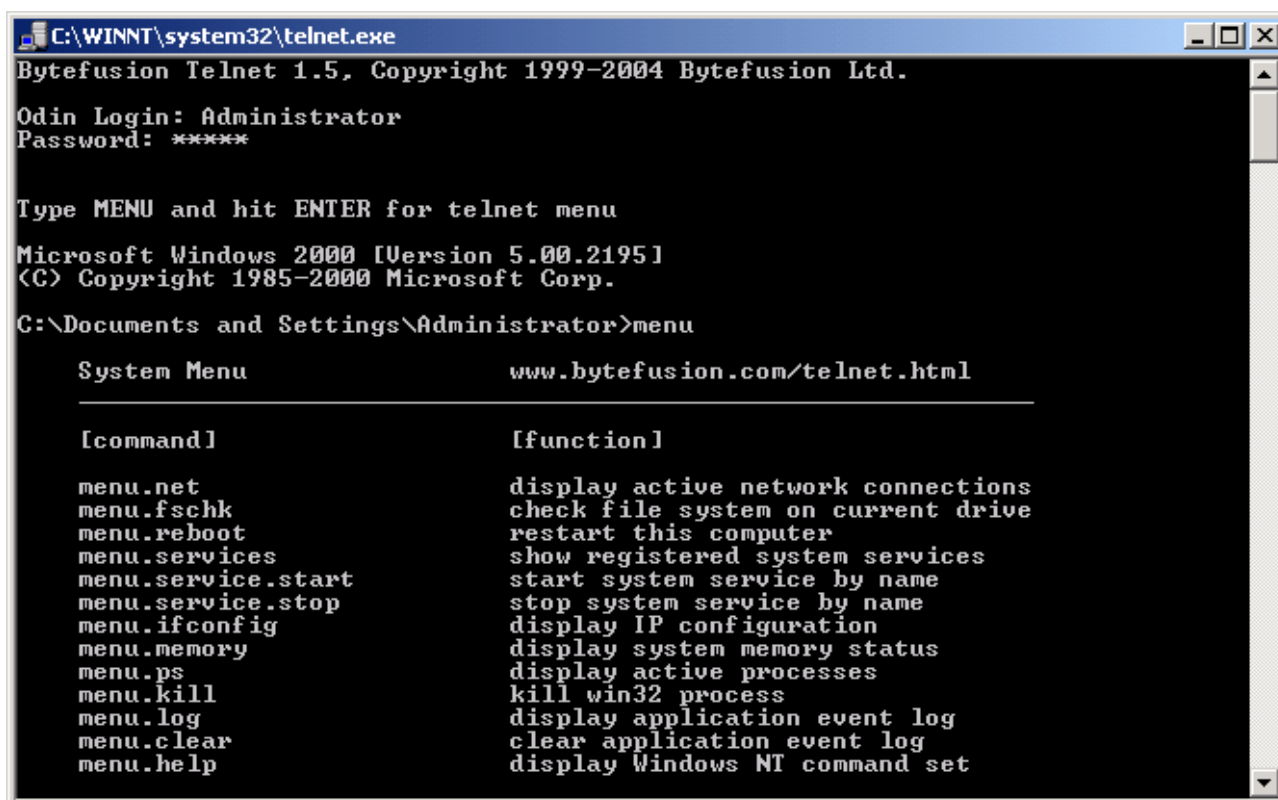


Antes de empezar les comento que estamos avanzando con la nueva web y aunque faltan unos cuantos detalles, aquí es lo que vamos haciendo [clases.hackingdesdecero.org](http://clases.hackingdesdecero.org). Allí podrán descargar todas las clases y también ejercicios resueltos hechos por el alumno Rollth -que prácticamente es parte del staff-.) Vayan comentando que tal les parece.

