

Y sí, llegamos a nuestra clase 55. Hablando un poco de Windows, si llegan a tenerlo en el S.O. host que utilizan siempre, por favor actualicen que ha sido descubierta una vulnerabilidad muy grave y en estos días liberaron el parche. Los que lo tienen pirata y no pueden actualizar, nada, suerte :D.

# HDC

Bueno, definitivamente llegamos a la consola de comandos de Windows. Sé que este camino anterior entre resistencias, programación en C, y cracking parece no tener nada que ver pero en los cruces de todas estas cosas es cuando aparece el verdadero hacking.

**"Nos toca abrir la... pantalla negra de letras blancas ¿Verdad?"**

**Consola de comandos**, Manolo. Recuerden que para abrir ésta, tenemos que hacerlo desde el ejecutar y escribir **cmd** en ella. También pueden hacerlo desde el menú de accesorios o desde la ruta **C:/Windows/system32/cmd.exe**.

A screenshot of a Windows Command Prompt window. The title bar at the top reads "C:\Windows\system32\cmd.exe". The main area of the window is black with white text. The text displayed is: "Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation. All rights reserved. C:\Users\w7>". The window has standard Windows window controls (minimize, maximize, close) in the top right corner.

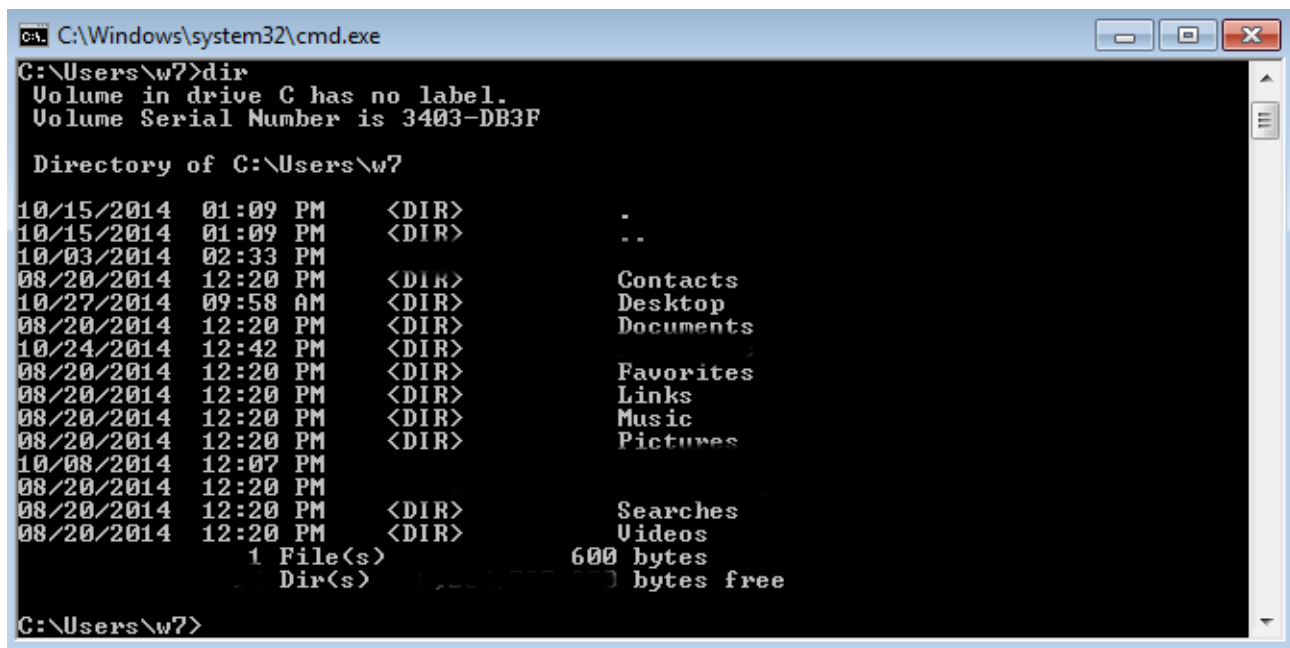
Aquí podemos escribir paparruchadas y que anden y parecer todo un hacker. Aunque podríamos

estar creando carpetas y eliminándolas, la gente se sorprende y como ve algo así piensa que es mega complejo, cuando muchas veces nos enfrentamos a cosas muy **simples** que puede realizar una abuela en silla de ruedas -¿o éso era para los deportes?-.

