Ustawienia bezpieczeństwa skryptów – info

Wprowadzenie do certyfikatów

Zaufany certyfikat główny

Certyfikat wydawcy kodu

Ograniczenia podczas uruchamiania skryptów

Opcja Execution Policy

Uruchamianie powłoki PowerShell z parametrami

Przyjrzymy się jak autorzy PowerShell zaprojektowali bezpieczeństwo uruchamiania się skryptów.

Utworzymy prosty skrypt, który będzie miał do wykonania dwie czynności

Pierwsza z nich to wyświetlenie komunikatu „Podaj twoje imię:" po to, aby zapisać wprowadzoną nazwę, do zmiennej która zostanie wykorzystana w kolejnej linijce

```
1   $name=read-host "Podaj twoje imię"
```

```
PS C:\WINDOWS\system32> $name=read-host "Podaj twoje imię"
Podaj twoje imię: Irek
```

Gdzie skrypt przywita się wyświetlając "Witaj a następnie wprowadzone imię

```
2   Write-Host "Witaj $name"
3   cd C:\Users\admin
```

```
PS C:\Windows\system32> Write-Host "Witaj $name"
Witaj Irek
```

Obie komendy zapisujemy w pliku na dysku C:\Users\admin\Witaj.ps1

```
1   $name=read-host "Podaj twoje imię"
2   Write-Host "Witaj $name!"
```

Jeżeli przejdę do tego katalogu i spróbuję uruchomić ten skrypt to otrzymam komunikat błędu, że

```
PS C:\Windows\system32> cd C:\Users\admin

PS C:\Users\admin> Witaj.ps1
Witaj.ps1 : The term 'Witaj.ps1' is not recognized as the name of a cmdlet, function, script file, or operable program. Check
the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ Witaj.ps1
+ ~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (Witaj.ps1:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException
```

Nie wolno uruchomić tego skryptu o ile nie podasz do niego pełnej ścieżki dostępu. To dobrze.

Administrator uruchamiając skrypt powinien wyraźnie wskazać ścieżkę i skrypt a nie zdawać się na to, że skrypt jest w katalogu bieżącym. Przecież ktoś mógłby podłożyć skrypt, który wykonuje inne

polecenia. Dla administratora to nie problem, bo może podać ścieżkę dostępu a chroni siebie i innych przed przypadkowym uruchomieniem nie tego skryptu.

Ścieżkę można podać

bezwzględną która opisuje w jednoznaczny sposób umiejscowienie folderu lub pliku

np. C:\Users\admin\Witaj.ps1

```
PS C:\Windows\system32> C:\Users\admin\Witaj.ps1
C:\Users\admin\Witaj.ps1 : File C:\Users\admin\Witaj.ps1 cannot be loaded because running scripts is disabled on this system.
For more information, see about_Execution_Policies at https:/go.microsoft.com/fwlink/?LinkID=135170.
At line:1 char:1
+ C:\Users\admin\Witaj.ps1
+ ~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : SecurityError: (:) [], PSSecurityException
    + FullyQualifiedErrorId : UnauthorizedAccess
```

Próba uruchomienia skryptu nie powiodła się.

Spróbujmy z ścieżką względną która wskazuje na plik lub folder względem aktualnej lokalizacji np. aktualna lokalizacja C:\Users\admin\ ścieżka względna do pliku .\Witaj.ps1

```
PS C:\Users\admin> .\Witaj.ps1
.\Witaj.ps1 : File C:\Users\admin\Witaj.ps1 cannot be loaded because running scripts is disabled on this system. For more info
rmation, see about_Execution_Policies at https:/go.microsoft.com/fwlink/?LinkID=135170.
At line:1 char:1
+ .\Witaj.ps1
+ ~~~~~~~~~~
    + CategoryInfo          : SecurityError: (:) [], PSSecurityException
    + FullyQualifiedErrorId : UnauthorizedAccess
```

Próba uruchomienia skryptu również nie powiodła się dlatego że o tym czy na komputerze można uruchamiać skrypty czy nie decyduje opcja konfiguracyjna PowerShell tzw Execution_Policies

Sprawdzam jak ustawiony jest ten parametr

