

SHELL IS ONLY THE BEGINNING

When getting shell is only the start of the journey.

BLOG INFOSEC TACTICO PODCAST SEARCH
BLOG SERIES MSF INSTALLATION GUIDES
PROJECTS ABOUT ME

PowerShell Basics–The Environment

JANUARY 09, 2013 BY CARLOS PEREZ

I do have to say last year I started to write about PowerShell Basics and I then stopped. The main reason was that after talking with Dave Kennedy I decided to write a class for DerbyCon 2012 and boy did I thought it was going to be simple. I started believing that I could write it in a month or two and have it done since I use PowerShell on a daily basis, took me over 6 months, ended up with over 600 slides and was even modifying the slides on the airplane ride to Louisville since Microsoft came out with PowerShell Version 3.0 as part of the Windows Management Framework 3 a week before the conference. The good part is

that I have now more than enough material to re-start the series and cover more fun stuff for the security professional and the admin alike.

I have given the PowerShell for Security Professionals class 3 times and one thing I decided for the blog posts that differs from the class it self is to provide short segments of fast and easy to use information for people to start getting in to Powershell.

What is PowerShell

PowerShell is Microsoft new Command Line Interface for Windows systems, it provides access to:

- Existing Windows Command Line tools.
- PowerShell Cmdlets (PowerShell own Commands)
- PowerShell Functions
- Access to the .Net Framework API
- Access to WMI (Windows Management Instrumentation)
- Access to Windows COM (Component Object Model)
- Access to function in Windows DLL (Dynamic Linked Libraries)

As it can be seen PowerShell does provide a lot of access to different technologies and APIs on a Windows system making it ideal for administration and for security work alike.

Microsoft is making PowerShell the default management interface for many of its server products like Exchange, System Center Operations Manager, SQL Server, SharePoint Server and more, not only that but with Windows 2012 server the default install is core (GUI-Less System) and management is done via the command line or using Remote Administration Tools. Microsoft included over 4 thousand new PowerShell cmdlets to make the administration of the new server the easiest ever using the command line.

PowerShell

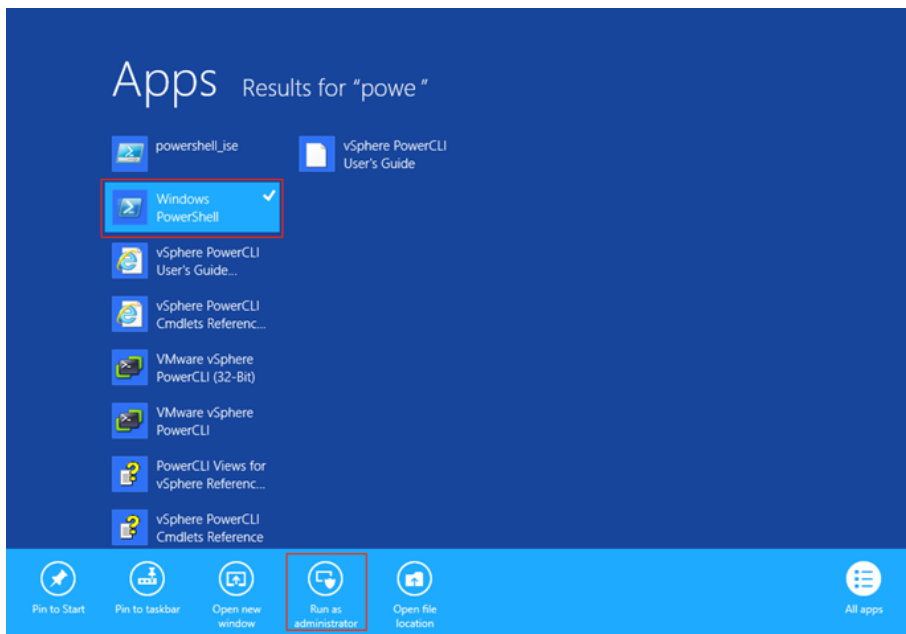
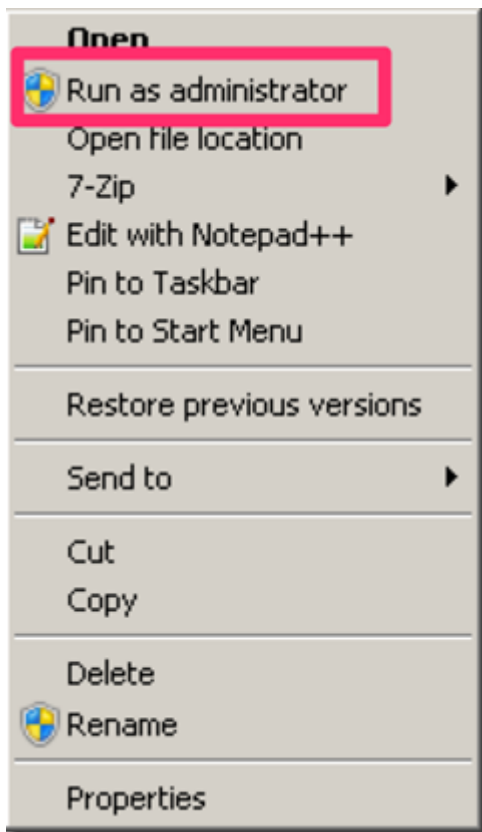
Depending on the environment and systems you work with there are 2 main versions of PowerShell you will find yourself working with:

- PowerShell v2 –Included with Windows 7 and Windows 2008 R2. Available as a separate download for Windows XP SP3, Windows 2003 SP2, Windows Vista SP1 and Windows 2008 SP2. It can be pushed to hosts via Windows Server Update Service. Download t
<http://support.microsoft.com/kb/968929>
- PowerShell v3 – Included with Windows 8 and Windows 2012. Available as a separate download for Windows 7 SP1 and Windows 2008 R2 SP2. It can not be pushed to hosts via Windows Server Update Service. Download
<http://www.microsoft.com/en-us/download/details.aspx?id=34595>

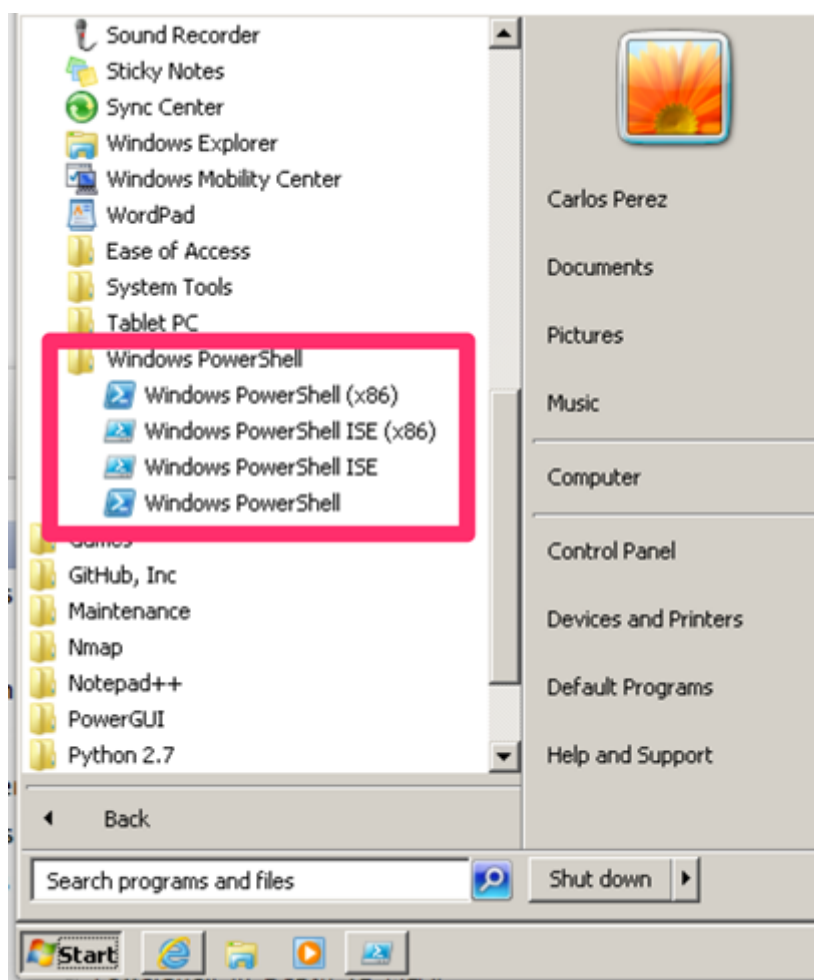
On Windows System prior to Windows 8 and Windows 2012 PowerShell can be found under **Start → All Programs → Accessories → System Tools** Depending on the architecture of the operating system there will be an x86 version and a x64 version of PowerShell. In addition to the shortcut to the PowerShell terminal there will also be shortcuts to the ISE (Integrated Scripting Environment) and Editor for PowerShell scripts that was included with PowerShell v2 and greatly improved on PowerShell v3. On Systems running Windows 8 and Windows 2012 with the Metro Interface one just need to type **PowerShell** or **PowerShell_ISE** to access the components. On a Windows 2012 Core System one just needs to type **powershell.exe** in the command prompt to load it.