"**Mi abuela no está en silla de ruedas.**"

¿Qué hablás Manolo? Concentración, concentración.

El primer comando que veremos es el comando **dir**. Esta instrucción **imprime en pantalla** (imprime = muestra en este caso) una **lista** de todos los directorios y aplicaciones que se encuentran en el directorio en donde estemos parados. Como ven, antes de donde podemos escribir hay una ruta "**C:\Users\w7**" y es la que nos indica que estamos en el directorio del usuario w7, dentro de la carpeta **Users**, que está dentro del disco C.



```
C:\Windows\system32\cmd.exe
C:\Users\w7>dir
Volume in drive C has no label.
Volume Serial Number is 3403-DB3F

Directory of C:\Users\w7

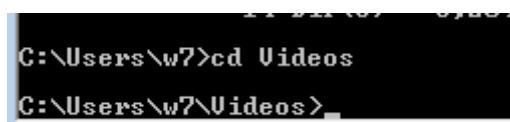
10/15/2014  01:09 PM  <DIR>          .
10/15/2014  01:09 PM  <DIR>          ..
10/03/2014  02:33 PM
08/20/2014  12:20 PM  <DIR>          Contacts
10/27/2014  09:58 AM  <DIR>          Desktop
08/20/2014  12:20 PM  <DIR>          Documents
10/24/2014  12:42 PM  <DIR>
08/20/2014  12:20 PM  <DIR>          Favorites
08/20/2014  12:20 PM  <DIR>          Links
08/20/2014  12:20 PM  <DIR>          Music
08/20/2014  12:20 PM  <DIR>          Pictures
10/08/2014  12:07 PM
08/20/2014  12:20 PM
08/20/2014  12:20 PM  <DIR>          Searches
08/20/2014  12:20 PM  <DIR>          Videos
                1 File(s)          600 bytes
                Dir(s)          bytes free

C:\Users\w7>
```

Yo tengo varias cosas, pero tapo algunas por seguridad.

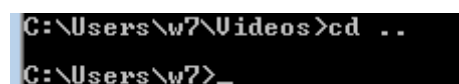
Y entre estas **carpetas** yo voy a querer **navegar** y para ésto usamos el comando **cd** (también puede ser **chdir**). Se usa poniendo primero el **comando** y luego el **parámetro** -que en este caso ese parametro es el próximo directorio.

Si hago **cd Videos** (ojo que acá se tiene en cuenta **mayúsculas** y **minúsculas**), vamos a ingresar a esa carpeta.



```
C:\Users\w7>cd Videos
C:\Users\w7\Videos>
```

Fíjense que cambio la ruta en donde estamos. Pero ¿si queremos ir para **atrás**? Bueno, en ese caso el parámetro es **".."**.



```
C:\Users\w7\Videos>cd ..
C:\Users\w7>
```

Y volvemos al mismo directorio que estábamos antes. Pero **cd** sirve para otra cosa. Si lo ejecutamos sin **ningun parámetro**, vamos a tener la **devolución** de cual es la **ruta del directorio** en el que estamos parados.

```
C:\Users\w7>cd
C:\Users\w7
C:\Users\w7>_
```

**"Pero ésto ya nos lo dice. No me sirve de mucha información adicional que digamos."**

Pasa, que luego veremos como automatizar las tareas con comandos y además existe un comando para cambiar el prompt de la consola (es decir, todo lo que aparece atras de lo que escribimos que por **defecto** es "**directorioEnElQueEstamos**>". Pero lo podríamos **cambiar** a "soyUnPezRadioactivo\$\$\$" o "soyManolo " y cualquier cosa que se les ocurra.