```
PS C:\Users\admin> Get-ExecutionPolicy
Restricted
```

Restricted - Ograniczony

- Domyślna zasada wykonywania dla komputerów klienckich z systemem Windows.
- Zezwala na pojedyncze polecenia, ale nie zezwala na skrypty.
- Zapobiega uruchamianiu wszystkich plików skryptów, w tym plików formatowania i konfiguracji (.ps1xml), plików skryptów modułu (.psm1) oraz profili PowerShell (.ps1).

Są jeszcze inne zasady wykonywania skryptów PowerShell

AllSigned - Wszystkie podpisane

- Skrypty mogą działać.
- Wymaga, aby wszystkie skrypty i pliki konfiguracyjne były podpisane przez zaufanego wydawcę, w tym skrypty, które piszesz na komputerze lokalnym.
- Wyświetla monit przed uruchomieniem skryptów od wydawców, których jeszcze nie sklasyfikowałeś jako zaufanych lub niezaufanych.
- Ryzyko związane z uruchamianiem podpisanych, ale złośliwych skryptów.

Bypass - Pomiń

- Nic nie jest zablokowane i nie ma żadnych ostrzeżeń ani podpowiedzi.

- Te zasady wykonywania są przeznaczone dla konfiguracji, w których skrypt PowerShell jest wbudowany w większą aplikację lub dla konfiguracji, w których PowerShell jest podstawą programu, który ma własny model zabezpieczeń.

Default - Domyślny

- Ustawia domyślną zasadę wykonywania.
- Ograniczone dla klientów Windows.
- RemoteSigned dla serwerów Windows.

RemoteSigned - Zdalnie podpisany

- Domyślna zasada wykonywania dla komputerów z systemem Windows.
- Skrypty mogą działać.
- Wymaga podpisu cyfrowego od zaufanego wydawcy w skryptach i plikach konfiguracyjnych pobieranych z Internetu, w tym w programach do obsługi poczty e-mail i komunikatorów.
- Nie wymaga podpisów cyfrowych w skryptach napisanych na komputerze lokalnym, a nie pobranych z Internetu.
- Uruchamia skrypty, które są pobierane z Internetu i nie są podpisane, jeśli skrypty są odblokowane, na przykład za pomocą polecenia Unblock-Filecmdlet.
- Zagrożenie uruchamianiem niepodpisanych skryptów ze źródeł innych niż Internet oraz podpisanych skryptów, które mogą być złośliwe.

Undefined - Nieokreślony

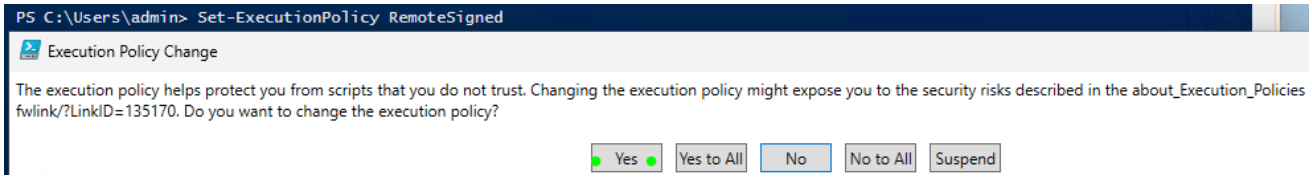
- W bieżącym zakresie nie ustawiono zasad wykonywania.
- Jeśli zasada wykonywania we wszystkich zakresach to Undefined , obowiązująca zasada wykonywania to Restricted for Windows Clients i RemoteSigned for Windows Server.

Unrestricted - Nieograniczony

- Domyślne zasady wykonywania dla komputerów innych niż Windows i nie można ich zmienić.
- Można uruchamiać niepodpisane skrypty. Istnieje ryzyko uruchomienia złośliwych skryptów.
- Ostrzega użytkownika przed uruchomieniem skryptów i plików konfiguracyjnych, które nie pochodzą ze strefy lokalnego intranetu.

Parametr Execution_Policies administrator może zmienić

Set-ExecutionPolicy RemoteSigned spowoduje ż będą uruchamiane z pytaniem tylko skrypty wykonywane skrypty umieszczone na zasobach sieciowych pozostałe bez, zmiana wymaga potwierdzenia więc jest istotną czynnością.



Uruchomię skrypt