Some recommendations when loading PowerShell:

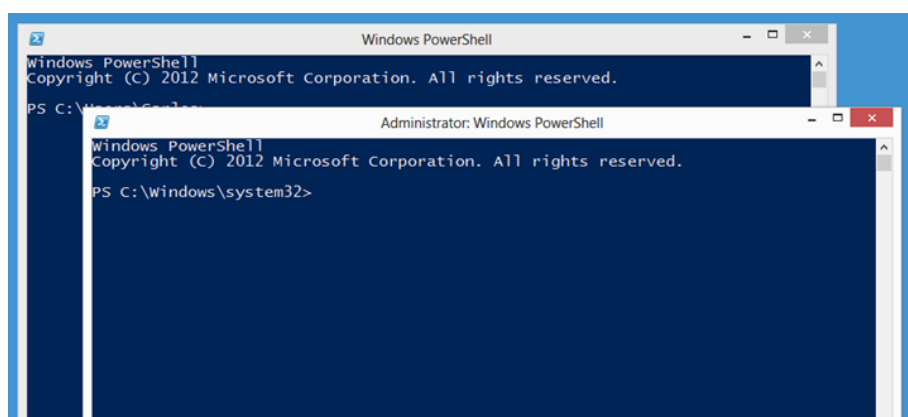
- Since PowerShell provides access to many administrative functions it is recommended to run it as Administrator.



- If you are on a x64 system make sure you run the x64 version of it (The one with no x86 in the name of the shortcut)



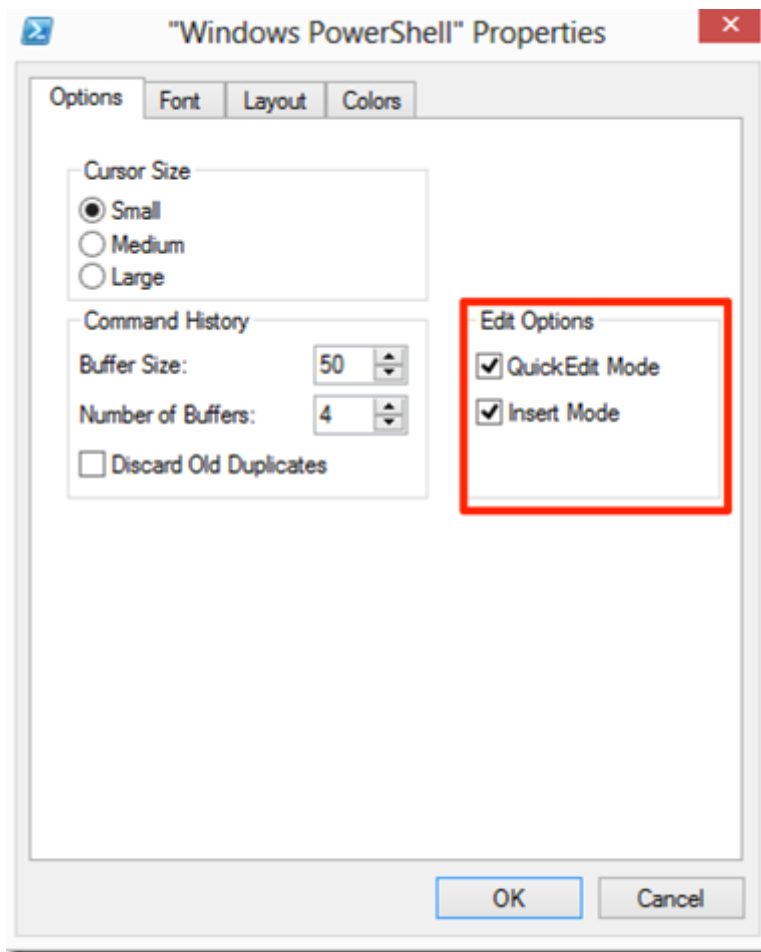
When we launch PowerShell we are greeted with a blue command window with white text.