Así que tenemos el comando **prompt** -fácil de recordar-, que lo utilizaremos como **prompt parámetro**, donde el parámetro va a ser lo que aparezca. Escribamos "hola" como parámetro para hacer la **prueba**.

```
C:\Windows\system32\cmd.exe
C:\Users\w7>prompt hola
holaAca Escribo
'Aca' is not recognized as
operable program or batch
hola_
```

Nos quedó un poco feo y sin sabor. Vamos a ponerle algo como "H4x0r>\$"

```
holaprompt H4x0r>$
H4x0r_
```

No nos quedó como queríamos porque los **símbolos** como el espacio, el "\$" el ampersand y demases, se escriben de otra manera. Si buscamos un poco nos daremos con la **tablita**:

Character	Description
<b>Sq</b>	= (equal sign)
<b>SS</b>	\$ (dollar sign)
<b>St</b>	Current time
<b>Sd</b>	Current date
<b>Sp</b>	Current drive and path
<b>Sv</b>	Windows XP version number
<b>Sn</b>	Current drive
<b>Sg</b>	> (greater-than sign)
<b>Sl</b>	< (less-than sign)
<b>Sb</b>	(pipe)
<b>S_</b>	ENTER-LINEFEED
<b>Se</b>	ANSI escape code (code 27)
<b>Sh</b>	Backspace (to delete a character that has been written to the prompt command line)
<b>Sa</b>	& (ampersand)
<b>Sc</b>	( (left parenthesis)
<b>Sf</b>	) (right parenthesis)
<b>Ss</b>	space

Y ahora sé que el comando debería ser "H4x0r\$g\$\$". Veamos si funciona:)

```
H4x0r prompt H4x0r$g$$
H4x0r>$
```

Excelente. Igualmente para el curso voy a dejarlo como viene por **defecto** para comodidad de visión de ustedes y no tener que desorientarlos tanto. Para esto, usamos el comando **prompt sin parámetros**, y vuelve a su configuración por defecto.

```
H4x0r>$ prompt
C:\Users\w7>
```

Como en realidad la idea de esta consola es que podamos hacer todo lo mismo como si tuviésemos interfaz gráfica, tenemos **todo tipo de comandos**. La instrucción **copy** (se usa **copy loQueQueremosCopiar aDondeQueremosCopiarlo**) nos sirve perfectamente. Hagamos una prueba. Yo hice un fichero de texto para poder copiarlo a la carpeta **Links**.

```
C:\Users\w7>copy prueba.txt Links
1 file(s) copied.

C:\Users\w7>dir Links
Volume in drive C has no label.
Volume Serial Number is 3403-DB3F

Directory of C:\Users\w7\Links

11/13/2014  10:05 AM    <DIR>          .
11/13/2014  10:05 AM    <DIR>          ..
08/20/2014  12:20 PM                Desktop.lnk
08/20/2014  12:20 PM                Downloads.lnk
11/13/2014  10:05 AM                0 prueba.txt
08/20/2014  12:20 PM                RecentPlaces.lnk
              4 File(s)              1,606 bytes
              2 Dir(s)    8,202,223,616 bytes free

C:\Users\w7>_
```

¡Ah, sí! Casi me olvidaba. Con el comando **dir** seguido de un **directorio** cualquiera, nos **lista** las cosas que hay allí. :)

La cosa es que si queremos **copiar** una **carpeta** o **directorio**, debemos hacerlo de la misma manera pero con el comando **xcopy**.