```
PS C:\Users\admin> .\Witaj.ps1
Podaj twoje imię: Irek
Witaj Irek
```

Działa, ale rozwiązanie nie jest idealne ze względu na bezpieczeństwo.

Wybiorę AllSigned i spróbuję uruchomić skrypt

```
PS C:\Users\admin>  Set-ExecutionPolicy AllSigned -Force

PS C:\Users\admin> Get-ExecutionPolicy
AllSigned

PS C:\Users\admin> .\Witaj.ps1
.\Witaj.ps1 : File C:\Users\admin\Witaj.ps1 cannot be loaded. The file C:\Users\admin\Witaj.ps1 is not digitally signed. You c
annot run this script on the current system. For more information about running scripts and setting execution policy, see abou
t_Execution_Policies at https:/go.microsoft.com/fwlink/?LinkID=135170.
At line:1 char:1
+ .\Witaj.ps1
+ ~~~~~~~~~~
    + CategoryInfo          : SecurityError: (:) [], PSSecurityException
    + FullyQualifiedErrorId : UnauthorizedAccess
```

Jak widać nie działa, bo skrypt nie jest podpisany.

Jak wygenerować podpis? Potrzebny będzie certyfikat służący do popisywania kodu.

W organizacji certyfikat będzie wystawiany przez lokalny urząd certyfikacji.

Skorzystamy z certyfikatu własnego który uznamy za zaufany.

Tworzenie certyfikatu z podpisem własnym

Aby utworzyć certyfikat z podpisem własnym, użyj polecenia cmdlet New-SelfSignedCertificate w module PKI. Ten moduł został wprowadzony w programie PowerShell 3.0 i jest zawarty w Windows 8 i Windows Server 2012.

```
1  $params = @{
2      Subject = 'CN=PowerShell Code Signing Cert'
3      Type = 'CodeSigning'
4      CertStoreLocation = 'Cert:\CurrentUser\My'
5      HashAlgorithm = 'sha256'
6  }
7  $cert = New-SelfSignedCertificate @params
```

W tym przykładzie:

Aby sprawdzić, czy certyfikat został wygenerowany poprawnie, użyj następującego polecenia, aby uzyskać certyfikat w magazynie certyfikatów na komputerze. Plik certyfikatu nie będzie można znaleźć w katalogu systemu plików.

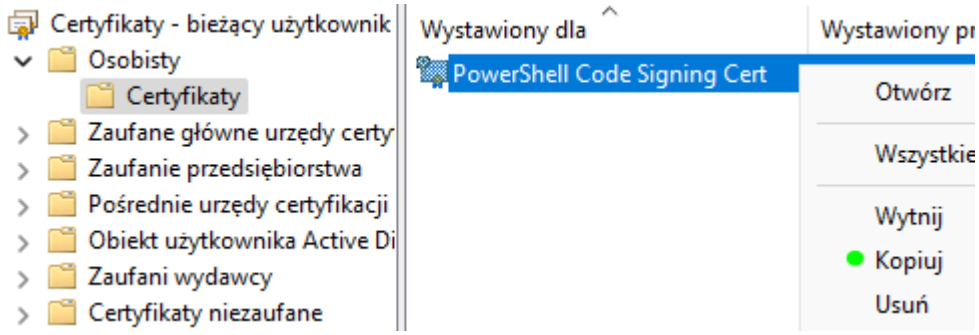
W wierszu polecenia programu PowerShell wpisz:

