**Command Line Command - The Basics**

|  |  |  |
| --- | --- | --- |
| **Command** | **Purpose** | **Extras / Examples** |
| COLOR <hex><hex> | Changes the font and background color of console window. It uses 2 hex values to set the background, Font colors | COLOR /? - Lists colors  COLOR 84 - Gray Background, Red Text  COLOR - Resets to default |
| CLS | Clears screen |  |
| DATE | Displays and allows Date to be changed |  |
| TIME | Displays and allows Time to be changed |  |
| EXIT | Exits from the console |  |
| HELP | Lists available console commands | HELP COLOR - Gives specific info about COLOR command (Color /?) |
| wmic logicaldisk get name | Tells which drive letters are available |  |
| H: | Jumps to a different drive (network or physical) |  |
| DIR | Shows contents of current folder | /b - bare  /s - show subfolders as well  \* - wildcard (can be used on filename or extension  dir \*.exe - shows all executable files  dir a\*.\* - shows all files that start with a |
| CD (Change Directory) | Change to a new directory (folder) | cd folder\_name (must exists)  cd.. - Move you up one file system level  cd workspace\tam  cd\ - Moves to root of that directory |
| MD <Directory\_Name> | Make a Directory | MD PC\_Repair |
| RD <Directory\_Name> | Removes Directory (must be empty) |  |
| DEL <Filename> | Deletes the file in the current directory | Wildcards work here  DEL \*.DOC (Deletes all word documents) |
| TYPE <Filename.txt> | Outputs the contents of a text file | Type readme.txt |
| REN <Filename> <NewFilename> | Gives a new name to a file. Be sure to include extension | rename hi.txt bye.txt |
| COPY <Filename> < Path> | Copies files to a new destination | COPY readme.txt h:\practice |
| NSLookup <domain> | Returns the IP address of a domain name | NSLOOKUP google.com  returns 216.58.216.75 |
| telnet <IP> | Connects to a remote IP address | Telnet 10.3.1.1 |
| tree | shows the file system hierarchy |  |
| echo | Used to show message at the console level | echo hello there |
| @echo off | Hides the command syntax from the output of a batch file |  |
| :<Label> | Gives a name to a location in a batch file, which you can jump to with GOTO | :Start |
| GOTO <Label> | Jumps to the label mentioned. Can cause console commands to repeat | GOTO Start |
| Pause <Message> | Pauses the running of the batch file | Pause Do you want to continue? |
| Call <Drive><Path><Filename> | Calls another file to run. | Call H:\hacking\runme.bat |
| msg \* <message> | Generates a message box with message | msg \* Hello |
| pkgmgr /iu:”TelnetClient” | Enables Telnet |  |
| telnet towel.blinkenlights.nl | Wait and see |  |

Building a Batch File

A batch file is a simple notepad document that will run the console commands inside it in order. We can string together a series of commands that will perform an operation.

**matrix.bat**

@echo off

color 02

:tricks

echo %random%%random%%random%%random%%random%%random%%random%%random%

goto tricks