Otro comando que tenemos es **rename** o **ren** y un **parámetro** que puede ser un fichero o directorio y un segundo parámetro que es el nombre que va a reemplazar al original.

```
C:\Users\w7>ren Links Linksrenombrado

C:\Users\w7>dir
Volume in drive C has no label.
Volume Serial Number is 3403-DB3F

Directory of C:\Users\w7

11/13/2014  10:20 AM    <DIR>          .
11/13/2014  10:20 AM    <DIR>          ..
11/13/2014  09:52 AM
10/03/2014  02:33 PM
08/20/2014  12:20 PM    <DIR>          Contacts
10/27/2014  09:58 AM    <DIR>          Desktop
08/20/2014  12:20 PM    <DIR>          Documents
10/24/2014  12:42 PM
08/20/2014  12:20 PM    <DIR>          Favorites
11/13/2014  10:05 AM    <DIR>          Linksrenombrado
08/20/2014  12:20 PM    <DIR>          Music
```

Ahí lo hice con la carpeta Links para que vean como quedó.

Si queremos. Podemos **limpiar la consola** con **cls** -es la abreviación de clear screen-. Volviendo a cero como si no hubiésemos hecho nada.

Siguiendo con los comandos simples, el comando **del** (o **erase**) elimina un **archivo** que nosotros queramos poniendo este archivo como **único parámetro** del comando.

```
C:\Users\w7>del prueba.txt
C:\Users\w7>
```

El tema es que si lo hacemos hacia una carpeta, éste sólo elimina los archivos que se encuentran dentro de ese directorio, pero la carpeta en sí la deja sana y coleando.

Vamos a crear una carpeta. Esto lo hacemos con el comando **md** o **mkdir** (seguramente la abreviación de make dir) y un parámetro que será el nombre de la carpeta.

```
C:\Users\w7>md hola
C:\Users\w7>dir
Volume in drive C has no label.
Volume Serial Number is 3403-DB3F

Directory of C:\Users\w7

11/14/2014  09:52 AM    <DIR>          .
11/14/2014  09:52 AM    <DIR>          ..
11/13/2014  09:52 AM
10/03/2014  02:33 PM
08/20/2014  12:20 PM    <DIR>          Contacts
10/27/2014  09:58 AM    <DIR>          Desktop
08/20/2014  12:20 PM    <DIR>          Documents
10/24/2014  12:42 PM    <DIR>
08/20/2014  12:20 PM    <DIR>          Favorites
11/14/2014  09:52 AM    <DIR>          hola
11/13/2014  10:05 AM    <DIR>          Linksrenombrado
08/20/2014  12:20 PM    <DIR>          Music
```

Para borrarla, dijimos que el comando **del** no iba, pero queremos borrar a esa maldita del mapa. Para ésto, usamos **rd** o **rmdir**. Aclaro que para poder eliminarlo, el directorio tiene que estar vacío (aquí es donde si lo combinamos con el anterior comando podemos borrar una carpeta con las cosas de adentro).

```
C:\Users\w7>rd hola
C:\Users\w7>dir
Volume in drive C has no label.
Volume Serial Number is 3403-DB3F

Directory of C:\Users\w7

11/14/2014  09:55 AM    <DIR>          .
11/14/2014  09:55 AM    <DIR>          ..
11/13/2014  09:52 AM
10/03/2014  02:33 PM
08/20/2014  12:20 PM    <DIR>          Contacts
10/27/2014  09:58 AM    <DIR>          Desktop
08/20/2014  12:20 PM    <DIR>          Documents
10/24/2014  12:42 PM
08/20/2014  12:20 PM    <DIR>          Favorites
11/13/2014  10:05 AM    <DIR>          Linksrenombrado
08/20/2014  12:20 PM    <DIR>          Music
```

Bueno, lo voy dejando acá. Vayan practicando para que no se les olviden los comandos. La próxima lo mataré un poco más.

-----  
Pueden seguirme en Twitter: [@RoaddHDC](https://twitter.com/RoaddHDC)

Cualquier cosa pueden mandarme mail a: [r0add@hotmail.com](mailto:r0add@hotmail.com)

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

Roadd.  
-----

**Este tutorial puede ser copiado y/o compartido en cualquier lado siempre poniendo que es de mi autoría y de mis propios conocimientos.**