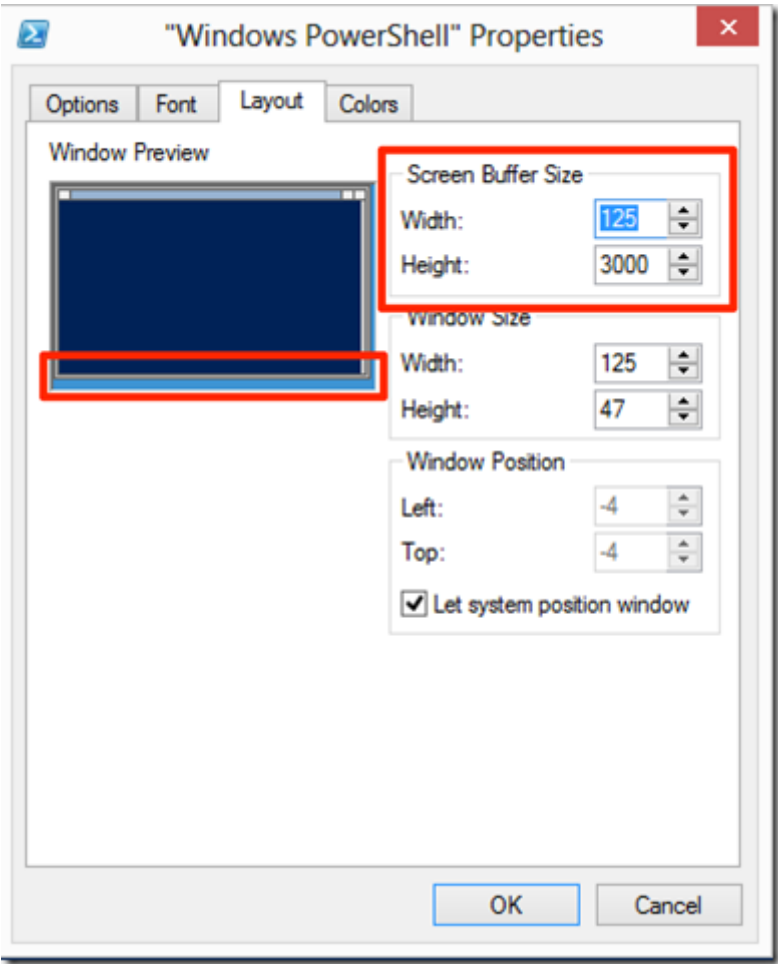
As it can be seen one can easily determine by looking at the title bar of the window if one is running as Administrator or not.

I would recommend to take the chance and customize the shortcut for launching PowerShell so as to provide the best experience. **Right click** on the PowerShell blue icon on the top

left of the PowerShell Window and select Properties, make sure on the **Options** tab that the **Edit Options** are selected



On the Layout tab adjust the **Screen Buffer Size Width** to one where there is no need for side scroll bar making sure that both **Width** fields have the same value in both the **Buffer Size** and **Window Size**.

