este directorio: **C:\Documents and Settings\Administrador**
Pero es exactamente lo mismo que el anterior, allí está el Disco C solo que en lugar de **Users** tenemos la carpeta **Documents and Settings** y el usuario se llama **Administrador.**

Si te salió eso no hubo problemas para usar los comandos que mencionamos en el artículo anterior; pero si obtuviste algo así: **C:\Windows\System32** las cosas se van a complicar tantito :)

-A mi me apareció eso y no me funcionó ningún comando, creo que me has engañado y yo que confiaba perdidamente en ti :(

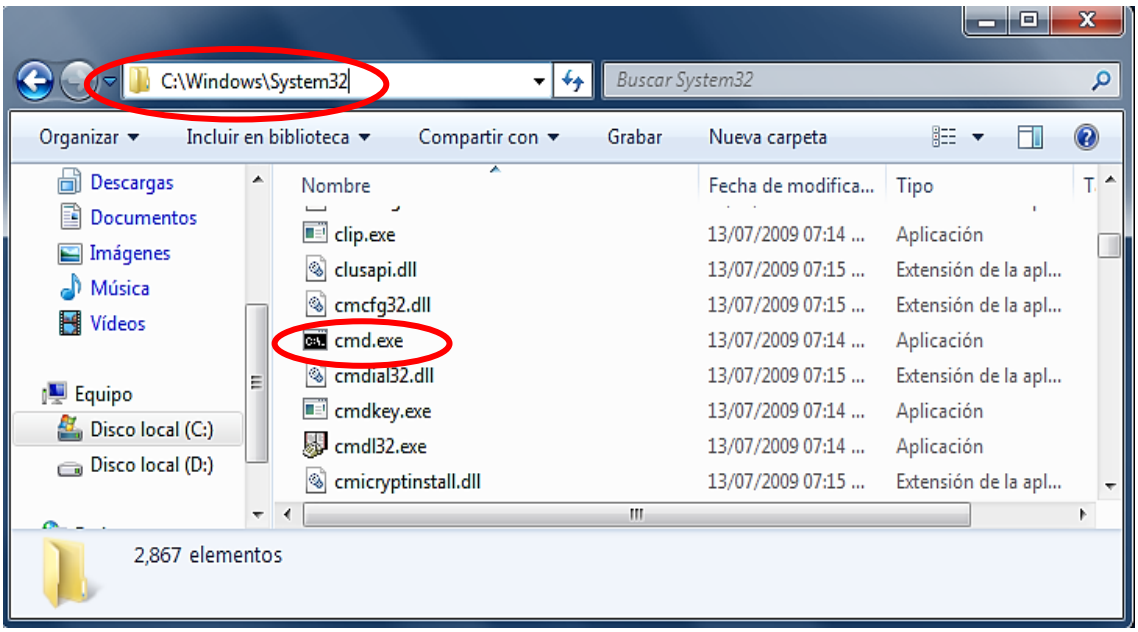
Hombre si me decidí hacer esta sección fue para que nadie se quedara con dudas, así que ahí te va ;)

¿Sabes en que directorio está el CMD?

Está en este: **C:\Windows\System32** Anda que esperas para abrir ventana por ventana hasta que lo halles tal como hicimos la vez pasada (Usando el ***Explorador de Windows***) No!!! Una mejor idea es que escribas ese directorio en la barra de direcciones de cualquier carpeta y des enter, pero si no quieres trabajar tanto también se vale que lo copies y pegues ;)

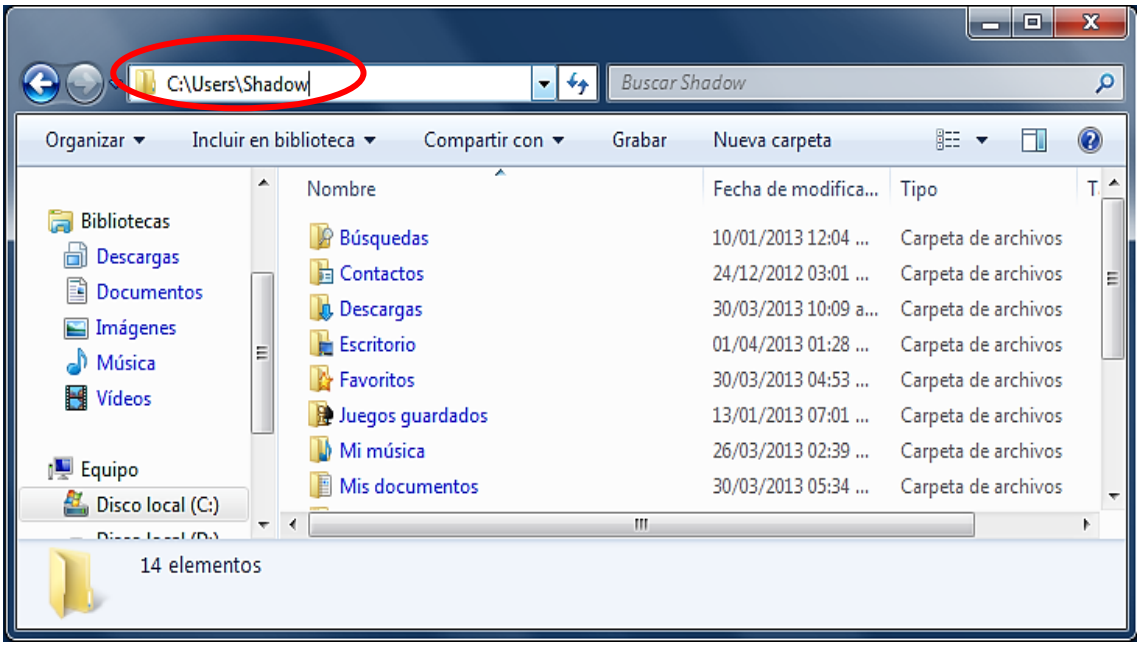
Aquí abajo está la imagen, ya solo falta que lo encuentres, normalmente todo está ordenado de manera alfabética.

Nota: Uno de los directorios (carpeta) más importante de tu computadora es precisamente **C:\Windows\System32** por eso normalmente tiene el atributo **+H** y **+S** descuida si sigues leyendo lo entenderás e incluso podrás quitar esa patética protección :)

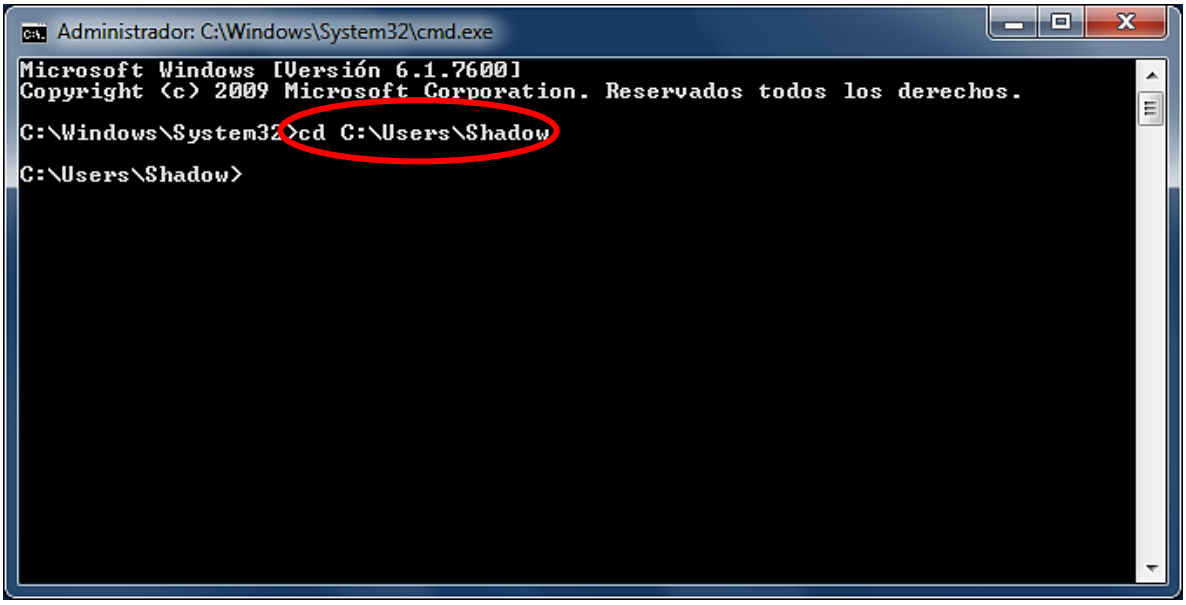


-OK y eso que tiene que ver?¿?

Pues que estás dentro de esa carpeta y es muy diferente a esta otra:



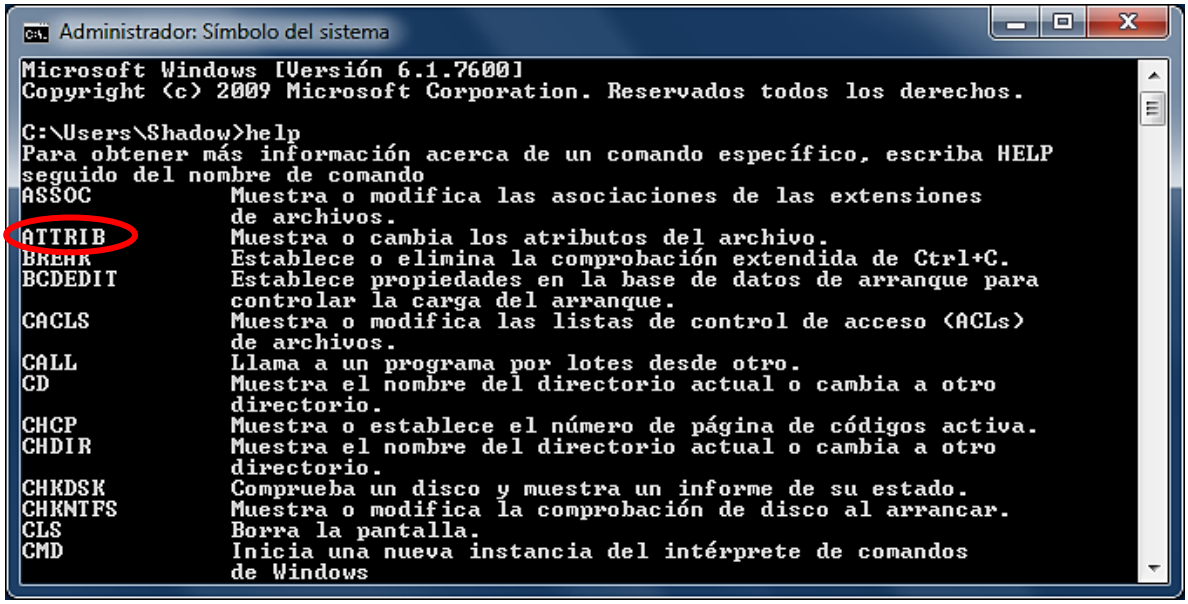
La manera más fácil de arreglar este asunto es escribiendo en el CMD: **cd C:\Users\Shadow** y dar enter. *Recuerda que la última palabra depende del nombre de usuario que te diste.*



Si tienes *Windows XP* puedes probar con:
cd C:\Documents and Settings\Administrador (recuerda, en lugar de *Administrador* escribe tú nombre personal de usuario)

No olvides que el comando **CD** sirve para cambiar de directorio. Listo a partir de ahora se han acabado las dudas, así que continuemos con nuestro curso :)

Entonces escribamos **help** y busquemos algún comando interesante :)

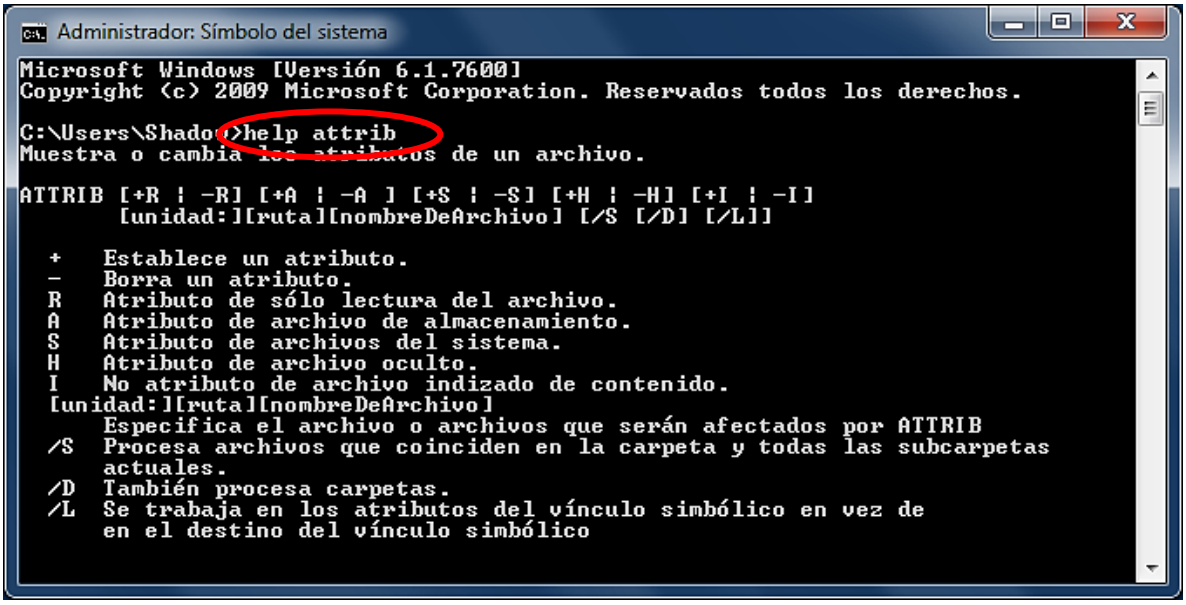


Vamos a usar un clásico: Attrib (Atributo). Su descripción dice: *"Muestra o cambia los atributos del archivo"*

Como te diste cuenta necesitamos más información para poder usarlo, ¿Cómo hacemos esto? Si eres observador notaste que después de escribir help, dice lo siguiente:

"Para obtener más información acerca de un comando específico, escriba HELP seguido del nombre de comando"

Más claro no podría estar. Entonces escribamos help y después Attrib.



La anterior es una manera de obtener más información, la segunda y **mejor** manera es escribiendo el nombre del comando pero acompañándolo de: /? Es decir, en nuestro ejemplo haríamos esto **Attrib /?**

Parámetros

Ha llegado el momento de hablar sobre parámetros. ¿Qué es un parámetro? Es algo que no se puede ver; sin embargo existe. De ahí que el voltaje sea un parámetro, también lo son la corriente, la potencia y ese tipo de cosas. Pero como nosotros estamos hablando del CMD, podríamos decir que un parámetro *es una funcionalidad extra que tiene un comando* y aunque no podamos mirarlos allí están y existen.

En este caso al comando Attrib lo podemos acompañar de varios parámetros y cada uno hace cosas muy interesantes :)

-Aún no entiendo a que te refieres, yo no veo en ningún lugar la palabra parámetro :(

Abre los ojos!!! Al menos yo alcanzo a contar 10 de ellos. Es más te los voy a poner en una tabla ;)

Apunte: Un comando también puede considerarse una **Orden** y un parámetro un **Modificador.**

Parámetro	¿Qué hace?
+	Establece un atributo.
-	Borra un atributo.
R	Atributo de sólo lectura del archivo.
A	Atributo de archivo de almacenamiento.
S	Atributo de archivos del sistema.
H	Atributo de archivo oculto.
I	No atributo de archivo indizado de contenido.
/S	Procesa archivos que coinciden en la carpeta y todas las subcarpetas actuales.
/D	También procesa carpetas.
/L	Se trabaja en los atributos del vínculo simbólico en vez de en el destino del vínculo simbólico.

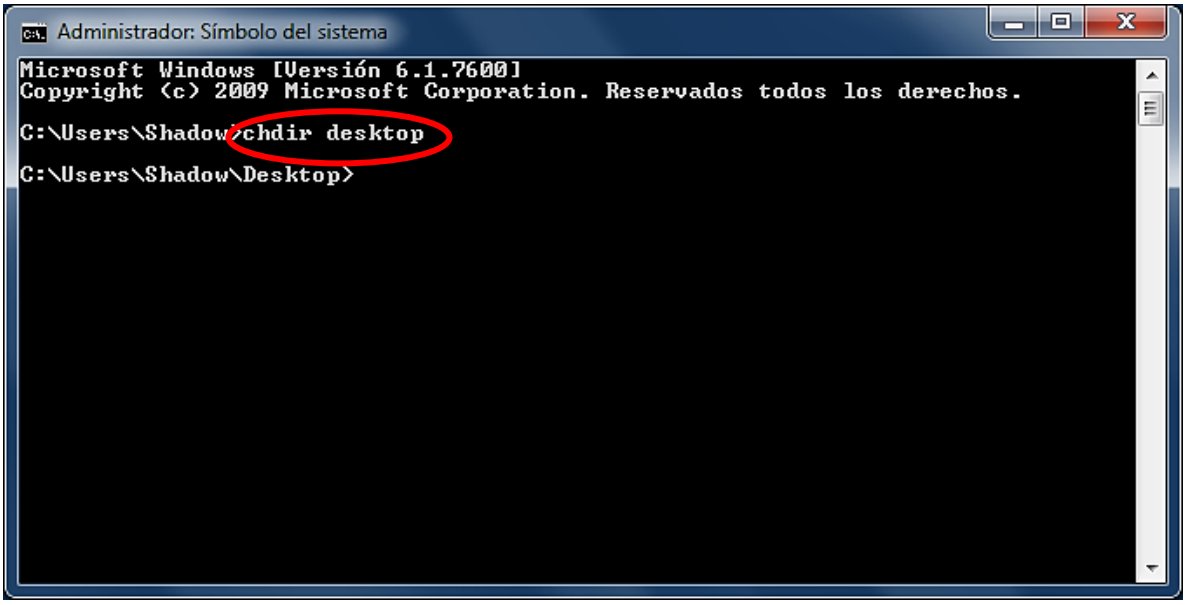
-Haaa!, ahora sí los veo, que todo fuera como eso :)

Pues que bueno, porque los vamos a usar :) Quedamos que Attrib iba acompañado de esos parámetros; hagamos una prueba. Espero que no hayas borrado la carpeta Hack que hicimos en el artículo anterior porque con ayuda del comando Attrib vamos a volverla invisible :)

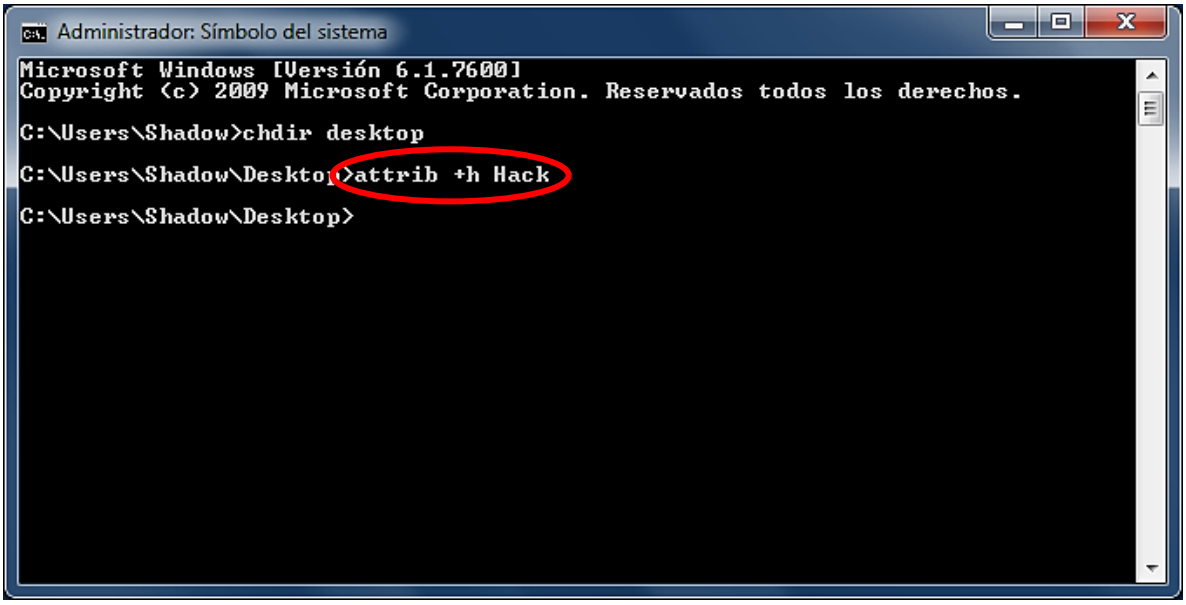
Como la carpeta quedó en el escritorio debemos movernos hacia allá.

-Entonces tengo que escribir cd desktop o sino cd escritorio, ves que a mí no se me olvida como hacer las cosas :)

Muy bien, no está nada mal pero lo podemos mejorar ;) Si eres curioso habrás notado que hay otro comando que hace lo mismo que el CD, me refiero al **CHDIR (C**hange **D**irectory**)**. Probémoslo!



Te das cuenta? Hicimos lo mismo y además aprendimos a usar otro comando. Ahora escribe **Attrib +h Hack** y da enter con esto la carpeta Hack desaparecerá de tu vista ;)



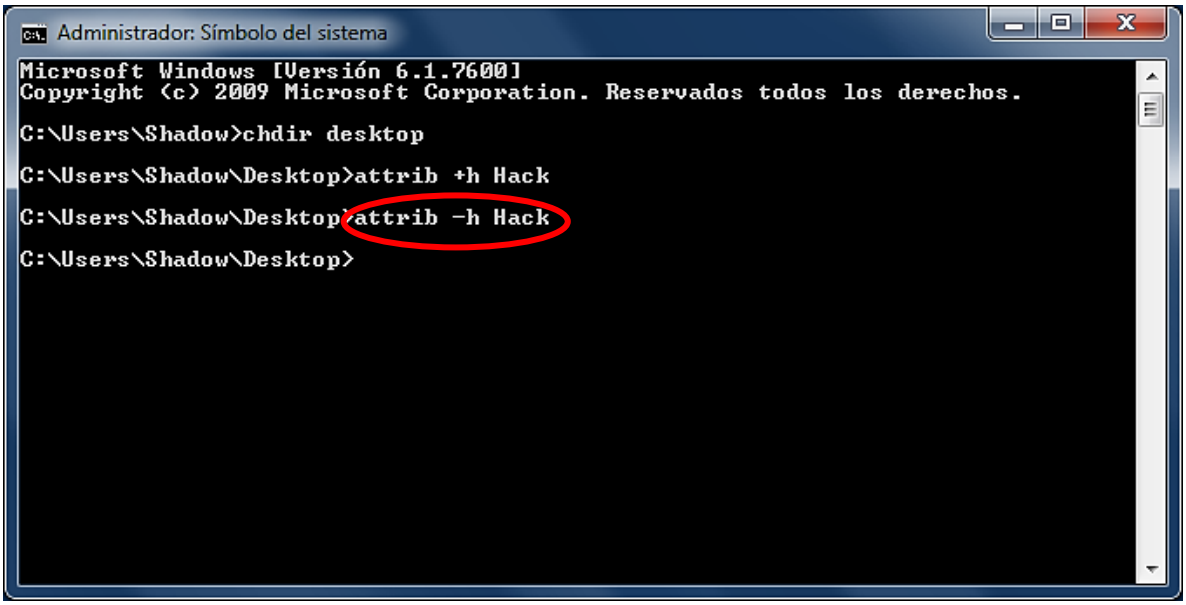
-No puede ser!!! En un momento la carpeta estaba en mi escritorio y en otro momento ya no estaba, como pasó esto???

Lo primero que escribimos fue el comando Attrib, después pusimos el signo **+** recuerda que fue el primer parámetro de los 10 que enumeramos y servía para establecer un atributo y por último al ladito del **+** tecleamos la **h** que fue el sexto parámetro y significaba *"Atributo de archivo oculto*"

Así fue como conseguimos esfumar la carpeta Hack ;) Ahora, ¿cómo hacemos para que regrese?

