TUTORIAL DE PROGRAMACION BATCH!!

ESTE DOCUMENTO PDF FUE POSTEADO POR EL ADMINISTRADOR DE HACKXCRACK, EYES

POR PETICION DE ALGUNOS USUAROS DEL FORO, DEJO EL TUTORIAL EN UN ARCHIVO DESCARGABLE, PARA AQUELLOS QUE NO POSEEN UNA COMPUTADORA PROPIA PARA LEERLO SDIRECTAMENTE DESDE ALLI!!

---

1. **Introducción**

Las siglas BAT caracter??sticas de los guiones en entorno MSDOS provienen del hecho de que son procesos BATCH. En Msdos los nombres de los archivos pod??an tener hasta 8 letras para el nombre y tres letras para la extensi??n. Dado que solo se dispon??a de tres letras para identificar la clase de archivo se opt?? por poner BAT (aunque a partir de Windows 2000 tambi?©n se puede usar CMD).

Las siglas BAT caracter??sticas de los guiones en entorno MSDOS provienen del hecho de que son procesos BATCH. En Msdos los nombres de los archivos pod??an tener hasta 8 letras para el nombre y tres letras para la extensi??n. Dado que solo se dispon??a de tres letras para identificar la clase de archivo se opt?? por poner BAT (aunque a partir de Windows 2000 tambi?©n se puede usar CMD).
Los proceso batch son nativos de MVS/DOS y VSE/DOS que suelen funcionar con JCL. RPG es un lenguaje basado ??ntegramente en la metodolog??a batch.

Desde entonces cada sistema operativo que ha salido ha inclu??do un sistema de scripting. Los grandes sistemas se quedaron con JCL/JOBS mientras que la aparici??n de UNIX, MINIX y dem??s empezaron a utilizar una shell diferente y mas interactiva con un espacio de consola para los usuarios y un lenguaje apropiado para administrar la estaci??n (esto no era necesario en MVS o VSE porque el usuario actuaba sobre pantallas tontas 3270) Se llam?? shell y se conoce habitualmente como sh. Posteriormente salieron otras entre las cuales est?? bourne shell again conocida como bash.

Microsoft hizo una para su sistema operativo que copi?? descaradamente de bash. Invirti?? la barra para identificar el path correcto a un archivo y adapt?? el lenguaje a un sistema operativo monousuario e incapaz de trabajar en red. Este es el lenguaje BAT. Con los a?±os microsoft se ha visto obligado a modificarlo considerablemente (sobre todo los comandos de entorno de red) dadas las muchas limitaciones que ten??a. A??n hoy es incre??blemente pobre en comparaci??n con las de otros sistemas operativos. El lenguaje bat es un complemento en windows y no una parte fundamental como en los dem??s.

2. ¨¯Qu?© se puede hacer con ellos?

Pues se puede hacer de forma automatizada todo aquello que se pueda hacer en la consola de msdos. Se pueden ejecutar programas, enviar y recibir par??metros y automatizar tareas

2.

3. Creaci??n de un programa.BAT

Pues son texto plano. Quiere eso decir que se pueden escribir en el block de notas, utilidad Edit de msdos o alg??n editor ascii.

Al guardarlos deben tener la notaci??n de nombres propia de msdos. Esto es un nombre con m??ximo 8 letras (espacios y \ no permitidos), luego un punto y la extensi??n que en este caso es obligatoriamente BAT (para compatibilidad con todas las versiones windows) o CMD (a partir de Windows 2000).

Para crearlos desde la misma consola puedo utilizar varios sistemas
Mediante la orden COPY

copy con: nombre_de_archivo.bat Orden de creaci??n de archivo con el nombre 'nombre_de_archivo.bat'
...
...
comandos ??rdenes a ejecutar
...
...
Ctrl + Z Fin y grabaci??n del archivo en el directorio actual

M?©todo 2 mediante la redirecci??n
echo 1¨? l??nea a insertar >nombre_de_archivo.bat Se graba el fichero 'nombre_de_archivo.bat con la primera orden a ejecutar
echo restantes l??neas >>nombre_de_archivo.bat Se a?±ade la segunda orden
echo restantes l??neas >>nombre_de_archivo.bat Se a?±ade la tercera orden ...