# HDDC

¿Cómo andan? Hemos llegado a ver el servicio de **Telnet**. Para los que no lo conocen, se los presento:



```
C:\WINNT\system32\telnet.exe
Bytefusion Telnet 1.5, Copyright 1999-2004 Bytefusion Ltd.
Odin Login: Administrator
Password: *****

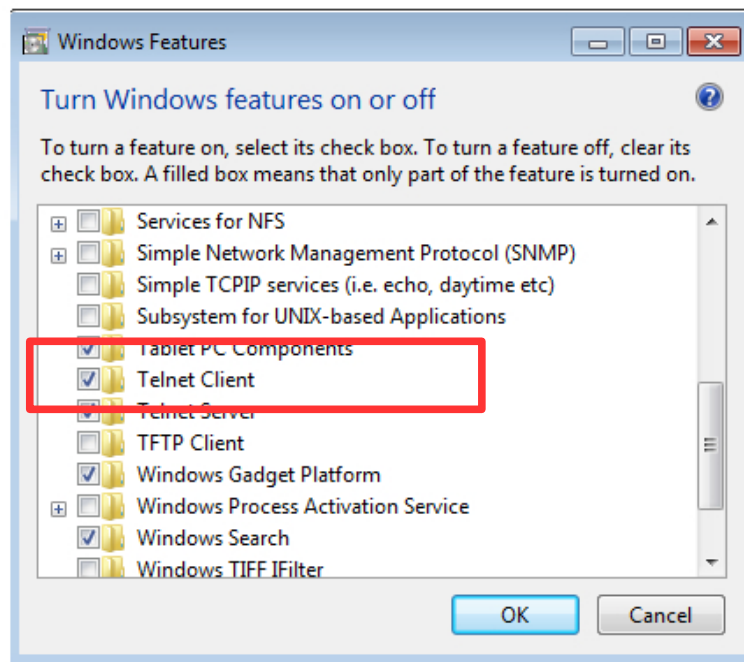
Type MENU and hit ENTER for telnet menu
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
C:\Documents and Settings\Administrator>menu

System Menu                               www.bytefusion.com/telnet.html
-----
[command]                                  [function]
menu.net                                   display active network connections
menu.fschk                                 check file system on current drive
menu.reboot                                restart this computer
menu.services                              show registered system services
menu.service.start                         start system service by name
menu.service.stop                          stop system service by name
menu.ifconfig                              display IP configuration
menu.memory                                display system memory status
menu.ps                                    display active processes
menu.kill                                   kill win32 process
menu.log                                    display application event log
menu.clear                                 clear application event log
menu.help                                  display Windows NT command set
```

Así de feo es, **sin gráficos lindos**. Pero ya los vengo amoldando a la idea de esta pequeña

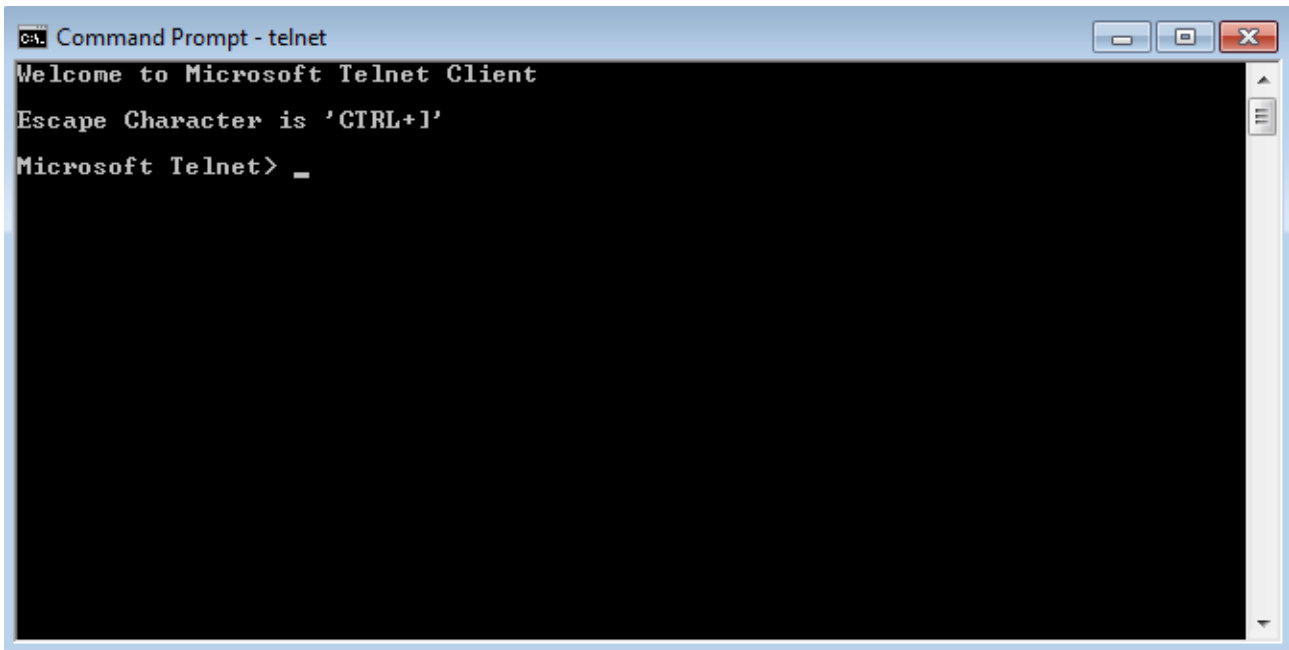
ventana y le agarrarán el gusto, y dejarán los gráficos bonitos para los **muggles** :). **Telnet** es una **aplicación** -en realidad es un **protocolo**, pero el protocolo se llama así por la aplicación- que nos permite conectarnos a **otro ordenador** de manera **remota** y **controlarla** desde donde estemos -...y las ideas malvadas aparecen-. El servicio se utilizaba para poder ser un administrador de sistemas y no tener que viajar a todos lados en razón de hacer su trabajo.