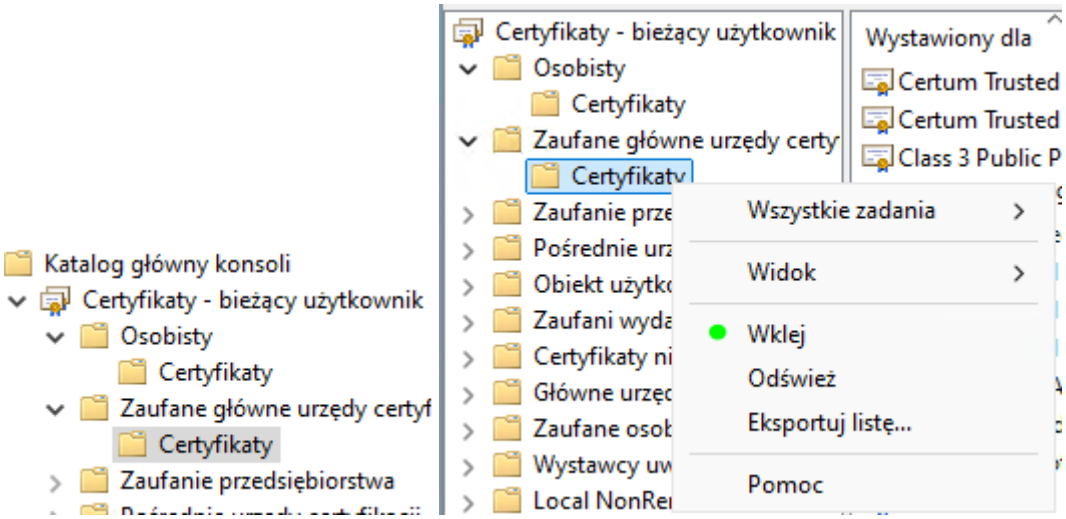
Get-ChildItem cert:\CurrentUser\my -codesigning

```
PS C:\Users\admin> Get-ChildItem cert:\CurrentUser\my -codesigning


   PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\my

Thumbprint                                Subject
----------                                -------
79A084D346B1EB857BB551F0291F33FF8ADF6FC5  CN=PowerShell Code Signing Cert
```

Po utworzeniu certyfikatu z podpisem własnym można podpisywać skrypty.

Po wygenerowaniu certyfikatu należy z konsoli zarządzania przechowywaniem certyfikatów (certmgr.msc) go skopiować z kontenera pośredniego do zaufanego katalogu głównego.





Jeśli używasz zasad wykonywania AllSigned, podpisywanie skryptu umożliwia uruchomienie skryptu na komputerze.

```
PS C:\WINDOWS\system32> Get-ExecutionPolicy
AllSigned
```

Jeśli jednak używasz zasad wykonywania AllSigned, musisz podpisać skrypt C:\Users\admin\Witaj.ps1 przed jego uruchomieniem.

Wpisz następujące polecenia w wierszu polecenia programu PowerShell:

$cert = @(Get-ChildItem cert:\CurrentUser\My -codesigning)[0]

Wyświetl listę certyfikatów w magazynie CurrentUser\My:

Get-ChildItem -Path Cert:\CurrentUser\My | Format-List -Property Thumbprint, Subject

To polecenie wyświetli listę certyfikatów wraz z ich thumbprintami i subjectami (nazwami). Odszukaj thumbprint swojego certyfikatu.

```
Thumbprint : 18231B1B8973AD6B7C4E3CAE9004B5E5BDF436CE
Subject    : CN=PowerShell Code Signing Cert
```

Przypisz thumbprint swojego certyfikatu do zmiennej:

$thumbprint = "18231B1B8973AD6B7C4E3CAE9004B5E5BDF436CE"