En cualquier caso para modificarlos podemos utilizar la utilidad Edit de msdos (abriendo el archivo concreto y luego grabando los cambios) o el bloc de notas.

Redirecci??n de entrada/salida

Pues al igual que en Unix se puede hacer que la salida de un comando sirva como entrada de otro. Cada proceso tiene ya predeterminados sus dispositivos de entrada y salida. Mediante la redirecci??n podemos cambiar eso.

DISPOSITIVO	SALIDA
CON	Salida por la pantalla
PRN	Salida por la impresora por defecto
LPT1	Salida por la 1¨? impresora en paralelo
COM1	Salida por el primer puerto serie
COM2	Salida por el segundo puerto serie

As??, si ejecuto la orden 'dir' la orden saldr?? en su dispositivo por defecto (CON) y ver?© el resultado por pantalla
Para redireccionar se utilizan los operadores < y > que sirven para indicar que salida debe ir a que lugar
Por ejemplo si yo quiero redireccionar la salida estandar de dir para que en vez de ir a la pantalla vaya a la impresora har?©
dir >prn
Con lo que la salida natural del comando DIR en vez de ir a su sitio natural (la pantalla) ir?? a la impresora por defecto.

5. Filtros

Los filtros son ??rdenes que sirven para formatear la salida del comando de acuerdo a nuestros intereses. Se utilizan mediante la barra vertical (Alt 124).
El filtro SORT sirve para ordenar la salida
DIR | SORT
El filtro MORE sirve para pausar la salida cada pantalla para que pueda ver todos los datos de salida con tranquilidad. Pasa de pantalla a pantalla al pulsar una tecla.
DIR | MORE

6. M??scaras y comodines

Para seleccionar varios archivos a la hora de realizar una determinada operaci??n existe la posibilidad de utilizar m??scaras. Estas m??scaras utilizan los caracteres comodines para describir que archivos deben verse afectados. Para ello y teniendo en cuenta que los nombres de los archivos deben cumplir la notaci??n de msdos (8 letras sin espacios como m??ximo, luego un punto y tres letras como m??ximo de extensi??n) se pueden utilizar los llamados comodines.
*** Equivale a varios caracteres**
? equivale a un solo carácter.

EJEMPLOS:

```
      *.cfg      seleccionar todos los archivos que tengan la extensi??n cfg

 a*.cfg  seleccionar todos los archivos que comienzen por a y tengan la extensi??n
cfg


 a*b.cfg         seleccionar todos los archivos que comienzen por a, acaben por b y
tengan la extensi??n cfg


 *asa*.cfg       seleccionar todos los archivos que contengan 'asa' y tengan la
extensi??n cfg


 c?asa.cfg       seleccionar todos los archivos que contengan una C, luego un
caracter cualquiera y luego 'asa'. Debe tener tambi?©n la extensi??n cfg


 c?b*.*  seleccionar todos los archivos que empiezen por c, tengan un caracter
cualquiera, luego una b y cualquier extensi??n


 *.b?t   seleccionar todos los archivos que tengan una extensi??n que empieze por
b, luego un caracter cualquiera y luego una t.
```

7. **Trayectos (paths)**

   La trayectoria es el nombre completo de un archivo e indica la situaci??n exacta de un archivo y su nombre.

   leeme.txt el archivo se llama indico su nombre, pero nada mas. Se da por supuesto que se encuentra en el directorio actual.
   c:\leeme.txt el archivo que me interesa se llama leeme.txt y se encuentra en el directorio ra??z de C.

   Dado que en msdos no se admiten nombres largos (mas de 8 letras) ni espacios, cuando quiero utilizar un nombre de windows en msdos debo saber que este ser?? reconvertido a su nombre corto. Este se obtiene a?±adiendo los seis primeros car??cteres v??lidos del nombre, luego el signo ~ (alt 126) y luego un n??mero.