**En resumen: Telnet, control remoto.** Saltemos a la parte **práctica**. Ésto no sera ni largo ni demasiado entretenido pero debemos aprenderlo.

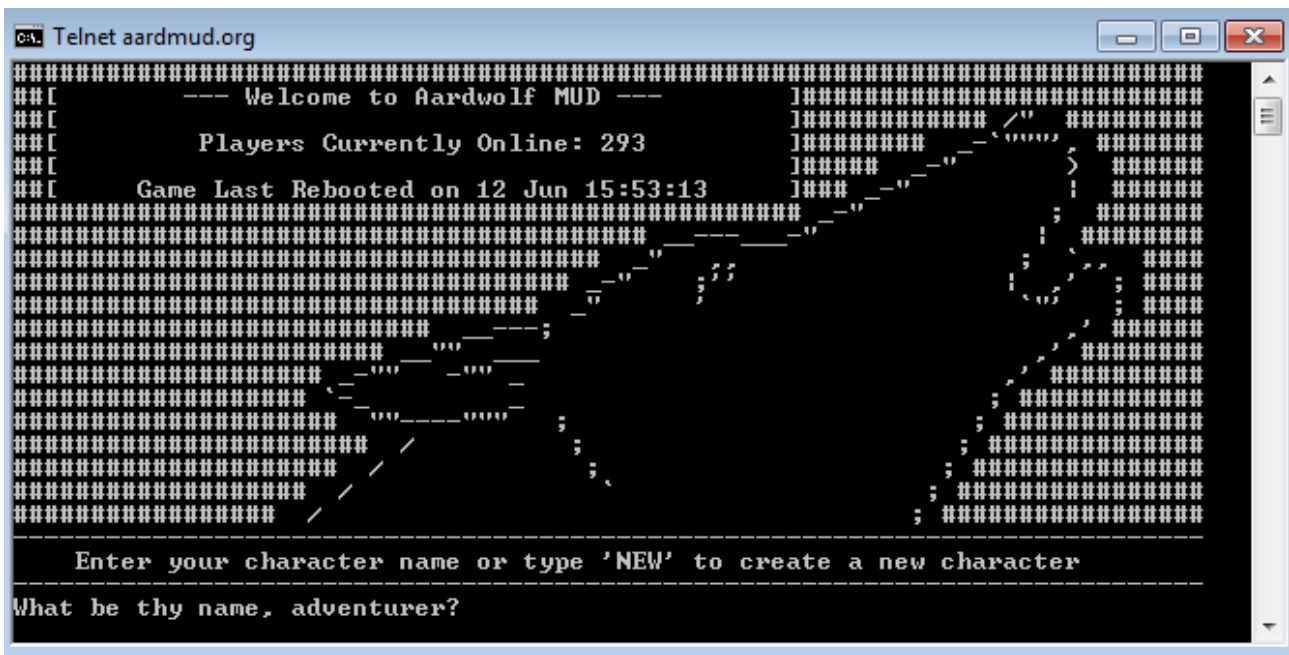


Primero debemos activarlo desde las opciones de Windows, vamos a **“Desinstalar o cambiar un programa”** → **“Activar o desactivar las características de Windows”** y le ponemos tilde a la opción **“Telnet Client”** o **“Cliente Telnet”**.