Znajdź certyfikat według odcisku palca (thumbprint)

```
$cert = Get-ChildItem -Path Cert:\CurrentUser\My | Where-Object { $_.Thumbprint -eq $thumbprint }
```

Sprawdź, czy zmienna $cert została poprawnie przypisana

```
if ($null -eq $cert) {
    Write-Host "Certyfikat nie został znaleziony. Upewnij się, że podany odcisk palca jest poprawny."
} else {
    Write-Host "Certyfikat został poprawnie załadowany."
}
```

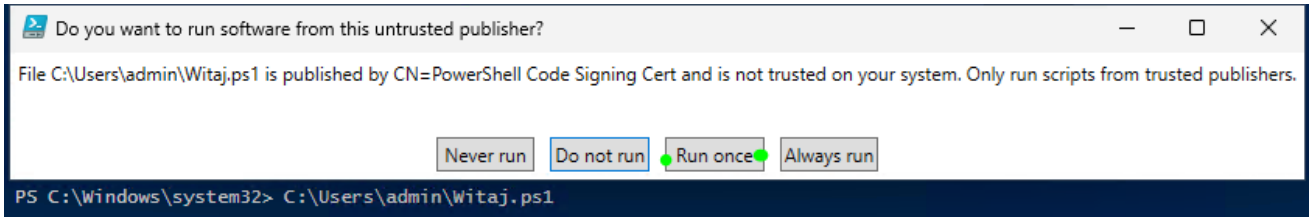
Podpisz skrypt

```
Set-AuthenticodeSignature -Certificate $cert -FilePath "C:\Users\admin\Witaj.ps1"
```

```
PS C:\Windows\system32> Set-AuthenticodeSignature -Certificate $cert -FilePath "C:\Users\admin\Witaj.ps1"

    Directory: C:\Users\admin

SignerCertificate                         Status                                 Path
-----------------                         ------                                 ----
18231B1B8973AD6B7C4E3CAE9004B5E5BDF436CE  Valid                                  Witaj.ps1
```

Skrypt jest podpisany.

Uruchomię skrypt C:\Users\admin\Witaj.ps1




```
PS C:\Windows\system32> C:\Users\admin\Witaj.ps1
Podaj twoje imię: Irek
Witaj Irek
```

Działa

Podpis jest poprawny a certyfikat zaufany mamy pewność skąd pochodzi skrypt, ale jak widać należy jeszcze potwierdzić, że ufam wydawcy. Jeżeli wydawca jest godny zaufania to decyduję się wyrazić zgodę, aby uruchomić skrypt raz lub zawsze.

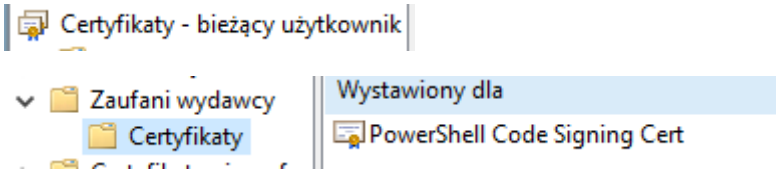
Always run umieści certyfikat wydawcy oprogramowania w magazynie zaufanych wydawców.

Jeśli nie ufasz wydawcy nie uruchamiaj skryptu.

Pamiętaj podpis mówi tylko o tym kto utworzył skrypt, zaufanie do wydawcy to odpowiedzialność administratora – Twoja

Włączę skrypt C:\Users\admin\Witaj.ps1 i wybierz **Always run**

Sprawdzę zawartość



(gdyby było pusto należy odświerzyć)

Od tej pory wszystkie skrypty podpisane naszym certyfikatem będą uruchamiały się bez pytań.

Oczywiście na innym komputerze lokalnym procedurę należy powtórzyć.