-Tengo una teoría :) Debo escribir Attrib -h Hack porque con el signo menos quitamos un atributo y la h significa oculto. Es decir quitar el atributo oculto a la carpeta Hack ;)

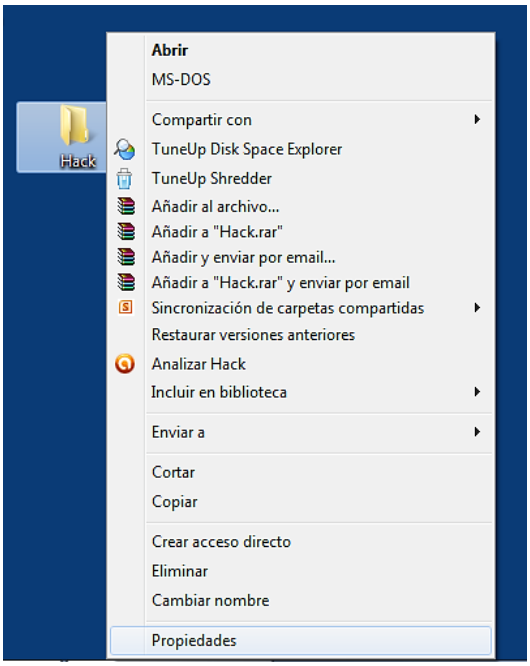
Excelente!!!, me has sorprendido, mira la cara que me dejaste :0

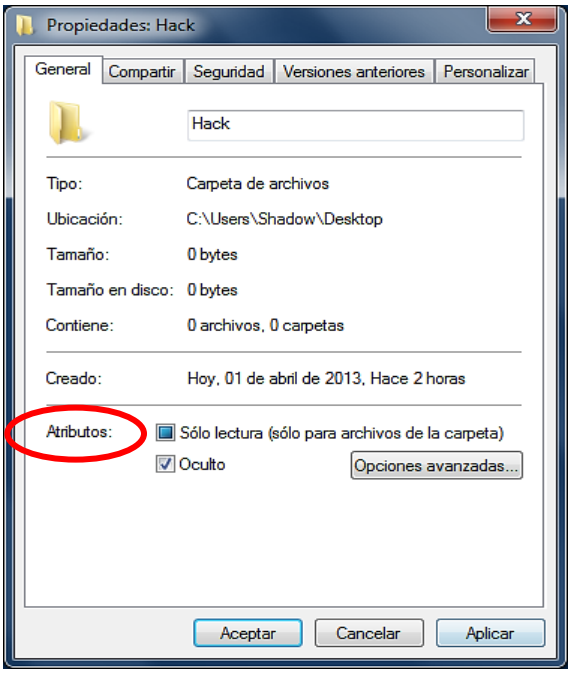


Habíamos dicho que el CMD servía para hacer muchas tareas sin necesidad de usar el ratón. Así que mi pregunta es ¿cómo consigo ocultar la carpeta usando el ratón? O más propiamente dicho ¿cómo consigo ocultar la carpeta usando el explorador de Windows?

-Le doy clic derecho a la carpeta, después selecciono propiedades, palomeo la opción Oculto y le pico en Aplicar :)

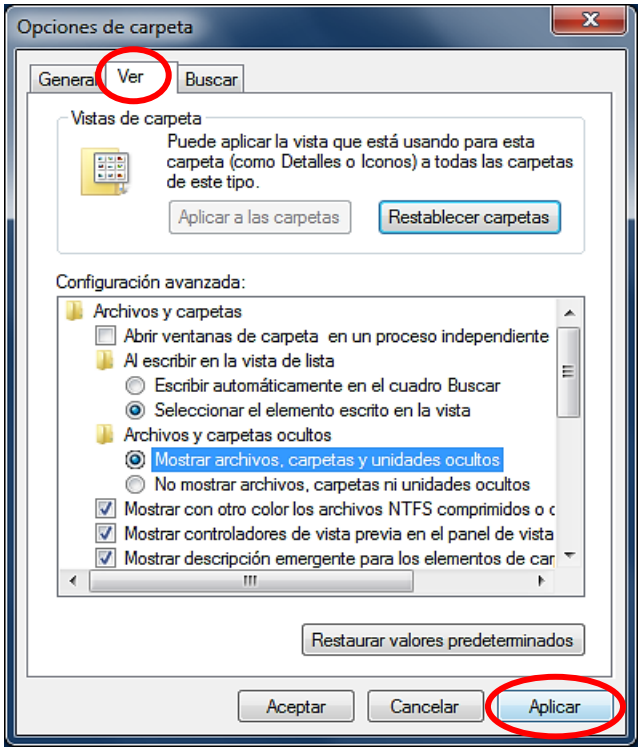
Perfecto!!! Amigo ten cuidado que un día de estos pueden venir los rusos por ti ;)





Qué te parece si te invierto la pregunta ¿cómo puedo aparecer la carpeta? Solo te digo que al menos hay 2 maneras diferentes de hacerlo ;)

-Voy a Panel de Control, después en Apariencia y Personalización entro en donde dice ***Opciones de Carpeta****; la ventanita que apareció arriba tiene una pestaña que dice Ver, pulso sobre ella y marco la opción "Mostrar archivos, carpetas y unidades ocultos" ;)*



Vaya, realmente sabes lo que haces! Solo permíteme una sugerencia; cuando entres a panel de control, en la esquina superior derecha vas a ver algo que dice **"Ver por: Categoría"** en lugar de categoría escoge Iconos pequeños (Para Win7)

Nota: Para acceder al panel de control escribe ***control*** en *Ejecutar*

-Hombre que te pasa, si nada más estaba haciéndome el que no sabía para ver si tú sabías, soy tan astuto!!! ;)

Lograste engañarme!!! Aunque te apostaría que no sabes cual es la segunda manera de aparecer la carpeta ;)

-Ahhh… Pues.., este,, mmm.,, y cambiando de tema, tengo una pregunta que se me acaba de ocurrir ¿de que me sirve saber usar la consola, si puedo hacer las mismas cosas con el Explorador?

Yo dije que con la línea de comandos podías hacer *muchas* cosas sin necesidad de usar el ratón, la verdad es que puedes hacer *todas y más*. El CMD tiene más poder del que crees. El día que consigas una *shell remota* con *privilegios root* vas a apreciar saber usarlo :)

Nota: Se me pasaba comentarte que en la ventana "Opciones de carpeta" también te asegures de **desmarcar** las opciones *"Ocultar archivos protegidos por el sistema operativo"* y *"Ocultar las extensiones de archivo para tipos de archivo conocidos"* Con eso te llevarás una sorpresita ;)

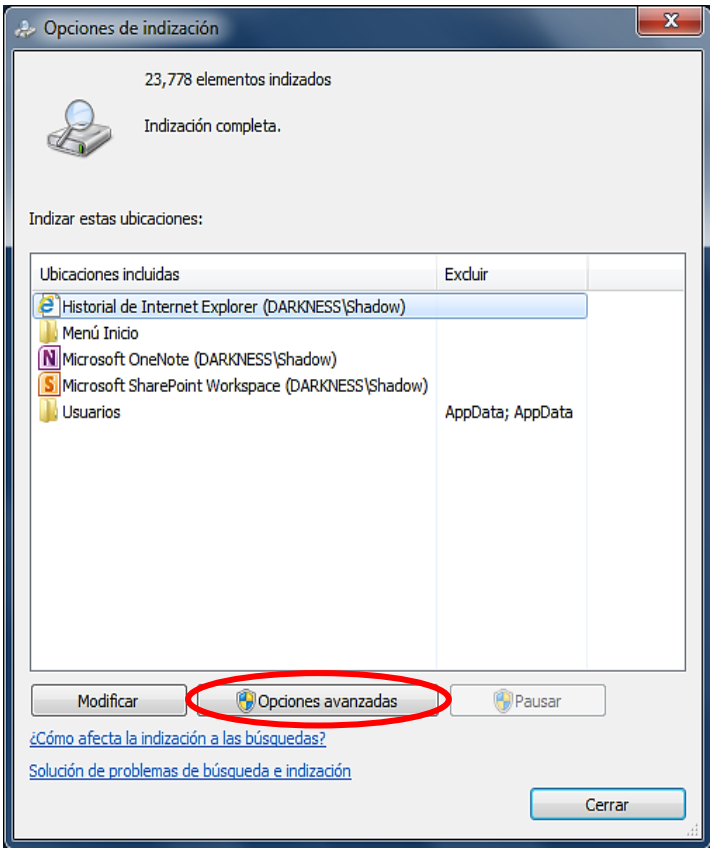
-Ahh bueno es que yo no sabía eso; y tampoco sé que significa el atributo indizado (I) y el de sólo lectura (R) :(

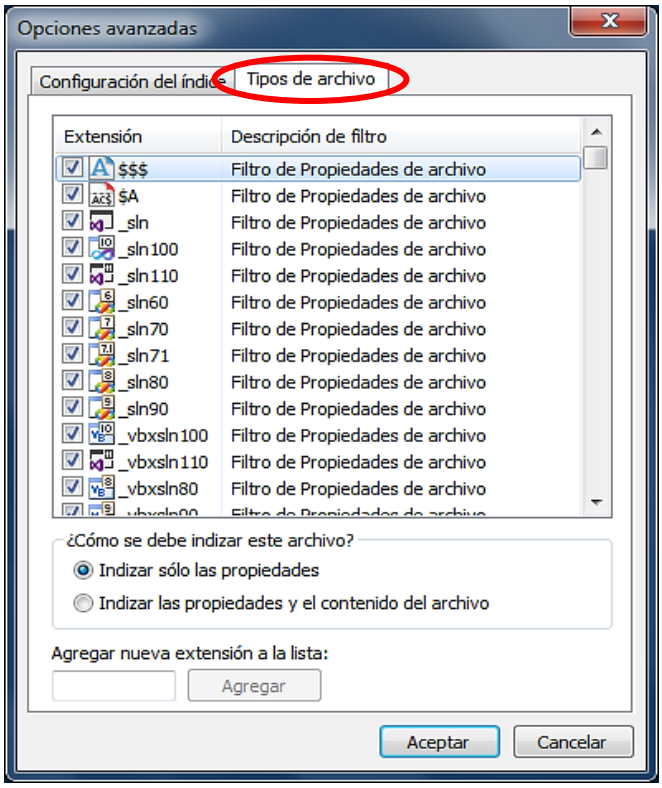
Para empezar, si abrimos un archivo en modo de lectura nunca podremos escribir dentro de él (No puede ser editado, solo leído)

Por otra parte Windows usa *el índice* para realizar búsquedas muy rápidas de los ficheros más comunes, utilizando el servicio *WSearch (Windows Search)* con el proceso *SearchIndexer.exe*. Si intentas buscar un tipo de archivo "inusual" nunca lo encontrarás.

Entra en panel de control y busca "Opciones de indización".

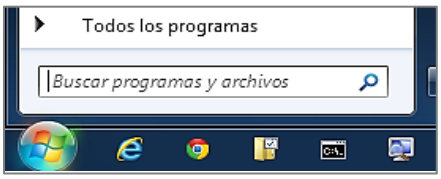
Comentario: En *"Opciones de Carpeta"* abre la pestaña *"Buscar"* allí podrás acceder a más configuración para las búsquedas. (Presionando la tecla **F3** obtendrás la carpeta especial para realizar búsquedas)





Las *ubicaciones* indizadas son las que muestra la imagen 1. Los *archivos* indizados son los que muestra la imagen 2; para ambos casos puedes poner y quitar :) (Entre más agregues más tardarán las búsquedas)

De esta manera cuando escribas en el cuadro de búsqueda del menú inicio; los resultados solo mostrarán aquello que esté indizado.



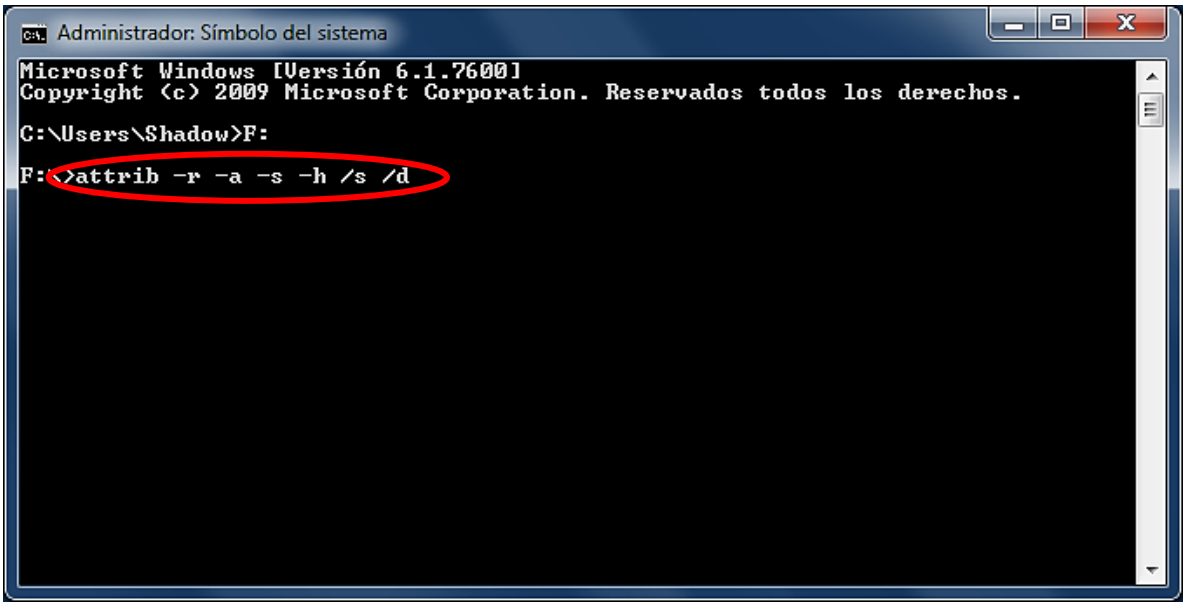
No se incluyen archivos de programa y de sistema. Además al incluir una carpeta en la biblioteca, se agrega automáticamente al índice.

Para terminar con esto solo nos falta conocer que tan útil es el comando attrib, por ejemplo todos nos hemos infectado más de una vez por el virus RECYCLER; al que no le haya pasado eso es porque no tiene ni una memoria USB, de echo yo ya no gasto energías en borrarlo porque al rato allí está nuevamente :(

En fin, este virus oculta las carpetas que tenemos en nuestra memoria y solo las muestra como acceso directo (.lnk), además actúa como un fastidioso *gusano* (copea cientos de veces archivos repetidos hasta llenar la memoria)

La información no se ha borrado, solo que no la podemos ver. Para comprobarlo podemos entrar en las propiedades de la USB y veremos que si tenemos espacio ocupado, o bien, abrimos la memoria con el **WinRAR** y de nuevo allí estarán las carpetas originales :)

Para eliminarlo, abrimos el cmd y nos desplazamos a la memoria; suponiendo que la memoria sea la unidad "F", (El sistema le asigna una letra al azar) tipeamos **F:** (o bien, cd /d F:\) y después de un enter dejamos lo que falta en manos de attrib y sus múltiples parámetros :)



Apunte: Claro que puedes usar más de un parámetro a la vez. El modificador /d es para cambiar la *unidad* actual; tipea cd/?

Con esa línea quitamos todos los atributos que protegían al virus, ahora ya lo podemos ver y borrar. Los cambios se aplicarán a todas las carpetas y a todos los archivos que contengan gracias a los parámetros /s y /d. Quizá lo único que no será afectado es el famoso AUTORUN.INF

-Que eso?, y por qué me dice Acceso denegado?

Ya tienes tarea :)

Por último, si el RECYCLER no se rinde puedes *FORMATEAR* la USB, solo asegúrate de tener respaldados tus archivos. Sería conveniente que antes de todo terminaras su proceso, si no está escondido se llamará IEXPLORER.EXE

Terminaremos esta parte con el comando Mode (modo) Su descripción dice: *"Configura un dispositivo de sistema"*

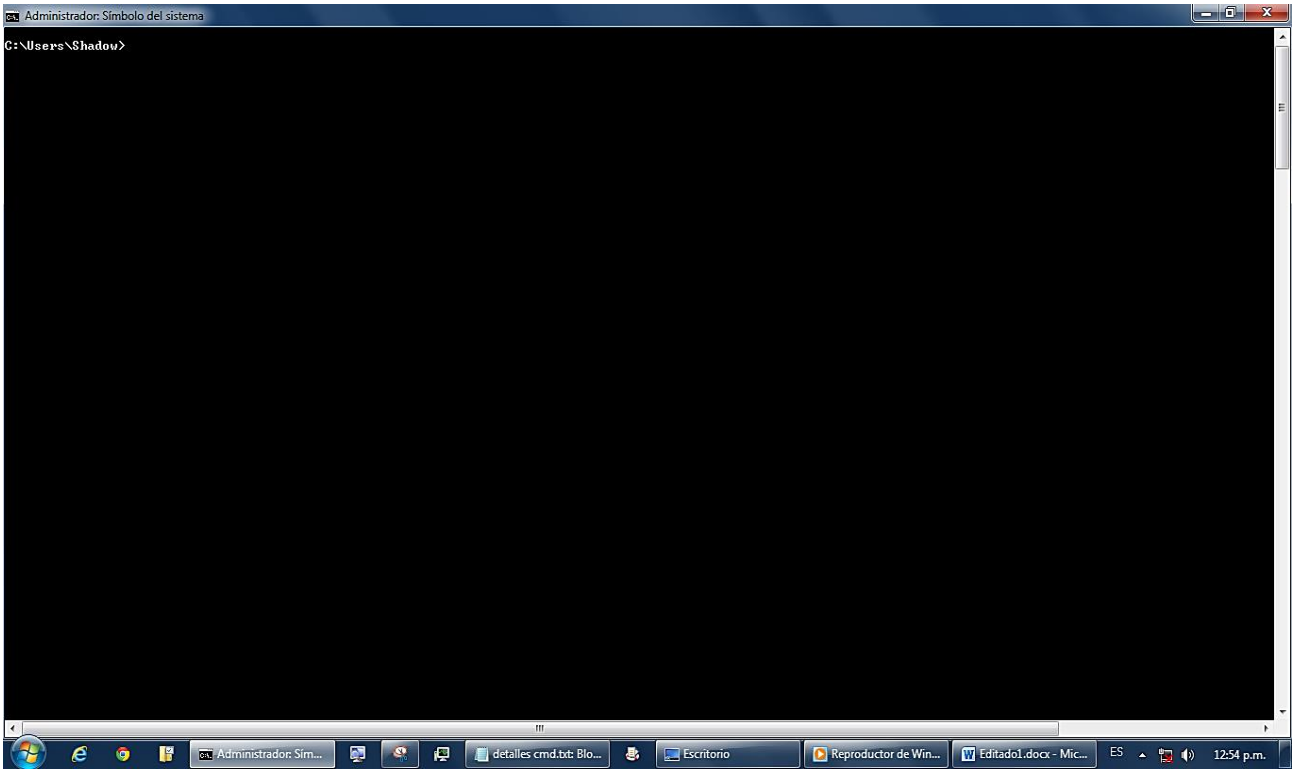
Nota: Un dispositivo puede ser el teclado, la impresora, el mouse, los auriculares, el celular, un CD-ROM, USB… (Lo que podamos conectar) Muchas veces necesitan software especial para que puedan instalarse, los llamados *controladores de dispositivos (drivers)*. Escribe *SystemPropertiesHardware* en **Ejecutar** y selecciona Administrador de Dispositivos, para ver los que tienes instalados (o simplemente escribe este último en la búsqueda del menú inicio) que a todo esto es más rápido poner *devmgmt.msc* en **Ejecutar** :)

Si gustas puedes escribir Help Mode o Mode /? Para que conozcas más de él, yo solo te voy enseñar un truco que no vas a encontrar en la ayuda ;)

Como habrás percibido el CMD tiene una pantalla muy chiquita y como a mí me gustan las cosas grandes que se vean bien, eso representa un gran problema, pero en este momento lo solucionamos ;)

Escribe Mode y el tamaño que quieras darle a la Shell, a mi me gusta el tamaño 200, así que debo escribir Mode 200 y dar enter :)

Con esto lo maximizamos a tamaño completo y tendremos mucho espacio para leer bien a gusto :)

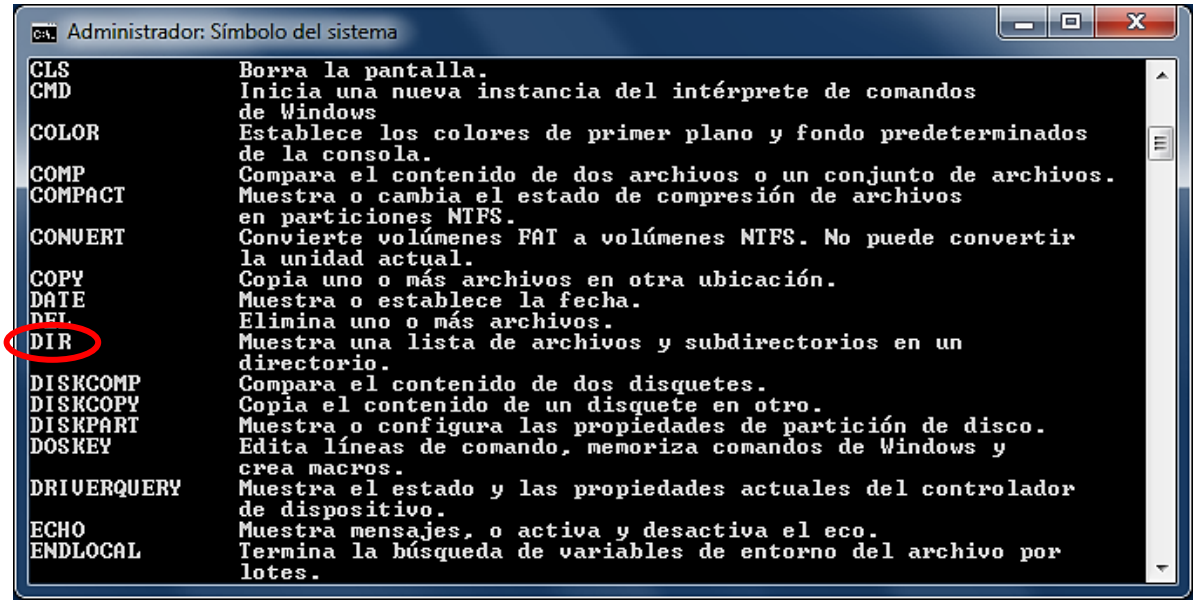


Curiosidad: Sobre el cmd aplasta las teclas Alt+Enter haber si te funciona :)

Espero que tengas la iniciativa para escribir cada uno de los comandos acompañado del parámetro **/?** y te vuelvas más experto ;)

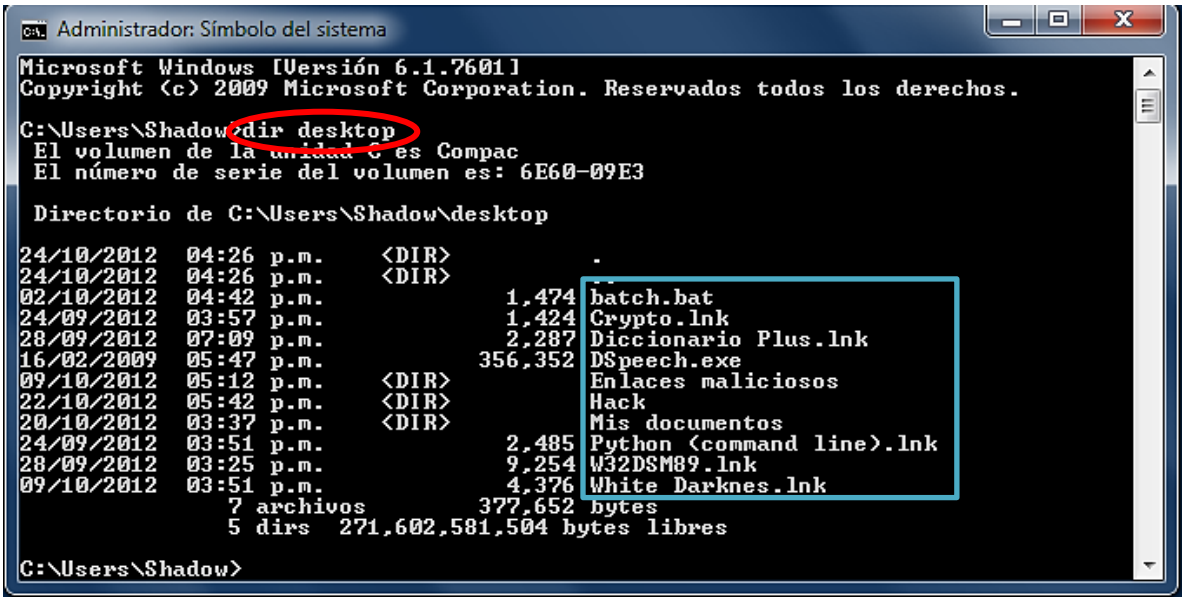
Apunte: Un directorio también puede considerarse una **Ruta** o una **Ubicación**

Sigamos aprendiendo, como siempre comencemos escribiendo help



Como estarás imaginando hablaremos del comando Dir (**Dir**ectory) Este también es uno de los grandes clásicos de siempre :) Lo que hace es mostrar una lista con todos los archivos que estén en un directorio.