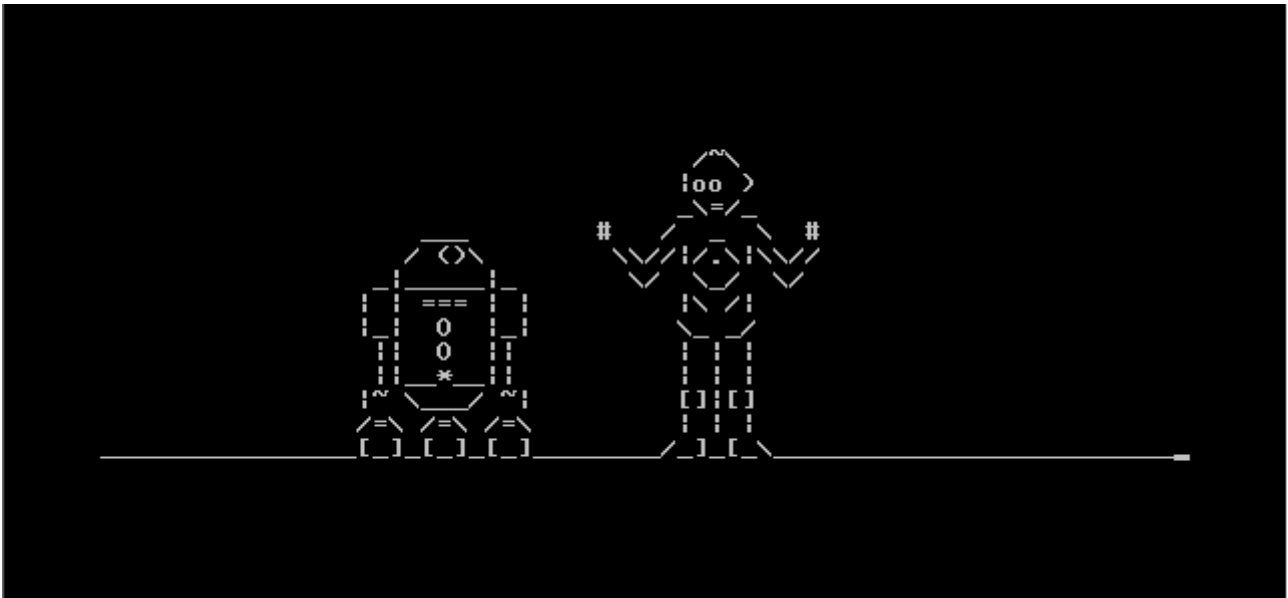
Si entramos a la línea de comandos y escribimos **“Telnet”**, nos abrirá el cliente para que podamos interactuar.



Para hacer una prueba, tenemos por ejemplo a “aardmud.org”, correspondiente a un **juego MUD**. Veamos de qué va la cosa. Para abrir, simplemente usamos el comando **open <Dirección server>**.



Es impresionante que con una simple pantalla con caracteres puedan hacer cosas gráficas como éstas. Es un gran juego, en inglés. Si tienen ganas, pueden probarlo aunque sea como experiencia. Hay muchas como ésta pero otra, que se ha hecho viral fue la presentación de Star Wars. La dirección es **towel.blinkenlights.nl**.



Otra de las cosas que podemos hacer es **pedir una web**. Para ésto, abrimos por ejemplo “[www.telnet.org](http://www.telnet.org)”, pero recuerden que el **puerto** de los servidores web es el número **80**. Por suerte, Telnet te deja personalizar el puerto (**por defecto era el 25**), de manera que el comando queda “**open <direccion server> <puerto>**”. Lo mas posible es que una vez que se conecte quede un cursor con la pantalla en negro, y que cuando escriban no vean lo que estan tipeando. No importa, vamos a escribir igual **-ojo** con error a las teclas-. Para hacer el **request** de una página lo hacemos mediante el comando **GET**. Hagamos “**GET /htm/places.html**” y debería darnos en respuesta, el **código html** de la página web -que digamos es la manera en como se distribuye el contenido-. Debería ser algo así:

```
HTTP/1.1 200 OK
Date: Mon, 13 May 2013 13:19:02 GMT
Server: Apache/2.4.2 (Win32) OpenSSL/1.0.1c PHP/5.4.4
Last-Modified: Fri, 21 Dec 2007 02:01:16 GMT
ETag: "ca-441c240f37300"
Accept-Ranges: bytes
Content-Length: 202
Connection: close
Content-Type: text/html

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
  <head>
    <title></title>
  </head>
  <body>
    <h1>It works!</h1>
  </body>
</html>

Connection to host lost. Hacking-tutorial.com
```

Bien ordenado, y con información como cuál es la **version** de **Web Server** que están utilizando (muy útil para saber a qué estaremos atacando). Aunque en mi caso me devolvió algo no tan lindo xD.

```
ca: Telnet telnet.org
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that
this server could not understand.<br />
</p>
<hr>
Server at files.garzapost.com Port 80</address>
<address>Apache/2.2.22 (Ubuntu)</address>
</body></html>

Connection to host lost.
-
```

Igualmente tenemos buena **información** y hasta encuentro al lado del nombre del web server, el nombre del **sistema operativo**. Interesante. Lo importante es que podamos entender que Telnet puede hacer **más que controlar una pc** a distancia en donde simplemente tiene una línea de comandos remota. También les aclaro que en realidad ya no se usa para ese fin (por eso no lo agregue a la clase), porque en reemplazo está **SSH**. Ya veremos más adelante la ventaja de cada uno.

-----  
**Pueden seguirme en Twitter: @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.**