A jak wygląda plik C:\Users\admin\Witaj.ps1

```
13  Get-Content C:\Users\Witaj.ps1
PS C:\WINDOWS\system32> Get-Content C:\Users\Witaj.ps1
$name=read-host "Podaj twoje imię"
Write-Host "Witaj $name!"
# SIG # Begin signature block
# MIIFlAYJKoZIhvcNAQcCoIIFhTCCBYECAQExCzAJBgUrDgMCGgUAMGkGCisGAQQB
# gjcCAQSgWzBZMDQGCisGAQQBgjcCAR4wJgIDAQAABBAfzDtgWUsITrck0sYpfvNR
# AgEAAgEAAgEAAgEAAgEAMCEwCQYFKw4DAhoFAAQUVVEjwH8LRcIhM6cb4e/YKK9y
# 5yOgggMiMIIDHjCCAgagAwIBAgIQG6YzaQc8FahFAO3OXroHWzANBgkqhkiG9w0B
# AQsFADAnMSUwIwYDVQQDDBxQb3dlclNoZWxsIENvZGUgU2lnbmluZyBDZXJ0MB4X
# DTIxMTAwMjEyNDk1M1oXDTIyMTAwMjEzMDk1M1owJzElMCMGA1UEAwwcUG93ZXJT
# aGVsbCBDb2RlIFNpZ25pbmcgQ2VydDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
# AQoCggEBAO+IZMWnODa+ph9P1QHnfs0c5DSMh3OejEsgE/ie0L/keZEBQDjcYpJ2
# /tBc2wjQmpy6lZ8hwZNw9aqNNnHEzWHntxWuAuxZJ6gj1Dzqds7zQpQ/3wH2trrF
# lrmDxI2Ce+uOL7eAx2/wMWQs3wkz+fzMF52p7cOurpY5Xetz5TNityxkPlLKuf75
# marmOpkROm9V/ICzhSWNFNU5OtPL4/N2cbpO+9lQU6RGMHkyz+KDTWj2vPWoy2fh
# pI5pnyjAHBLEFNzjKuyMnC7qL+KyIdLXezkOo5z92rLj3zYMVTj7CPoncKuKvWo6
# B/AQZDR9yg5jW4QN2IWoGc0EOhL9NdkCAwEAAaNGMEQwDgYDVR0PAQH/BAQDAgeA
# MBMGA1UdJQQMMAoGCCsGAQUFBwMDMBOGA1UdDgQWBBRPJ4NtRp1JcLmRxtXzdfHa
# /3Wd3zANBgkqhkiG9w0BAQsFAAOCAQEAxQ7PzjPg8nEV8gFEGMOl5OYsOEdXBpjB
# RcFKXJ+3eLTp4sy47e7o1ZiCKa2BOmP35O63Gq1oncp53NXH4lOdPYalRpOLBClK
# Y/zzqz9FxpfdhoMDJ729r5DF5ydh3+FrbEPdkm2OMDdKG7ySxvpLhgofhcUaOo2V
# nroCRDnV4ZUanWfcmPkdXIVwu5NhmusFi7+kBCEdB1H+X8wfLRp+lVt22dCamN1K
# dn2vmNiaGuHOFzKUr9i8rXyfPBX5te72ZfjdP8/lpbzap+VQjQNg6MzKbOQXMt/o
# cQw4dUTeBhbzr0cadRqcG+3IIQNTGX9+kjcGQ45pcVgStcGvel1SMzGCAdwwggHY
# AgEBMDswJzElMCMGA1UEAwwcUG93ZXJTaGVsbCBDb2RlIFNpZ25pbmcgQ2VydAIQ
# G6YzaQc8FahFAO3OXroHWzAJBgUrDgMCGgUAoHgwGAYKKwYBBAGCNwIBDDEKMAig
# AoAAoQKAADAZBgkqhkiG9w0BCQMxDAYKKwYBBAGCNwIBBDAcBgorBgEEAYI3AgEL
# MQ4wDAYKKwYBBAGCNwIBFTAjBgkqhkiG9w0BCQQxFgQUCEOM84Y6WCkqjlZ/wVDu
# Y61euMYwDQYJKoZIhvcNAQEBBQAEggEAD4rZXXM2S9Lu6iiCQHJsJ5DAby39T3OP
# Eg+ORGlB8VxOLIkKhovLkDGlpKEdJvlMHswkOhC+opiXuGGsiRwgVCkvlRI2OiPs
# O+PQ7eEYFXOY7paOMYtzvvyfo3YAsXtNmfAZIzxP3tg7ls+ORRG8yn8ZPyq29Z/l
# eDTNrMR+EETGKV9O+uJ1pOQaQ/EUtn1MvlG+oUFuwMv4XWAePlsfaFJxo5k3QKFC
# wsALxOoaluQsGSk+/9HZRFMf7uXbOVtzD8RgtTzKyHwSaE/S2up1y7SB+MdsBYtl
# n3ltbjXP1RL6+fg3kEfyhMCMclk32z3lSKlU/6kMGapP+LypgKKEJA==
# SIG # End signature block
```