Por ejemplo si escribimos **dir desktop** vamos a ver todo lo que tenemos en el escritorio, aquí está lo que obtuve yo:



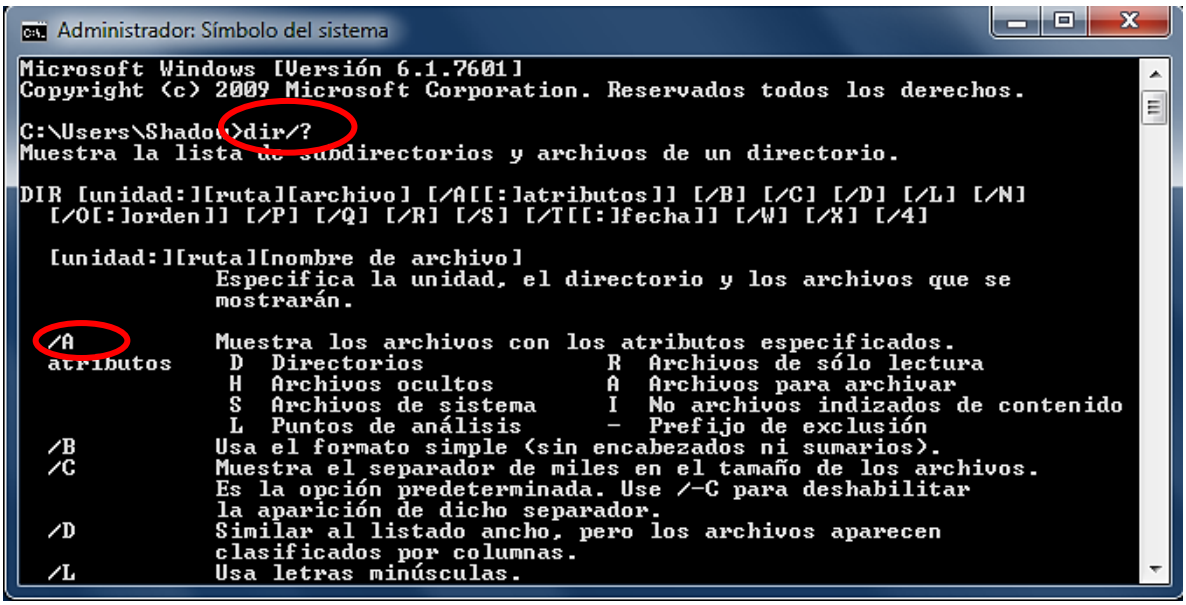
Te diste cuenta?? En el cuadro azul que puse está nuestra querida carpeta Hack (El sexto de arriba hacia abajo) Así es, con solo hacer un dir podemos darnos una idea de lo que nos rodea :) También tengo que mencionarte que obtienes el mismo resultado si escribes cd desktop das enter y luego escribes dir y das enter ;)

Pero pareciera que este comando funciona muy bien sin usar parámetros. Pero hagamos una prueba.

Oculta la carpeta Hack y después haz un dir al escritorio.

Qué ha pasado?? Pues que la carpeta ya no aparece en la lista :(

Para poder verla necesitamos acompañar el comando dir de un parámetro que nos deje ver archivos ocultos. Anda que esperas para escribir **dir/?**



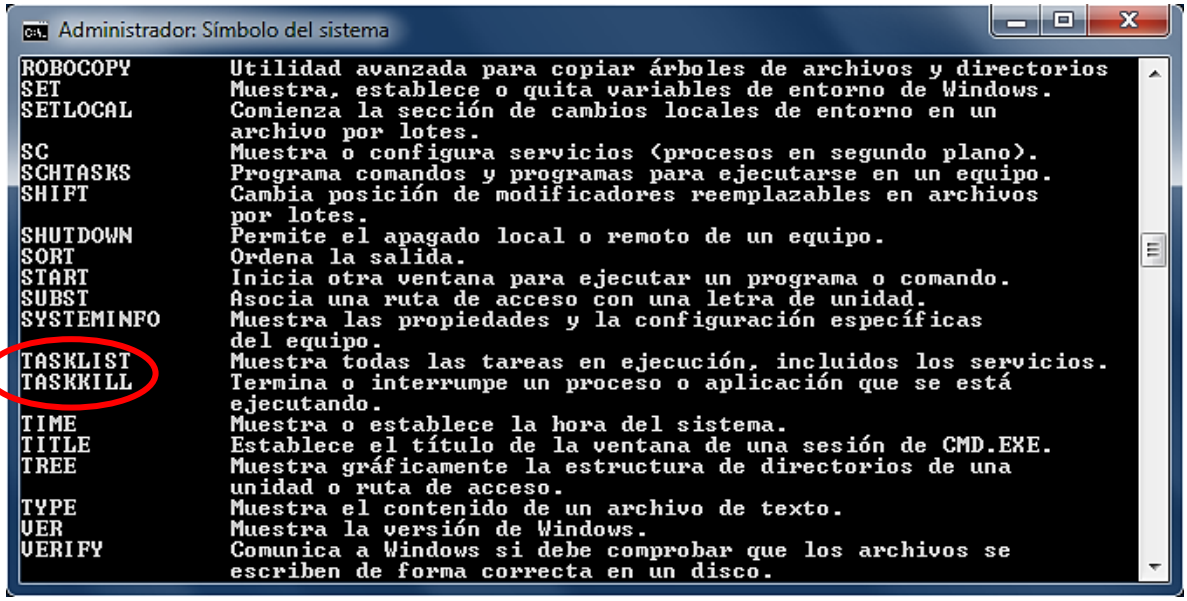
-Haaa!!! Gracias por encontrarlo por mí ;) debo usar ***dir /a*** *para poder ver la carpeta porque la descripción del parámetro dice que muestra archivos con atributos H, S, R… y el atributo H viene de la palabra* Hidden *que significa oculto.*

Vaya, sin comentarios ;)

Como te diste cuenta el comando dir tiene bastantes parámetros que no los explicaré porque te me vas a dormir :) mejor juega tu solito con cada uno.

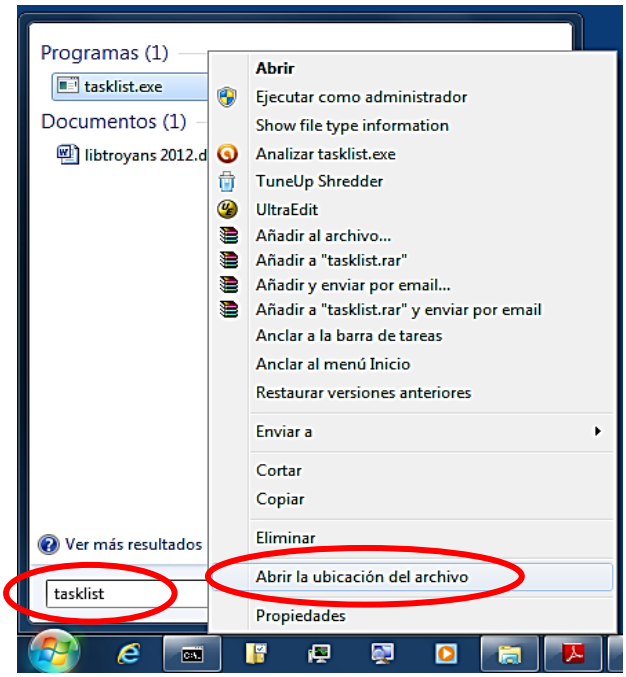
Comandos internos y externos

Este es un tema muy pero muy importantísimo, así que pon atención :)



Los comandos Tasklist y Taskkill son comandos **externos**. Pero ¿Cómo es que puedo saberlo? Muy fácil, si tienes Windows 7 puedes hacer esto:

En inicio hay un espacio para buscar programas y archivos allí escribe Tasklist (Lista de Tareas) te va a quedar un archivo con ese nombre; posiciónate sobre él, dale clic derecho y selecciona la opción "Abrir la Ubicación del Archivo".

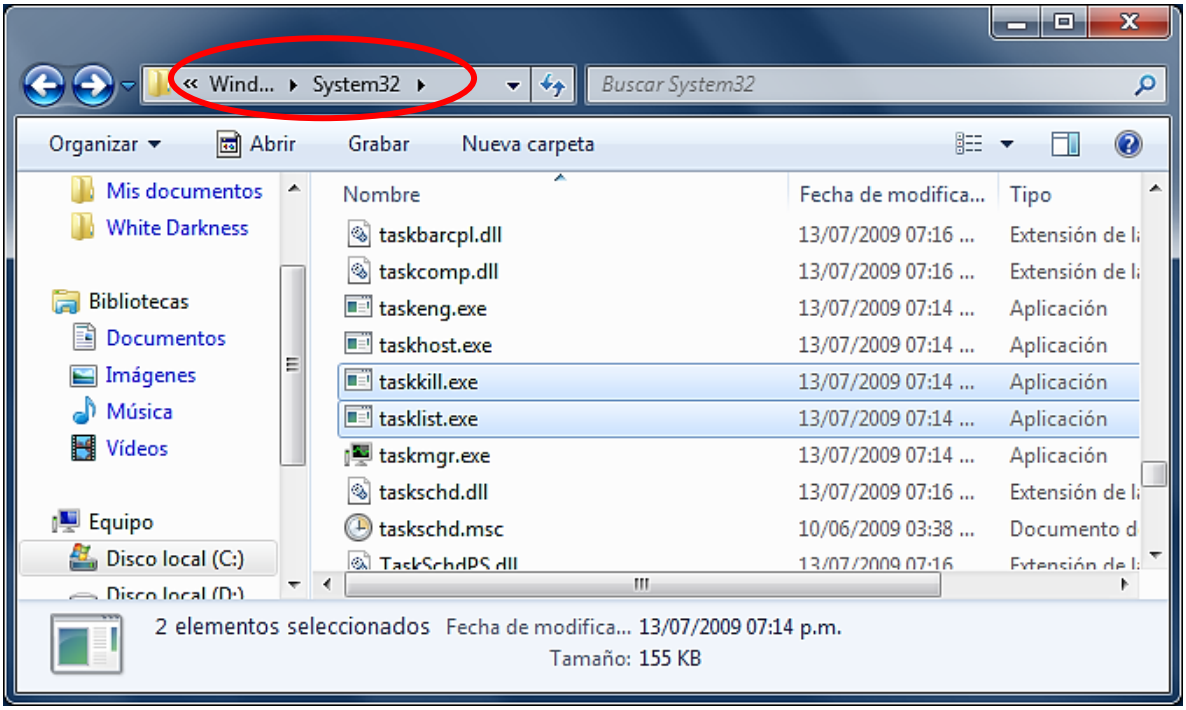


Te va a aparecer la carpeta que está en la siguiente página y Oh!! surprise allí están los dos comandos que estábamos buscando. Ahora comprendes?¿? Se llaman externos porque están fuera del CMD son programas muy aparte que están ubicados en los directorios:

C:\Windows

ó

C:\Windows\System32



-Si es cierto yo también los encontré; eso quiere decir que Tasklist y Taskkill son archivos indizados, ¿verdad?

Exacto!!! En un momento veremos lo importantes que son ambos comandos. Por lo pronto aquí tienes estas tablas donde ya vienen separados unos de otros. Que coincidencia hay 43 comandos internos y 43 externos :)

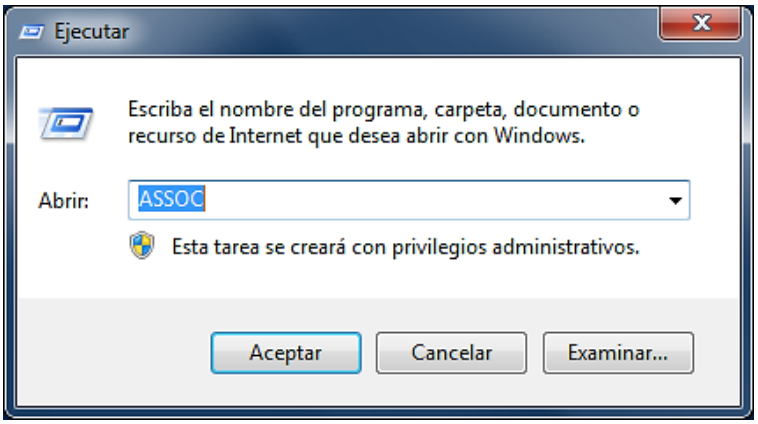
COMANDOS EXTERNOS			
ATTRIB	DISKCOPY	HELP	SCHTASKS
BCDEDIT	DISKPART	ICACLS	SHUTDOWN
CACLS	DOSKEY	LABEL	SORT
CHCP	DRIVERQUERY	MODE	SUBST
CHKDSK	FC	MORE	SYSTEMINFO
CHKNTFS	FIND	OPENFILES	TASKLIST
CMD	FINDSTR	PRINT	TASKKILL
COMP	FORMAT	RECOVER	TREE
COMPACT	FSUTIL	REPLACE	XCOPY
CONVERT	GPRESULT	ROBOCOPY	WMIC
DISKCOMP	GRAFTABL	SC	

COMANDOS INTERNOS			
ASSOC	ECHO	MOVE	SET
BREAK	ENDLOCAL	PATH	SETLOCAL
CALL	ERASE	PAUSE	SHIFT
CD	EXIT	POPD	START
CHDIR	FOR	PROMPT	TIME
CLS	FTYPE	PUSHD	TITLE
COLOR	GOTO	RD	TYPE
COPY	IF	REM	VER
DATE	MD	REN	VERIFY
DEL	MKDIR	RENAME	VOL
DIR	MKLINK	RMDIR	

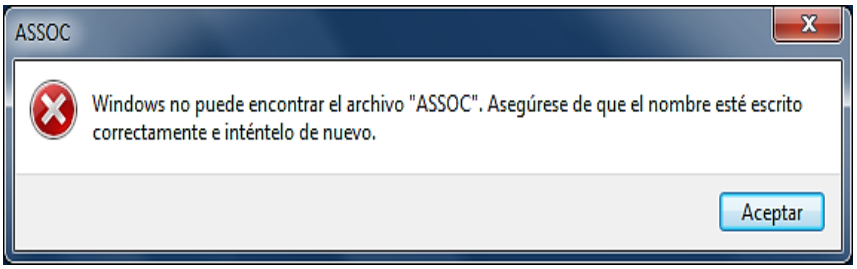
-Oye y si tuviera Windows xp ¿cómo podría comprobar cuando un comando es externo o interno?

Usando nuestra querida ventanita Ejecutar :)

Presiona al mismo tiempo las teclas  y como ya sabes perfectamente nos aparece esto:



Lo único que hay que hacer es ir escribiendo el comando que deseemos y dar enter; si es **interno** nos aparecerá una ventana de error como la de abajo



Pero si es externo nos saldrá una ventana como la del CMD que desaparece en menos de 2 segundos -aunque a veces puede durar un poco más- esto se debe a que esos comandos son programas (Herramientas) que ***"corren sobre la shell"*** es decir, necesitan del CMD para poder funcionar.

A diferencia de los comandos internos que ya están incorporados en la consola.

Muchos buenos programas solo funcionan con la terminal (ese término se usa para la Shell de Linux) como el popular SpeedTouch que sirve para hackear las contraseñas wi-fi y tantísimos interpretes de lenguajes.

Otro detalle interesante de los comandos externos es que podemos ejecutarlos mediante un acceso directo. El caso más conocido es el de Shutdown. Si lo acompañamos de un **/?** Veremos que puede apagar o reiniciar el equipo.
En tú escritorio da clic derecho sobre una zona libre. Selecciona **Nuevo, Acceso Directo**. Después te preguntan *¿A que elemento le desea crear un acceso directo?* Allí ponemos Shutdown /s /t 15 /c "En 15 segundos se apaga la máquina". Damos clic a siguiente y por último escribimos el nombre que le deseamos dar.
Nosotros ya sabemos que el archivo que acabamos de crear **NO** es un troyano –no le creas tanto a YouTube- tan solo es un comando acompañado de los parámetros que nos permiten apagar el equipo (**/s**), establecer cuantos segundos pasarán antes de apagarse (**/t**) y mostrar un mensaje (**/c**)
-Jeje y yo que me dejé engañar por uno de esos videos, es que parecía muy convincente hasta se podía enviar por correo :)

Recuerda el lema de HacxCrack "Solo el conocimiento te hará libre"

Nota: Para cancelar el apagado abrimos el cmd y tipeamos Shutdown /a pero si pusiste muy pocos segundos sería mejor que lo hagas en ***Ejecutar***. Esta técnica puede ser utilizada con todos los comandos externos.

Ahhhh!!! Y recuerdas que hace unas cuántas páginas arriba te mencioné que la *orden* Help solo nos mostraba algunos de los comandos que podíamos usar?¿?

-Si!!!! Entonces los que faltan deben ser más comandos externos, no es así?¿?

Así es, son herramientas que están "escondidas" en los directorios que ya anteriormente te adelantaba: **C:\Windows** y **C:\Windows\System32**

Que te parece si los buscamos!!! Como la mayoría de ellos y también los más importantes se concentran en **C:\Windows\System32** he decido mostrarte los resultados solo de ese directorio, pero no estaría mal que revisaras a **C:\Windows** quizá encuentres algunas cosas interesantes ;)

Aquí tienes esta tabla con mis resultados :)

append	forfiles	nlsfunc	setver
ARP	ftp	nltest	setx
at	getmac	nslookup	sfc
auditpol	gpupdate	ocsetup	spinstall
bcdboot	GRAPHICS	odbcconf	sxstrace
bitsadmin	HOSTNAME	PATHPING	takeown
bootcfg	**hwrcomp**	pcwrun	tcmsetup
choice	**hwrreg**	PING	telnet
cipher	ipconfig	PkgMgr	TFTP
clip	iscsicli	PnPUnattend	timeout
cmdkey	KB16	PnPutil	tracerpt
COMMAND	klist	powercfg	TRACERT
cscript	ksetup	printui	TsWpfWrp
debug	ktmutil	rasautou	typeperf
diantz	LOADFIX	rasdial	tzutil
diskperf	lodctr	rasphone	unlodctr
diskraid	logman	ReAgentc	VaultCmd
Dism	makecab	redir	vssadmin
dispdiag	manage-bde	reg	w32tm
djoin	mctadmin	regini	waitfor
Dosx	mem	regsvr32	wbadmin
Edit	mountvol	**relog**	wecutil
edlin	MRINFO	repair-bde	wevtutil
esentutl	MuiUnattend	ROUTE	where
eventcreate	nbtstat	RpcPing	whoami
exe2bin	net (net1)	runas	winrs
expand	netcfg	sdbinst	WinSAT
finger	netsh	SecEdit	WSManHTTPConfig
fltMC	NETSTAT	setspn	xwizard

Pues allí tienes **116** comandos extra-externos más para estudiar ;). Además aquí abajo están otros 4 que estaban en un directorio distinto:

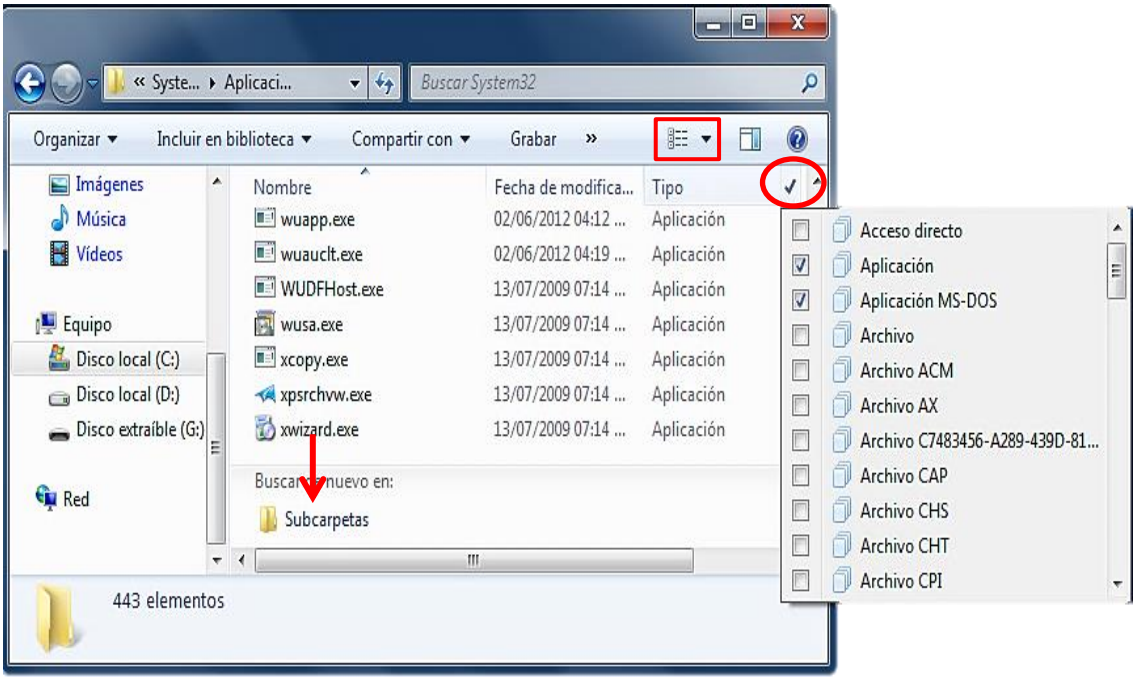
Directorio	Comando Externo
C:\Windows\System32\com	Comrepl
C:\Windows\System32\IME\IMEJP10	Imjpuexc
C:\Windows\System32\wbem	WinMgmt
C:\Windows\System32\wbem	mofcomp

Nota: Para poder usar esos 4 comandos necesitaremos entrar en sus respectivos directorios y después invocarlos (ejecutarlos), más abajo se explica por qué.