De esta forma un archivo que se encuentre en Mis documentos en win98 tendr?? el path

c:\misdoc~1\leeme.txt
Y en Windows 2000/XP

c:\Docume~1\Usuario\misdoc~1\leeme.txt
Tambi?©n se pueden utilizar (mientras las comillas para delimitar el nombre

"c:\Mis Documentos\leeme.txt"
Esta ser??a la trayectoria de mimusica.mp3 (en Mis Documentos en Win 98)

c:\misdoc~1\mi~1\mimusica.mp3
Qu?© equivale a
"c:\Mis Documentos\Mi M??sica\mimusica.mp3"

8. Unidades L??gicas

Siempre es una letra seguida del signo dos puntos.

- **A: = disquetera**
- **B: = reservada para segunda disquetera**
- **C: = primera partici??n (normalmente es la que arranca)**
- **D: = segunda partici??n (generalmente el cdrom)**

Por eso si se crea una unidad l??gica mediante netbios en windows, esta puede tener un nombre msdos para poder acceder a ella desde la consola. La letra que se asigne no puede corresponder a una unidad l??gica existente.

Comandos MSDOS

Los comandos en msdos tienen las siguientes caracter??sticas:
a) el formato general es COMANDO [OPCIONES] [ARGUMENTOS]
b) Da igual que se usen may??sculas o min??sculas
c) Los argumentos y opciones se separan por espacios

9.1 Comandos b??sicos de consola

9.1.1 CLS

Borra la pantalla (viene de CLear Screen) ^^

9.1.2 Echo [par??metros]

Tiene varias posibilidades:

- **ECHO sin par??metros saca el estado en que se encuentra la variable echo (on u off)**
- **ECHO ON activa el echo (como en un terminal TTY) por lo que los comandos se ver??n en pantalla y luego su resultado**
- **ECHO OFF desactiva el comando echo y ya se ver??n los resultados de la ejecuci??n del comando, pero no el comando en s?? mismo**
- **ECHO LITERAL saca por pantalla el literal. Por eso al hacer echo literal >fichero.bat estamos redirigiendo la salida de echo literal (que tendr??a que salir por la pantalla) al archivo fichero.bat.**

9.1.3 Pause [mensaje]

Sirve para sacar un mensaje y parar la ejecuci??n hasta que se pulse una tecla

9.1.4 Prompt [par??metros]

Sirve para cambiar el prompt de msdos.
$p Mostrar el trayecto actual
$g Mostrar el separador >
$l Mostrar el separador <
$b Mostrar el separador |
$q Mostrar el separador =
$$ Mostrar el separador $
$t Mostrar la hora
$d Mostrar la fecha
$v Mostrar la versi??n del sistema
$n Mostrar la unidad actual
$h Retroceso. Borra el caracter previo
**$e Escape. Muestra el caracter **
$_ Retorno de carro y salto de l??nea (equivale a chr 10 y chr 13 ascii

Por eso si ponemos prompt pg el cursor muestra la trayectoria donde estamos y luego el separador

Es posible a?±adir texto (por ejemplo prompt Mi_nombre pg

9.1.5 Date [fecha]

Ver/poner la fecha del sistema

9.1.6 Time [hora]

Ver/poner hora del sistema

9.1.7 Ver

Versi??n del sistema

9.1.8 Vol [Unidad]

Volumen de la unidad especificada.

9,1,9Path [trayecto]

Indica un trayecto por defecto si se produce una petici??n de un archivo que no est?? en el directorio actual.
Por eso en windows 98 suele haber una l??nea en autoexec.bat que es
path c:\windows; c:\windows\command que indica que si se solicita un ejecutable que no est? © en el directorio actual, lo busque primero en la carpeta windows y luego en la subcarpeta command.

En Windows 2000 y XP no se utiliza autoexec.bat pero se existe una variable del sistema llamada PATH.

9,10KEYB c??digo_pais,juego_de_caracteres,definici??n_de_teclado,

El c??digo de pa??s de espa?±a es el 'sp'
El juego de caracteres aplicable a espa?±a es el 850 ?? 437
El archivo de definici??n de teclado es keyboard.sys
Para configurar un teclado en espa?±ol
keyb sp,,c:\windows\command\keyboard.sys

9.1.11 SYS [unidad]

Transfiere el sistema operativo msdos a la unidad especificada.

