

PowerShell en la filtración de WikiLeaks (Vault 7: CIA Hacking Tools Revealed)

Create and Modify Your Powershell Profile

1. First check whether or not your profile exists.
 1. `Test-Path $profile`
2. If the query returned «False», then your profile does not exist.
3. Create your profile
 1. `New-Item -path $profile -type file -force`
4. The output of the previous command will tell you where your profile was created. The path given as the «Directory» output is the directory containing your profile. It will be something like `C:\Users\user1\Documents\WindowsPowerShell`.
5. Open Windows Explorer and go to that directory. Your profile will be «Microsoft.PowerShell_profile.ps1».
6. By default your profile will be empty. You can edit your profile to customize your powershell window default settings. One setting that you will likely need is modifying the PATH environment variable to include the python directory.
7. To add the python directory to your path, open your profile (Microsoft.PowerShell_profile.ps1) in a text editor and add the following line.
 1. `$env:Path += «;C:\python27»`
8. You can test your settings by opening a powershell window and typing «`$env:Path`». You should see «`C:\python27`» added to the end of your path.

Execution of Scripts is Disabled on this System

When you try to run a powershell script on Windows, you may receive the following error stating that the execution policy on your computer does not allow you to run the script.

```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

File C:\Users\User1\Documents\WindowsPowerShell\Microsoft.PowerShell_profile.ps1 cannot be loaded because the execution
of scripts is disabled on this system. Please see "get-help about_signing" for more details.
At line:1 char:2
+ . <<<< 'C:\Users\User1\Documents\WindowsPowerShell\Microsoft.PowerShell_profile.ps1'
+ CategoryInfo          : NotSpecified: (:) [1], PSSecurityException
+ FullyQualifiedErrorId : RuntimeException
```

To fix this error, you must change the PowerShell execution policy for this computer. If you issue the command «get-get about_signing» you will get plenty of information about this error. However, because we are on a closed network these instructions will explain how to allow «Unrestricted» access to running scripts on your computer.

1. To set the execution policy to unrestricted, enter the following command (PowerShell must be run as an Administrator):
 1. Set-ExecutionPolicy Unrestricted
2. You will receive a warning indicating that you are trying to change the execution policy and the risk that is associated with the change. Enter 'Y' and press enter.
3. Your execution policy is now changed. You can verify this by executing the command «Get-ExecutionPolicy». You can now try to run your script again and you should not receive any errors.