Quizá se me pudieron haber pasado algunos, creo que a la segunda tablita le van a faltar, pero hace poco se me ocurrió una manera más fácil para encontrarlos :)

Te la voy a decir por si quieras revisar si están completos (si hallas uno que no apunté me dices luego)

Primero entramos en C:\Windows\System32, después de asegurarnos de estar usando la vista detalles (está en el rectangulito rojo) vamos a darle clic en la flechita que está en la columna “Tipo” (la del circulito rojo) y por último marcamos las dos opciones que muestra la imagen, con eso tendremos una *lista continua* de todos los exe y com que están en System32 :)



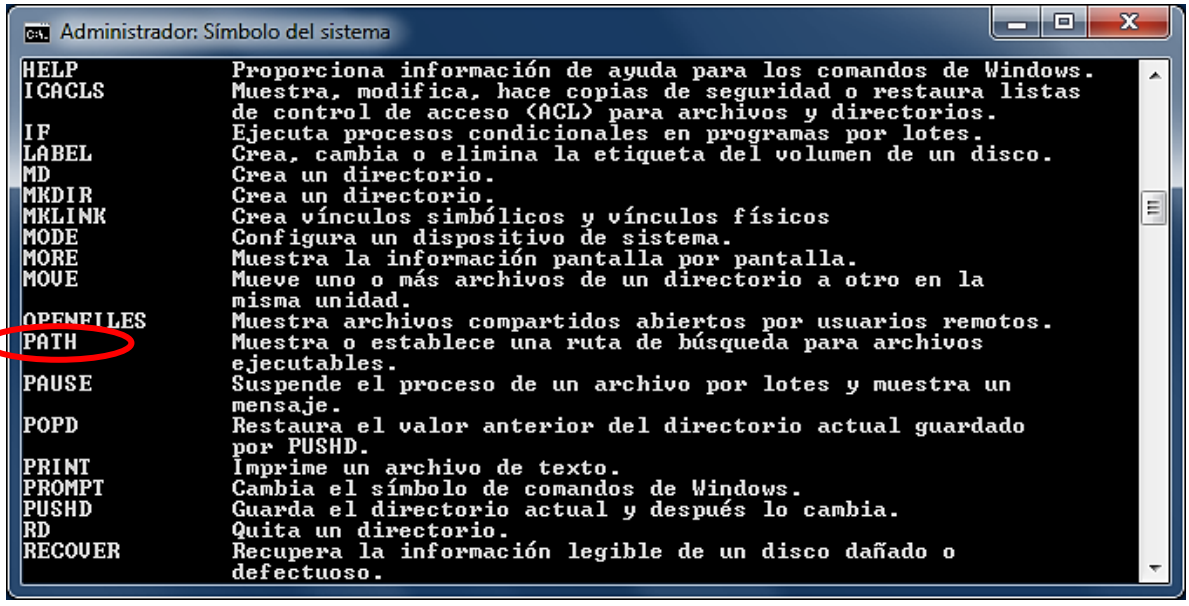
Si quieres puedes abrir la carpeta que señala la flechita roja para que la búsqueda también se haga en los demás directorios que tiene C:\Windows\System32 y presta atención al mensaje que aparece arriba, dice que va a tardar más porque no están indizados :)

Apunte: Hay muchas aplicaciones que no incluí porque solo son procesos o servicios, por allá mencionaba *SearchIndexer.exe* quizá luego veamos más :)

Te mentiría si te digo que se como usar cada uno de ellos; de echo yo sabía que había muchos comandos escondidos por ahí pero nunca pensé que fueran tantos; pero eso no es ningún problema porque nosotros ya sabemos que tenemos que ir al CMD y acompañar a cada comando con un **/?** y jugar con sus distintos parámetros, después de un buen y kilométrico rato ya los vamos a dominar ;)

En la tabla anterior hay comandos que nos permiten hacer varias cosas malévolas :) Pero eso es otro tema ya que para poder usarlos antes debemos conocer algo de TCP/IP.

PATH



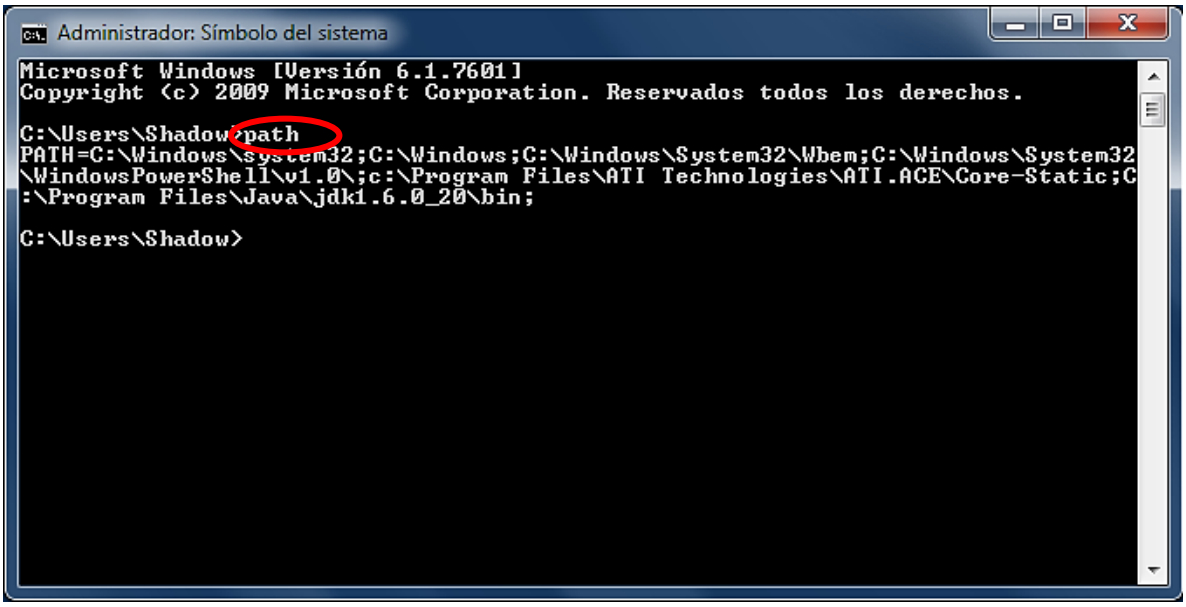
Es turno de hablar sobre el comando PATH (Ruta, Senda) A pesar de las explicaciones dadas hasta entonces, aún debes tener una muy buena pregunta que no ha sido contestada :)

Se supone que los comandos externos están en un directorio distinto a C:\Users\Shadow y si queremos usar uno de ellos en teoría tendríamos que escribir **cd C:\Widows\System32** dar enter y después teclear el comando.

¿Por qué no es necesario que hagamos eso?

-Justo eso me estaba cuestionando y también me cuestionaba cuando se te iba a ocurrir darme una respuesta, menos mal que ya me vas a decir, hombre anda que estoy impaciente :)

Escribe el comando Path en el CMD y da enter. Algo así debes tener:



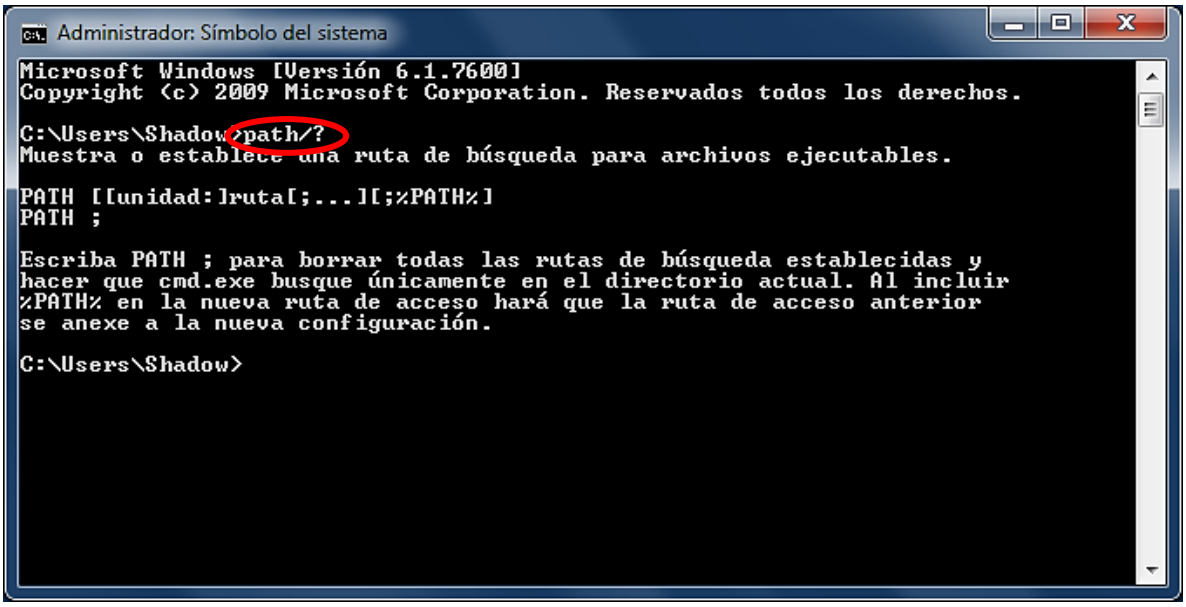
Obviamente lo que vemos son varios directorios, en concreto son los siguientes:

- C:\Windows\system32
- C:\Windows
- C:\Windows\System32\Wbem
- C:\Windows\System32\WindowsPowerShell\v1.0
- C:\Program Files\ATI Technologies\ATI.ACE\Core-Static
- C:\Program Files\Java\jdk1.6.0_20\bin

Path nos dice que aparte de buscar archivos en el directorio en que estemos, también los va a buscar en los 5 anteriores y en su lista incluye a

C:\Windows\system32. Cualquier programa que esté en ellos podrá ser ejecutado directamente.

Veamos que más podemos hacer con él:



Si escribimos **Path;** y damos enter, según la información, vamos a borrar todas las rutas anteriores y solo va a quedar el directorio en el que estemos, lo cual significa que no vamos a poder usar ningún comando **externo.**

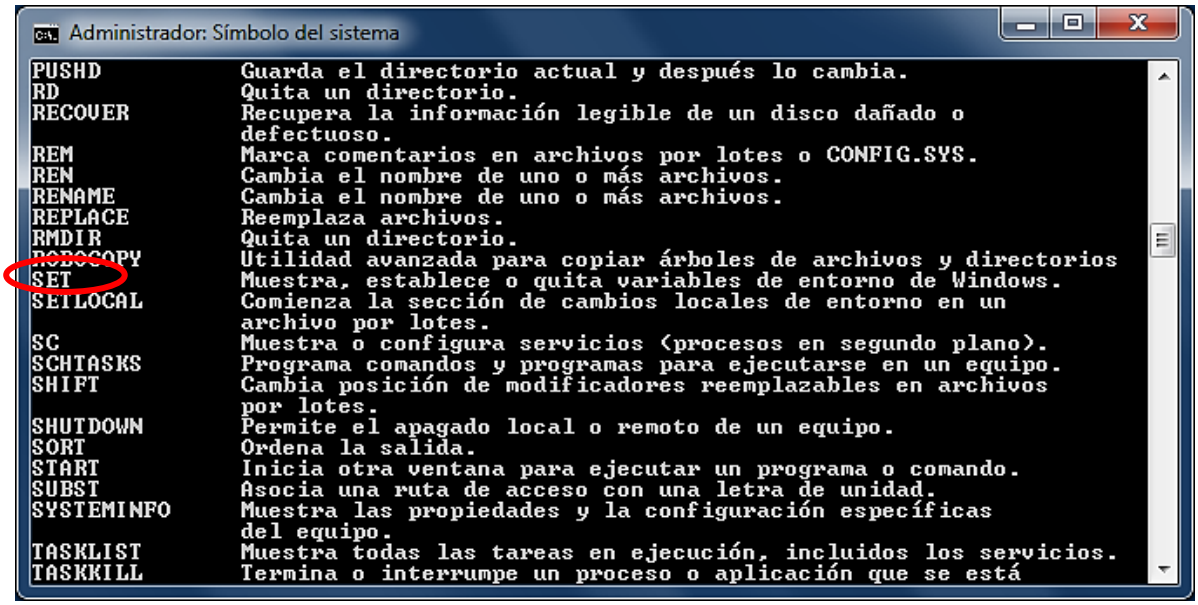
Si ya lo hiciste no te preocupes basta con cerrar y abrir de nuevo el CMD para dejar todo como estaba. Si en cambio queremos agregar un nuevo directorio para que el CMD también busque archivos allí sin tener que estar dentro de él, se debe escribir esto: **Path C:\Users\shadow\desktop;%path%** con esta instrucción estoy añadiendo mi escritorio a la lista de Path.

Fíjate que justo después de escribir el directorio que quiero anexar puse un punto y coma (Remarcado en negritas) seguido del comando Path pero encerrado entre signos de porcentaje, si no lo escribes así también vas a borrar todo. De cualquier modo lo que modifiques es temporal.

Si deseas causar cambios perdurables en la configuración de Path deberás hacerlo desde *Variables de Entorno* en Panel de Control; aunque eso es terreno del siguiente comando :)

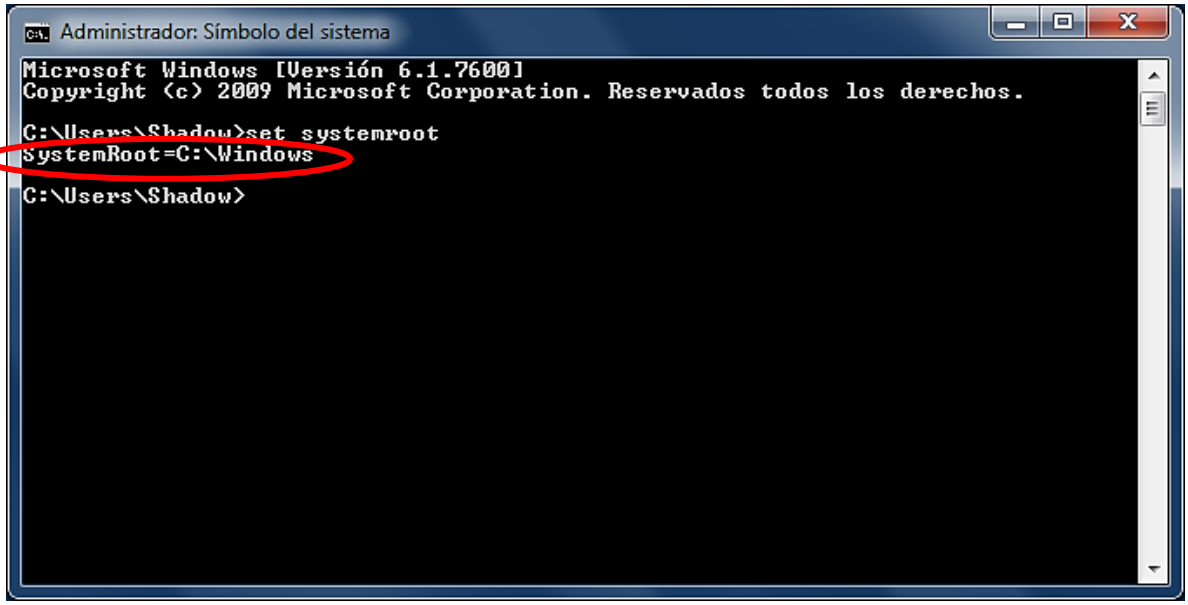
NO ES BUENO JUGAR CON LA CONFIGURACIÓN DE PATH.
Quedaste advertido!

Set



Este comando es indispensable y muy práctico. La mayoría de nosotros ha visto alguna vez algo como esto **%SystemRoot%** y nos quedamos con cara de what?¿? Bueno la respuesta nos la da el comando Set (Colocar, Fijar) :)

La anterior es una de las muchas *Variables de Entorno* que encontraremos en Windows. Para una solución rápida escribe en el cmd Set SystemRoot o bien; Echo %SystemRoot%



-Ahh!! El cmd dice que %systemroot% es el directorio C:\Windows

Muy bien!! Y para comprobarlo tenemos 3 maneras de hacerlo :)

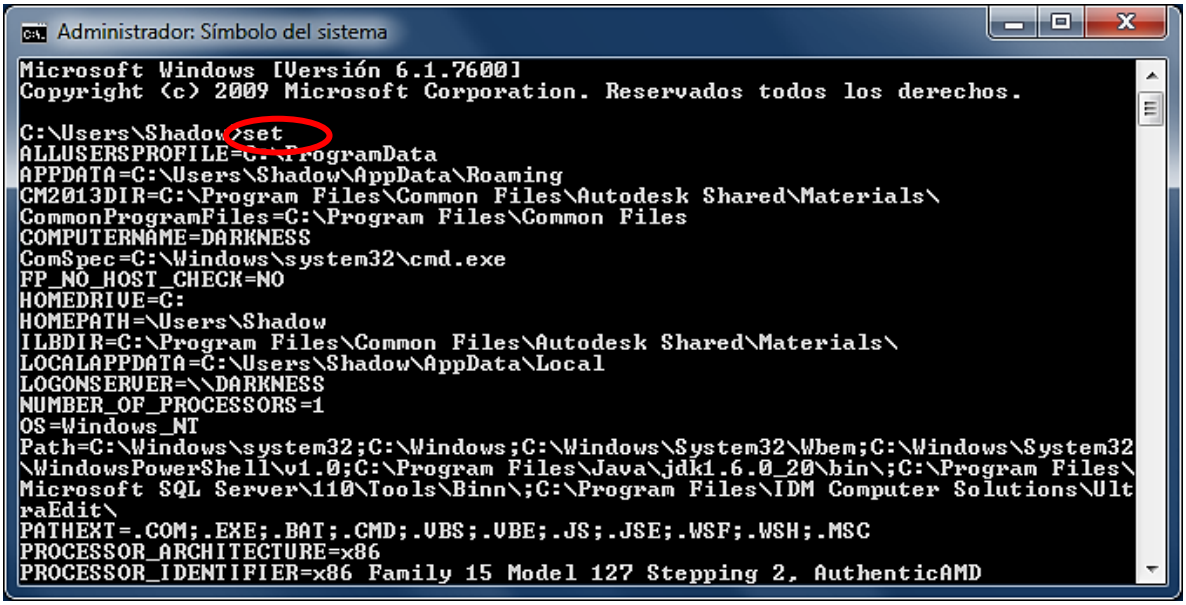
- En *Ejecutar* escribe **%SystemRoot%**
- En el cmd escribe **cd %SystemRoot%**
- En una barra de direcciones ingresa **%SystemRoot%**

-Todas me llevaron al directorio C:\windows!!!

Exacto; conseguimos entrar **al directorio** raíz del sistema sin escribir tanto :)

-Oye!!! Se me acaba de ocurrir que en ves de escribir cd C:\windows\System32 *mejor ponga cd %SystemRoot%*\System32

Esa es la idea de haber inventado las variables de Entorno :)
Para que veas las demás y sus valores tipea Set en el cmd



-Son un montón!

Pues yo diría que hasta otro poquito más :) así que solo mencionaremos las más destacadas:

Observación: Fíjate que Path es una variable de entorno. Además **userinit** no aparece (la encontré sin querer por ahí) pero nos abre la biblioteca y con **system** accedemos a C:\Windows\System :)

Dato: La ventana ***Ejecutar*** funciona con los directorios de path.

Variable	Propósito
%APPDATA%	Es una carpeta oculta donde las aplicaciones guardan sus datos.
%COMPUTERNAME% %LOGONSERVER% %USERDOMAIN%	Devuelven el nombre del equipo.
%COMSPEC%	Es la ruta de la Shell. Si la ponemos en *Ejecutar* tendremos al CMD con directorio C:\windows\System32
%DATE%	Devuelve la fecha actual.
%TIME%	Devuelve la hora actual.
%PATHEXT%	Esta variable contiene una lista de varias extensiones. Si el nombre de un archivo termina con una extensión incluida en esa lista, se puede omitir al invocarlo.
%PROGRAMDATA% %PROGRAMFILES%	Carpetas donde se instalan los programas.
%SYSTEMDRIVE%	Devuelve **la unidad** del sistema.
%TEMP% %TMP% %LOCALAPPDATA%	Son las carpetas donde los programas guardan sus archivos temporales.
%USERNAME%	Es el nombre del usuario. Estando en C:\Users, teclea cd %username%
%USERPROFILE%	Es el directorio de la carpeta personal.

Nota: %WINDIR% equivale a %Systemroot%

Si un programa necesita escribir valores en tu carpeta personal; solo podrá hacerlo con la variable %USERNAME%. Porque la ruta y el nombre de usuario son diferentes en cada equipo; los programas muchas veces agregan sus propias variables.

Un archivo **.bat** o **.cmd** deberá usar la variable %USERPROFILE% si desea funcionar en cualquier computadora. Por ejemplo, si va a ingresar al escritorio, su código debe contener %USERPROFILE%\Desktop ya que la carpeta Escritorio se encuentra dentro de la carpeta del usuario.

También hay algunas variables que dan información del procesador, la mayoría también funciona para XP.

-Y que son los archivos temporales que decía la tabla?

Son los culpables del mal rendimiento de tú computadora; tienen la extensión **.tmp**, no sirven de nada y están por todos lados!
Si quieres aprender algo muy interesante navega por esta página:

http://www.configurarequipos.com/doc476.html

Es un gran tutorial de un gran autor, enserio que vale la pena leerlo. Para una sorpresa extra revisa los comentarios 26, 76, 80 y 89 :)

Si tu disco duro está lleno, ¿por qué no cambiar %temp% a una carpeta que esté en otra unidad? Así todos los archivos temporales y demás basura se acumularán en tú segundo disco duro :)

Nota: Hay varios programas para borrar de una sola pasada los archivos temporales, los más usados son el **Ccleaner** y el **TuneUp**.

-Que interesante, oye y puedo hacer mis propias variables de entorno?

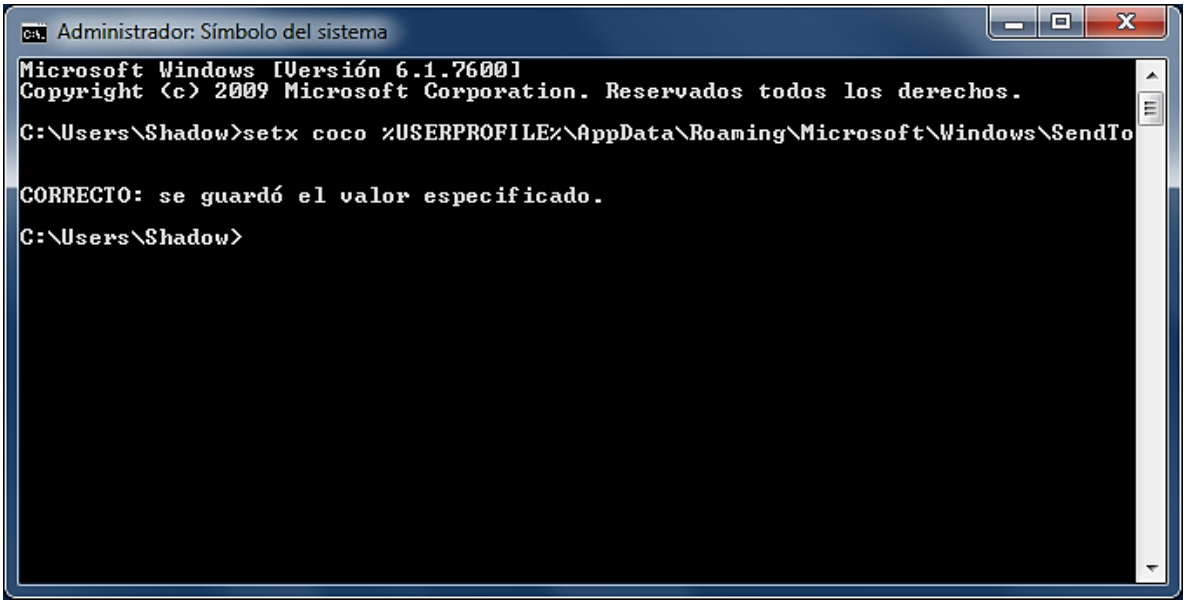
Claro, porque contamos con nuestro buen amigo SetX :) Por ejemplo, imaginemos que necesitamos una variable que contenga al directorio:
C:\Users\Shadow\AppData\Roaming\Microsoft\Windows\SendTo
obviamente en XP será diferente:
C:\Documents and Settings\Administrador\Sendto

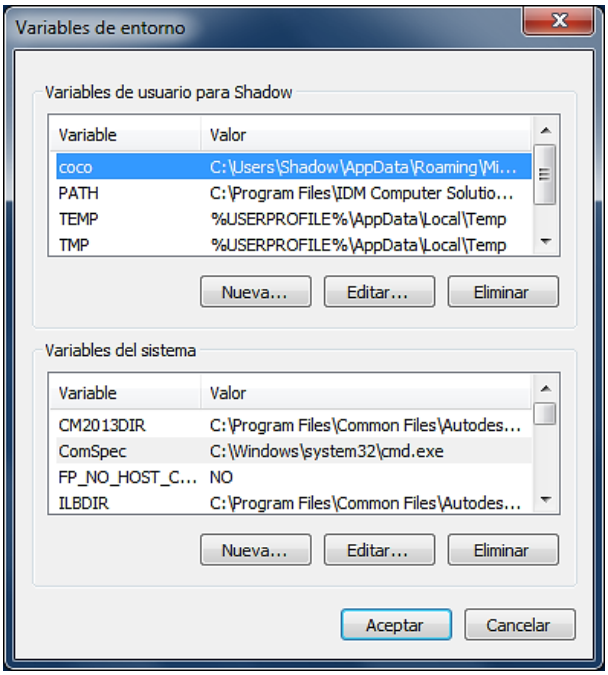
Por cierto, cuando damos clic derecho sobre un archivo tenemos la opción *"Enviar a"* y hay varios lugares a donde mandarlo (Escritorio, Disco Extraíble, Documentos…) pues bien; lo que esté en la ruta Sendto aparecerá como una de esas opciones, por eso podría ser útil una variable de entorno para él.