9.1.12 DOSKEY

Muestra los comando utiliados anteriormente al pulsar la tecla arriba del teclado.

9.1.13 MEM [par??metros]

Muestra la memoria usada y libre en el sistema
/p Muestra por programas
/d por programas y controladores
/c por tama?±o

9.2 Comandos de manejo de archivos

9.2.1 COPY [opciones] [origen] [destino]

Sirve para copiar archivos de un lugar a otro. el origen debe ser un trayecto completo de donde est??n los archivos a copiar. Si se omite se entiende que en el directorio actual.
El destino debe ser una trayectoria completa de donde dejar el/los archivo(s)
copy miarchivo.txt c:\ copiarlo al directorio ra??z de C
copy miarchivo.txt c:\miarch.txt copiarlo y adem??s cambiarle el nombre a miarch.tx
copy *.txt a:\ copiar todos los archivos que tengan la extensi??n txt a la unidad A
copy *.txt c:\misdoc~1 copiar todos los archivos que tengan la extensi??n txt al directorio Mis documentos (cuyo nombre corto es misdoc~1).

Tambi?©n se pueden concatenar archivos
copy archivo1.txt+archivo2.txt c:\archivo3.txt Unir archivo1.txt y archivo2.txt y dejarlo en archivo3.txt en C:

Las opciones son
/A Tratar el archivo como un archivo ASCII
/B Tratar el archivo como un archivo binario
/D Permite que el archivo destino se grabe descifrado
/V Verifica la copia
/N Al copiar usa el nombre corto en vez del nombre largo
/Y Suprime la pregunta de confirmaci??n si se va a sobreescribir alg??n archivo
/Z Copia archivos de red en modo reiniciable
/S Copia subdirectorios
/E Crea subdirectorios en el destino aunque los subdirectorios originales est?©n vac??os.

Se pueden guardar estos valores por omisi??n en la variable de entorno COPYCMD (solo a partir de Windows 2000).

9.2.2 DEL [opciones] [archivo]

Borra archivos
/P Pide confirmaci??n en cada caso
/F Modo force. Borra incluso los archivos de solo lectura
/S Borra tambi?©n los subdirectorios.
/Q Modo silencioso. No pide confirmaci??n en ning??n caso

9.2.3 MKDIR o MD [directorio]

Crear directorio

9.2.4 RMDIR o RD [directorio]

Borra un directorio. El directorio debe estar vac??o

9.2.5 CHDIR o CD [path]

Cambia al directorio indicado.
CD "c:\archivos de programa" Trasladarse al directorio Archivos de programa
CD .. Trasladarse al directorio superior
CD \ Trasladarse al ra??z

9.2.6 DIR [opciones][trayecto]

Saca una lista del contenido del directorio especificado en el trayecto. Si no se especifica nada, se entiende el actual.
Si se pone como par??metro /W saca un listado resumido.
Si se pone como par??metro /P saca un listado utilizando el filtro more.

9.2.7 ATTRIB [/S] [archivo]

Muestra los atributos de los archivos indicados y en su caso permite cambiarlos.

Con el par??metro /S busca tambi?©n en subdirectorios.

Los atributos son:
H -> oculto. Se activa con +h y desactiva con -h
R -> Lectura. Solo lectura con +r, normal con -r
S -> Sistema. Se activa con +s y desactiva con -s
A -> Modificado. Para copias de seguridad incrementales. +a indica modificado y -a indica no modificado.
ATTRIB archivo.txt Muestra los atributos de ese archivo
ATTRIB -r archivo.txt Pone el atributo solo lectura a archivo.txt

Attrib miarchivo.txt (mostrar los atributos de miarchivo.txt)
attrib *.exe +r +r +s (pone a todos los archivos con extensi??n exe como ocultos, del sistema y read only)

9. RENAME o REN [Nombre_antiguo] [Nombre_nuevo]

Renombra un archivo.