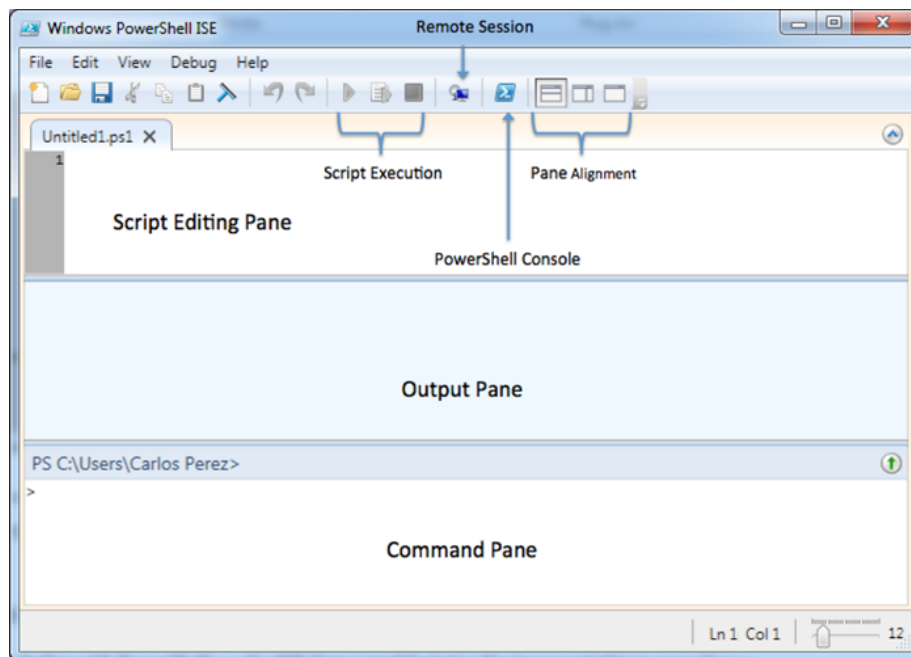


Ensuring a proper width will make the management of large amounts of output generated by some cmdlets easier to look at on the screen.

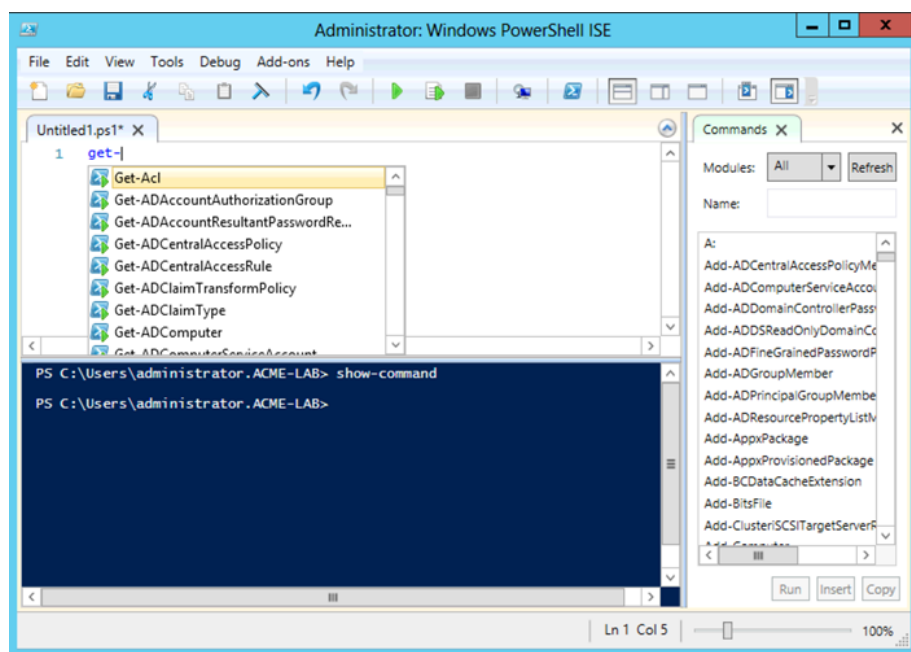
The terminal has several keyboard shortcuts that can be used, a list of the most common are in the table below:

Keyboard	Action
Left/Right Arrow Keys	Move Cursor left and right
Crtl+Left Arrow, Crtl+Right Arrow Keys	Move Cursor one Word each time
Home	Move Cursor to Beginning
End	Move Cursor to End
Up/Down Arrow Keys	Move thru Command History
Tab	Command and Option Completion
F7	Command History Window
Insert Key	Toggle Character Insertion/Overwrite
Delete Key	Delete character under cursor
Backspace Key	Delete character to left of cursor

On PowerShell v2 the ISE can also be use as an interactive command prompt where commands are entered in on window and output is shown in the next, in addition it is a script editor with syntax highlighting



On PowerShell v3 the ISE has been greatly improved, offering a consolidated command prompt and also provides a cmdlet help pane













In addition ISEv3 also provides:

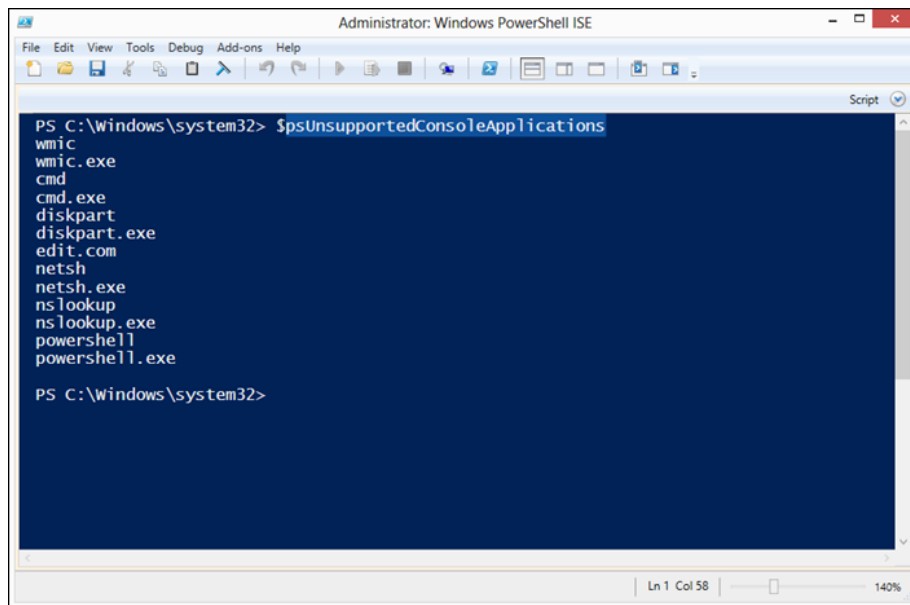
- Intellisense for Cmdlets and parameters with parameter help popup.

- Intellisense will provide values for parameters based on enumerations and pre-defined sets.
- Intellisense will perform smart matching for cmdlet names
- Intellisense will show path options for filesystems and PSProviders
- Intellisense will show variables
- Intellisense will show for objects properties and methods available

It will also provide an Icon Reference that makes it easier to select in Intellisense what one wants to choose.

- : Command
- : Container
- : File / item
- : Method
- : Property
- : Parameter
- : Parameter value
- : Variable
- : History
- : Type

The command prompt on ISEv3 can be said to be the closest one can get to the perfect terminal for PowerShell with the exception that since it is not a true terminal several console commands are not supported. To get a list of the unsupported console commands one can take a look at the **\$psUnsupportedConsoleApplications** variable



The screenshot shows the Windows PowerShell ISE interface. The title bar reads 'Administrator: Windows PowerShell ISE'. The menu bar includes File, Edit, View, Tools, Debug, Add-ons, and Help. The toolbar contains various icons for file operations and execution. The main console area has a dark blue background and displays the following text:

```
PS C:\windows\system32> $psUnsupportedConsoleApplications
wmic
wmic.exe
cmd
cmd.exe
diskpart
diskpart.exe
edit.com
netsh
netsh.exe
nslookup
nslookup.exe
powershell
powershell.exe

PS C:\windows\system32>
```

The status bar at the bottom indicates 'Ln 1 Col 58' and a zoom level of '140%'.

There are some other alternatives to consoles I recommend people to also try out if they find the one included with Windows to limiting:

- PowerCMD <http://www.powercmd.com/>
- Console <http://sourceforge.net/projects/console/>
- conemu-maximus5 <http://code.google.com/p/conemu-maximus5/>

For my next blog post I will go in to running commands, exploring the commands and using the help system.

♥ 41 LIKES

< Newer Older >

Comments (11)

Newest First Subscribe via e-mail

Preview Post Comment...



vickey palzor lepcja 2 years ago · 0

Likes

what a nice - short but brilliant write up



Suchen Oguri 2 years ago · 0 Likes

Nicely written. Thank you.



Vasu 2 years ago · 0 Likes

Thanks you



ram 2 years ago · 0 Likes

short and sweet intro, where is the link for next blog post or continuation ?



akowe 3 years ago · 0 Likes

Great Basic introduction to anyone new to PowerShell. Do you have a book written on PowerShell?



Carlos Perez 3 years ago · 0

Likes

I do not but pleas do check out the PowerShell Cookbook by Lee Holmes



fred 4 years ago · 0 Likes

This is a great site. Thank you Carlos.



Carlos Perez 4 years ago · 0

Likes

Thanks



Tanzy 4 years ago · 0 Likes

Simple and concise..Thanks much for sharing this..



praveen 4 years ago · 0 Likes

thanks it's well explained



stephan 6 years ago · 0 Likes

Well written, well structured. Keep it up.

Copyright Carlos Perez 2014