Como ese directorio está muy largo que te parece si lo resumimos así:
%USERPROFILE%\AppData\Roaming\Microsoft\Windows\SendTo

Quedó casi igual :) pero procedemos, tipea el comando Setx seguido del nombre que le quieres dar a tu variable, yo le voy a poner coco :) y por último escribe su valor, en este caso el directorio SendTo (No se te olvide dar intro)

Para comprobar que todo salió bien, escribe %coco% en **Ejecutar** y vas a entrar a esa carpeta :)





*Aplasta inicio y sobre Equipo (o mi PC) da clic derecho y selecciona propiedades. En la parte izquierda de la ventana que apareció está la opción "Configuración Avanzada del Sistema" ábrela y por último entra en "Variables de Entorno"

*Por si no se te ocurre también podemos crear una variable para ejecutar una aplicación, como lo hace %COMSPEC% que abre de manera rápida al cmd.

Avanzado: Con SetX también podemos crear variables para ramas del **registro**. Escribe SetX/? para que aprendas como hacerlo. No estaría mal que revisaras el contenido de las llaves:

- HKEY_CURRENT_USER\Environment
- HKEY_CURRENT_USER\Volatile Environment
- HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment

Nota: Como habrás notado desde hace rato en el CMD da igual si usas minúsculas, mayúsculas o las combinas, **lo que si reconoce son los acentos.** Ahora vamos a aprender como usar este recién descubierto directorio :)

Experimento I

Usando la variable %coco% entramos en SendTo, una vez dentro damos Clic derecho- Nuevo- Acceso directo (lo mismo que hicimos para Shutdown) y selecciona ***Examinar***, allí busca cualquier carpeta, de preferencia una que uses seguido, yo escogí una que está en mi escritorio que se llama XML :)

Le picas en ***Siguiente***, le pones un nombre, como *Copiar en XML* y finalizas. Ya solo nos queda verificar; sobre algún archivo que tengas, da Clic derecho- Enviar a...- Copiar en XML. Por último abre la carpeta que elegiste y allí tendrás el fichero que habías mandado :)

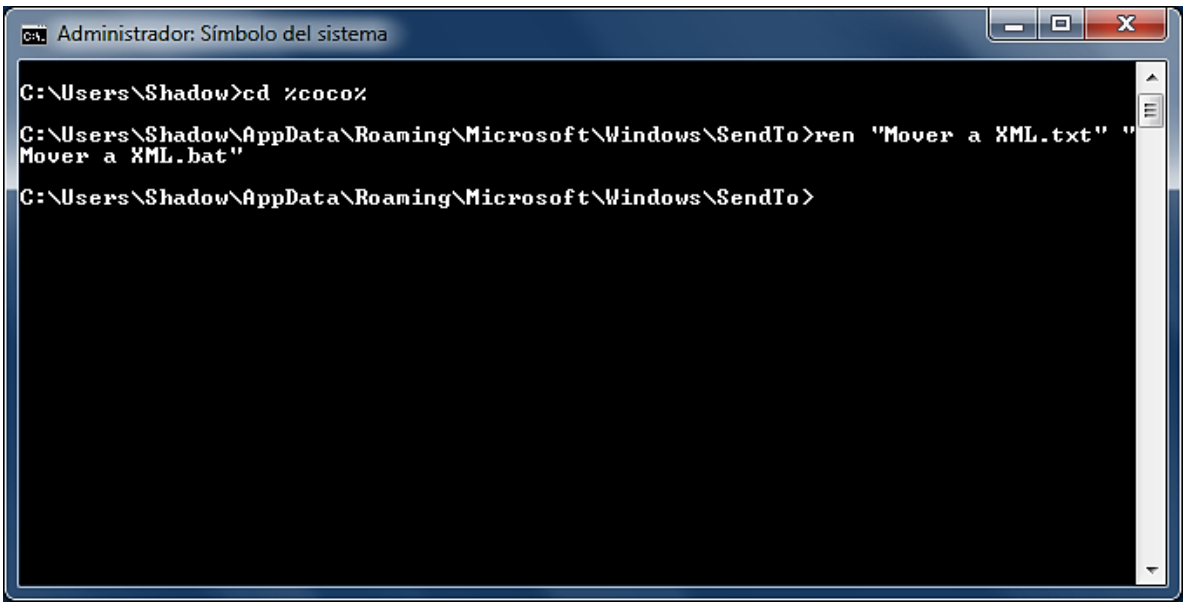
Experimento II

Haremos la misma cosa pero al estilo HackxCrack, es decir, **MÁS PRO :)**
En SendTo da Clic derecho-Nuevo-Documento de texto llámalo *Mover a XML*, luego cambiamos su extensión hay al menos 3 formas de hacerlo, nosotros usaremos la siguiente línea en el cmd:

ren "Mover a XML**.txt**" "Mover a XML**.bat**"

*Si no entendiste que es eso que sale del punto a la izquierda ve a la pág. 46

Aquí tienes la imagen :)



¿Te fijaste? Primero tienes que estar dentro del directorio donde está el archivo que quieres modificar, porque esa ruta no se encuentra dentro de path. ¿Qué tal? nuestro archivo tiene el mismo nombre pero un icono distinto. Ahora encima de él da clic derecho y escoge la opción ***Editar*** se abrirá el bloc de notas, allí pega esto y guárdalo aplastando **Ctrl+G**

```
@move %1 C:\Users\Shadow\Desktop\XML
```

Bueno solo espero que no me hagas tanto caso y pegues el mismo directorio que tengo yo :)

-Eso no importa yo puse el mío ;) pero ese porciento uno me tiene bastante preocupado, que percebes es!

Justo eso esperaba que preguntaras y tranquilo que pienso dejarte con la duda :p

Ese %1 lo vas a ver y necesitar en varias ocasiones (también cuando trabajemos en el registro) se llama parámetro posicional pero no puedo decirte más porque sería mucho meterse en batch y este es un manual de CMD solo era para que le dieras un vistazo y no te pareciera tan desconocido cuando te lo toparas de nuevo :)

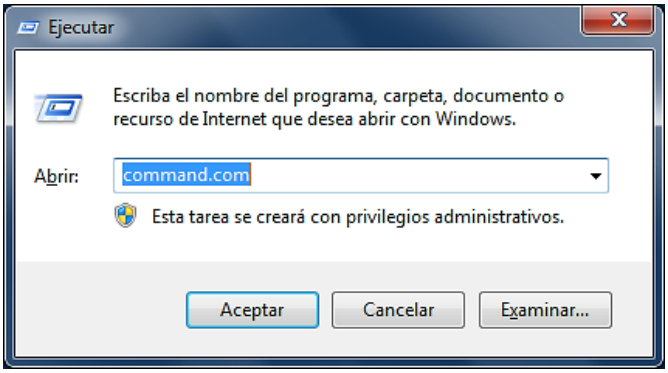
¿Y cuando tiene dos signos de porcentaje?, ¿qué sería esto %%1?

Observación: La extensión **.bat** puede ser cambiada por **.cmd** pues son equivalentes.

Ok, en la sección pasada te deje una tabla con 116 comandos adicionales si la analizaste habrás notado que algunos no necesitaban del CMD para funcionar; ellos ya tienen su propia interfaz, vaya su propia ventanita negra :)

Esto es de mucha ventaja porque si queremos también los podemos ejecutar desde el CMD.

Uno que vale la pena destacar es el famosísimo **COMMAND.COM** y como posee su propia interfaz que te parece si lo abrimos desde Ejecutar ;)

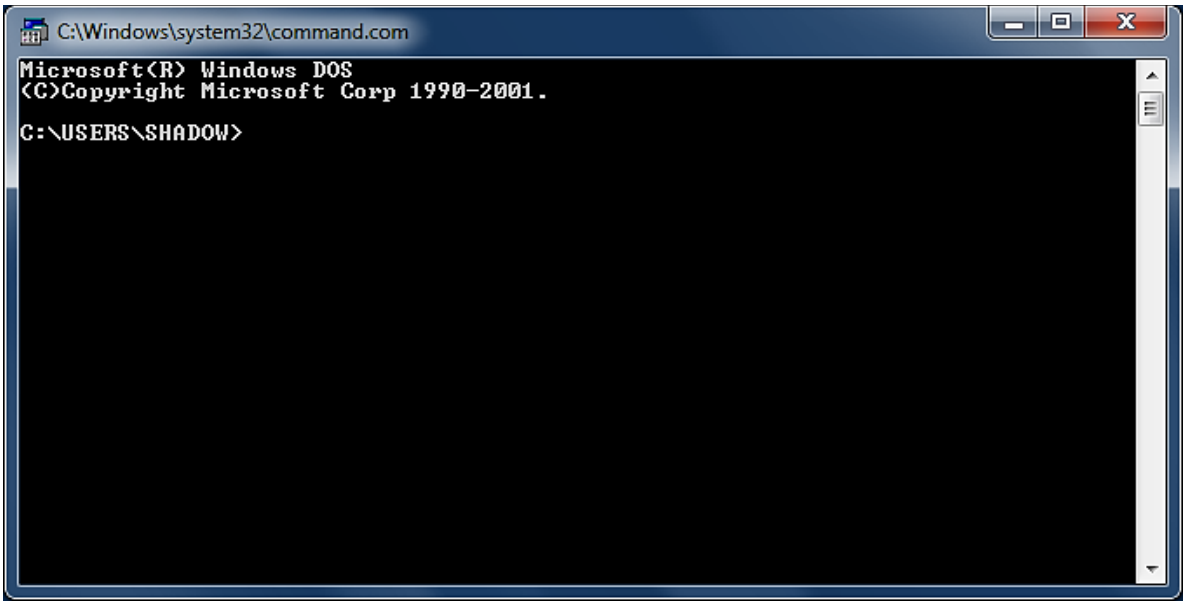


Al igual que el CMD el Command.com también se conoce con muchos nombres:

-MS-DOS

-El DOS

-Prompt del DOS



-Vaya!!! Enserio que se parece mucho al CMD!!!

No solo se parece sino que *funciona exactamente igual* que el CMD, de hecho este programa fue su antepasado. Para entender esto necesitamos retroceder hasta el comienzo de los tiempos :)

¿Recuerdas cuando escribimos Mode 200? El CMD abarco toda la pantalla; pues ahora imagina que enciendes tu computadora y lo único que ves es una enorme pantalla negra con un cursor parpadeando :(Justo eso es lo que tuvieron que padecer nuestros ancestros!!!

Así es, antes de que nuestro hermoso Windows existiera las computadoras funcionaban con el Sistema Operativo MS-DOS, o sea con el COMMAND maximizado ;) Por cierto MS-DOS significa **M**icrosoft **D**isk **O**perating **S**ystem.

Si tú hubieras estado en esa generación y en C:\Users\%username%\Desktop tuvieras una canción llamada Rola.mp3 y quisieras esconderla en **C:\Users\%username%\AppData\Local\Temp** tendrías que haber escrito todo esto: cd C:\Users\%username%\Desktop dar enter, en caso de que lo requieras hacer un dir, ubicar el archivo y después escribir
Move rola.mp3 C:\Users\%username%\AppData\Local\Temp y dar enter.
Esa es la razón por la cual nuestros padres nos dicen que nunca pudieron aprender a usar una computadora. En cambio nosotros tuvimos "más suerte" porque Windows tiene una **Interfaz Grafica** con bonitos iconos de muchos colores :)
Los programadores opinan que Windows convirtió a sus usuarios en ignorantes informáticos porque les priva de tener "contacto directo" con el sistema ya que les facilita mucho hacer cualquier tarea. Aunque en parte es verdad también es cierto que ayudó a las personas no especializadas a tener acceso a una computadora :)

Apunte: Si tenemos abierto el cmd con el comando dosx podemos pasar directamente al command. Ten en cuenta que se acostumbra usar MS-DOS para ambas líneas de comandos.

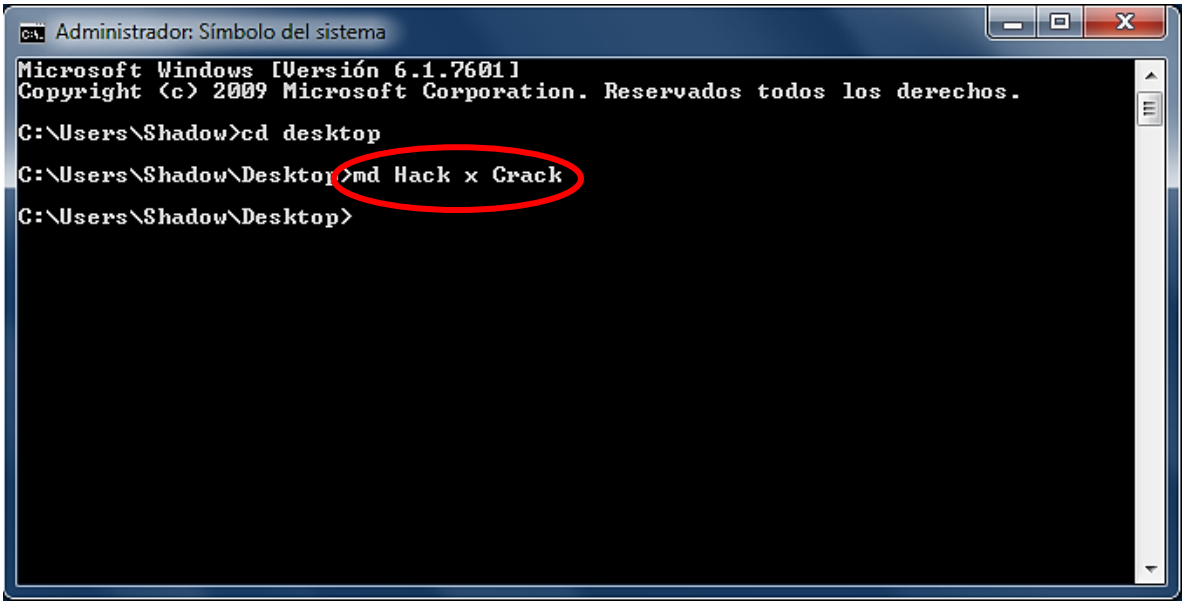
Nota: El directorio **C:\Users\Shadow\AppData\Local\Temp** tiene atributo oculto.

Después de esa nota cultural podemos continuar con nuestro curso :)

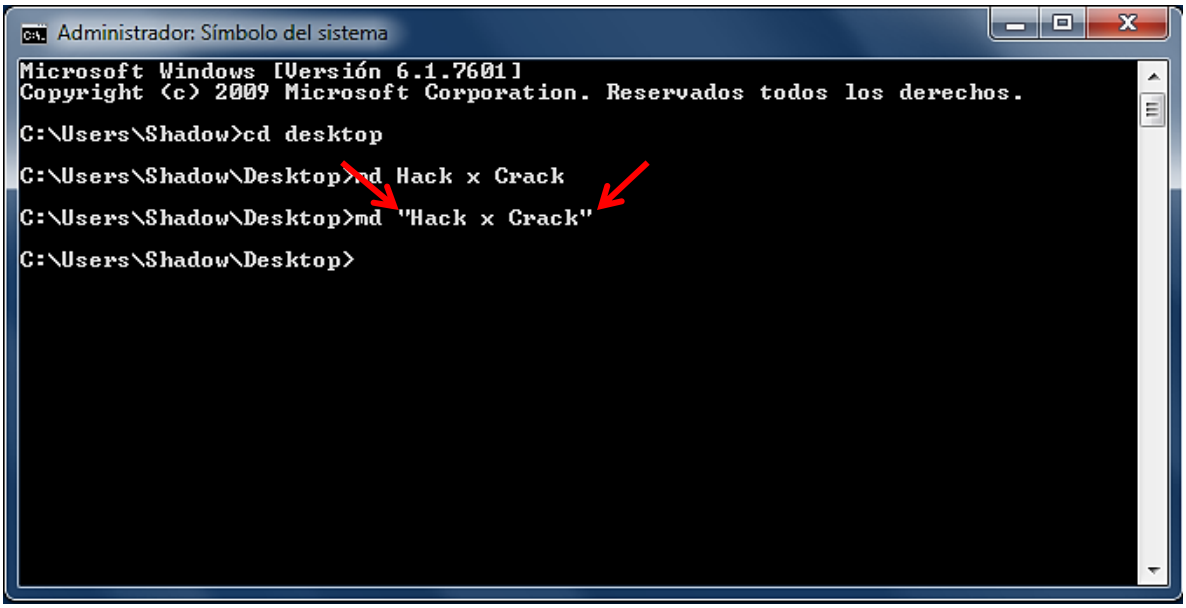
"COMILLAS"

Esto es indispensable que lo sepas, de hecho debí de habértelo mencionado casi al comienzo pero le fui dando más importancia a otras cosas.

Necesito que hagas una carpeta en tu *escritorio* llamada Hack x Crack obviamente usando el CMD.

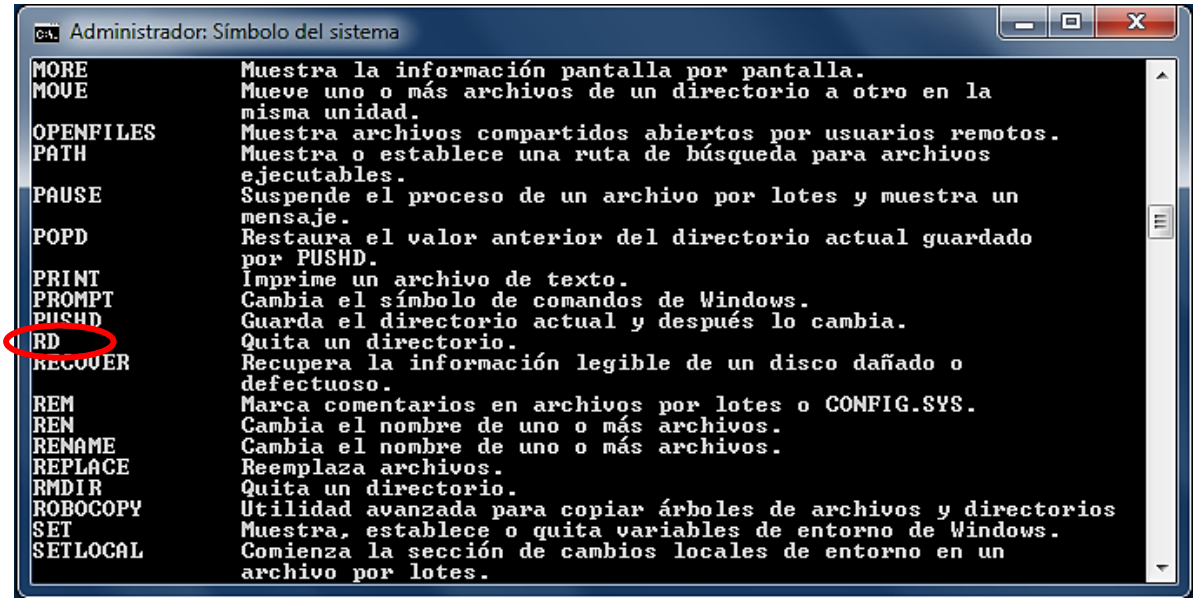


Que ha pasado?¿? Porque aparecieron 3 carpetas en lugar de una? La razón es que nosotros le dimos mal la orden al intérprete y entendió eso. La manera correcta es así:



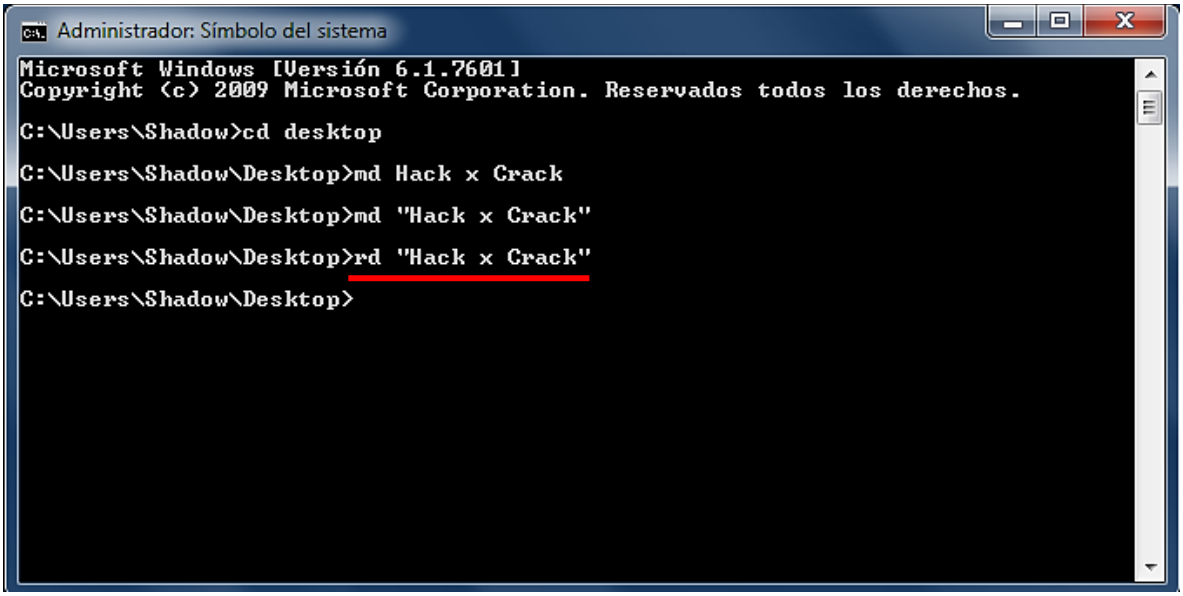
Cuando son dos o más palabras que están separadas, debemos de escribirlas entre comillas, tal y como se ve en la imagen. De igual manera si nosotros queremos entrar en ella, debemos escribir esto: cd "Hack x Crack"

Para eso nos sirven las comillas. Ahora qué dices si la borramos. ¿Qué? ¿Acaso no sabes que comando nos sirve para eliminar un directorio (carpeta)? Bien aquí lo tienes encerrado con rojo :)



Claramente es RD (Remove Directory) Incluso su descripción dice:
"Quita un directorio"

La ayuda nos dice que RD tiene dos parámetros: **/S** y **/Q.** El primero borra un directorio **aunque tenga contenido** y el segundo no pide que confirmemos si estamos seguros de querer borrarlo. Como nuestra carpeta está vacía basta con hacer esto:

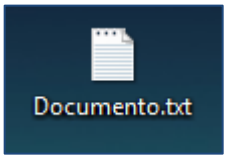


Te diste cuenta? Otra vez puse entre comillas Hack x Crack, esa regla jamás cambia. Si la carpeta tuviera algún archivo dentro para poder borrarla tendríamos que escribir: rd /s /q "Hack x Crack"

Extensiones

Esto también debí de haberlo dicho al principio: *"Todo archivo de tu ordenador tienen un nombre y una extensión [Nombre.Extensión]"*

¿Quién no ha mirado alguna vez esto?



Como estarás deduciendo el nombre de este archivo es **Documento** y su extensión es **.txt**

La extensión le dice al sistema que tipo de archivo es. Por ejemplo, si un archivo tiene una extensión .EXE, significa que se trata de un archivo **ejecutable**, es decir, de un programa.