Si se ponen m??ltiples archivos todos se renombran mediante la misma regla
REN *.txt *.bak Renombra todos los archivos TXT a BAK

9.2.9 TYPE fichero

Muestra el fichero. Se suele utilizar con el filtro MORE si se desea que se vea paginado
type archivo.txt | more

o bien con redirecci??n a la impresora para imprimirlo
type archivo >prn

9.3 Comandos de disco

9.3.1 Diskcopy [origen] [destino]

Copia un disquete completo de origen a destino
diskcopy a: a: copia un disquete de unidad A a la unidad A
diskcopy a: b: copia un disquete de unidad A a la unidad B

9.3.2 Fdisk [/mbr]

Utilidad para gestionar las particiones de un disco.

Con el par??metro /mbr se puede borrar el mbr (Master Boot Record) de un disco

9.3.3 Format [/s] [/a]

Formatear disquetes.

Con el par??metro /s se transfiere adem??s el sistema operativo (v??lido para win98 y anteriores)

Con el par??metro /a se realiza un formateo r??pido.

9.3.4 label [unidad][etiqueta]

Poner etiqueta a un volumen
label a: copia Poner etiqueta copia en el disquete
label c: DiscoDuro Poner etiqueta DiscoDuro al disco duro

9.3.5 Mscdex [/d:montaje]

Monta un cdrom o dvd ya configurado mediante un driver de dispositivo. El punto de montaje es el especificado en config.sys en el driver de dispositivo.

V??lido en Win98 y anteriores

9.3.6 Scandisk [unidad] [/autofix] [/scanonly] [/surface]

Comprueba la integridad de un disco en Windows 98 y anteriores.

Con el par??metro autofix repara autom??ticamente los errores encontrados.

Con el par??metro scanonly solo comprueba el disco y muestra estad??sticas

Con el par??metro Surface realiza una comprobaci??n de superficio del disco

9.4 Comandos de red

9.4.1 ARP [opciones]

Ver/Modificar la tabla de ARP.
arp -aMuestra la tabla de arp
apr -s IP mac Agrega una entrada a la tabla de arp

9.4.2 FTP

Cliente ftp de windows

9.4.3 IPCONFIG [Par??metros]

Mostrar los par??metros de conexi??n tcp/ip

ipconfig /all muestra toda la informaci??n de configuraci??n
/release adaptador libera la ip del adaptador especificado
/renew adaptador renueva la ip para el adaptador especificado
/flushdns purga la cach?© de resoluci??n de dns
/registerdns actualiza las conexiones dhcp y vuelve a registrar los nombres dns
/displaydns muestra el contenido de la cache de resoluci??n dns

9.4.4 NBTSTAT [opciones]

Hace un estado de la red por netbios
nbtstat -a Lista la tabla de nombres por nombre
nbtstat -A Lista la tabla de nombres por IP
nbtstat -c Lista la cach?© nbt mostrando nombres y direcciones IP
nbtstat -n Lista los nombres netbios locales
nbtstat -r Lista de nombres resueltos por difusi??n y WINS
nbtstat -R Purgar y recargar la cache nbt
nbtstat -S Lista las sesiones con las IP de los destinos
nbtstat -s Lista las sesiones con los nombres de los destinos

9.4.5 Net [opciones]

Conmando para acceder a dominios, crear/quitar sesiones netbios, montar unidades netbios, ...

Algunos comandos tambi?©n funcionan en win9X, pero a partir de Win2k se a?±adieron muchos par??metros nuevos.

Tiene muchas posibilidades y se usa siempre con par??metros. Los par??metros son: Servicios

net start X Inicia el servicio X
net stop X Termna el servicio X
net config server Muestra/modifica servicios.
/hidden=yes/no indica si el servidor debe mostrarse en la lista de ordenadores. Se corresponde con el comando Samba 'browseable'
/autodisconnect:X minutos antes de que se desconecte un usuario del servidor
net pause X Detiene el servicio X
net continue X Reanuda el servicio X

Recursos
net view X /domain: Y mostrar dominios enteros o recursos en un equipo
/Domain: y → muestra equipos en el dominio
X es el servidor que se desea ver (\\X)
net print impresora Permite ver/modificar la cola de impresi??n
/hold:x → no imprimir el trabajo X
/release:x → reanudar trabajo X
net share Mostrar/modificar recursos compartidos
net use nombre \\recurso Crear una conexi??n de red