Pojawił się signature blok

Jeśli użytkownik dokona jakichkolwiek zmian w skrypcie to unieważni podpis i skryptu nie będzie można użyć.

Ważność podpisu ustala się w oparciu o ważność certyfikatów które wcześniej zostały wygenerowane i umieszczone w odpowiednich magazynach certyfikatów lokalnego komputera.

Gdyby komputer by stacją w AD to administrator AD decydował by o tym jakie certyfikaty mają być dostępne na komputerze za pomocą zasad grup.

Zmień ExecutionPolicy na Restricted

```
PS C:\WINDOWS\system32> Set-ExecutionPolicy Restricted -Force

PS C:\WINDOWS\system32> Get-ExecutionPolicy
Restricted
```

Próba uruchomienia C:\Users\admin\Witaj.ps1

```
PS C:\WINDOWS\system32> C:\Users\Witaj.ps1
C:\Users\Witaj.ps1 : File C:\Users\Witaj.ps1 cannot be loaded because running scripts is disabled on this system. For more i
nformation, see about_Execution_Policies at https:/go.microsoft.com/fwlink/?LinkID=135170.
At line:1 char:1
+ C:\Users\Witaj.ps1
+ ~~~~~~~~~~~~~~~~~
    + CategoryInfo          : SecurityError: (:) [], PSSecurityException
    + FullyQualifiedErrorId : UnauthorizedAccess
```

Nawet fakt, że skrypt jest podpisany nic nie pomaga uruchomić nie można

Uruchomimy PowerShell z parametrem -ExecutionPolicy AllSigned

```
C:\Users\admin>PowerShell -ExecutionPolicy AllSigned
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\admin> .\Witaj.ps1
Podaj twoje imię: Irek
Witaj Irek
```

Sprawdzam, czy zadziała uruchomienie niepodpisanego skryptu Witaj2.ps1

```
PS C:\Users\admin> .\Witaj2.ps1
.\Witaj2.ps1 : File C:\Users\admin\Witaj2.ps1 cannot be loaded. The file C:\Users\admin\Witaj2.ps1 is not digitally sig
ned. You cannot run this script on the current system. For more information about running scripts and setting execution
 policy, see about_Execution_Policies at https:/go.microsoft.com/fwlink/?LinkID=135170.
At line:1 char:1
+ .\Witaj2.ps1
+ ~~~~~~~~~~~~
    + CategoryInfo          : SecurityError: (:) [], PSSecurityException
    + FullyQualifiedErrorId : UnauthorizedAccess
```

Uruchomimy PowerShell z parametrem RemoteSigned

```
C:\Users\admin>PowerShell -ExecutionPolicy RemoteSigned
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\admin> .\Witaj2.ps1
Podaj twoje imię: Irek
Witaj Irek
```

Wprowadzenie do cenyfikatów

Zaufany certyfikat główny

Certyfikat wydawcy kodu

Ograniczenia podczas uruchamiania skryptów

Execution Policy

Uruchamianie powłoki PowerShell z parametrami