Si, por otro lado, un archivo tiene una extensión **.DOCX**, el sistema operativo sabe que este tipo de archivo es un documento de Word.

La mayoría de los programas tienen la extensión **.exe**. De hecho todas las herramientas que hemos visto tenían esa extensión, excepto el Command. Podemos ver la extensión de cualquier archivo en sus **Propiedades**.

Observación: Cada tipo de archivo tiene un icono asociado que nos permite identificarlo sin necesidad de mirar la extensión.

 Documento PDF (*.pdf*)

 Archivo comprimido (*.rar*)

 Archivo de Música (*.mp3*)

 Virus (*.exe*)

El inconveniente es que los virus pueden manipularlos. ¿Qué clase de virus pondría una calaverita de icono? Todos usarían uno menos sospechoso y que estemos acostumbrados a ver. Ahh!!! y que ni se te ocurra pensar que todos los .exe son virus eh :|

Nota: Si no puedes visualizar la extensión de ningún archivo es porque no has **desmarcado** la casilla *"Ocultar las extensiones de archivo para tipos de archivo conocidos"* en Opciones de Carpeta.

Tasklist & Taskkill

Antes de empezar a usar estos comandos quiero que veamos como haríamos lo mismo de forma gráfica.

Nos apoyaremos en una herramienta nativa de Windows:

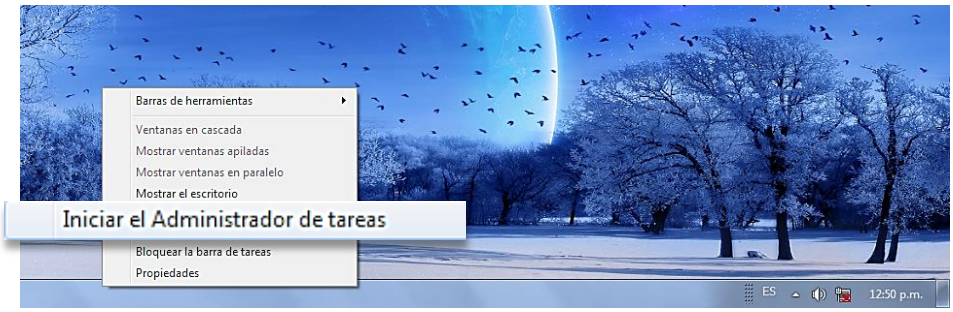
El ADMINISTRADOR DE TAREAS, o como antes se conocía, EL MATAPROCESOS.

Hay al menos 3 maneras cortas para abrirlo.

1- Observa tú teclado y presiona al mismo tiempo las siguientes teclas:

*Si tienes Windows XP el mata procesos se te abrirá al instante pero si tienes otro Windows te saldrá una ventana con varias opciones, adivina cual tienes que elegir xD

2- Da un clic con el botón secundario del mouse en una zona en blanco de la barra de tareas, saldrán algunas opciones ya sabes cual es, de todas formas aquí la resalta la imagen.



3- Presiona al mismo tiempo las teclas 

Solo escribe **taskmgr** y presiona Aceptar.

¿Qué es un proceso?

En palabras simples un proceso es una tarea que se está realizando en tu ordenador. Puede haber procesos importantes, procesos que esconden virus, procesos sin mucha importancia o procesos indispensables.

¿Qué es un Servicio?

Los servicios son los que nuestro ordenador brinda siempre que estemos corriendo algún tipo de servidor (FTP, web, etc.). Los servicios son los principales puntos de vulnerabilidad para los atacantes, que pueden aprovechar los privilegios y capacidades de un servicio para obtener acceso al servidor local o a otros servidores de la red.

Recomendación: Escribe **services.msc** en ejecutar y tipea el comando **SC/?** en cmd haber que te sale.

Imagina que un desgraciado lamer ha logrado colarnos un troyano; algo muy malo para nosotros pero muy divertido para él :(

Todos los procesos y servicios que están en marcha los encuentras en tu Administrador de Tareas y un troyano también inicia un proceso :) Así que para sacar a este tipo solo bastaría con identificar al troyano y "matarlo"

-No es mala idea pero como crees que encontraré al troyano si me están apareciendo un montón de procesos!!!

Deja te ayudo poquito, te voy a dejar los procesos que siempre vas a encontrar.

-explorer.exe. Se trata del Explorador de Windows. Si lo cerramos se nos borra todo el escritorio, por lo que no podrás abrir una sola ventana más. (Escribe explorer.exe en ejecutar para recuperarlo.)

-lsass.exe. Gestiona todo lo relacionado con la seguridad del sistema, servicios, aplicaciones, y componentes de Windows, que son los directores de la seguridad de tu sistema.

-svchost.exe. Este merece su propio artículo, te recomiendo investigarlo a fondo. Hospeda, o contiene, otros servicios individuales que Windows usa para realizar diversas funciones por eso normal encontrar bastantes svchost.exe.

-csrss.exe. Es el proceso que se encarga de gestionar las ventanas que tienes abiertas, que funcionen bien, y su debido tamaño.

-taskmgr.exe. Si te fijaste bien habrás notado que en la columna descripción dice sobre él: “Administrador de Tareas de Windows” xD (Ahora ya sabes porque pusiste taskmgr en ejecutar para iniciarlo :)

Ya sé que aún te quedarán muchos otros procesos que desconozcas, esto es porque cada programa que instalas inicia uno o varios procesos, pero no te desesperes y siempre empieza por mirar la DESCRIPCIÓN que tienen para que sepas de qué se trata y para que no digas que no te quiero te dejo tres consejos más para que no te engañen c:

Bailes de letras: Es un truco muy común que consiste en cambiar la posición de algunas letras. Ejemplo: Tu puedes ver un día el proceso csrrs.exe y piensas que no hay problema pero en realidad deberías tener csrss.exe

l=l=1: Windows tiene un problema de tipografía, es decir que el número uno, la letra ele, y la i mayúscula se parecen mucho, por ejemplo, tú tienes el proceso lsass.exe, este se escribe con la ele minúscula, y quizás tengas un virus que también se llame lsass.exe, solo que esta vez nuestro invasor lo escribió con la letra ele para confundirte :(

Aplicaciones nunca ejecutadas: Ejemplo. El proceso notepad.exe es el bloc de notas, pero si no lo iniciaste tú, probablemente, se trate de un virus que se hace pasar por él.

Si matamos algún proceso que no debíamos, y el ordenador se bloquea, ya sabemos para la próxima vez que ese proceso no es un troyano, y que no hay que finalizarlo no te preocupes lo peor que puede ocurrir es que tengas que reiniciar la computadora.

Ya con todo esto debiste descartar varios procesos y quedarte solo con los sospechosos, si ya tienes uno ubícate sobre él presiona clic derecho y selecciona “Abrir Ubicación del Archivo”. Analiza el fichero con el antivirus que tengas instalado, si salió positivo te preguntará que quieres hacer:

1- Mover al Baúl de Virus 2- Reparar

3- Eliminar 4- No hacer nada

Te recomendaría que usaras la primera si no fuera trampa, nosotros lo quitaremos manualmente c:

Si quieres estar más seguro de que en realidad ese es un troyano, ejecuta el comando **Netstat –a** y toma nota de todos los puertos que aparecen como abiertos vamos a identificar cual parece estar sobrando. (Están en la columna "Dirección local")

Cualquier dirección IP tiene MÁS de 65000 puertos, los cuales son como "entradas" a las direcciones IP, las direcciones IP son como "tú casa". Siendo así "TÚ CASA" (el IP) tiene 65000 "puertas" (PUERTOS)

Lo que hacen los puertos es recibir información; el puerto 21 es del FTP y el 80 de HTTP. Busca la lista de puertos que todo ordenador debe tener.

Recuerda que cualquier conexión al menos necesita 4 parámetros: IP de Origen, Puerto de Origen, IP de Destino y Puerto de Destino. Si se cierra la puerta que abrió el troyano el lamer quedará desconectado de nuestro ordenador.

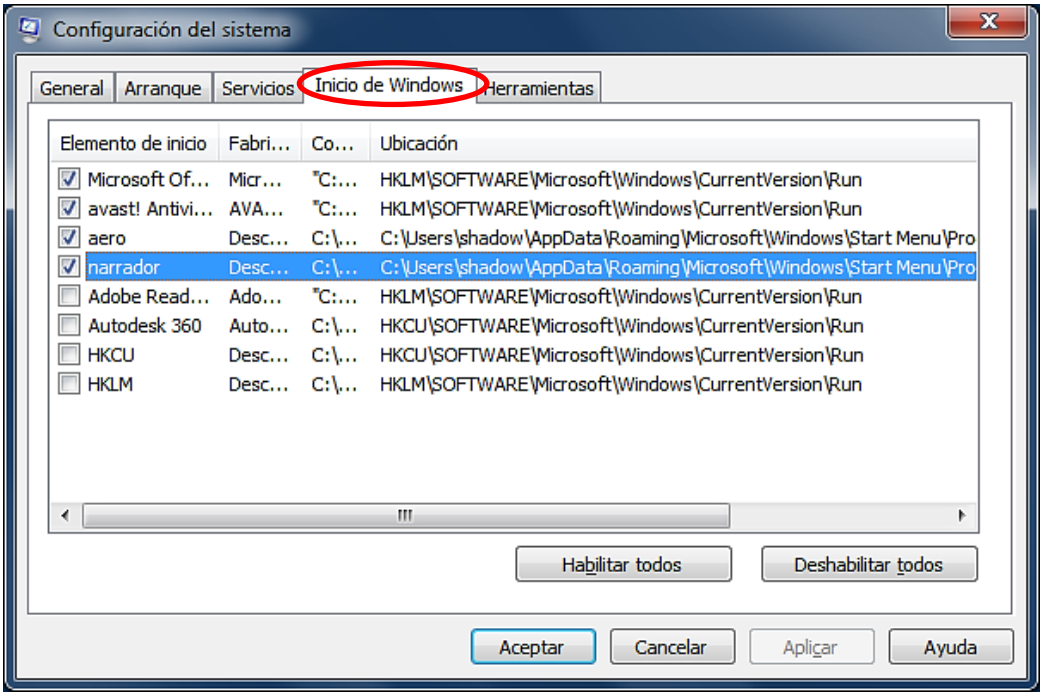
Netstat te arrojó una lista de los procesos que están esperando conexión (LISTENING). Ahora sí, mata a tu sospechoso, selecciónalo y en la esquina inferior derecha verás un botón que dice FINALIZAR PROCESO presiónalo y dile que sí a la pregunta que te haga.

Volvemos a la línea de comandos y lanzamos otro **Netstat –a** compara la lista anterior con esta nueva y encuentra el puerto que se ha cerrado.

Ya casi terminamos, busca el server del troyano *(Recuerda: "La parte que se instala en el ordenador de la víctima se llama servidor, y el acceso se logra mediante el cliente")* y elimínalo como lo harías con un archivo común.

Hace ya bastante tiempo curioseando por C:\Windows\System32 me encontré una increíble herramienta. Escribe **MSconfig** en ejecutar para abrirla.

Allí se muestran todas las aplicaciones que se inician cuando arranca el sistema junto con su nombre y su ubicación :D



El directorio que marqué en azul no se alcanza a ver completo pero es este:

C:\Users\shadow\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup

Cumple la misma función que la rama **Run** del registro, todo lo que esté allí se inicia con Windows.

En XP será diferente pero más fácil:

C:\Documents and Settings\Administrador\Menú Inicio\Programas\Inicio

Yo ya le quité la palomita al lugar que ocupaba mi virus :b

Apunte: Los tres directorios donde prefiere alojarse el malware:

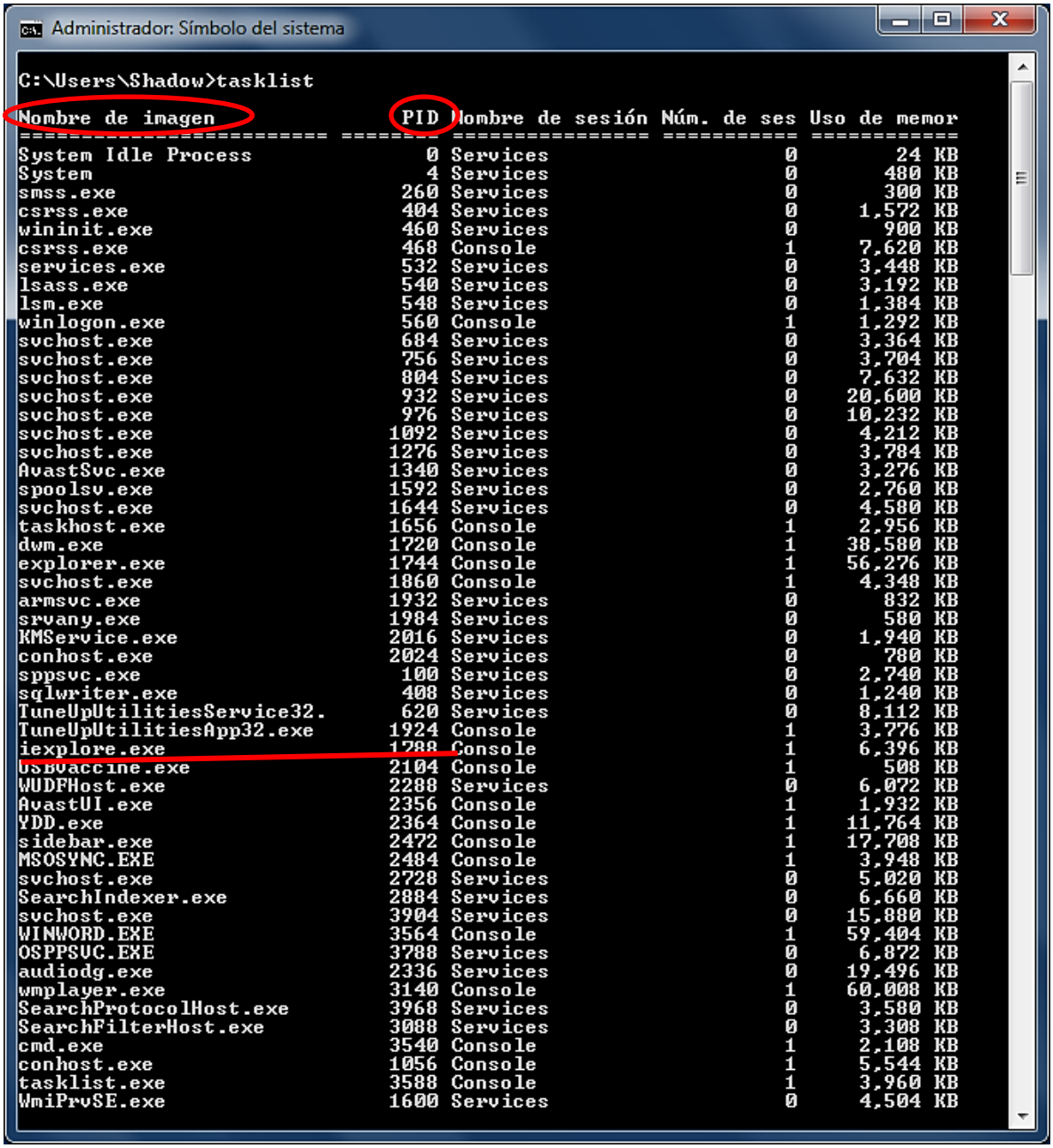
- C:\Windows
- C:\Windows\System32
- C:\Users\Shadow\AppData\Local\Temp

Ya que sabemos como usar el taskmgr es hora de hacerlo con nuestro viejo camarada monocromático y los comandos que dijimos al comienzo.

La herramienta **Tasklist** (Listar Tareas) *"muestra una lista de procesos que se están ejecutando en un equipo local o remoto"*. Escribe **Tasklist /?**

La herramienta **Taskkill** (Matar Tarea) *"se usa para terminar tareas mediante el **Id**entificador de **P**roceso (**PID**) o nombre de imagen (IM)".* Escribe **Taskkill/?** para ver los parámetros que utiliza.

Tipea **Tasklist** sin parámetros y podrás ver todos los procesos que están en marcha igual que en el Administrador de Tareas:



El **PID** es un número que identifica de forma ***exclusiva*** a un proceso mientras se está ejecutando es lo mismo que el **Nombre de Imagen** (IM). Con el

comando **TASKKILL** podremos finalizar el proceso que hayas seleccionado de la lista. Ejemplo:

Decido Finalizar el Proceso iexplore.exe (Es el programa Internet Explorer)

Posibles líneas a ejecutar:

- **Taskkill /T /F /IM iexplore.exe** 'Usando el nombre de imagen del Proceso
- **Taskkill /T /F /PID 1788** 'Usando el PID del Procesos

Lo cual te devolverá el siguiente mensaje:

CORRECTO: señal de terminación enviada al proceso "iexplore.exe" con PID 1788

Nota: El PID será diferente en cada sesión por eso es mejor usar el parámetro **/IM**

Aclaro que no siempre puedes quitarte una infección con este método pero no está por demás conocerlo c:

Copy

Como ya sabemos lo que son las extensiones podemos hacer la siguiente práctica :)

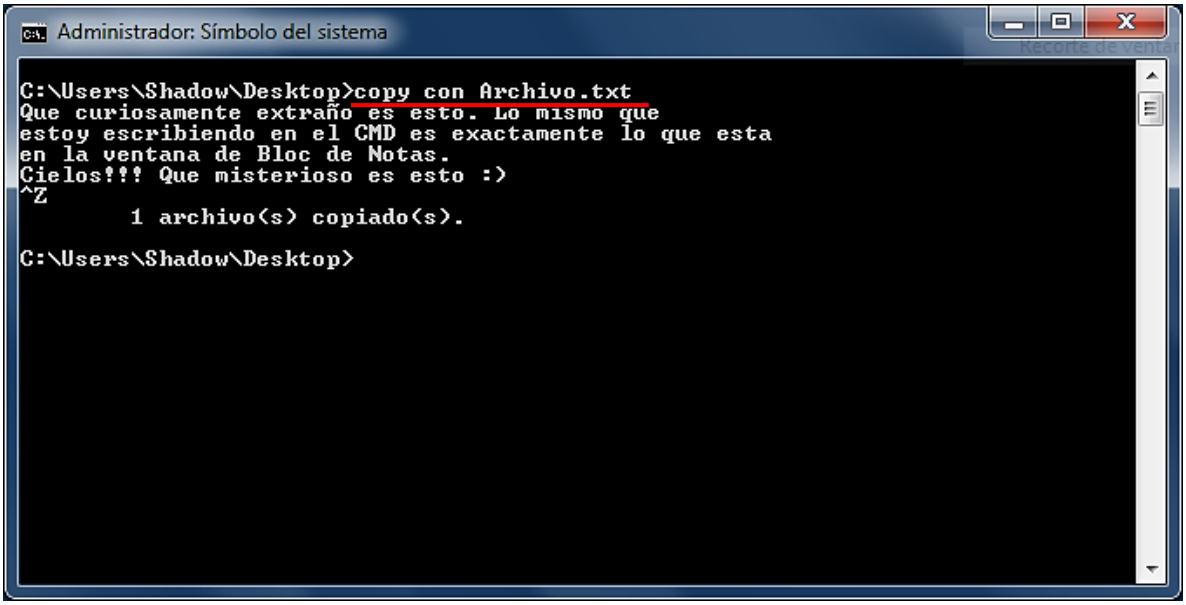
Escribe el comando **copy con** seguido del nombre y la extensión que quieras darle a tu archivo. En mi caso será uno de texto y se llamará archivo. Después de dar enter verás que tienes espacio para escribir el contenido de tu nuevo documento. Puedes ponerle lo que desees. Pero cuando termines no olvides aplastar la tecla **F6** (o Ctrl + Z) y dar enter.

Fíjate como estoy dentro de mi escritorio por lo tanto el documento aparecerá allí con el nombre Archivo.txt y como es simple texto se abrirá con el Bloc de Notas. Las palabras que escribas serán su contenido.

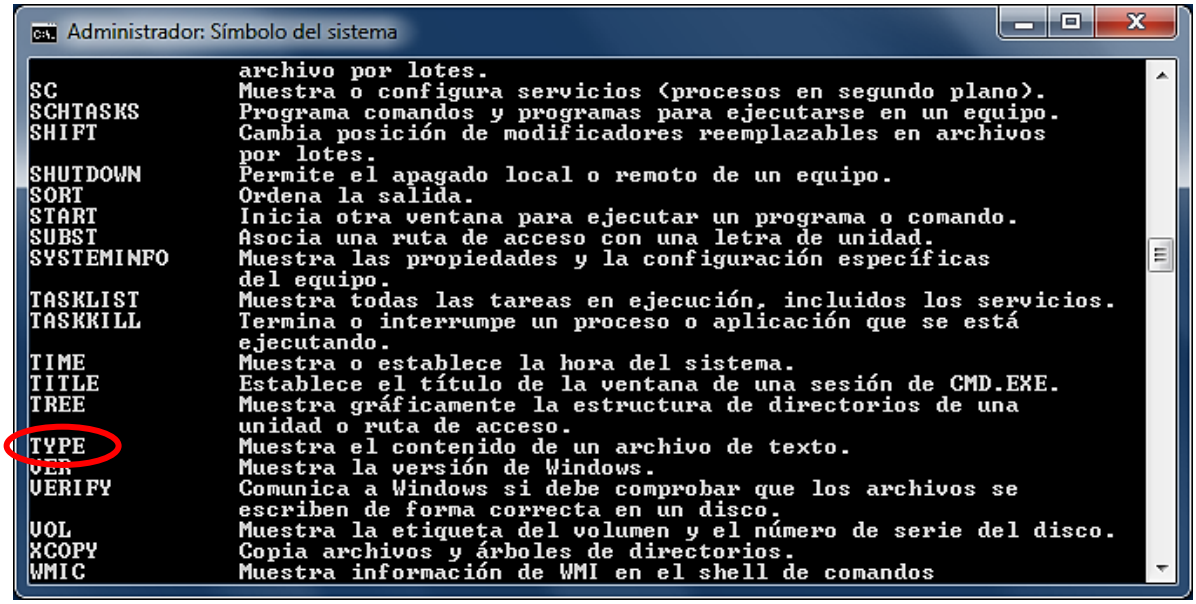
Nota: Al aplastar la tecla **F6** saldrá el símbolo **^Z**

Alternativa: Otra manera de hacerlo sería usando la instrucción: echo Un mensaje para mostrar>Archivo.txt Esta vez usamos un carácter especial,

llamado *operador de redireccionamiento,* también están otros como el **|** (pipe, tubería) o **^** (carácter de escape. Permite usar caracteres reservados)



Si gustas puedes abrirlo con el *explorador* y darte cuenta de que es lo mismo, pero como nosotros ya nos acostumbramos a la **interfaz de comandos** preferimos abrirlo con el CMD :)

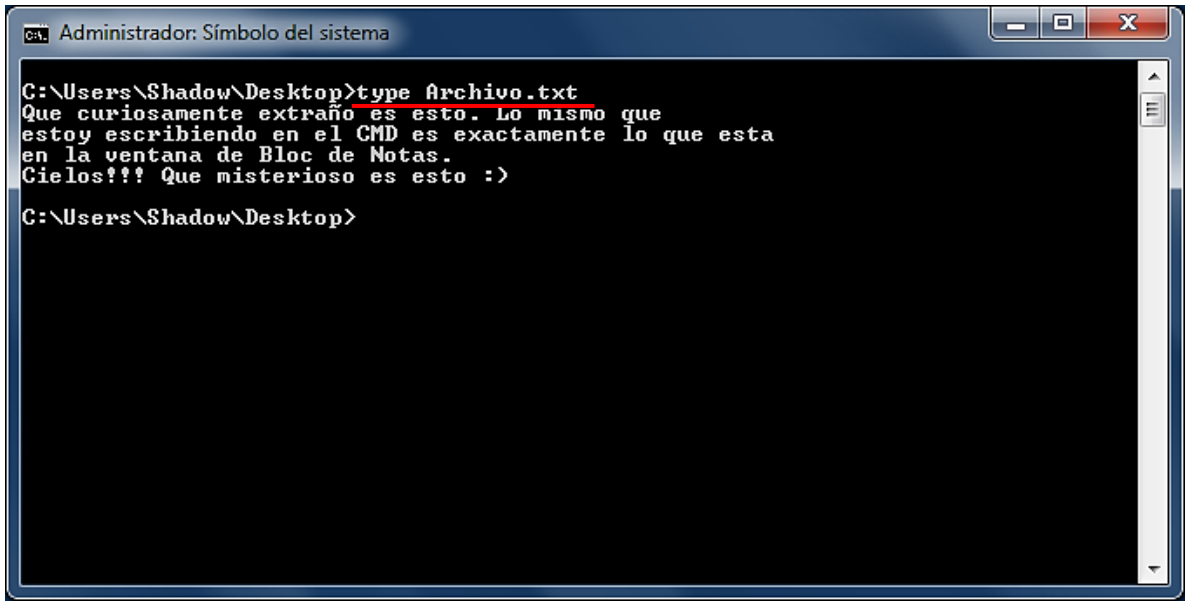


Así es, el comando que usaremos para esta tarea es **Type** (Tipo) Escribe **type archivo.txt** y da enter. Con eso podrás ver y leer su contenido :)

Ahora te dejo con estas preguntas: ¿Qué pasaría si escribo el mismo comando pero no pusiera la extensión? Es decir, si tecleara **type archivo** y diera enter.