Usuarios

net group x A?±adir/ver/modificar grupos de usuarios en un dominio
/Domain:x → nombre del dominio
/add x → a?±adir un grupo nuevo
net user usuario clave A?±adir/ver/modificar usuarios en un dominio
/domain:nombre → nombre del dominio
/add x → agregar usuario al dominio
Si en clave se pone * se indica ue hay que preguntar cada vez
/delete → borrar usuario
net accounts Muestra/modifica la cuenta de un usuario
/minpwlen:x → longitud m??nima de password
uniquepw:x → solo se puede usar la clave x veces. Luego hay que cambiar
/domain: nombre → nombre del dominio
/sync → sincronizar los cambios en los servidores BDC

Comunicaciones

net send x y Enviar mensaye Y a usuario/ordenador X
Si nombre es * se env??a a todos los miembros del grupo/dominio
/domain: nombre -> nombre del dominio

9.4.6 Netstat [opciones]

Comando para comprobar el estado actual de la red
netstat -a Mostrar todos los puetos y conexiones
netstat -n Mostrar n??mero de puerto y direcciones
netstat -r Mostrar la tabla de rutas
netstat -s Mostar estad??sticas por protocolo
netstat -p tcp/udp Mostrar las conexiones activas TCP o UDP

9.4.7 Nslookup[opciones]

Utilidad para interrogar dns

9.4.8 Ping [opciones]

Enviar paquetes icmp a un determinado destino.
ping -t ping al host hasta que se pare
ping -a resolver direcciones en nombres de host
ping -n numero N??mero de peticiones a enviar
ping -l tama?±o tama?±o del buffer

9.4.9 Telnet [host] [puerto]

Inicia una sesi??n telnet al host especificado en el puerto especificado. Si el puerto se omite se usa el 23.

9.4.10 Tracert [destino]

Tracear el destino hasta llegar a la ruta indicada.

9.5 Comandos de programaci??n

9.5.1 Edit [archivo]

Editor de textos (equivalente al bloc de notas)

9.5.2 Debug [archivo] [opciones]

Inicia el desensamblador con el programa indicado.

9.5.3 choice [texto] [opciones]

Se utiliza en programas bat para dar a elegir a un usuario entre un conjunto de opciones
La respuesta se devuelve mediante la variable errorlevel
Mostrar el literal "elija una opci??n y dar a elegir s (s??), n (no) o C (continuar). las tres siguientes l??neas especifican a donde debe saltar el flujo del programa seg??n la tecla pulsada.
choice Elija una opci??n snc
Mostrar el texto y las opciones (S, N, C)
if errorlevel 1 goto ... si se ha pulsado S
if errorlevel 2 goto ... si se ha pulsado N
if errorlevel 3 goto ... si se ha pulsado C

9.5.4 If [condicion] [comando]

Sirve para hacer bifurcaciones en el c??digo.
Admite 6 sintaxis distintas:
if exist fichero orden si existe 'fichero' ejecutar la orden
if not exist fichero si no existe fichero ejecuar la orden
if cadena1==cadena2 orden comparar cadena1 y cadena2
if not cadena1 == cadena2 orden si son distintos
if errorlevel numero orden si el comando anterior acab?? con un errorlevel igual o superior a numero ejecutar orden
if not errorleven numero orden si el comando anterior acab?? con un errorlevel inferior a numero ejecutar orden

9.5.4 for

El formato general es
for %%variable in lista do (orden 1
orden 2
orden 3
)

La variable siempre lleva dos veces el signo %

Ejemplo
FOR %%x IN (texto1.txt texto2.txt texto3.txt) do delete %%i

Esta orden har??a lo siguiente: repetir??a 3 veces la orden delete. En cada vez %%i valdr??a cada valor de la lista de manera que la primera vez ser??a texto1.txt, la segunda vez texto2.txt y la tercera vez texto3.txt.

As?? esta orden har??a:
DELETE TEXTO1.TXT
DELETE TEXTO2.TXT
DELETE TEXTO3.TXT

ESO ES TODO POR ESTE TUTORIAL!!!

TUTO POSTEADO EN EL FORO POR : EYES OF DEAD

TUTORIAL CREADO EN PDF

POR:

EL_CELLU5.

SALU2