¿Y si hubiera escrito solamente **copy con Archivo** y que tal si intentara borrarlo, moverlo o renombrarlo sin especificar ningún tipo de extensión?

¿Qué ocurriría?



Si deseas editarlo digita la siguiente línea: **edit archivo.txt**

Para finalizar el tema de las extensiones te propongo que escribas el comando **copy con** seguido de un nombre y una extensión distinta a .txt quizá pueda ser **.rtf, .html** o **.pif** para crear un acceso directo a un programa MS-DOS, las posibilidades son muchas :)

-Aguarda… Los comandos externos tienen la extensión .exe o .com, ¿verdad?

Si, tienes toda la razón

-Entonces, para invocar a SUBST tendría que escribir SUBST.exe o FINGER.exe para FINGER ¿no?

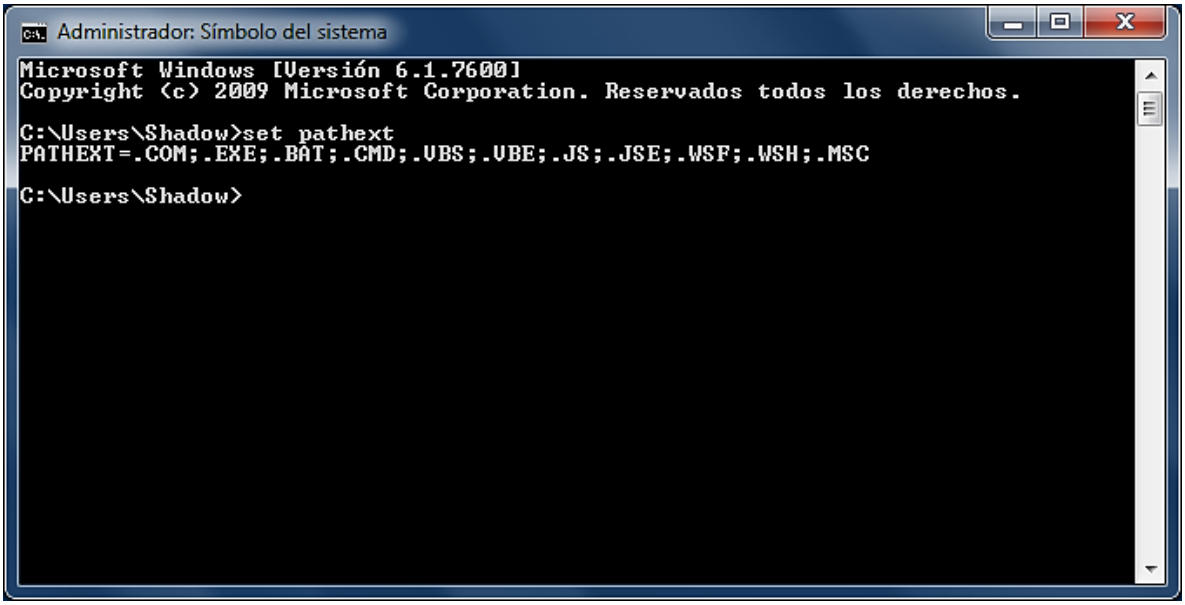
Creo que ya se lo que me vas a preguntar, tú quieres saber si mi hermana tiene novio, ni hablar no tengo hermanas.

-No puede ser!!! Voy a morir solo, dame un minuto :(

Adelante, por mí tómate todo el año, mientras te digo porque no se ocupa poner la extensión .exe en los comandos externos :) La tabla de la página 37 tenía esto:

%PATHEXT%	Esta variable contiene una lista de varias extensiones. Si el nombre de un archivo termina con una extensión incluida en esa lista, se puede **omitir** al invocarlo.

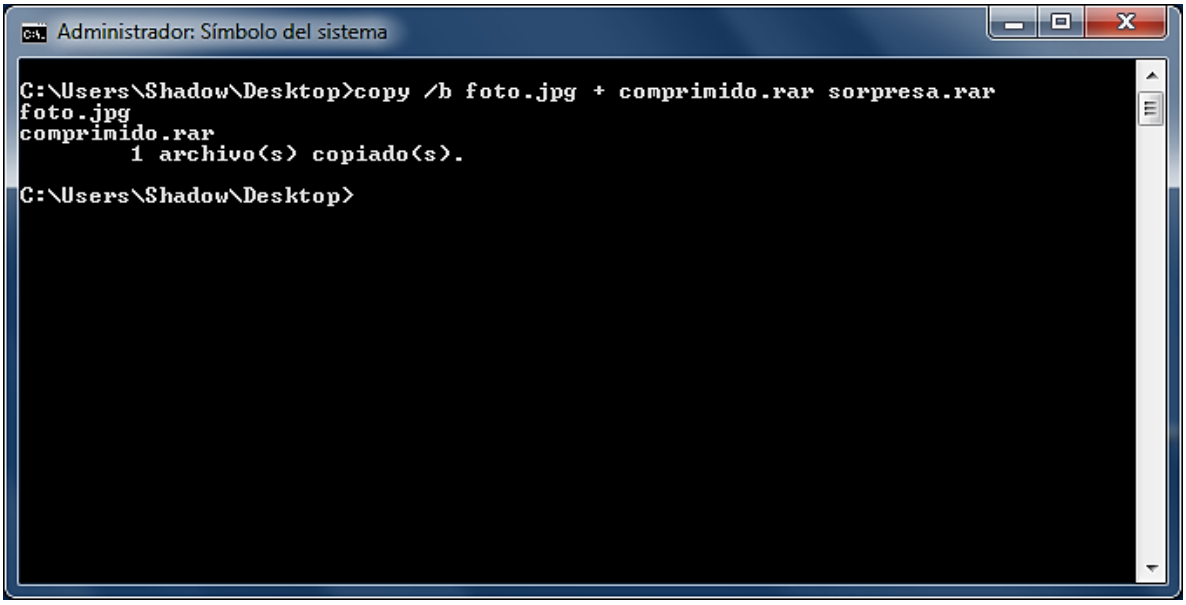
Ni el agua turbia está más clara que eso, por eso tendremos que explicarlo :) Tipea set pathext. Todas las extensiones que veas te las puedes **saltar**. Listo :)



Pero el comando COPY nos tiene más sorpresas :)

Selecciona una imagen cualquiera y un archivo **.rar** con algún fichero dentro que vamos a ocultar el primero dentro del segundo en un tercero :)
Si no entendiste no hay problema, ya verás como está el asunto. La imagen que escogí se llama *foto.jpg* y al archivo WinRAR le puse *comprimido.rar*
Ahora escribe esta instrucción en el cmd:

Copy /b foto.jpg + comprimido.rar sorpresa.rar



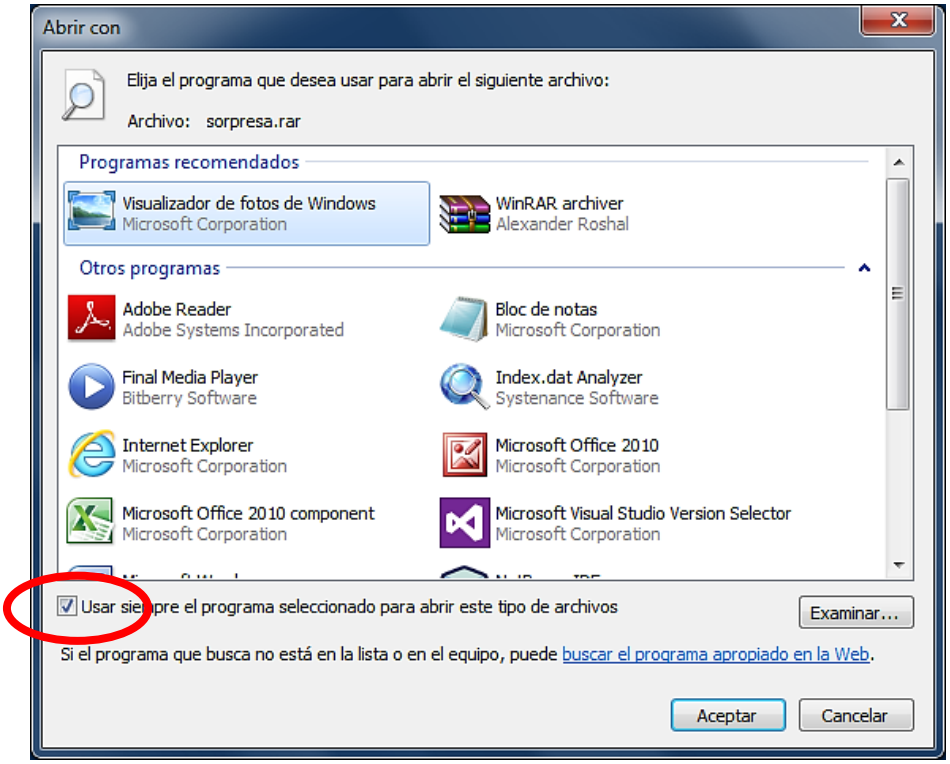
Recuerda que estamos en nuestro escritorio, por lo tanto la imagen y el fichero .rar también los debes de tener allí. Si escribiste la misma línea que yo, al dar enter aparecerá otro archivo .rar llamado sorpresa; primero ábrelo normalmente usando el WinRAR.

-Mmm… pues me salió el fichero que estaba dentro de Comprimido.rar, ¿Qué tiene eso de sorpresa?

Ahora, prepárate para caerte de tu silla!

-Pero estoy acostado en mi cama bien triste por lo de tu hermana :(

Es igual, solo necesito que sobre *sorpresa.rar* des clic derecho, selecciones "Abrir con" y luego "Elegir programa predeterminado…" En la nueva ventana que te salió debes buscar el programa que tengas instalado para mirar tus fotos. Por default está el *Visualizador de fotos de Windows.*



Selecciónalo y dale en aceptar pero **NO OLVIDES <u>DESMARCAR</u>** la opción que señala el elipse rojo; si la dejas allí cualquier archivo .rar se abrirá con el Visualizador de Fotos.

Si no te apareció el programa a la primera, puedes darle clic en “Examinar” para buscar ese o uno mejor como el PhotoShop si es que ya lo conseguiste :)

-Santo hacker Linus Tordvals!!! El programa me abrió la imagen que había seleccionado. Cielos!!! Esto es realmente grande. Permíteme ir por una silla para poder caerme. 💬

Así es, metimos dos ficheros en uno solo, gracias al parámetro **/b** que le dimos a Copy, te toca buscar que hace :)

Comodines

Los comodines son caracteres especiales. La interrogación y el asterisco son ejemplos.

La **interrogación** sustituye a cualquier carácter, pero solo a uno, mientras que el **asterisco** reemplaza a varios.

El asterisco sólo puede aparecer al final del nombre o de la extensión, y quiere decir "cualquier combinación de letras y números"

Ejemplo 1:

Al escribir: **dir a????*.***

Se nos mostrará una lista con las carpetas y archivos que empiecen con la letra *a* y otras 4 letras más, no importa cuales sean, y el ***.*** nos listará archivos con cualquier extensión. Por eso el asterisco se conoce como *comodín global.*

Del mismo modo si tecleamos **dir *.exe** miraremos todos los archivos que tengan extensión **.exe** en el directorio en que nos encontremos.

Ejemplo 2:

Por análoga razón, si queremos copiar todos los ficheros del directorio actual al disco C, haríamos **COPY *.* C:**

Luego, imagina que deseamos copiar al disco C: todos los documentos que empiecen por *Do* y cuya extensión empiece por *j*, entonces hay que poner **COPY Do*.j* C:** y dar enter.

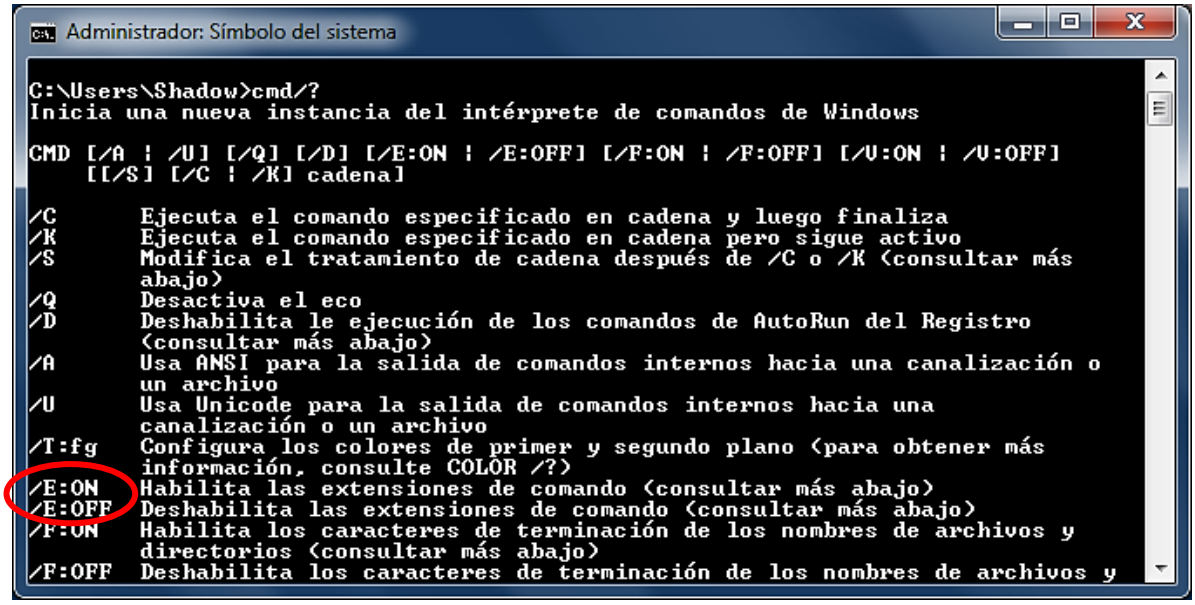
Pero sería mejor usando el comando **ROBOCOPY**, según dice su descripción es una “Herramienta para copia eficaz de archivos” y que tal **XCOPY** :)

Habilitando Extensiones de Comando

Las extensiones de comando implican **cambios y ampliaciones** (hacen que acepten más parámetros) en los siguientes comandos:

DEL o ERASE	MD o MKDIR	POPD	ENDLOCAL	CALL	START
COLOR	PROMPT	SET	IF	SHIFT	ASSOC
CD o CHDIR	PUSHD	SETLOCAL	FOR	GOTO	FTYPEY

¿Sabes? Varios detalles interesantes, como las extensiones de comando, nos los regala cmd/?



Pues allí tienes para leer un rato, por lo pronto fíjate en la parte que encerré con rojo, según eso tenemos que escribir cmd /E:ON para habilitar las extensiones o cmd /E:OFF para apagarlas :)

Iniciar CMD en la pantalla de inicio

Ingresa a C:\Windows\System32 y localiza el archivo sethc.exe puedes hacerlo más rápido si escribes su nombre en el cuadro de búsqueda de la ventana, le das clic derecho y escoges “abrir ubicación del archivo”.

Ya lo encontramos, éste funciona cuando estás por escribir tu contraseña para iniciar sesión, si aplastas varias veces la tecla **SHIFT** harás que está aplicación se abra y aparecerá un cuadro titulado “Teclas de método abreviado de accesibilidad” o algo parecido.

¿Qué pasaría si de alguna manera logramos reemplazar sethc.exe por cmd.exe?

Que ahora cuando aplastemos la tecla SHIFT se abrirá el cmd, algo muy útil porque con los comandos correctos podemos evadir la contraseña y entrar sin identificarnos.

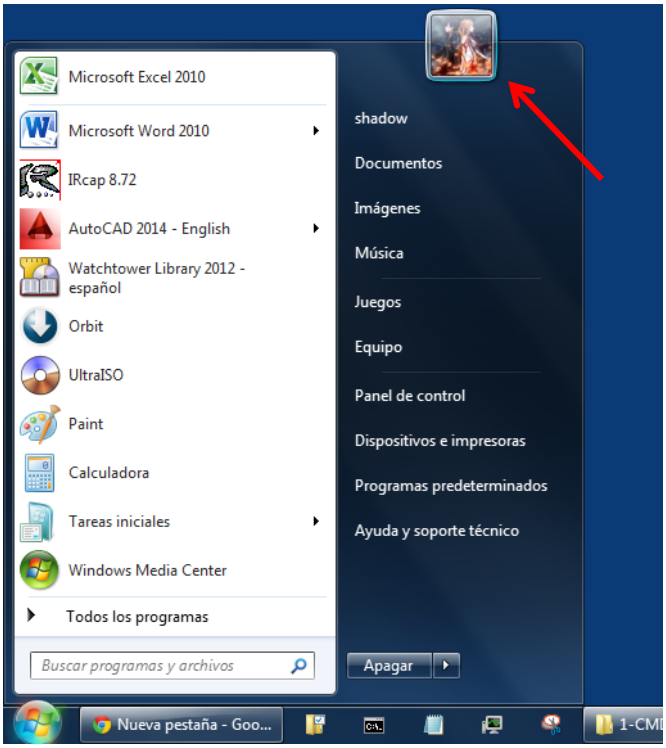
Los pasos a seguir parecen sencillos.

1) Deshacernos del sethc.exe original cambiando su nombre a sethc.xxx

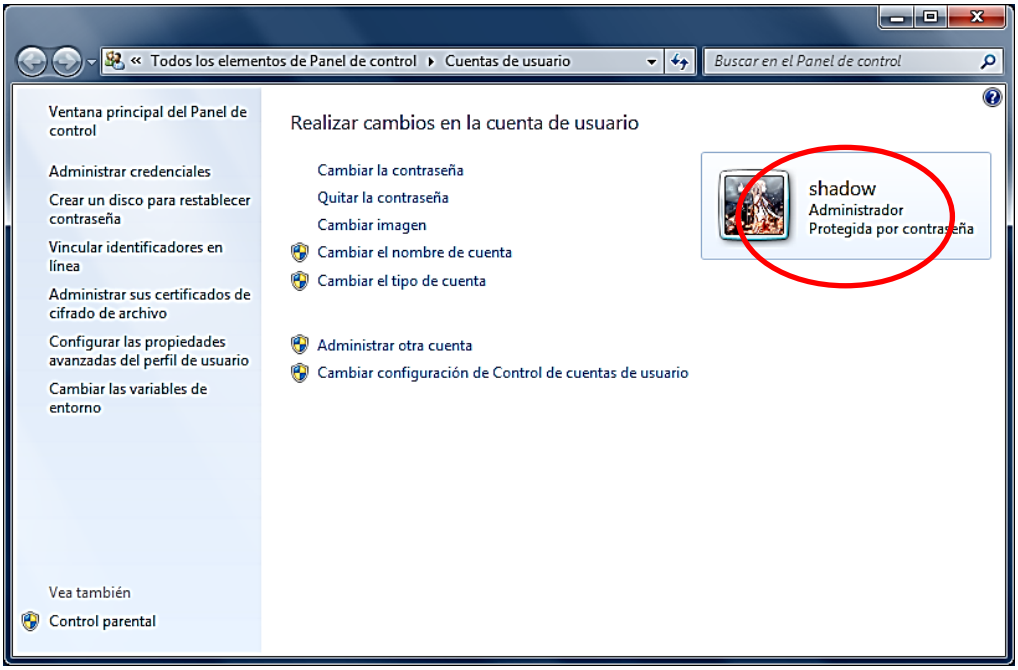
2) Copiar el cmd.exe pero con el nombre sethc.exe

Antes que todo necesitamos ser administradores o para que se escuche más Unix tener una cuenta root :b

¿Cómo saber? Clic menú inicio, clic en la imagen de usuario.



* En la esquina superior derecha encontrarás la respuesta. Da clic en Administrar otra cuenta allí verás los demás usuarios que hay, si tu cuenta dice estándar no podrás continuar, mira la lista e inicia sesión con uno de los usuarios que sea administrador, lo más probable es que tenga contraseña.



Apunte: Otra manera de saberlo es fijándote si dice la leyenda *Administrador Símbolo del Sistema* en la esquina superior izquierda del cmd.

-Percebes soy estándar y mi mamá no me presta su cuenta, dice que es para tener más control :|

No es para tener más control, es para tener el control total, por eso a los administradores se les llama superusuarios o usuarios con privilegios avanzados y obviamente parece que no confía en ti xD

Tienes que averiguar su contraseña, no creo que funcione pedírsela, quizá en un descuido que la deje abierta (el descuido lo tienes que causar tú xD) y ejecutes rápido todos los pasos. Otra es hacer una USB booteable (autoarrancable) con el LiveCD de ophcrack, entrar al BIOS (oprimiendo las teclas *F2, F10, supr o delete* en los primeros segundos de encendido) y configurarlo para que se inicie (bootee) desde esa USB, el programa te dará la contraseña.

Y queda una tercera, en vez de usar ophcrack, recomiendo el LiveCD de HIREN'S BOOT Restore Edition, funciona igual pero tiene muchísimas más utilidades y entre ellas aparece el **Password Remover** (Removedorde Contraseñas)

Te advierto que estas opciones son trampa, porque nosotros queremos saltarnos la identificación con el cmd!!! >:c

Además está la probabilidad de que la BIOS tenga contraseña y no te deje modificar nada; percebes a quién engaño, hay mil formas de arreglar eso, el mismo HIREN'S BOOT tiene una utilidad llamada **UniFlash** para eliminar el password sin siquiera haber configurado previamente la BIOS para que inicie desde el pendriver (USB) :|

Apunte: El comando **debug** del cmd también pudiera desbloquear la BIOS.

OK ya, haz lo que quieras, el caso es que necesitas ser administrador, supongamos que ya lo eres, ¿Qué sigue?

Anda intenta cambiar el nombre de sethc.exe por sethc.xxx, tipea:

cd C:\Windows\System32

y luego…

ren sethc.exe sethc.xxx

-El ophcrack es increíble ya soy administrador c: pero no me funciona dice Acceso denegado ._.

Exacto, ahora hazlo gráficamente ponte sobre él, aplasta F2 y cámbiale el nombre.

-Nada, dice que requiero de permisos especiales de un tal TrustedInstaller.

Ese tipo se ganó la confianza de Windows y le otorgó la posesión y protección de varios archivos del sistema, para evitar que los usuarios idiotas los modifiquen y descompongan todo.

Entonces a quitarle su poder! Pasos:

1) Clic derecho encima de sethc.exe y elige Propiedades.
2) Clic en pestaña Seguridad de la parte de arriba. Y pulsa el botón Opciones avanzadas que está abajo a la derecha.
3) Clic en la pestaña Propietario. Verás que TrustedInstaller es el Propietario actual. Pulsa abajo a la izquierda el botón Editar.
4) En medio, en la lista de Nuevo propietario, selecciona tu nombre de usuario (Si escoges Administradores todos los usuarios de este nivel tendrán acceso). Aplicar, Aceptar todo y cerrar.
5) Vuelve a acceder a las propiedades de sethc.exe.
6) Clic en la pestaña Seguridad y pulsa el botón Editar que está a media ventana, a la derecha.
7) Selecciona tu nombre de usuario (o Administradores) en la lista de Nombres de grupos o usuarios de la mitad superior. Abajo, en el campo Permisos de Administradores, haz clic en la casilla de Control total bajo la columna Permitir. Aceptar todo.

Está largo, mejor hubiéramos usado esta orden y así facilitarnos los pasos 1-4

takeown /F "c:\windows\system32\setch.exe"

Luego, esta otra se hubiera encargado de los pasos 5-7:

icacls " c:\windows\system32\setch.exe " /grant shadow:(M,F)

-Que bestia está más fácil usando el cmd >.<

Si, eso quería que vieras y lo mejor es que ambas pueden modificarse para que abarquen directorios enteros (incluyendo archivos y subdirectorios y archivos que estén en esos subdirectorios)
La primera línea destrona a TrustedInstaller y nos otorga el puesto; como ya somos poderosos el segundo nos regala el control total al que tenemos derecho.
Ten en cuenta que en lugar de escribir /grant shadow:(M,F) vas a poner el nombre de tú usuario, no creo que también sea shadow y si es, pues cámbiatelo porque ese ya lo gané yo ._.

El parámetro /grant indica que concederemos permisos a un usuario. (Lo contrario de /Deny que es para denegar)
M y F son permisos de modificación y acceso total respectivamente.
¿Qué esperas? Se que te mueres de ganas por digitar takeown/? y icacls/?

Observación: icacls es la actualización del comando cacls.

Excelente, ya quitamos los obstáculos es hora de cambiarle el nombre a setch.exe por setch.xxx, una vez que lo hayas echo abre el cmd y desplázate hasta C:\windows\system32 después teclea:

copy cmd.exe sethc.exe

Esa línea copiará el cmd original en el directorio actual pero con el nombre de sethc.exe, entonces cuando estemos en la pantalla de inicio de sesión y aplastemos la tecla SHIFT varias veces el sistema abrirá la aplicación llamada sethc.exe pero como la convertimos en el cmd, ¿qué crees que se vaya a abrir?

Listo, tenemos una Shell con acceso root que se abre antes de que inicie el mismo sistema, ¿qué comando escribo para esquivar la contraseña? Esa parte le corresponde al siguiente subtítulo c:

Comando Net

Tenemos varias alternativas para jugar con Net ya sabes como mirarlas. Lo más fácil puede ser eliminar la contraseña del usuario o cambiársela con la línea:

net user Shadow *

Si queremos quitársela solo damos un enter pero si queremos una nueva tendremos que escribirla y luego dar enter (no se miran las letras que vas escribiendo pero si se graba). Lo que lo hace poderoso es que nos deja hacer todo eso sin saber la contraseña del usuario original :D

-¿Me estás diciendo que pude haber escrito ese comando en la sesión de mi mamá y así de simple le hubiera quitado la contraseña?

Si :D, tranquilo no te enojes, siempre tenemos que buscar lo más difícil para poder aprender, aclarado eso continuamos :b

El comando **Net User Shadow** me proporcionará información de mi cuenta.

-Oye pero la primera idea que tuvimos no creo que sea tan buena, puede que mi mamá note que su cuenta se quedó sin contraseña o que ni siquiera acepta la suya .-.

Cierto, por eso mejor le damos privilegios administrativos a tu cuenta c:

Net localgroup

Ese comando te dará la lista de grupos existentes, si lo acompañas del nombre de uno de ellos te mostrará una pequeña descripción con los usuarios que pertenecen a él. Por ejemplo: *Net localgroup Invitados.*
Si te das cuenta en primer lugar está administradores y nosotros queremos estar en ese grupo, por lo tanto:

Net localgroup administradores shadow /add

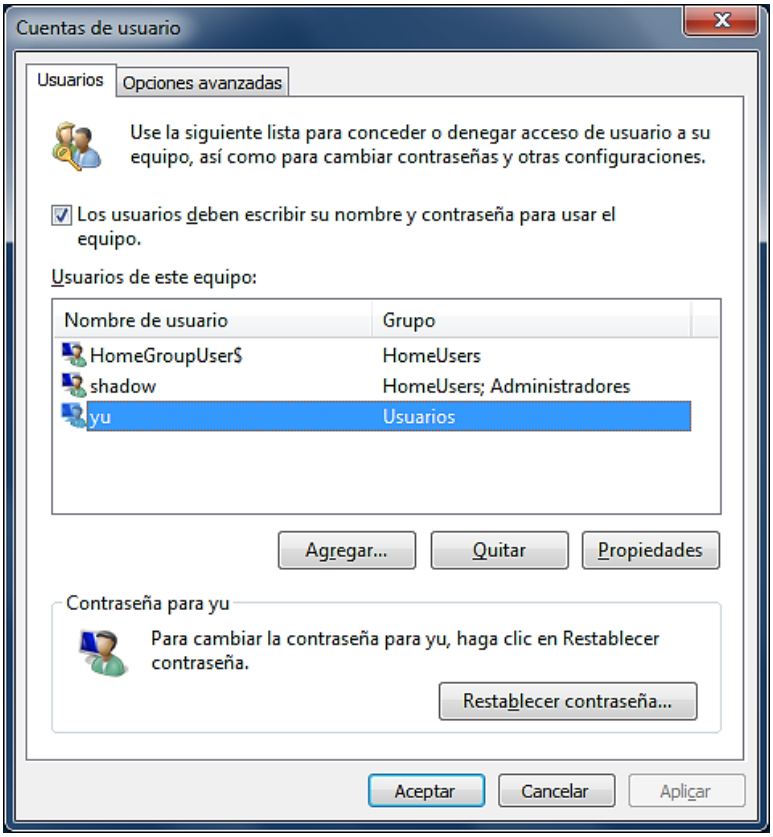
De esta manera si shadow ya existe pero es estándar esa instrucción lo hará administrador, si no existe se creará con ese nivel. Si no especificas el grupo al que pertenecerá por defecto será estándar. Por ejemplo: *Net user MiNuevaCuenta /add.*

Si te hartaste de la interfaz negra y sin vida también puedes ejecutar una aplicación que está en C:\Windows\System32 llamada **Netplwiz**.

Escribe **Netplwiz** en el cmd y da enter, se abrirá una ventanita, abre la cuenta que sea estándar con dos clics, en la pestaña "Pertenencia a Grupos" palomea "Otros" y elige "Administradores" después allí mismo palomea "Administrador" y finalmente clic en "Aplicar".

Si eres observador esa misma ventana te da la opción de eliminar a un usuario sea cual sea y con toda su información :O

Curiosidad: Un equivalente Netplwiz es Control userpasswords2



Lo último que net puede enseñarnos en esta parte es esta línea:

Net user Administrador /active:yes

La cuenta con el nombre Administrador y del tipo administrador en forma predeterminada esta deshabilitada, lo anterior la habilita, para deshacer los cambios solo cambia *yes* por *no.*

Como ya eres administrador tienes los permisos necesarios para instalar cualquier programa que desees, por ejemplo un **KEY LOGGER**, no te recomendaré uno porque hay muchos; descarga el que mejor se te acomode.

Este tipo de software es un grabador de teclas pulsadas, es decir, registra cuando el usuario ingresa su contraseña y la guarda. También muestra cuales han sido las acciones de los usuarios en el sistema.

¿Viste cuántas formas de burlar la contraseña hay en Windows?

Si por alguna razón todavía no diferencias entre el nombre de la cuenta de usuario y el nombre del equipo; escribe el comando **whoami** que primero nos mostrará el nombre del equipo y después el del usuario o bien solo **HostName** (Nombre de Host) para ver el nombre del puro **EQUIPO**.

Últimos detalles :)

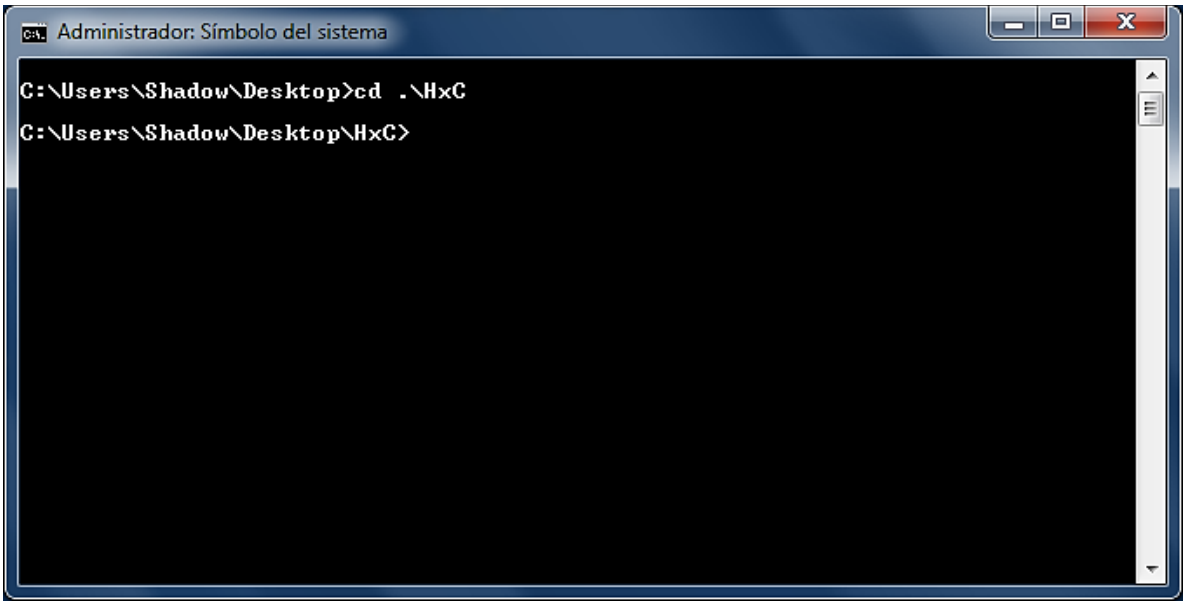
También existen formas de abreviar los comandos para llegar al mismo resultado.

Por ejemplo, si nosotros nos encontramos en el directorio **C:\Users\Shadow** y deseamos irnos hasta el disco C tendríamos varias opciones:

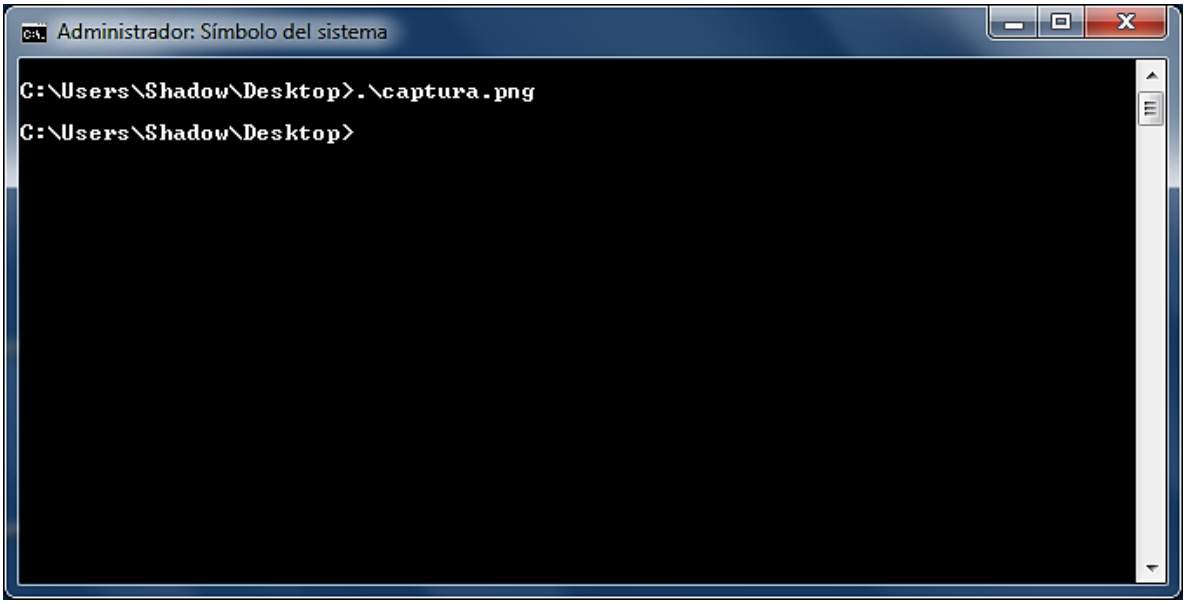
- Tipear cd.. dar enter y de nuevo escribir cd.. y dar enter.
- Poner cd..\..
- Teclear cd c:\
- Escribir cd\

Dependiendo de que tan largo o corto esté el directorio al que deseemos desplazarnos, podríamos usar la primera, segunda, tercera o cuarta opción :)

Hay otro parecido que no es tan importante pero hay que saber que es hablamos de **.** cuando lo veas significa que estamos en el directorio actual. Ejemplo, si queremos abrir una carpeta llamada HxC que está en el escritorio y ya estamos allí, bien podríamos hacer esto:



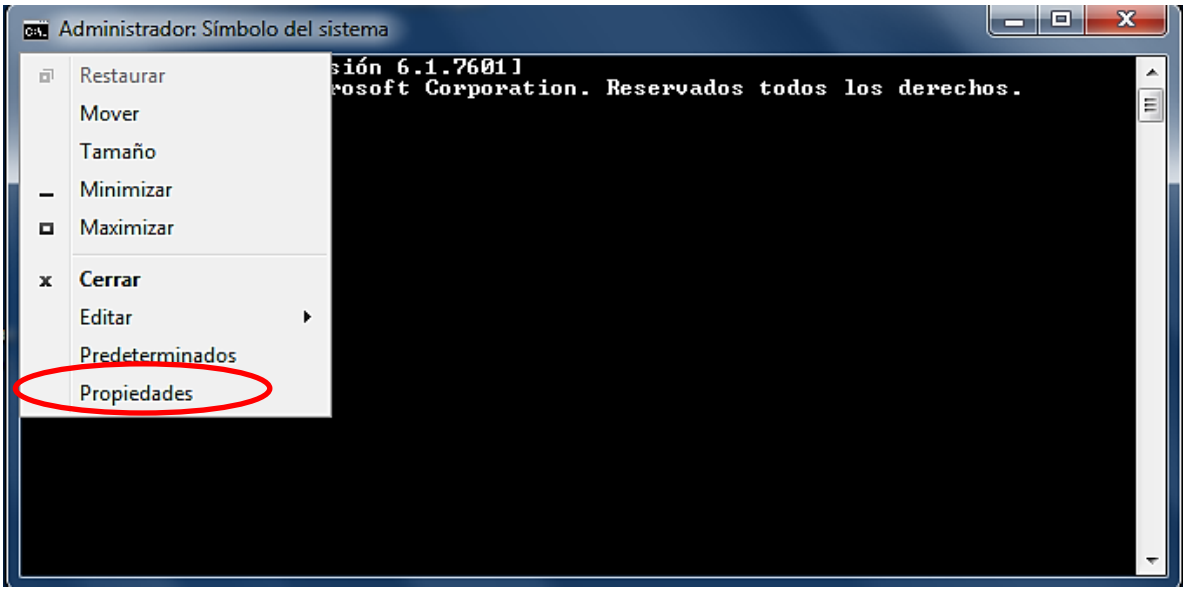
Si quisiéramos abrir una imagen que también esté en el escritorio y ya estuviéramos en él podríamos hacerle así:

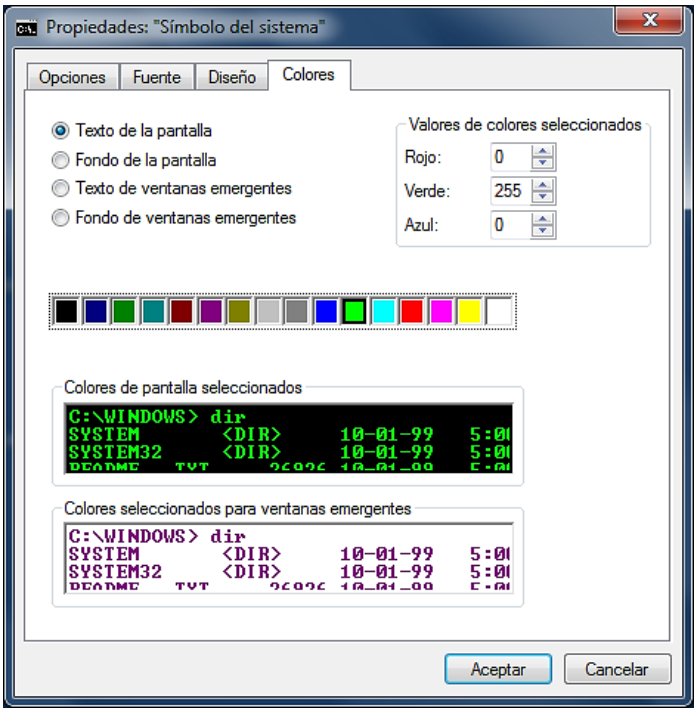


Ya pasando a otro asunto ¿nunca te has preguntado cómo hacen algunos para que al abrir el cmd se inicie con un color diferente?

-see, me vas a enseñar? c:

Da clic en la esquina superior izquierda y elige PROPIEDADES.





Ve a la pestaña *"COLORES"* marca la opción Texto de la pantalla, selecciona uno de los cuadritos con color y por último en Aceptar. Listo!

Recomiendo usar el último cuadrito, el blanco, por defecto usa el gris y no es muy claro.

Aquí también puedes cambiar el tipo de letra y el tamaño de la consola.

Curiosidad: ***Ejecutar*** sirve para muchas cosas, telnet towel.blinkenlights.nl nos pone un episodio de Starwars, iexplore -k www.hackxcrack.es visualiza el navegador en pantalla completa (igual que aplastar **F11**), además hay otros buenos atajos de teclas aparate de Win+E y Win+R el que más me gusta es el

Aero Flip 3-D con las teclas Win+TAB si tienes Windows 7 Ultimate, Home Premium o Professional te funcionará :)

Como experimento te propongo que ejecutes la línea **net stop uxsms** con ella desactivamos el Aero se perderá el estilo pero rendirá mejor la interfaz del PC, para activarlo digita: **net start uxsms**.

Presiona **F1** para acceder a la Ayuda allí escribe *"Métodos abreviados de teclado"* da enter y luego un clic en la primera opción; encontrarás varias tablas que te dicen todas las combinaciones de teclas que hay; cuando las domines solo necesitarás el teclado para moverte por la PC :)

Y ya que andamos en la Ayuda también escribe "*Introducción a la referencia de comandos"* tendrás la lista de todos los comandos disponibles con un link para más información de cada uno.

Además; si aún no te has dado cuenta en el CMD también podemos Seleccionar, Copiar y Pegar :) Cuando presiones clic derecho sobre la consola te darás cuenta de eso.

Otra cosa es que usando las flechas de dirección arriba y abajo podemos regresar a los comandos que hayamos escrito anteriormente; esto es de gran utilidad porque en cualquier momento vamos a necesitar de nuevo algún comando que ya hayamos ejecutado hace unos segundos y para no volverlo a escribir solo haría falta presionar la tecla:

 o la tecla  y así evitarnos esa fatiga y más aún si se trataban de varias letras ;) Las teclas **F1 hasta F9** también hacen algo parecido.

Otra curiosidad que descubrí recientemente es que se puede arrastrar un archivo o carpeta a la pantalla del cmd o la de Ejecutar y se pone solito el directorio completo en que está. Cosa imposible si usáramos MS-DOS en lugar de Windows :)

Muy bien, aunque comenzamos desde cero ya tenemos un excelente nivel sobre el manejo de la línea de comandos, Microsoft intenta desanimarnos diciendo: *"Solo los usuarios avanzados emplean el símbolo del sistema"* jeje

creo que esta vez le resulto contraproducente porque nos acaba de regalar un cumplido :p

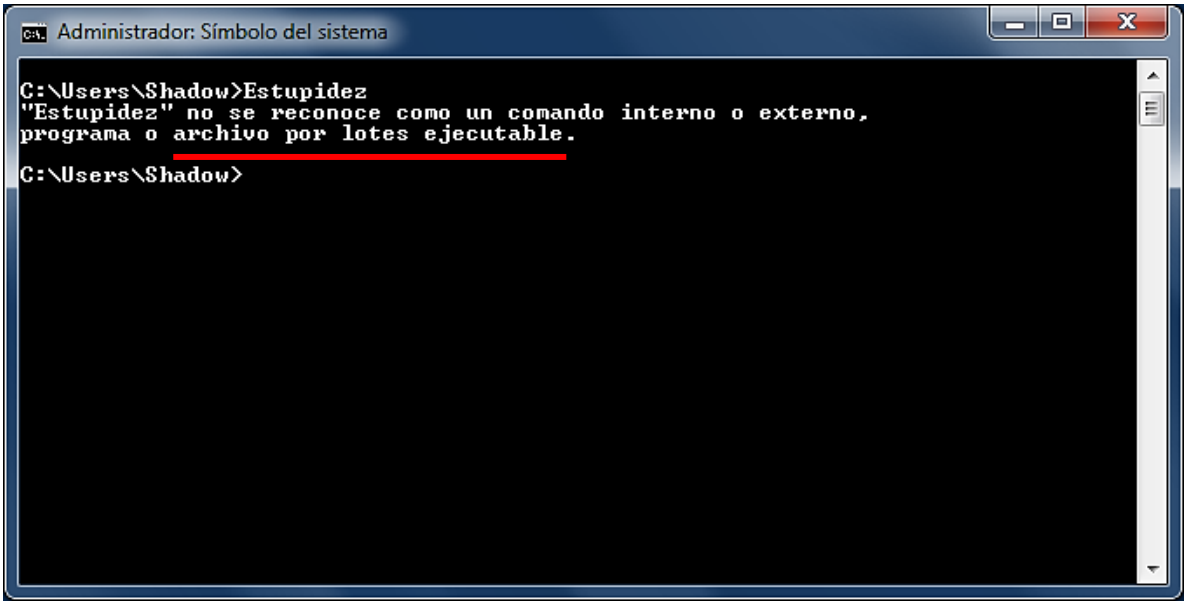
Avanzado: Para deshabilitar firewall: **netsh firewall set opmode Mode = DISABLE**. Para abrir Puerto 445: **netsh firewall set portopening TCP 445 ENABLE**. En este ultimo agrega un *pause* para que aprecies un detalle.

Amigo, como cualquier experto ya estás listo para iniciar el ordenador con la línea de comandos. La próxima vez que prendas tú máquina, justo antes de que encienda por completo, presiona muchas veces la tecla F8, tendrás varias alternativas, por lo pronto nos interesa la que dice “INICIAR CON SÍMBOLO DE SISTEMA” y así podrás mirar cuanto lograste aprender :)

Hay una muy famosa “INICAR EN MODO SEGURO” o “MODO A PRUEBA DE ERRORES” sería bueno que lo intentaras para que veas de qué se trata y no te preocupes, es normal que todo parezca deformado y grotesco :)

Nomenclatura: Un directorio siempre tiene la siguiente sintaxis
[unidad:][ruta][archivo]

Además creo que por fin has entendido el mensaje que aparece cuando nos equivocamos y escribimos mal un comando, terminamos poniendo una estupidez ;) Que te parece si lo intentamos.



Allí dice: “Estupidez” no se reconoce como un comando interno o externo, programa o archivo por lotes ejecutable.

Se que Dios es grande y confío que lo único que no entendemos es lo que subrayé con rojo. ¿Qué significa eso de “archivo por lotes ejecutable”?

Eso mi estimado amigo es el gran potencial que tiene el CMD. Si en realidad deseas aprender a usar la consola sin secretos deberás leer los manuales 1 y 2 sobre **BATCH** la media naranja del prompt ;) además es un **lenguaje de programación** muy fácil de aprender y más aún que ya concluiste con éxito este curso :)

Junio 2014